T.C.
KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
İLERİ TEKNOLOJİLER ANABİLİM DALI

VERİ MERKEZİ KATMANLI GÜVENLİK TASARIMI İLE ETKİN OLAY ANALİZİ VE YÖNETİMİ

ALİ AKPINAR

YÜKSEK LİSANS TEZİ

KIRŞEHİR / 2020

T.C.
KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
İLERİ TEKNOLOJİLER ANABİLİM DALI

VERİ MERKEZİ KATMANLI GÜVENLİK TASARIMI İLE ETKİN OLAY ANALİZİ VE YÖNETİMİ

ALİ AKPINAR

YÜKSEK LİSANS TEZİ

DANIŞMAN
Doç. Dr. Mustafa YAĞCI

KIRŞEHİR / 2020

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Ali AKPINAR

20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, Kırşehir Ahi Evran Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Yüksek Lisans eğitimim ve tez sürecimde doğru yönlendirmeleri ile büyük katkı sağlayan sayın Doç. Dr. Mustafa YAĞCI hocama emeklerinden ve ilgisinden dolayı teşekkürü borç bilirim.

Tezimi, her alanda olduğu gibi tez sürecimde de motivasyonumu yüksek tutan eşim Psk. Gülşah AKSAKALLI 'ya ithaf ederim.

Ağustos 2020 Ali AKPINAR

İÇİNDEKİLER

ÖNSÖZ iv

İÇİNDEKİLER v

ŞEKİL LİSTESİ viii

TABLO LİSTESİ x

SİMGE VE KISALTMA LİSTESİ xi

ÖZET xiii

ABSTRACT xiv

1. GİRİŞ 1

2. SIEM ANATOMİSİ VE VERİ MERKEZİ 3

2.1. SIEM Çözümlerinde Temel Bileşenler 4

2.1.1. Kaynak Cihaz 4

2.1.2. Log Toplama 8

2.1.3. Normalizasyon 8

2.1.4. Kural ve Korelasyon Motoru 10

2.1.5. Log Depolama 11

2.1.6. İzleme 12

2.2. SIEM Neden Gereklidir? 12

2.3. Log Yönetimi 14

2.3.1. Log Formatları 15

2.3.2. Etkin Log Yönetimi 18

2.3.3. Log Yönetimi ve SIEM Farkı 20

2.4. Yasalar ve Standartlar 21

2.4.1. 5651 Sayılı Kanun 21

2.4.2. Kişisel Verileri Koruma Kanunu 22

2.4.3. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi 23

2.4.4. PCI Güvenlik Standartları Konseyi 24

2.5. Veri Merkezi Nedir? 25

2.5.1. Veri Merkezi Türleri 25

3. VERİ MERKEZİ BİLGİ GÜVENLİĞİNİN SAĞLANMASI VE ETKİN SIEM YÖNETİMİ 28

3.1. Kurulum Aşamasında Kritik Noktalar 28

3.1.1. Kapasite Planlama 29

3.1.2. EPS Değerinin Hesaplanması 30

3.1.3. Disk Boyutunun Hesaplanması 30

3.2. SIEM Yönetiminde Kritik Noktalar 32

3.2.1. Korelasyon 32
3.2.2. Alarm 34
3.2.3. Taksonomi 35
3.2.4. Log Kaçırma 35
3.2.5. Arama Hızı 36
3.2.6. Davranış Analizi 36
3.2.7. SIEM Çözümlerinde Dikkat Edilmesi Gerekenler 37

3.3. Etkin Korelasyon Örnekleri 39
3.3.1. Kaba Kuvvet Saldırıları 39
3.3.2. Hizmet Durdurma Saldırıları 40
3.3.3. Veritabanı Saldırıları 41
3.3.4. Exploit Tespitleri 42
3.3.5. Kötücül Yazılım Tespitleri 43
3.3.6. Keşif Saldırıları 44
3.3.7. Sistem Olayı Tespitleri 45
3.3.8. Trafik 46
3.3.9. Web Saldırılarına Yönelik Korelasyonlar 46
3.3.10. Geçmiş Loglara Göre Tespit 47
3.3.11. KVKK'ya Yönelik Senaryolar 48

3.4. Veri Merkezi Mantıksal Güvenlik Tasarımı 50
3.4.1. Veri Merkezi Güvenliği 51
3.4.2. Güvenlik Bölgeleri 54
3.4.3. Güvenlik Çözümleri 57
3.4.4. Güvenlik Çözümlerinden Alınması Gereken Loglar 76
3.4.5. Veri Merkezi Mantıksal Güvenlik Tasarımı 79
3.4.6. Bilgi Güvenliğinde Önemli Noktalar 90
3.4.7. Olay Müdahale Planı 95

3.5. Siber Tehditlerin Tespiti 96
3.5.1. Anomali Tespiti 97
3.5.2. Davranış Analizi 97
3.5.3. Referans liste analizi: 98
3.5.4. İstihbarat ile Tespit 98
3.5.5. Verilerin Korunması 98

3.6. En Çok Bilinen Siber Saldırı Çeşitleri 99
3.6.1. Hizmet Durdurma Saldırısı 99
3.6.2. Ortadaki Adam Saldırısı 100
3.6.3. Oltalama Saldırısı 101
3.6.4. Drive-by download 101
3.6.5. Parola Saldırısı 101
3.6.6. SQL Injection Saldırısı 101
3.6.7. Cross-site Scripting (XSS) Saldırısı 103
3.6.8. Dinleme Saldırısı 104

3.6.9. Doğum Günü Saldırısı 104
3.6.10. Malware Saldırıları 104
3.7. Kritik Kurumlara Yapılan Saldırı Örnekleri 105
3.7.1. Almanya Kamu Kurum ve Özel Sektör İşletmelerine Yönelik Saldırılar 105
3.7.2. NASA Sistemlerine Yönelik Saldırı 105
3.7.3. Amerika Personel Yönetim Ofisine Yönelik Saldırı 106
4. DEVLET KURUMUNA AİT VERİ MERKEZİNDE SIEM UYGULAMASI 107
4.1. Korelasyon Nasıl Tanımlanır? 107
4.2. Veri Merkezi Uygulamasında Yazılan Korelasyonlar 110
4.2.1. Veritabanı Güvenliğine Yönelik Korelasyonlar 110
4.2.2. Web Saldırılarına Yönelik Korelasyonlar 116
4.2.3. Reconnaissance Saldırılarına Yönelik Korelasyonlar 121
4.2.4. Oltalama Saldırılarına Yönelik Korelasyonlar 125
4.2.5. Custom Korelasyonlar 127
4.3. Gösterge Tablosu Yapılandırma 135
4.3.1. Atak, Malware, Virüs ve Spam Aktiviteleri 135
4.3.2. Web Sayfalarına Yapılan Atak Türleri 138
4.3.3. SIEM Sistem Olayları 139
4.4. Raporlama 140
4.4.1. Rapor 1: Eşler Arası Uygulamaları Kullanan Kullanıcıların Raporu 141
4.4.2. Rapor 2: Karantina Bölgesinden Yapılan Erişimlerin Tespiti 142
5. SONUÇ ve TARTIŞMA 144
5.1. Veri Merkezi Uygulamasında Yazılan Korelasyonlar ve Çıktıları 145
5.2. ÖNERİ 151
6. KAYNAKÇA 153
ÖZGEÇMİŞ 163

ŞEKİL LİSTESİ

Şekil 2.1: SIEM Çözümlerinin Temel Bileşenleri....4
Şekil 2.2: SIEM'in İlk Aşaması Olan Kaynak Cihazın Belirlenmesi....4
Şekil 2.3: SIEM Çözümlerine Log Aktaran Sistemler [8]....7
Şekil 2.4: SIEM'in İkinci Aşaması Olan Log Toplama Bileşeni....8
Şekil 2.5: Taksonomi İşlemi Örneği....9
Şekil 2.6: SIEM Bileşenlerinden Korelasyon....10
Şekil 2.7: SIEM Log Depolama Aşaması....11
Şekil 2.8: SIEM İzleme Bileşeni....12
Şekil 3.1: Örnek Mantıksal Güvenlik Tasarımı....80
Şekil 3.2: Dâhili Ağın, İnternet Ağından Yalıtılması....90
Şekil 4.1: Korelasyon Tanımlama Ekranı....108
Şekil 4.2: Liste Tanımlama Ekranı....109
Şekil 4.3: İstatistik Liste Tanımlama Ekranı....110
Şekil 4.4: Oracle Veritabanında Spool Komutu Çalıştırılmasının Tespiti....111
Şekil 4.5: MSSQL Veritabanında Sqlcmd Komutu Çalıştırılmasının Tespiti....112
Şekil 4.6: Mongo Veritabanında Mongoexport Komutu Çalıştırılmasının Tespiti....113
Şekil 4.7: Kritik Bir SQL Tablosunda Delete Komutu Çalıştırılmasının Tespiti....114
Şekil 4.8: Kritik Bir SQL Tablosunda Update Komutu Çalıştırılmasının Tespiti....115
Şekil 4.9: SQL Injection Saldırısı Korelasyon Kuralı....117
Şekil 4.10: Cross Site Scripting Korelasyon Kuralı....119
Şekil 4.11: 8 Byte'lık Arabellek Kapasitesinin Aşılması....120
Şekil 4.12: BufferOverFlow Korelasyon Kuralı....120
Şekil 4.13: Command Execution Saldırısı Korelasyonu....121
Şekil 4.14: Port Tarama Saldırısının Tespit Edilmesi....122
Şekil 4.15: Port Tarama Saldırısının Tespit Edilmesinde İstatistiksel Liste Tanımlaması....123
Şekil 4.16: Alt Domain Saldırılarının Tespit Edilmesi....124
Şekil 4.17: Alt Domain Saldırılarının Tespitinde İstatistiksel Liste Tanımlaması....124
Şekil 4.18: Oltalama Saldırısına Yönelik Korelasyon....125
Şekil 4.19: İç Ağdan Dış Ağa 10'dan Fazla Trafiği Engellenen IP'nin Tespiti....126
Şekil 4.20: Şüpheli Bir IP'ye Trafik Yapan IP'nin Tespit Edilmesi....127
Şekil 4.21: Sahte DHCP Sunucusunun Tespitine Yönelik Korelasyon....128
Şekil 4.22: Sahte DHCP Sunucusun Tespitine Yönelik Liste Tanımlaması....128
Şekil 4.23: Psexesvc.Exe Dosyasının Çalıştırılmasının Tespitine Yönelik Korelasyon....129
Şekil 4.24: Psexecsvc.exe Dosyasının Çalıştırılması Tespiti İçin Liste Tanımlaması....130
Şekil 4.25: 3 Farklı Kullanıcı Adıyla VPN Denemesinin Tespitine Yönelik Korelasyon....132

Şekil 4.26: 3 Farklı Kullanıcı Adıyla VPN Denemesinin Tespitinde Liste Tanımlaması.....133
Şekil 4.27: Komut Satırı ile Uzak Bağlantıların Tespit Edilmesine Yönelik Korelasyon 134
Şekil 4.28: Komut Satırı ile Uzak Bağlantıların Tespit Edilmesinde Liste Tanımlaması.....134
Şekil 4.29: Atak Aktivitelerinin Takibi için Gösterge Tablosunun Yapılandırılması.....136
Şekil 4.30: Malware Aktivitelerinin Takibi için Gösterge Tablosunun Yapılandırılması 136
Şekil 4.31: Atak ve Malware Aktivitelerinin Gösterge Tabloları.....137
Şekil 4.32: Güvenlik Aktiviteleri Gösterge Tablosu 137
Şekil 4.33: Web Atak Tiplerinin Gösterge Tablosunun Yapılandırılması.....138
Şekil 4.34: Web Saldırı Türlerinin Gösterge Tablosu 139
Şekil 4.35: Sistem Olaylarının Gösterge Tablosunda Gösterimi 140
Şekil 4.36: Peer-to-Peer Uygulama Kullanan Kullanıcıları Tespit Raporu 142
Şekil 4.37: Karantina Bölgesinden Başarılı Erişimin Tespitine Yönelik Korelasyon.....143
Şekil 4.38: Karantina Bölgesinden Başarılı Erişim Sağlayan IP'nin Tespit Raporu 143

TABLO LİSTESİ

Tablo 3.1: 500 Windows Sunucu ve 500 Linux Sunucunun Ürettiği Log Miktarı.....31
Tablo 5.1: Uygulama Bölümünde Yazılan Korelasyon Bulgularının Değerlendirilmesi 145
Tablo 5.2: Uygulama Bölümünde Yazılan Rapor Bulgularının Değerlendirilmesi 149

SİMGE VE KISALTMA LİSTESİ

API : Application Programming Interface (Uygulama Programlama Arayüzü)

BT : Bilgi Teknolojileri

CVE : Common Vulnerabilities and Exposures (Ortak Güvenlik Açıkları ve Riskler)

IT : Information Technology (Bilgi Teknolojileri)

DDoS : Distributed Denial of Service (Dağıtık Hizmetin Reddi)

DHCP : Dynamic Host Configuration Protocol (Dinamik Host Yapılandırma Protokolü)

DLP : Data Lost Prevention (Veri Kaybı Önleme)

DoS : Denial of Service (Hizmet Reddi)

EPS : Event Per Second (1 saniyedeki olay sayısı)

FISMA : Federal Information Security Management Act (Federal Bilgi Güvenliği Yönetim Yasası)

HIPAA : Health Insurance Portability and Accountability Act (Amerikan Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası)

HIPS : Host-Based Intrusion Prevention System (Host Tabanlı Saldırı Önleme Sistemi)

IDS : Intrusion Detection Sistem (Atak Tespit Sistemi)

IIS : Internet Information Services (İnternet Bilgi Servisleri)

IPS : Intrusion Prevention Sistem (Atak Önleme Sistemi)

ISO : International Organization for Standardization (Uluslararası Standardizasyon Organizasyonu)

LDAP : Lightweight Directory Access Protocol (Basit İndeks Erişim ProtokFolü)

MAC : Media Access Control (Ortam Erişim Yönetimi)

MsSQL : Microsoft Structured Query Language (Microsoft Yapılandırılmış Sorgu Dili)

NFS : Network File System (Ağ Dosya Sistemi)

NIPS : Network-Based Intrusion Prevention System (Ağ Tabanlı Saldırı Önleme Sistemi)

ODBC : Open Database Connection (Açık Veritabanı Bağlantısı)

OSI : Open Systems Interconnection (Açık Sistemler Bağlantısı)

PCI DSS :Payment Card Industry Data Security Standart (Kartlı Ödeme Endüstrisi Veri Güvenlik Standardı)

POP3 : Post Office Protocol 3 (Postane Protokolü 3)

SIEM : Security Information and Event Management (Bilgi güvenliği Tehdit ve Olay Yönetimi)

SNMP : Simple Network Management Protocol (Basit Ağ Yönetim Protokolü)

SSL : Secure Socket Layer Inspection (Güvenli Giriş Katmanı)

USB : Universal Serial Bus (Evrensel Seri Veriyolu)

WMI : Windows Management Instrumentation (Windows Yönetim Araçları)

2FA : Two Factor Authentication (Çift Faktörlü Kimlik Doğrulama)

ÖZET

YÜKSEK LİSANS TEZİ

VERİ MERKEZİ KATMANLI GÜVENLİK TASARIMI İLE ETKİN OLAY ANALİZİ VE YÖNETİMİ

Ali AKPINAR

Kırşehir Ahi Evran Üniversitesi

Fen Bilimleri Enstitüsü

İleri Teknolojiler Anabilim Dalı

Danışman: Doç. Dr. Mustafa YAĞCI

Günümüzde veri merkezleri, bazı yasalara veya standartlara uyum sağlayabilmek, siber risklere karşı savunma oluşturabilmek, şüpheli durumları önceden tespit edebilmek, adli vakalarda deliller sunmak için güvenlik, sistem veya uygulama olay kayıtlarını depolayan ve analiz eden Bilgi Güvenliği ve Olay Yönetimi anlamına gelen SIEM (Security Information and Event Management) çözümlerini kullanmaktadırlar. Ancak doğru yönetilemeyen SIEM çözümlerinde, çok sayıda log kaçırma, yanlış alarmların oluşması, siber tehditleri gözden kaçırma gibi risklerle karşı karşıya kalınmaktadır. Ayrıca güvenlik tasarımı doğru yapılmayan, doğru güvenlik ürünleri kullanılmayan veri merkezleri, siber tehditlere karşı savunmasız hale gelmektedir. Bu çalışmada siber risklere karşı veri merkezi güvenliğinin sağlanmasına yönelik güvenlik yaklaşımları ve veri merkezlerinde SIEM çözümlerinin etkin kullanımına yönelik inceleme yapılmıştır. Yapılan bu inceleme devlete bağlı bir veri merkezinde gerçekleştirilen SIEM uygulamasıyla desteklenmiştir.

Ağustos 2020, 163 Sayfa

Anahtar Kelimeler: Veri Merkezi Güvenliği, SIEM, Log Yönetimi

ABSTRACT

MASTER THESIS

EFFICIENT EVENT ANALYSIS AND MANAGEMENT WITH DATA CENTER LAYERED SECURITY DESIGN

Ali AKPINAR

Kirsehir Ahi Evran University

Graduate School of Natural and Applied Sciences

Advanced Technologies Department

Supervisor: Assoc. Dr. Mustafa YAĞCI

Today, data centers use SIEM (Security Information and Event Management) solutions that have the ability to store and analyze security, system or application event logs to comply with certain laws or standards, to defend against cyber risks, to detect suspicious situations in advance, to provide evidence in forensic cases. However, SIEM solutions that cannot be managed correctly and are configured incorrectly cause many unnecessary logs to be collected, many unnecessary or false alarms to occur, log hijacking, cyber threats to be overlooked. In addition, data centers whose security design is not made correctly and security products are not used correctly become vulnerable to cyber threats. This situation leads to the expected benefit not being achieved from SIEM. In this context, security approaches to provide data center security against cyber risks were examined.and an investigation has been made for the effective use of SIEM solutions in data centers, and this review has been supported by the SIEM application carried out on a government data center.

August 2020, 163 Pages

Keywords: Datacenter Security, SIEM, Log Managament

1. GİRİŞ

Bilgisayar iletişim ve ağ teknolojilerinin gelişmesiyle birlikte siber saldırıların da çeşitliliği artmış ve farklı güvenlik problemleri ortaya çıkmıştır. Bu problemler bilgi güvenliği kavramının önemini daha da artırmıştır. Bilginin güvenliğini sağlamak amacıyla kurumlar çeşitli güvenlik ürünleri kullanmaktadırlar. Kurumlarda kullanılan güvenlik ürünlerinin amacı, bilginin işlenirken, taşınırken veya depolanırken yetkisiz erişimlere karşı gizliliğini sağlamak, bozulmasını, değiştirilmesini veya silinmesine karşı bütünlüğünü korumak, ihtiyaç duyulan sürede istenilen bilgiye ulaşabilmek ve bu bilgileri eksiksiz kullanabilmek için erişilebilirliği sağlamaktır [1].

Güvenlik, ağ cihazları, sistemler ve uygulamalar, kullanıcıların erişimlerini, sistem ve güvenlik olaylarını, siber tehditlerin tespit edilmesi, hatalı yapılandırma değişikliklerinin takip edilmesi, sistem arızalarının incelenmesi için kayıt altına alırken, bazı yasa ve standartlara uyum sağlayabilmek için de kayıt altına almaktadırlar. Siber saldırıların çeşitliliğinin artması sebebiyle bu kayıtların tutulması günümüz için tek başına yeterli değildir. Siber olaylarla mücadele edebilmek, sistemler içerisinde şüpheli olayları tespit edebilmek, siber olay öncesi tedbir alabilmek için bu olay kayıtlarının (logların) analiz edilebilmesi gerekmektedir.

Kritik veri merkezleri bünyesinde kritik bilgilerin saklanması, işlenmesi ve korunması için birçok güvenlik (güvenlik duvarı, tehdit önleme sistemi vb.), ağ (anahtar, yönlendirici vb.) ve uygulama (veritabanı, web sunucu, uygulama sunucuları vb.) cihazları barındırmaktadır. Bu cihazlar her gün çok sayıda günlük anlamına gelen log üretmektedir. Eğer bu loglar merkezi bir noktada toplanmazsa yönetimi hem çok zor olacak hem de bir problem esnasında çözümün süresini uzatacaktır. Yalnızca logların toplanması yeterli değildir. Her bir kaynaktan gelen logların, saldırı öncesi tespiti, sistem probleminin çözümü gibi durumlarda analiz edilmesi de gerekmektedir.

Bilgi Güvenliği ve Olay Yönetimi anlamına gelen SIEM (Security Information and Event Management) ile birden çok kaynaktan gelen günlük veriler toplanarak ve analiz edilerek bir tehdide maruz kalındığında bilgi güvenliği yaklaşımına bütüncül bir bakış açısı kazandırılabilir. SIEM çözümlerinin korelasyon, raporlama, log toplama gibi yetenekleri sayesinde yasalara ve standartlara uyum sağlanması amacıyla loglar toplanmakta, sistemler

içerisinde şüpheli davranışlar, siber saldırılar, sistem olayları kısacası BT (Bilgi Teknolojileri) bileşenlerinin nasıl bir tehditle karşı karşıya kaldığının anlaşılması sağlanmaktadır.

Bu çalışmada SIEM ile kritik alt yapıya sahip veri merkezlerinde SIEM yönetiminde maksimum faydanın sağlanabilmesi amaçlanmıştır. Bu doğrultuda bir devlet kurumuna ait veri merkezi örnek uygulaması ile bu çalışma desteklenmiştir. Ayrıca veri merkezlerinde bilgi güvenliğinin sağlanmasına yönelik katmanlı güvenlik mimarisi incelenmiştir.

2. SIEM ANATOMİSİ VE VERİ MERKEZİ

Günümüz teknolojileri geliştikçe bilginin hacmi de genişlemektedir. Bu bilgilerin depolanması ve işlenmesi ihtiyacı daha da artmaktadır. Veri miktarının artmasıyla, bu verilerin depolanması için kaynak alanına ihtiyaç duyulmaktadır. Verilerin artması, ağ trafiğinin artmasına da sebep olmaktadır. Artan ağ trafiğinin güvenli ve kesintisiz şekilde iletilebilmesi için ağ ve güvenlik cihazlarının sayısı da artmaktadır. Bu yüzden büyük verilerin işlenebilmesi ve depolanabilmesi için veri merkezlerine ihtiyaç duyulmaktadır. Veri merkezleri, kurumsal bilgi ve uygulamaları bünyesinde toplu halde barındırdığı için siber saldırganların hedefi haline gelmiştir. Bu nedende veri merkezlerinde bilgi güvenliğinin sağlanması her zamankinden daha da önemli hale gelmiştir.

Bilgi güvenliğinde önemli bir rolü bulunan tehdit ve olay yönetimi anlamına gelen SIEM (Security Information and Event Management) çözümleri, gerçek zamanlı raporlama ve güvenlik olay analizi ile ağa yönelik tehditleri tespit etmektedir. Bu tehditlerin her geçen gün çeşitliliği ve gücü artmaktadır. Ağlara bağlanan cihaz sayısı arttıkça, bu cihazların yönetimi de zorlaşmakta ve siber saldırganların ağa sızma noktaları artmaktadır. SIEM, birden fazla kaynaktan aldığı verileri analiz ederek, aksiyon planlarının ortaya çıkarılmasında önemli rol oynamaktadır. Bunun yanında, saldırı tespiti, dijital delillerin saklanması, bütünsel güvenlik analiz raporu ve güvenlik risklerinin gerçek zamanlı olarak izlenmesi gibi gücü olan SIEM, kritik BT (Bilgi Teknolojileri) bileşenlerinin nasıl bir saldırı ile karşı karşıya kaldığı ve kalabileceği konusunda detaylı rapor üretmektedir.

SIEM, Security Event Management (SEM) ve Security Information Management (SIM) teknolojilerinin birleşimiyle oluşmaktadır. SIM, günlük verilerin toplanmasının otomatikleştirilmesini sağlayan bir yazılımdır. SEM ise, bir yazılım, sistem veya BT ortamında güvenlikle ilgili olayları tanımlama, toplama, izleme ve raporlama işlemidir. Güvenlik duvarları, ağ ekipmanları ve sunuculardan toplanan olay verileri, güvenlik açıkları, tehdit veya riskleri tespit etmek için güvenlik algoritmaları ve istatistiksel hesaplamalarla analiz edilmektedir. SEM, olayların kaydedilmesini ve değerlendirilmesini sağlamaktadır [2].

SIEM çözümleri pasif önleyici, aktif izleme sistemleridir. Klasik bir SIEM ürünü bir saldırıyı önleme kabiliyeti yoktur fakat korelasyon motoru ve diğer güvenlik cihazlarıyla

entegreli çalışması sayesinde bu saldırıların önlenmesini sağlamakta ve bir ihlal durumunda yöneticileri bilgilendirmektedir. Aktif izleme ekranı ile de olay durumlarını anlık olarak izleme imkânı sunmaktadır.

SIEM doğru bir şekilde yapılandırıldığında, içeriden ve dışarıdan gelen tehditleri yakalama, sistemde yetki sahibi kişilerin hareket ve erişim haritasını çıkarma, raporlama, sistem problemi veya saldırı sonrasında hata ayıklama konusunda yardımcı olmak gibi faydalar sağlamaktadır.

Bu çalışmanın amaçlarından birisi de veri merkezlerinde etkin SIEM yönetimini incelemektir. Bölüm 2'de SIEM mimarisi ve veri merkezi tanımına yer verilmiştir.

2.1. SIEM Çözümlerinde Temel Bileşenler

Standart bir SIEM mimarisi, Şekil 2.1'de gösterildiği gibi altı ayrı bileşenden oluşmaktadır. Bu bileşenler, kaynak cihaz, log toplama, günlüklerin ayrıştırılması veya normalleştirilmesi, kural motoru, log depolama ve olay izleme ekranlarıdır. Bu bileşenlerin her biri diğerinden bağımsız olarak çalışabilir fakat hepsi birlikte çalışmadan, SIEM bir bütün olarak çalışmayacaktır.

Şekil 2.1: SIEM Çözümlerinin Temel Bileşenleri

2.1.1. Kaynak Cihaz

SIEM'in ilk aşaması, bilgi alabileceği kaynak cihazların belirlenmesidir. Bu kaynaklar ağ, güvenlik cihazı ya da bir uygulama olabilir. Burada önemli olan nokta hangi cihazlardan logların alınacağının tam olarak belirtilmesidir. Kaynak cihazların belirlenmesi SIEM proje süreçlerinin hayati bir parçasıdır.

Şekil 2.2: SIEM'in İlk Aşaması Olan Kaynak Cihazın Belirlenmesi

Çoğu sistem yöneticisi, günlük aktivitelerden kaynaklı her gün üretilen logların hacmini fark edememektedir. Örneğin bir web tarayıcısını açan ve bir web sitesine giden kullanıcının bu eylemi, çok sayıda farklı cihazda log üremesine sebep olmaktadır. Kullanıcının bilgisayarı, trafiğin geçtiği yönlendirici, anahtar, güvenlik duvarı ve gidilen web sitesi sunucusunun her biri kullanıcının tam olarak ne yaptığını gösteren loglar üretmektedir. Basit bir kullanıcı trafiği bile birçok cihazda log üremesine sebep olabilmektedir. Bir problem esnasında her bir cihazın loglarının incelenmesi yerine bu bilgiler SIEM ile merkezi olarak toplanabilmekte, yönetilebilmekte ve analiz edilebilmektedir.

SIEM, kendisine verilen bilgiler ne ise o bilgileri alarm üretme, raporlama ve depolamak için kullanmaktadır. Bu kapsamda log toplanabilecek bazı kaynaklar Bölüm 2.1.1'in alt başlıklarında belirtilmiştir.

2.1.1.1. İşletim Sistemleri

Günümüzde en yaygın kullanılan işletim sistemlerinden bazıları Microsoft Windows, Linux, ve UNIX, AIX, Mac OS X işletim sistemleridir [3]. Bu işletim sistemlerinin çoğunun alt yapısında farklı görevler için geliştirilmiş teknolojiler barınmaktadır. Ancak hepsinin ortak özelliği log oluşturmalarıdır. Bu günlükler tüm sistem istatistiklerini, kimin giriş yaptığını ve temel olarak kullanıcının sistemde ne yaptığı gibi bilgileri tutmaktadır.

2.1.1.2. Ağ ve Güvenlik Cihazları

Cihaz, sistem kullanıcılarının işletim sistemine müdahale edemediği sistemlerdir. Ağ ve güvenlik cihazlarının yöneticilerinin, cihazın temelinde kullanılan işletim sistemine doğrudan erişim yetkisi bulunmamaktadır. Bunun yerine sadece cihazın özel bir ara yüz üzerinden yönetilmesi sağlanmaktadır. Ağ cihazlarına örnek olarak yönlendiriciler, anahtarlar verilebilirken [4] güvenlik cihazlarına örnek olarak ise güvenlik duvarları, saldırı önleme sistemleri, veritabanı güvenlik duvarları, web uygulama güvenlik duvarları verilebilir [5]. Güvenlik duvarları üzerinden kullanıcıların olağan dışı iç ağ veya dış ağ trafikleri, yönlendirici üzerinden yapılandırma değişikliği yapan kullanıcıların hangi yapılandırmaları değiştirdiğinin bilgileri alınabilir. Bu cihazlar loglarını sistemde dâhili olarak depolar veya genellikle logları syslog veya FTP (File Transfer Protocol) yoluyla gönderecek şekilde yapılandırmaktadır [6]. Cihazlar yalnızca fiziksel değil, sanal işletim sistemi üzerine de kurulabilmektedir.

2.1.1.3. Web Sunucuları

Web sunucular, web sayfalarının barınmalarını ve yayında kalmalarını sağlamaktadır. Bir web sayfası ziyaret edildiğinde sayfadaki tüm içerikler, bir sunucu üzerinden indirilmektedir. IIS (Internet Information Service), Apache, Tomcat, Web Sphere, NGINX (engine x) ve diğer tüm web motorları, web sunucusu günlüğünün ihtiyaç duyulan bir kısmını karşılayabilmektedir [7]. İhtiyaçlara bağlı olarak, bazen kullanıcıların web sitesine ne zaman gittiğini ve kullanıcıların ihtiyaçlarını anlayabilmek için logların kullanım amaçları değişkenlik gösterebilmektedir.

2.1.1.4. Kimlik Doğrulama Sunucuları

Active Directory'yi, OpenLDAP uygulaması veya başka bir alternatif tercih edilse de, kimlik doğrulama sunucularının her biri bir miktar log kaydı sağlamaktadır. Fakat önemli olan bu günlüklerden neye ihtiyaç duyulduğunun, ne arandığının anlaşılmasıdır. En temel olarak bir kullanıcı hesabının süresinin dolması, başarısız oturumların açılması gibi durumların incelenmesi için bu günlükler incelenmelidir [7].

2.1.1.5. Kullanıcı Bilgisayarları

Kullanıcıların yaptıkları Powershell netclient kullanılarak dosya indirmeleri, şüpheli dizinlerde dosya çalıştırılması gibi aktivitelerin takip edilebilmesi için kullanıcı bilgisayarlarının logları SIEM'e gönderilmelidir. Bu sayede kullanıcıların bilgisayarlarındaki şüpheli olaylar için alarm yazılarak kritik bir olay için erken tedbir alınabilir veya incelemeler için ilgili loğlar kolay bir şekilde raporlanabilir.

2.1.1.6. Uygulamalar

Uygulamalar, belirli işletim sistemlerinin üzerinde çalışan çok çeşitli işlevler için kullanılmaktadır. Standart bir kurumsal ortamda Etki Alanı Adı Sistemi (Domain Name System-DNS), dinamik ana bilgisayar yapılandırma protokolü (Dynamic Host Configuration Protocol-DHCP), web uygulamaları, e-posta sistemleri (Exchange 2010, Exchange 2013, Exchange 2016, IIS SMTP, SendMail/Qmail), veritabanları (Oracle, MSSQL, MySQL, Sybase vs.) ve çok sayıda başka uygulama türü olabilmektedir. Bu uygulama logları, sistem istatistikleri, hatalar veya bilgilendirici iletiler gibi uygulamanın durumu hakkında ayrıntılı bilgiler içermektedir. Bu uygulama loglarının tamamının

kullanılması ve bir yasaya veya standarda uygun olması gerekmekte midir? Bu tarz soruların cevaplarının verilebilmesi iyi bir SIEM süreci için önemlidir.

Şekil 2.3'de gösterildiği gibi genel olarak SIEM için log toplama kaynakları, güvenlik olayları, ağ günlükleri, uygulamalar ve cihazlar, IT (Information Technology) altyapısı şeklinde gruplandırılabilir [8].

Şekil 2.3: SIEM Çözümlerine Log Aktaran Sistemler [8].

Log kaynaklarının belirlenmesi sistemlerde yer alan ürünlere ve ihtiyaçlara göre değişmektedir. Önemli olan hangi kaynaktan hangi logların alınacağının başlangıçta iyi analiz edilmesidir. SIEM için logların hangi kaynaklardan alınacağının belirlenmesinin ardından, SIEM kaynaklarının ne kadarının bu logların işlenmesine ve saklanmasına ayrılacağının tanımlanması gerekmektedir. Gerekli kaynaklar belirlenirken, kaynak cihazın önceliğinin belirlenmesi ve belirlenen cihazlardan alınacak logların kritikliğinin tanımlanması, dikkate alınması gereken bazı hususlardandır.

SIEM çözümlerine log aktaracak kaynak cihazların sayısı ve belirli bir zaman diliminde oluşan logların boyutunun bilinmesi, SIEM'in log boyutuna göre ne kadar kaynak kullanacağını ve gereken depolama alanının miktarını belirlemek için gerekmektedir. Ayrıca bazı SIEM çözümlerinde lisanslama için önemlidir.

Kaynakların logları toplanırken, bu logların büyüklükleri ve ağ kullanım miktarının bilinmesi önemlidir. Ortamda hangi kaynakların olduğu net bir şekilde belirlendikten sonra, bu kaynaklardan hangi logların, hangi amaç için alınacağının belirlenmesi gerekmektedir.

Kaynaklardan tüm logların alınması SIEM'i log yığını haline dönüştürebilir. Bu log kalabalığının içerisinde istenilen bilgiye odaklanmak, yönetmek, performans sağlamak zor olabilir. Ayrıca hiç bir SIEM aracının sonsuz depolama alanı ve işlem gücü olmayacaktır. Gereğinden fazla log toplanması, sistemin çalışmamasına sebep olabilirken, gerektiği kadar log toplanmaması da log analizinde yetersiz kalınmasına sebep olabilir.

2.1.2. Log Toplama

Kaynak cihazlardan log toplanırken itme veya çekme mekanizması kullanılmaktadır. İtme tabanlı log aktarmada, kaynak cihaz SIEM log toplayıcısına iletilecek logları Syslog, Log File / FTP yönetimi ile göndermektedir [9]. Çekme tabanlı log toplama mekanizmasında ise, SIEM log toplayıcısı, kaynak cihaza erişerek logu kendisi çekmektedir. Çekme tabanlı log toplamada, SMB (Service Message Block) ve WMI (Windows Management Instrumentation) kullanılan metotlardan bazılarıdır.

Şekil 2.4: SIEM'in İkinci Aşaması Olan Log Toplama Bileşeni

İtme tabanlı log aktarmada paketlerin alıcıya ulaşmasının %100 garantisi bulunmamaktadır [10]. Logların toplanma transfer durumu bu metotta takip edilmelidir. Diğer bir problem ise alıcıya uygun denetim olmaz ise yanlış yapılandırma veya kasıtlı bir saldırı sonucu çok fazla sayıda çöp logu SIEM'e enjekte edilebilir. Böylece odaklanılması gereken loglar gözden kaçabilir, performans sorunları ortaya çıkabilir ve hatta SIEM devre dışı kalabilir. Hangi log toplama metodunun kullanılacağı tamamen sistemdeki kaynaklara ve SIEM çözümünün yöneticilerine bağlıdır. SIEM çözümlerinde kullanılan diğer log toplama formatları API (Application Programming Interface), Ajan, MsSSQL (Microsoft Structered Query Language), NFS (Network File System), ORACLE formatlarıdır.

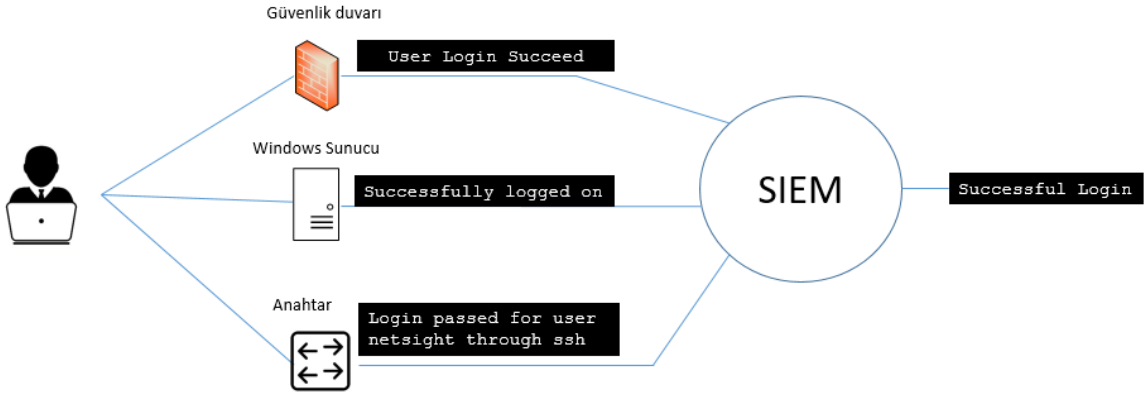
2.1.3. Normalizasyon

Her logun veri alanları ve değerlerini içeren yinelenen bir veri biçimi bulunmaktadır. Ancak log tutma biçimi sistemler arasında hatta aynı sistemdeki farklı loglar arasında bile değişiklik göstermektedir. Günlük ayrıştırıcı (log parser), belirli bir günlük biçimini alıp

yapılandırılmış verilere dönüştürebilen bir yazılım bileşenidir [11]. Parser ile birbirinden farklı biçimde toplanan loglar SIEM tarafından anlaşılabilecek tek bir formata dönüştürülmektedir.

Farklı marka ve modellerde gerçekleşen benzer olayların tek bir tek bir formata dönüştürme eylemine normalizasyon denmektedir. Her SIEM ürünü normalizasyon sürecini farklı ele almaktadır. SIEM'de ortak amaç tüm farklı türdeki loglara sahip olmaktır. Sistem olayları, kimlik doğrulama, yerel / uzak bağlantılar gibi loglara anlam eklenmesi durumuna ise sınıflandırma denilmektedir. Windows Server için, "administrator", Linux sunucusunda, yerel bir yöneticinin oturum açtığını belirtmek için "root" kullanıcı adı aranmaktadır. SIEM ile farklı yönetici oturum açma türleri için birden çok kural tetiklemek yerine, birden çok değişkeni temel alan bir kuralı tetiklemek için SIEM iç mantığını kullanarak tek bir kural yazılabilmektedir.

Şekil 2.5'de gösterildiği gibi bir güvenlik duvarı, bir Windows sunucu ve bir ağ cihazı olan anahtar üzerinde bir kullanıcı başarılı oturum açtığında "User Login Succeed", "Successfully Logged on..", "Login passed for user netsight through ssh" farklı sözdizimlerinde üreyen loglar, SIEM üzerinde tek bir sözdizimi "Successful Login" şeklinde görüntülenmektedir. Bu olaya da taksonomi adı verilmektedir.



Şekil 2.5: Taksonomi İşlemi Örneği

2.1.4. Kural ve Korelasyon Motoru

Korelasyon motoru, kural motorunun bir alt kümesidir. Korelasyon motorunun yaptığı iş, farklı kaynaklardan gelen olayları tek bir ilişkili olayla eşleştirmektir. Bu ilişki kurma işlemine korelasyon denmektedir. SIEM çözümlerinde hedef, farklı cihaz ve uygulamalardan toplanan logları birbiri ile ilişkilendirerek, oluşabilecek siber saldırılara karşı alarm üretmek ve olaya müdahale zamanını en aza indirmektir. Korelasyon sonrasında yazılan alarmlara ise korelasyon kuralları denmektedir. Bir SIEM sürecinin en can alıcı noktası korelasyon kısmıdır. Çünkü logların yalnızca toplanması bir işe yaramayacaktır. Bu loglar içerisinde anlamlı ilişkiler kurmak ve alarmlar üretmek SIEM sürecinde odaklanılması gereken noktadır.

Şekil 2.6: SIEM Bileşenlerinden Korelasyon

Örnek bir korelasyon kuralı:

Dış ağdan bir IP'nin, kurum içerisinde bir IP'ye 1 dakika içerisinde 10'dan farklı porta erişim isteği güvenlik duvarında engellendikten sonra başarılı bir erişim sağlamışsa sistem yöneticilerine bu kaynak IP'nin e-posta ile bilgilendirilmelidir.

SIEM korelasyon kuralları yazılırken dikkatli olunmalıdır. Çok sayıda yazılan yanlış korelasyonlar, tehditlere ve saldırılara yanıt vermek için uygulanabilecek çabalarını boşa harcanmasına neden olabilmektedir. SIEM korelasyon kuralları yapılandırılırken, yanlış pozitif uyarıları azaltma ile siber saldırıyı gösterebilecek olası şüpheli olayları kaçırmama arasında bir denge kurmak gerekmektedir [12].

Kullanılan SIEM çözümlerinde hazır korelasyonların sayısı ve hangi ihtiyacı karşıladığı önemlidir. Ancak bazı hazır SIEM korelasyon kuralları belirli ağlar için geçerli olmayabilir. Hangi önceden yapılandırılmış kuralların devre dışı bırakılacağına ve hangi kuralların sıfırdan yazılması gerektiğine karar vermek SIEM'in zorlu aşamalarından biridir [12].

2.1.5. Log Depolama

SIEM'e gelen loglarla çalışabilmek ve geçmişteki olaylar arasında sorgular yapabilmek için logları depolamanın bir yoluna ihtiyaç bulunmaktadır.

Şekil 2.7: SIEM Log Depolama Aşaması

Loglar canlı ve arşiv olarak depolanmaktadır. Canlı loglar, belirli süre içerisinde gerçekleşen olaylar arasında arama yapılması, izleme ekranında takip edilmesi, korelasyon ve alarm yazılması için depolanan olaylardır. Her SIEM üreticisinin canlıda tutma süresi farklıdır. Bazı üreticiler logları 1 ay canlıda tutarken, bazı SIEM çözümleri ise 2 yıl tutabilmektedir. Bu durum tamamen SIEM projesinde ayrılan kaynak ve ürünün kabiliyeti ile alakalıdır. Canlıda tutma süresinin dolmasının ardından loglar arşive alınmaktadır. Arşive alınan loglar bağlı olunan yasa ve standartlara bağlı olarak değişebildiği gibi ayrılan kaynağa göre de değişmektedir. Arşive alınan loglar, yalnızca yasalar ve standartlara uyum sağlamak için değil, geçmiş olaylar incelenmesi için de önemlidir. Logların ne kadar süre arşivde kalacağı disk boyutu ve uyulması gereken yasa ve standartlara bağlıdır.

Log depolamada kullanılacak disk boyutu, diske yazma hızı gibi etkenler önemlidir. SIEM çözümlerinde veritabanında, metin tabanlı veya ikili dosyada olmak üzere logları depolamanın üç yolu bulunmaktadır:

Veritabanı: Logları bir veritabanında depolamak, çoğu SIEM'in günlüklerini saklama biçimidir. Bunlar genellikle Oracle, MySQL, Microsoft SQL gibi standart veritabanı platformlarıdır.

Metin Tabanlı: Loglar metin tabanlı bir log dosyasına yazılmaktadır. Kaynak kullanımı bakımından avantajlıdır. Biçimi genellikle insanlar tarafından okunabilir formattadır. Örneğin Linux işletim sistemlerinin çoğunda yer alan “grep” komutuyla okunabilir [13].

İkili Dosya: İkili dosya biçimi, yalnızca belirli SIEM tarafından bilgi depolamak için kullanılan ikili bilgileri depolamak için özel bir biçim kullanan bir dosyadır. SIEM, bu son

derece tescilli dosyayı nasıl okuyacağını ve yazıldığını bilen tek uygulamadır. Uzun süreli saklamalar için önerilmemektedir [13].

2.1.6. İzleme

SIEM bileşenlerinde son aşama, SIEM'de saklanan loglarla etkileşim yöntemidir. SIEM'deki tüm günlükleri aldıktan ve olaylar işlendikten sonra, bu bilgilerle yararlı bir şey yapmanın bir yoluna ihtiyaç bulunmaktadır. Aksi takdirde günlükler depolama amacıyla sadece SIEM'de tutulacaktır. SIEM, web tabanlı veya uygulama tabanlı olacak ve iş istasyonuna yüklenecek bir arabirim konsoluna sahip olmalıdır. Her iki arabirim de kullanıcıların SIEM'de depolanan verilerle etkileşime girmesini sağlamalıdır. Bu konsol, ister web ister uygulama tabanlı olsun SIEM'i yönetmek için kullanılacaktır.

Şekil 2.8: SIEM İzleme Bileşeni

Gerçek SIEM uygulamasındaki bu ara yüz, olay işleyicilerine veya sistem mühendisleri için SIEM ortamına benzersiz bir görünüm kazandıracaktır. Normalde, SIEM'in topladığı bilgileri görüntülemek için, olay işleyicileri veya mühendislerin farklı cihazlara gitmesi ve günlükleri yerel biçimlerinde görüntülemesi gerekmektedir. SIEM verileri normalleştirdiğinden, tüm bu farklı günlükleri görüntülemeyi ve analiz etmeyi çok daha kolay hale getirmektedir. Yazılan alarmlar, tasarlanan görsel grafikler, raporlamalar bir ara yüzden takip edilebilmektedir. Bu yüzden bir SIEM çözümünde bir logu arama hızı ve takip edilen ekranın kullanıcı dostu, basit ve anlaşılabilir olması gerekmektedir.

2.2. SIEM Neden Gereklidir?

ISO 27001 (International Organization of Standardization 27001) ve BGYS (Bilgi Güvenliği ve Yönetim Sistemi) sürecinin en önemli kısımlarından birisi de log yönetimidir. Bunun dışında Bölüm 2.4'te bahsedilen bazı standartlar ve yasalar log yönetimini zorunlu kılmaktadır.

Loglar incelenerek, “kritik bir sunucuda kim oturum açtı”, “kritik bir servis neden çalışmayı durdurdu”, “kim hangi dosyalara erişti, değiştirdi, sildi” gibi soruların cevapları bulunabilmektedir. BT (Bilgi Teknolojileri) alt yapılarında bu logların toplanması, bir olay için delil niteliğinde saklanması, analiz edilmesi önemlidir [14]. Log toplamak ve saklamak çoğu amaç için önemlidir fakat yeterli değildir. Toplanan bu loglar analiz edilip, milyonlarca log birbiri ile ilişkilendirilerek tehdit ve zafiyetler tespit edilmelidir. Bu da log yönetiminde mevcut olmayan korelasyon, bir olay sırasında alarm üretmek gibi yetenekleri olan SIEM ile mümkündür.

SIEM çözümleri, toplanan loglar ile tehditleri gerçek zamanlı izlemekte, tespit ve analiz etmektedir. Bir olay karşısında aksiyon almak, adli olaylarda hızlıca delil sağlamak, olayları raporlamak, bu olayları görsel tasarım ile sunmak, farklı formattaki logları ilişkilendirmek gibi yetenekler ile BT alt yapılarının güvenliğinde önemli rol oynamaktadır.

Ortalama büyüklükte olan bir ağda bir ayda milyarlarca log üreyebilmektedir [15]. Siber bir olay olduğunda bu olay ağın farklı noktalarına sıçrayabilmektedir. Bu olay incelenmek istediğinde tehdidin bulaştığı tüm sistemlerin loglarının incelenmesi gerekmektedir. Tehdidin tespit edilmesi çok zaman alacak ve loglar aranırken odak noktası kaybedilecektir. Ancak SIEM sayesinde milyarlarca log içerisinde istenilen olay anında tespit edilebilmektedir.

Amaç ve ihtiyaçlara göre değişkenlik gösterse de genel olarak SIEM’in kullanılmasının nedenleri:

- Tehdit ve zafiyetlerin tespit edilmesi ve olay takibinin yapılması
- Domain hesaplarının denetlenmesi
- Bilinmeyen ihlallerin erken tespiti
- Kurumsal güvenlik standart ihlallerinin takibinin yapılması
- Standart ve yasalara uyum sağlamak ve raporlama yapılması
- Adli olaylar için delil sunma
- Zararlı IP ve URL’lere erişim sağlandığının tespiti gibi amaçlar için kullanılmaktadır.

Bilgi güvenliği risk yönetiminde de SIEM önemli rol üstlenmektedir. Risk yönetiminde amaç, tehditlerden kaynaklanan riskin tespit edilmesi ve riskin azaltılması için alınacak önlemlere karar vermektir. Bilgi güvenliği risk yönetimi yaklaşımının 5 ana kontrol noktası bulunmaktadır [16]. SIEM ile log kaynakları belirleneceği için, tanımlama fonksiyonu kontrol grubunda yer alan varlık yönetimine katkı verilebilir. SIEM ile yazılacak korelasyonlar sayesinde erişim kontrolü sağlanabilir. Kritik bir klasörün silinmesinin tespit edilmesi gibi noktalarda veri güvenliği sağlanabilir.

SIEM'in en önemli yeteneği korelasyondur. Korelasyon ise hayal gücü ile orantılıdır. Elbette hayal edilen bir kuralın gerçeğe dönüşebilmesi için ürünün o hayali hayata geçirecek yeteneği olmalıdır.

2.3. Log Yönetimi

Log, tüm sistem ve ağ cihazlarında oluşan olay kaydıdır. Bu logların her biri bir log girişinden oluşmaktadır ve bu girişlerin hepsi belirli bir olayı ihtiva etmektedir. Bunların en önemlileri güvenlik loglarıdır. Kuruluştaki birçok log bilgisayar güvenliği ile ilgilidir. SANS enstitüsüne göre loglar, güvenlik uzmanları için, belirli bir cihaz veya uygulama için bir olayın kim, ne, ne zaman, nerede ve neden hakkındaki verileri kaydetmek için kullanılmaktadır [14]. Bu bilgisayar güvenlik logları, virüsten koruma yazılımı, güvenlik duvarları ve izinsiz giriş algılama ve önleme sistemleri gibi güvenlik yazılımları, sunucular, iş istasyonları ve ağ ekipmanlarındaki işletim sistemleri ve uygulamalardan oluşmaktadır [17].

Büyük log yönetimi operasyonel süreçleri tipik olarak günlük kaynaklarını yapılandırmayı, günlük analizi gerçekleştirmeyi, belirlenen olaylara karşı yanıtları başlatmayı ve uzun süreli depolamayı yönetmeyi içermektedir. Ayrıca, günlük yönetimi logların gizliliğini, bütünlüğünü ve kullanılabilirliğini korumayı içermektedir [18].

Log yönetimiyle ilgili bazı unsurlar aşağıdaki gibidir [19]:

- Logların merkez bir noktada toplanması
- Logların saklanması
- Verilere hızlı erişimi ve gösteriminin sağlanması

- Çok sayıda log formatının desteklenmesi
- Veri analizinin yapılması
- Kayıtların saklanması
- Arşivleme ve arşivlenen logları geri getirme
- Verilerin yetkiler ve ilişkiler seviyesinde erişimi
- Veri bütünlüğünün sağlanması

Yukarıda belirtilen amaçların dışında logların depolanması ve güvenliğinin sağlanması belirli yasa ve standartlar doğrultusunda gerçekleştirilmektedir.

2.3.1. Log Formatları

Log formatı, günlüklerin makine tarafından okunabilmesini ve kolayca ayrıştırılabilmesini sağlayan yapılandırılmış bir biçimdir. Syslog, Common Log Format, Extended Log Format (ELF), W3C (World Wide Web Consortium) Log File, Microsoft IIS Log File, CEF (Common Event Format) gibi log formatları sistemler tarafından kullanılan log formatlarından bazılarıdır.

2.3.1.1. Syslog

Syslog, ağ aygıtlarının genellikle syslog sunucusu olarak bilinen bir günlük sunucusuna olay iletileri göndermesi için bir mekanizma sağlamaktadır. Syslog protokolü, farklı olay türlerini günlüğe kaydetmek için kullanılabilmekteve çok çeşitli aygıtlar tarafından desteklenmektedir. Syslog'un nasıl kullanılabileceğinin bir örneği, bir güvenlik duvarı engellenen bir bağlantı noktasına bağlanmaya çalışan sistemler hakkında mesaj gönderebilmekte, web sunucusu ise erişim reddedilen olayları günlüğe kaydedebilmektedir. Yönlendiriciler, anahtarlar ve güvenlik duvarları gibi çoğu ağ ekipmanı syslog mesajları gönderebilmektedir. Ayrıca, bazı yazıcılar ve Apache gibi web sunucuları Syslog mesajları gönderme olanağına sahiptir. Ancak Windows tabanlı sunucular syslog formatını yerel olarak desteklememektedir. Windows Olay Günlüklerinin toplanarak bir syslog sunucusuna iletilmesi için çok sayıda üçüncü taraf araçlar bulunmaktadır.

2.3.1.2. Windows Olay Günlüğü

Windows olay günlüğü, Windows işletim sistemi tarafından yakalanan ve depolanan işletim sistemi, uygulama, güvenlik ve olay bildirimlerinin ayrıntılı bir kaydını sağlamaktadır. Bu olaylar genellikle sistem yöneticileri tarafından olası sorunu teşhis etmek ve gelecekteki sorunları önlemek için kullanılmaktadır. İşletim sistemi ve yüklü uygulamalarla ilgili olası sorunları gidermek için kullanılabilecek önemli donanım ve yazılım eylemlerini kaydetmek için bu olay günlükleri kullanılmaktadır. Windows işletim sistemi, uygulama yüklemeleri, sistem kurulum işlemleri, hatalar ve güvenlik sorunları gibi olayları izlemek için günlük dosyaları oluşturmaktadır.

Windows Olay Günlüğü aşağıdaki öğeleri içermektedir:

- Etkinliğin gerçekleştiği tarih
- Olayın gerçekleştiği saat
- Olay meydana geldiğinde makinede oturum açan kullanıcının kullanıcı adı
- Bilgisayarın adı
- Olay Kimliği, olay türünü belirten bir Windows kimlik numarasıdır
- Olaya neden olan program veya bileşen olan kaynak

Ayrıca, Windows olay günlüğü işletim sistemi, kurulum, güvenlik, uygulama ve iletilen olayları da yakalamaktadır. Sistem olayları Windows işletim sistemindeki olaylardır ve bu olaylar aygıt sürücüleri veya diğer işletim sistemi bileşeni hataları gibi öğeleri içermektedir. Kurulum olayları, işletim sisteminin yapılandırma ayarlarıyla ilgili olayları içermektedir. Güvenlik olayları Windows sisteminin denetim ilkelerini kullanmaktadır. Bu olaylara kullanıcı oturum açma girişimleri ve sistem kaynağı erişimi de dâhildir.

Uygulama olayları, yerel işletim sistemine yüklenen yazılımla ilgili olaylardır. Yüklü bir uygulama çökerse, Windows olay günlüğü tarafından sorunla ilgili bir log oluşturulur. Bu logların içerisinde uygulama adı ve çökmesine neden olan olaylar yer almaktadır.

Windows olay günlükleri SIEM gibi üçüncü parti uygulamalara aktarılabilmektedir. Bu sayede SIEM ile bu loglar üzerinde log toplama ve korelasyon işlemleri gerçekleştirilebilmektedir.

2.3.1.3. Ortak Olay Biçimi Formatı

Ortak Olay Biçimi anlamına gelen CEF, metin tabanlı genişletilebilir bir formattır. CEF, farklı ağ cihazlarından, uygulamalardan ve araçlardan gelen güvenlik bilgilerinin kolayca paylaşılabilmesi için ortak bir olay günlüğü standardı olarak oluşturulmuştur. Bir aktarım mekanizması olarak hareket ederek hassas bilgilerin birlikte çalışabilirliğini geliştirmek ve güvenlik ile ilgili olmayan cihazlar arasındaki entegrasyonu kolaylaştırmak için kullanılmaktadır. CEF, UTF-8 Unicode kodlama yöntemini kullanır, bu nedenle tüm iletinin UTF-8 kodlanmış olması gerekmektedir.

2.3.1.4. Genişletilmiş Günlük Biçimi

W3C Genişletilmiş Günlük Biçimi, Microsoft Internet Information Server (IIS) sürüm 4.0 ve 5.0 tarafından kullanılan özelleştirilebilir bir biçimdir. Özelleştirilebilir olduğundan, gereksinimlere ve tercihlere göre farklı alanlar eklenebilmekte veya azaltılabilmektedir. Bu durum da dosyanın boyutunu artırabilmekte veya azaltabilmektedir. Veri günlüklerinin doğru bir şekilde arşivlenmesi, günlük yönetiminin önemli bir parçasıdır [20].

2.3.1.5. Açık Veritabanı Bağlantısı Günlük Dosyası

ODBC, Microsoft Access veya Microsoft SQL Server gibi bir Açık Veritabanı Bağlantısı (ODBC) veritabanıyla uyumlu sabit veri alanlarının günlük biçimidir [21].

ODBC günlük kaydı, çoğu günlük kaydı türünden biraz daha karmaşıktır ve biraz düzeltme gerektirmektedir. Hem oturum açmak istenilen veritabanının belirtilmesi hem de günlük verileri almak için veritabanı tablosunun el ile ayarlanması gerekmektedir.

IIS ‘de (Internet Information Server) SQL veritabanında çalıştırılması gereken bir SQL şablon dosyası vardır. “Logtemp.sql” adlı bu dosya varsayılan olarak “c:\winnt\system32\inetsrv\logtemp.sql“ konumunda bulunmaktadır.

2.3.2. Etkin Log Yönetimi

Log yönetimi herhangi bir SIEM çözümünün de ilk anahtarıdır. Toplanan bir log yok ise SIEM in de anlamı yoktur. Elbette her logun alınması gerekmemektedir. Bağlı olunan yasalar, standartlar ve güvenlik stratejileri doğrultusunda ihtiyaç duyulan loglar toplanmalıdır. Günlük yönetimi ihtiyaçlarını değerlendirmeye başlarken, çözümün sınırlarını tanımlamak istenebilmektedir. Bu sınırların tanımlanmasını sağlayacak bazı yaklaşımlar aşağıda belirtilmiştir.

2.3.2.1. Politika ve Prosedürlerin Tanımlanması

Başarılı günlük yönetimi etkinliklerini oluşturmak ve sürdürmek için standart süreçler geliştirilmelidir. Planlama sürecinin bir parçası olarak, bir kuruluş günlük tutma gereksinimlerini ve hedeflerini tanımlamalıdır. Bunlara dayanarak, bir kuruluş daha sonra zorunlu gereksinimleri açıkça tanımlayan politikalar geliştirmeli ve günlük oluşturma faaliyetleri için aktarma, depolama, analiz ve imha gibi aksiyon tanımlamaları olmalıdır.

2.3.2.2. Kuruluşa Uygun Log Yönetimi

Bir kuruluş günlük yönetimi süreci için gereksinimlerini ve hedeflerini tanımladıktan sonra, kuruluşun algılanan risk azaltma ve günlük yönetimi işlevlerini gerçekleştirmek için gereken zaman ve kaynaklara bağlı olarak gereksinimler ve hedeflerine öncelik derecelendirilmesi yapmalıdır. Ayrıca, kuruluş hem bireysel sistem düzeyinde hem de günlük yönetimi altyapı düzeyinde kilit personel için günlük yönetimi için rolleri ve sorumlulukları tanımlamalıdır. Günlük yönetimi görevleri oluşturmak da buna dâhildir.

2.3.2.3. Kuruluşların Günlün Yönetimi Oluşturması ve Sürdürmesi

Günlük yönetimi altyapısı, günlük verileri oluşturmak, iletmek, depolamak, analiz etmek ve silmek için kullanılan donanım, yazılım, ağlar ve ortamdan oluşmaktadır. Günlük yönetimi altyapıları, günlük verilerin analizini ve güvenliğini destekleyen çeşitli işlevleri gerçekleştirmektedir. Bir kuruluş yönetim ilkesi oluşturduktan, rolleri ve sorumlulukları belirledikten sonra ilkeyi ve rolleri etkin bir şekilde destekleyen bir veya daha fazla günlük yönetimi altyapısı geliştirmelidir. Kuruluşlar, merkezi günlük sunucularını ve günlük veri depolamasını içeren günlük yönetimi altyapılarını uygulamayı düşünmelidir. Altyapıları tasarlarken kuruluşlar, hem altyapıların hem de kuruluştaki bireysel günlük kaynaklarının

hem mevcut hem de gelecekteki ihtiyaçlarını planlamalıdır. Tasarımda dikkate alınması gereken önemli faktörler arasında işlenecek günlük verilerinin hacmi, ağ bant genişliği, çevrimiçi ve çevrimdışı veri depolama, veriler için güvenlik gereksinimleri ve personelin günlükleri analiz etmesi için gereken zaman ve kaynaklar yer almaktadır.

2.3.2.4. Günlük Yönetiminde Sorumlulukları Olan Personellere Uygun Desteğin Sağlanması

Bireysel sistemler için günlük yönetiminin kuruluş genelinde etkin bir şekilde gerçekleştirilmesini sağlamak için bu sistemlerin yöneticileri yeterli destek almalıdır. Bu, bilginin yayılmasını, eğitim verilmesini, soruların cevaplanması için temas noktalarının belirlenmesini, spesifik teknik rehberliğin sağlanmasını ve araçların ve belgelerin mevcut olmasını içermelidir.

Kuruluşlar standart günlük yönetimi operasyonel süreçlerini oluşturmalıdır. Büyük günlük yönetimi operasyonel süreçleri tipik olarak günlük kaynaklarını yapılandırmayı, günlük analizi gerçekleştirmeyi, tanımlanmış olaylara yanıtları başlatmayı ve uzun süreli depolamayı yönetmeyi içermektedir. Yöneticilerin diğer sorumlulukları:

- Tüm günlük kaynaklarının günlük durumunu izleme.
- Günlük döndürme ve arşivleme işlemlerini izleme.
- Kayıt yazılımındaki yükseltmeleri ve yamaları kontrol etme ve bunları edinme, test etme ve dağıtma.
- Her bir günlük sahibinin saatinin ortak bir zaman kaynağına senkronize edilmesini sağlamak.
- Günlük tutmayı, politika değişiklikleri, teknoloji değişiklikleri ve diğer faktörlere göre gerektiği gibi yeniden yapılandırma.
- Günlük ayarları, yapılandırmalar ve işlemlerde anormallikleri belgeleme ve raporlama.

2.3.2.5. Logların Saklanması Gereken Sürenin Belirlenmesi

Sektör yönetmelikleri veya yasaları, belirli bir süre boyunca belirli veri türlerini korumayı gerektirebilmektedir. Örneğin 5651 sayılı yasaya göre loglar 6 ay ila 24 ay arasında saklanmalıdır [22]. Ayrıca, belirli bir süre sonra (veri imhası) bilgilerin nasıl imha edilmesi gerektiğini belirleyen yasal ve işlevsel unsurlar olabilmektedir. Günlük bilgilerinin saklanması gereken süre süre, öncekinden daha kısa ve ikincisinden daha uzun olmamalıdır.

2.3.2.6. Log Saklama Miktarının Belirlenmesi

Küçük bir ağda bile üretilebilen günlük ve olay bilgisi miktarı sınırlı değilse kullanılabilir depolama alanının miktarı hızla aşılacaktır. Az sayıdaki ağ aygıtları bile günde olarak milyonlarca olay iletisi oluşturabilir. Veri merkezlerinde, günde yüz milyonlarca hatta milyarlarca log üreyebilmektedir. Bu sebeple veri saklama ve veri yok etme kriterleri ile birlikte, ne tür verilerin tutulması gerektiğine karar verilmesi gerekmektedir. Hedef çok log toplamak değil, toplanan logların hangi ihtiyacı gidereceğidir.

2.3.2.7. Ne Tür Bilgi Sistemi Logları Tutmak ve Analiz Etmek Gerekir?

Log sayısı arttıkça bunların yönetim problemi olacak ve SIEM ile hedeflenen başarı sağlanamayacaktır. SIEM ile bu başarının elde edilebilmesi, ne tür bilgilerin toplanacağı ile ilgilidir. Bu yüzden tek bir odak noktası olamaz. Veri merkezinde bulunan sistem, güvenlik ve ağ cihazlarından yalnızca ihtiyaç doğrultusunda loglar alınmalıdır. Kritiklik ve önem seviyesine göre seçim yapılmalıdır. Örneğin bir uygulama sunucusundan takip edilmesi gereken özel bir talep olmadıkça standart audit logları alınabilir.

Log yönetimi yalnızca logların saklanması değildir. Belirlenen hedeflerin sağlandığının görülmesidir. Log yönetimi ile hedefler; erişim istatistikleri, raporlama, sistemlerdeki anomali hareketlerin tespiti gibi belirli amaçlara yönelik sonuçların alınmasıdır.

2.3.3. Log Yönetimi ve SIEM Farkı

SIEM ve log yönetimi benzer işlevleri olan fakat farklı özelliklere sahip sistemlerdir. Log yönetimi, belirli kaynaklardan logları toplayan, onları anlamlandıran ve raporlama yapan sistemlerdir. SIEM ise toplanan bu logları anlamlandıran, gerçek zamanlı analiz eden ve istenilen durumlarda alarm üreten sistemdir. SIEM'in log yönetiminden farkı:

- Sınıflandırma (Taksonomi)
- Korelasyon
- Alarm tanımlamalarıdır.

Benzer yanları ise, logların toplanması ve raporlama kısmıdır.

2.4. Yasalar ve Standartlar

Siber güvenliğin sağlanması için ilk adım sahip olunan varlıkların tam olarak bilinmesi, bu varlıklar üzerinde önceliklendirme yapılmasıdır. Ayrıca, belirli politikalar ve standartlar ile korunması gerekmektedir. Güvenlik politikasında amaç, güvenlik seviyesinin belirlenmesi, uygulamaya konulması, iyileştirilmesi gibi konuların incelenmesidir. Standartların oluşmasında bu politikaların önemli etkisi bulunmaktadır.

Bilgi güvenliğinin sağlanması için bazı standartlar ve yasalar bulunmaktadır. Bunlar; Açık Anahtar Şifreleme Standartları (Public Key Crypto Standard-PCKS), Müttefik Kalite Güvence Yayınları Standardı (Allied Quality Assurance Publications-AQAP), IEEE (The Institute of Electrical and Electronics Engineers) Standartları, ETSI (European Telecommunications Standard Institute) Standartları, ITU (International Telecommunication Union) Standatları ve Siber Güvenlik Faaliyetleri, NIST (NIST Cybersecurity Framework) Siber Güvenlik Platformu, Bilişim Teknolojileri Yönetim ve Denetim Enstitüsü (Information Systems Audit and Control Association - ISACA) Standartları, ENISA (European Union Agency For Cybersecurity) standartları ve Türkiye'deki 5651 sayılı kanun ve Kişisel Verilerin Korunması Kanunudur (KVKK).

2.4.1. 5651 Sayılı Kanun

İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi hakkındaki kanun 23 Mayıs 2007 tarihinde resmi gazetede yayınlanarak yürürlüğe girmiştir. Kanuna göre, yönetmelikte belirtilen trafik bilgileri yine yönetmelikte belirlenecek süre kadar yani en az 6 altı ay, en fazla 2 yıla kadar saklanması gerektiği ve bu bilgilerin doğruluğu, gizliliği ve bütünlüğünün sağlanması gerektiği belirtilmiştir. Burada belirtilen trafik bilgileri, sistemlerden elde edilen log kayıtlarıdır. Bu kayıtlar adli vakalar için delil niteliğindedir. 5651 Sayılı kanunda; "Kullanıcılarına internet

ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler" tanımına karşılık gelen kamu kurumları, internet sağlayıcıları vs. altı aydan iki yıla kadar log kayıtlarını saklamak zorundadır.

Bu kanunun yönergelerine uymakla zorunlu olan kurumlar oteller, alışveriş merkezleri, üniversiteler, kafeler, internet kafeler, küçük ve orta boyutlu işletmeler, fabrikalar gibi interneti toplu kullanıma açan kurumlardır.

Kanun kapsamına, işletmelerin müşterilerine sunduğu ücretsiz internet hizmeti ve firmaların çalışanlarına şirket içerisinde sundukları internet hizmeti de girmektedir [22].

5651 sayılı yasa gereğince bazı yükümlülükler;

- İç IP adres dağıtım logları (Dynamic Host Configuration Protocol - DHCP)
- Web erişim logları
- Web erişimlerinde içerik tabanlı filtrelemenin yapılması
- Logların zaman damgası ile saklanması ve gizliliğinin temin edilmesi

Yukarıdaki yükümlülükler incelendiğinde kullanılan SIEM ürünü bu yükümlülükleri karşılamalıdır.

2.4.2. Kişisel Verileri Koruma Kanunu

6698 sayılı kişisel verileri koruma kanunu, günlük hayatta farklı sistemlere bir şekilde kaydolmuş olan kişisel verilerin kullanımına bir standart getirmektedir. Bu standart, kişisel bir verinin izin verilenden farklı amaçlarla kullanılmasının önüne geçmekte ve bu doğrultuda ciddi yaptırımları bulunmaktadır [23].

KVKK'nın kurumlardan beklentileri aşağıdaki gibidir:

- Kişisel bir verinin alınıp kayıt edilmesi için Açık Rıza almak gerekmektedir [24].
- Veriyi saklarken verilen taahhüt ve alınan açık rızanın beyan edildiği sözleşmeyi yasal otoritenin talep ettiği bir durumda onlarla paylaşılabilmelidir [25].

- Açık rıza ile kişisel verileri alınan bir kişiye, istediği herhangi bir anda, bu verinin silinmesini veya güncellenmesini sağlayabileceği yolları bildirilmeli ve bu yollar sürekli açık tutulmalıdır [25].

- Açık rıza ile alınan veriyi transfer ederken ve saklarken gerekli güvenlik önlemleri alınmalı, bu veriye ulaşma hakkı olmayan kişi ve kurumların eline geçmesi önlenmelidir. [25].

Bu doğrultuda sistemlerde yalnızca SIEM satın almak yeterli değildir. Satın alınan SIEM'in KVKK ile uyumlu olması gerekmektedir. KVKK'nın "Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Gratis İç ve Dış Tic. A.Ş." başlıklı duyurusunda bu durumun önemi daha da iyi anlaşılmaktadır [26]. Bu duyuruya göre 2092 Gratis müşterisinin site hesaplarının şifreleri, kimlik, iletişim ve müşteri işlem verilerinin ele geçirildiği anlaşılmaktadır. İhlal 04.03.2020 ile 06.03.2020 tarihleri arasında gerçekleşmesine rağmen şirket e-posta adresine kimliği belirsiz birisi tarafından web sitesi üyelerinin e-posta ve şifrelerinin ele geçirildiğine yönelik bir posta sayesinde son gün fark edilebilmiştir. İhlal incelendiğinde birden fazla başarısız giriş yapıldığı anlaşılmaktadır. Uygun bir SIEM korelasyonunda bu başarısız giriş denemeleri ile ilgili alarm üretilebilir ve önceden tespit edilerek önlem alınabilirdi.

2.4.3. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi

Merkezi güvenlik sisteminde gerçek anlamda güvenliğin oturtulabilmesi için kuruluşlar, ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission) 27001 standardında belirtilen bilgi güvenliği yönetim sistemini kurarak gerçek risklerini saptayabilmekte ve bu risklerin giderilmesi için gereken teknoloji, politika ve prosedürleri devreye alabilmektedirler [27]. Bu sayede güvenlik yönetim sistemi olarak oluşturulan ve yalnızca teknoloji ile değil aynı zamanda tüm şirket çalışanlarının da uyguladığı iş süreçleri ile de devamlılık sağlıklı bir şekilde sağlanabilmektedir.

ISO 27001'e uyum sağlayan çoğu kuruluş için, geniş kapsamı nedeniyle zorlu bir görevdir. Bu standarda uyum; varlık yönetimi, erişim kontrolü, günlüğe kaydetme ve izleme, ağ güvenliği yönetimi, uygulama güvenliği yönetimi, bilgi güvenliği olay yönetimi konularında fayda sağlamaktadır [28]. Bir kurumda SIEM kullanılıyorsa, logların alınacağı kaynaklar sisteme girileceği için varlık yönetimi yapılabilecektir. Alınacak loglardan bu kaynaklara

kimlerin erişmesi gerektiğinin takibi yapılabilecektir. Üretilen loglar depolanabilecek ve takip edilebilecektir. Ağ güvenliğinin sağlanması için korelasyon kuralları yazılabilecektir.

2.4.4. PCI Güvenlik Standartları Konseyi

PCI (Payment Card Industry) DSS (Data Security Standart), kredi kartı veya banka kartı verilerini saklayan, ileten veya işleyen işletmeleri hedeflemektedir [29]. Standartlar, tüm ağ altyapısı bileşenleri, sunucular, mesajlaşma sistemleri ve kart sahibi veri ortamına dâhil olan veya kart sahibi veri ortamına bağlı uygulamalar için de geçerlidir.

PCI DSS, her bir alanda çok sayıda özel gereksinime sahip 12 ayrı kontrol alanı içeren bir güvenlik spesifikasyonu içermektedir [30]:

- Sistemler güvenlik duvarı ile korunmalıdır.
- Güçlü parola ve yapılandırma tanımlamaları yapılmalıdır ve varsayılan şifreler kullanılmamalıdır.
- Saklanan kart sahibi bilgileri korunmalıdır.
- Kart sahibi verilerinin açık ve genel ağlar üzerinden iletimini şifrelenmelidir.
- Virüsten koruma yazılımı veya programlarını kullanılmalı ve düzenli olarak güncellenmelidir.
- Güvenli sistemler ve uygulamalar geliştirilmeli ve sürdürülmelidir.
- Kart sahibi verilerine erişimi, işletmenin bilmesi gerekenlerle kısıtlanmalıdır.
- Bilgisayar erişimi olan her kişiye benzersiz bir kimlik atanmalıdır.
- Kart sahibi verilerine fiziksel erişimi kısıtlanmalıdır.
- Ağ kaynaklarına ve kart sahibi verilerine tüm erişimi izlenmelidir.
- Güvenlik sistemlerini ve süreçlerini düzenli olarak test edilmelidir.
- Çalışanlar ve yükleniciler için bilgi güvenliğini ele alan bir politika sürdürülmelidir.

2.5. Veri Merkezi Nedir?

Veri merkezi, bir kuruluşun BT işlemlerini ve sistemlerini merkezileştiren, ayrıca verilerini depoladığı, yönettiği ve yaydığı bir tesistir. Veri merkezleri bir ağın en kritik sistemlerini barındırır ve günlük işlemlerin sürekliliği için hayati öneme sahiptir. Sonuç olarak, veri merkezlerinin ve veri merkezlerinde saklanan bilgilerin güvenliği ve güvenilirliği kuruluşlar için en önemli önceliktir.

Veri merkezi tasarımları benzersiz olsa da, genellikle internete dönük veya dâhili veri merkezleri olarak sınıflandırılabilir. İnternet'e dönük veri merkezleri nispeten az sayıda uygulamayı destekler, genellikle tarayıcı tabanlıdır ve genellikle bilinmeyen birçok kullanıcıya sahiptir. Buna karşılık, kurumsal veri merkezleri daha az kullanıcıya hizmet verebilmekte ancak kullanıma hazırdan özel uygulamalara kadar değişen daha fazla uygulama barındırabilmektedir.

Gün geçtikçe verilerin fazlalaşması ile depolama alanı ve bu verilerin işletilme ihtiyacı da artmaktadır [31]. Veri üreten veya kullanan her kurum, devlet kurumları, eğitim kurumları, telekomünikasyon şirketleri, finansal kurumlar, her büyüklükteki perakendeciler ve Google ve Facebook gibi çevrimiçi bilgi ve sosyal ağ hizmetlerinin tedarikçileri de dâhil olmak üzere farklı büyüklüklerde veri merkezine ihtiyaç duyulmaktadır. Örneğin Google şirketinin Kuzey Amerika'da 13, Güney Amerika'da 1, Avrupa'da 5, Asya'da 2 olmak üzere toplam 21 veri merkezi bulunmaktadır [32]. Bu doğrultuda verilere hızlı ve güvenilir erişimin olmaması, hayati hizmetler sağlanamaması veya müşteri memnuniyeti ve gelir kaybı anlamına gelebilmektedir.

2.5.1. Veri Merkezi Türleri

Tüm veri merkezleri esasen ağ altyapısı için alan, güç ve soğutma sağlayan binalardır. Bir işletmenin BT işlemlerini veya sistemlerini merkezileştirmekte, ayrıca verileri depolamakta, paylaşmakta ve yönetmektedir [33].

Verdikleri hizmetler kapsamında farklı veri merkezi türleri bulunmaktadır.

2.5.1.1. Hiber Ölçekli Veri Merkezi

Hyperscale (veya Enterprise Hyperscale) veri merkezi, desteklediği şirketin sahibi olduğu ve işlettiği bir tesistir. Buna Microsoft, Google ve Apple gibi şirketler dâhildir. Genellikle ultra yüksek hızlı, yüksek fiber sayısı ağına bağlı en az 5.000 sunucu bulunmaktadır [33].

2.5.1.2. Ortak Yerleşimli Veri Merkezi

Co-location olarak adlandırılan veri merkezleri, sunucuların "ortak barındırılması" anlamına gelen veri merkezleridir. Bu veri merkezleri tamamen profesyonel bir altyapıya sahip olmakla birlikte, tüm donanımı müşteriye ait olan sunuculara alan yaratmaktadır [34]. Co-location veri merkezleri, bir işletmenin sunucular ve diğer bilgi işlem donanımı için yer kiralayabileceği bir veri merkezi tesisidir. Genellikle, müşteri sunucu ve depolama sağlarken bina, soğutma, güç, bant genişliği ve fiziksel güvenlik sağlamaktadır [35]. Co-location veri merkezlerini genellikle büyük kurumsal şirketler, uzun süre erişim sağlanacak internet siteleri veya internet uygulamaları, video siteleri gibi içeriği yoğun olan siteler ve diğer büyük ölçekli internet siteleri kullanmaktadır [34].

2.5.1.3. Büyük Ölçekte Ortak Yerleşimli Veri Merkezi

Büyük ölçekli co-location veri merkezi, bir kiracının, tam dâhili veri merkezi alanını kiraladığı veri merkezidir. Çoğu zaman kiracı bu alandaki tüm BT işlemlerini her zaman olmamakla birlikte yürütmekten sorumludur [36]. Tipik olarak kabin sayısı 100 kabin ile 1.000'den fazla kabin arasında değişmektedir [33].

2.5.1.4. Kurumsal Veri Merkezi

Bazen hiper ölçekli veri merkezleri ile birbirinin yerine kullanılsa da, bir işletme tesisi, büyüklüğü ve kapasitesinden ziyade amacı ve mülkiyeti ile tanımlanmaktadır. Oldukça basit bir şekilde, bir kurumsal veri merkezi yalnızca tek bir kuruluşu desteklemek için kullanılan özel bir tesistir. Şirket içinde daha büyük bir kampüsün veya iş sitesinin bir parçası olarak yerleştirilebilirler ancak çoğu durumda bağlantı, güç ve güvenlik amaçları için seçilen bir sitede tesis dışında konumlandırılırlar [37].

2.5.1.5. Telekom Veri Merkezi

Telekomünikasyon veya Servis Sağlayıcı şirketin sahibi olduğu ve işlettiği bir tesistir. Bu tür veri merkezleri çok yüksek bağlantı gerektirir ve temel olarak içerik dağıtımını, mobil hizmetleri ve bulut hizmetlerini yönlendirmekten sorumludur.

Veri merkezleri Katman 1, Katman 2, Katman 3 ve Katmak 4 olmak üzere 4 veri merkezi katmanı bulunmaktadır [38]. Bunlar veri merkezinin çalışma süresini tanımlamak için kullanılan standartlaştırılmış bir metodolojiden başka bir şey değildir. Bu katmanlar performans, yatırım ve yatırım getirisi ölçümleri için faydalıdır.

Katman 4 veri merkezi en sağlam ve arızalara daha az eğilimli olarak kabul edilmektedir. Katman 4, tam yedekli alt sistemleri (soğutma, güç, ağ bağlantıları, depolama vb.) ve biyometrik erişim kontrol yöntemleriyle kontrol edilen bölümlere ayrılmış güvenlik bölgeleriyle kritik görev sunucularını ve bilgisayar sistemlerini barındırmak için tasarlanmıştır. Doğal olarak, en basit olanı, küçük işletmeler veya mağazalar tarafından kullanılan Katman 1 veri merkezidir. Kısaca bahsetmek gerekirse;

Katman 1: Sistemler burada yedeksiz çalışmaktadır.

Katman 2: Katman 1 + sistemler yedekli çalışmaktadır.

Katman 3: Katman 1 + Katman 2 + Yedekli enerji ve çoklu uplink ile çalışmaktadır.

Katman 4: Katman 1 + Katman 2 + Katman 3 + tüm bileşenler uplinkler, depolama, soğutucular, ısıtma, havalandırma ve iklimlendirme sistemleri, sunucular vb. dâhil olmak üzere tamamen hataya dayanıklıdır.

3. VERİ MERKEZİ BİLGİ GÜVENLİĞİNİN SAĞLANMASI VE ETKİN SIEM YÖNETİMİ

Veri merkezlerinde büyük ölçekte veriler toplanır, depolanır ve işlenerek belirli noktalara dağıtılır. Bu merkezler çeşitli hizmetlerin, ihtiyaçların karşılanması için sistem, uygulama, ağ ve güvenlik cihazlarını bir çatı altında toplamaktadır. Günümüzde bazı devlet, eğitim, finans kurumlarının yanında Google, Yandex gibi çevrimiçi hizmet sunan şirketler de veri merkezleri içerisinde hizmet sunmaktadır.

SIEM ile veri merkezi bünyesinde bulunan sistemlerden, uygulamalardan, ağ ve güvenlik cihazlarından toplanan loglar sayesinde kritik olayların analizi, şüpheli durumların tespiti ile saldırı öncesi tespit, bir problemin kök sebebinin tespit edilmesi gibi faydaların sağlanması amaçlanmaktadır.

Bir SIEM proje sürecinin başlangıcından itibaren her adımı çok önemlidir. Yanlış yapılandırılan, planlama aşaması iyi yönetilemeyen bir sürecin sonunda performans sorunları, logların yığılması, log kaçırma ve olayları analiz etmede güçlükler gibi problemler ortaya çıkabilmektedir.

Bölüm 3'te veri merkezlerinde bilgi güvenliğinin sağlanması ve bir SIEM projesinin başlangıcında nelere dikkat edilmesi gerektiği, korelasyon yeteneklerinin nasıl kullanılması gerektiğine yönelik bilgiler yer almaktadır.

Veri merkezleri için SIEM projesinin başlatılmasında planlama çok önemlidir. Kurulacak olan sistemin ihtiyacı olan kaynakların ve kapasitenin hesaplanması de bu doğrultuda planlama aşamasında çok kritik bir rol oynamaktadır.

3.1. Kurulum Aşamasında Kritik Noktalar

Veri merkezleri için SIEM projesinin başlatılmasında planlama çok önemlidir. Kurulacak olan sistemin ihtiyacı olan kaynakların ve kapasitenin hesaplanması de bu doğrultuda planlama aşamasında kritik bir rol oynamaktadır.

SIEM sistemlerinde bulunan donanımsal kaynaklar farklı amaçlarla kullanılmaktadır. Dolayısıyla sistem kaynaklarında ihtiyaç duyulan isterler bilinmelidir. Bu kaynaklar CPU, Disk ve RAM olmak üzere üç tanedir.

Bir SIEM çözümünde ihtiyaç duyulan kaynaklar:

- CPU: Toplanan loglar sisteme yazılma hızını doğrudan etkilemektedir. CPU değeri yükseltildikçe toplanan logların anlamlandırılma (parse işlemi) hızı ve diske işlenme hızı da artmaktadır.
- RAM: RAM kullanımı dashboard ve web sistesi görselleri açısından önemlidir. Ayrıca yapılan korelasyonlar da RAM kaynağından harcamaktadır. Diğer bir yandan raporlar veya geçmişteki log analizini yapmak için de RAM kullanılmaktadır.
- DİSK: Verilerin saklanması doğrudan disk boyutu ile ilgilidir. Disklerin okuma yazma performans değeri de logların daha hızlı saklanması için önemlidir. Bu yüzden giriş çıkış anlamına gelen IO (Input/Output) performansı çok iyi disklerin seçilmesi gerekmektedir.

Sonuç olarak sistemlerde bulunan her kaynağı eklemek ve bu kaynaklardan tüm logları almadan önce bu kaynakların sistemi ne kadar yoracağını hesaplamak gerekmektedir. Aksi takdirde performans sorunları, log kayıpları ortaya çıkabilecek ve hatta SIEM sisteminin çökme ihtimali olacaktır.

3.1.1. Kapasite Planlama

SIEM projelerinde korelasyon, raporlama, alarm gibi unsurlar kadar bir SIEM projesinin başlangıcındaki planlama süreci de çok önemlidir. Bu süreçte kapasite planlamasının iyi yapılması da projenin başarısıyla doğrudan bağlantılıdır.

SIEM sistemleri, maksimum düzeyde sistem özellikleri ile kurulmalıdır. Amaç, verilerin hiçbir şekilde kayba uğramadan toplanabilmesini ve analizini sağlamaktır. Bu sebeple sistem özelliklerinin hesaplanmasının nasıl yapılacağı iyi bilinmelidir. Burada kastedilen bir saniye içerisinde sisteme ulaşan veri miktarı anlamına gelen EPS (Events Per Second), RAM, CPU ve disk boyutu hesaplanmasıdır. CPU, toplanan logların SIEM'e yazılma hızını doğrudan etkilemektedir.

CPU kaynak miktarı arttıkça toplanan logların anlamlandırılma (parse) ve diske yazılma hızı da artacaktır. Dashboard, sistem görselleri, alarm&korelasyon işlemleri, rapor alma, geçmiş logların analizi RAM kaynağına bağlıdır. Disk boyutu ise, verilerin saklanması ile doğrudan ilişkilidir ve disklerin okuma yazma performansı da logların daha hızlı saklanması için

önemlidir. EPS hesabının yapılabilmesi için günlük kaynak bilgileri gerekmektedir. Ayrıca ne kadar EPS kullanıldığı, bazı SIEM çözümlerinde lisanslama için gerekmektedir.

3.1.2. EPS Değerinin Hesaplanması

EPS değeri, log kaynaklarından bir saniye içerisinde sisteme ulaşan veri miktarını tanımlayan değerdir. SIEM projelerinde genellikle en sık yapılan hatalardan birisi EPS değerinin göz ardı edilmesidir. Bu değerin iyi saptanabilmesi için sistem tasarımının iyi yapılması gerekmektedir. Yani log miktarı iyi analiz edilmelidir. Log alınacak sistem sayısının net olarak belirlenmesi gerekmektedir. Örneğin güvenlik duvarından saniyede kaç log satırı üretildiğinin belirlenmesi gerekmektedir. Bu verilerin saptanması proje tasarımında en kritik noktalardan birisidir. EPS değeri bir cihazda üreyen log miktarının 1 saniyeye bölünmesi ile elde edilmektedir.

EPS değeri NE (normal eps) ve PE (peak events per second) olmak üzere iki çeşittir. SIEM yönetiminde normal EPS değerine değil Tepe EPS değeri önemlidir. Normal EPS değeri, standart bir aktivite zamanında oluşan log sayısıdır fakat Tepe EPS ise sistemin dayanma noktasıdır yani siber saldırının olması gibi anormal bir durumda ortaya çıkmaktadır. Eğer standart loglar 3000 EPS e tekabül ediyorsa, beklenmedik bir olay karşısında sistem 3000 EPS'i geçecektir. Bu durumda log kaçırma söz konusu olacaktır. Sistemin PE değerini karşılaması önemlidir. NE ve PE depolama ihtiyacının belirlenmesinde hesap için kullanılmaktadır. NE, adından da anlaşılacağı gibi, saniye başına normal olay sayısını, PE ise güvenlik saldırısı gibi anormal etkinliklerin neden olduğu en yüksek olay sayısını temsil etmektedir.

EPS'in disk boyutu üzerindeki etkisi bölüm 3.1.3'teki örnekte gösterilmektedir.

3.1.3. Disk Boyutunun Hesaplanması

Disk boyutunun hesaplanmasında EPS ve verilerin toplandığı kaynaklar ortalama bir değer bulmakta yardımcı olmaktadır.

Kullanılacak minimum disk alanının hesaplanması için SIEM üreticilerin kullandığı farklı formüller bulunmaktadır. Önemli olan sisteme entegre edilecek SIEM ürününün kaç gün öncesine kadar canlıda log analiz yapabildiğidir. Bu da hız ve disk boyutu ile ilgilidir. Disk boyutunun hesaplamak için logların ne kadarı arşivde saklanacak ne kadarı canlı da takip

edilecek bu belirlenmelidir. Canlıdan kasıt, örneğin 15 gün öncesinin logunu incelenebilecek midir? Disk alanı bunu karşılayacak mıdır?

Öncelikle bilinmelidir ki EPS değerini %100 doğru hesaplayacak bir matematik formülü yoktur. Yapılan hesaplamalar öngörülen ortalama değerlerdir. Bunun sebebi, sistemlerden toplanan veri miktarı sürekli değişmektedir. Örneğin web hizmeti veren bir kurumun en yoğun trafik aldığı saatler mesai saatleri ise, gece – gündüz sürelerinde üretilen log miktarı farklılık gösterecektir.

Canlı loglar veri olarak kullanılabilmektedir fakat arşive alınan loglar ise sıkıştırılarak ve text dosya şeklinde kaydedilmektedir. Her SIEM çözümünün logları canlıda tuttuğu gün sayısı farklıdır. Bazı üreticiler logları 1 ay canlıda tutabilirken, bazıları ise 1 yıl tutabilmektedir. Belirtilen bu sürenin sonunda loglar arşive alınmaktadır. Örneğin 5 yıl öncesindeki bir log üzerinde rapor oluşturmak istenirse bu arşiv logları canlıya dönülmelidir. Buradaki en önemli parametre, canlıda tutulacak logların tutulabileceği maksimum süre ve minimum disk alanıdır.

Tablo 3.1'de yer alan g 500 Windows Server ve 500 Linux sunucunun ürettiği log miktarına göre disk ihtiyacının hesaplanması gösterilmiştir [39].

Tablo 3.1: 500 Windows Sunucu ve 500 Linux Sunucunun Ürettiği Log Miktarı

Sonuç	1 saniye	1 Gün	1 Ay
Normal Olaylar	2500	2.203.200.000	66.096.000.000
Pik Olaylar	-	826.200.000	24.786.000.000
Toplam Olaylar	35.063	3.029.443.200	90.883.296.000
Sıkıştırma Sonrası Oluşan Log Dosyası	1 MB	91 GB	3 TB

Tablo 3.1'deki çıktıda görüldüğü üzere bir sistemde yalnızca 500 Windows sunucu 500 linux sunucunun olması ki bu sayı bir veri merkezinde daha fazladır, günlük ihtiyaç duyulan alan 91 GB olarak hesaplanmıştır. Bu sistemlerde güvenlik duvarı, saldırı tespit ve önleme sistemi, anahtar, yönlendirici gibi diğer cihazlarda yer aldığında bu miktar çok daha artacaktır. SIEM çözümlerinin kullandıkları depolama yöntemleri değişeceğinden disk kullanım alanları da farklılık gösterecektir.

3.2. SIEM Yönetiminde Kritik Noktalar

Kritik bir veri merkezinde SIEM yönetiminde korelasyon, arama hızı, log kaçırma gibi dikkat edilmesi gereken bazı önemli noktalar bulunmaktadır. Bu noktaların önemi ve neler yapılması gerektiği Bölüm 3.2'nin alt başlıklarında yer almaktadır.

3.2.1. Korelasyon

SIEM'i tipik bir log yönetimi aracından ayıran en önemli özelliklerin başında korelasyon özelliği gelmektedir. Korelasyon, veriler arasında bir ilişkinin varlığını kontrol ederek, bir ilişki var ise bu ilişkinin etkisini incelemektedir.

Korelasyon kuralları tanımlanırken dikkat edilmesi gereken noktalar:

- Yazılan korelasyon kuralları kategorize edilebilmelidir. Böylece karışıklığın önüne geçilebilir ve bir kural standardı elde edilebilir.
- Bir SIEM ürünü satın alındığında varsayılan olarak gelen korelasyon kurallarının sayısı, yeteneklerinin ve kapsamının neler olduğu öğrenilmelidir.
- Tehdit istihbarat entegrasyonları önemlidir. Siber dünyada teşhisi konmuş zararlı IP'ler, dosyalar, imzaların bilgileri güncel olarak SIEM'de toplanabilmelidir.
- Gelişmiş korelasyon tekniklerine sahip olmalıdır. Örneğin standart bir SIEM aracı ile 1 dakikada 4 defa yanlış şifre ile oturum açma girişiminde bulunan bir IP tespit edilebilir. Fakat bir virüs aynı anda 5 farklı kullanıcıda görüldükten sonra bu kullanıcılar 5 dakika içerisinde şüpheli IP'lere istek yapması olayının yanıtı alınabilmelidir.

Bir olayın, korelasyon kurallarından birisine yakalanmasıyla aşağıdaki şekilde bildirimler alınabilmelidir.

- SIEM aracı, yöneticilere veya istenilen kişilere olay esnasında e-posta veya kısa mesaj gönderebilmelidir.
- Bir olaya karışan IP veya port engellenmesinin (kalıcı veya bir süre boyunca) sağlanması için güvenlik duvarı gibi bir güvenlik çözümü ile entegrasyonu olmalıdır.

Bir SIEM projesini zenginleştiren etken korelasyon mekanizmasıdır. Korelasyon olmadan SIEM, merkezi log toplayıcısından öteye geçmeyecektir.

3.2.1.1. Korelasyon Kategorileri

Korelasyon, sistem kaynakları tarafından SIEM'e aktarılan çok sayıdaki olayların anlam kazandırılmasıdır. Bu sayede önemli etkinlikler saptanabilmektedir. Kompleks yapıdaki olayların algılanması için korelasyon yaklaşımları bulunmaktadır.

Bir korelasyon kuralı tanımlanırken olay ilişkileri oluşturulmalıdır. Birbirinden bağımsız olaylar, sistemlerdeki güvenlik açıkları ile ilgili olaylar ve işletim sistemleri ile ilgili olaylar ilişkilendirilmelidir.

Korelasyon kurallarının kategorize edilebilmesi için aşağıdaki yaklaşımlar uygulanabilir:

- Son kullanıcı, güvenlik açıklıkları, kimlik denetimi, ağ oturumlarından elde edilen veriler ile olay bazlı korelasyonlar yazılabilmelidir.
- Bir olayın tespiti için daha önce gerçekleşen olaylar analiz edilerek ve önceki olaydan üreyen alarmların kullanılabilmesi için kural tabanlı korelasyon kuralları yazılabilmelidir.
- Tehdit istihbaratlarından, son kullanıcılardan, zafiyet açıklarını kapatan sistemlerden alınan loglar ile tehdit tabanlı korelasyonlar yaratılabilir. Bu korelasyon türevinde atak vektörlerinin tamamı değil, hangi içeriği kullanacağını bilinmelidir. Bu sayede farklı sistemlerden alınan tehdit verileri, tek bir korelasyon kuralı altında analiz edilmiş olur.
- Farklı ürünlerden alınan loglar üzerinde olaylar aynı kategoriler içerisinde barındırılabilmelidir. Örneğin güvenlik duvarı ara yüzünde "admin" kullanıcı adıyla ve anti-virüs uygulaması ara yüzünde "root" kullanıcı adıyla gerçekleşen başarılı oturum açma olayının, "oturum açılması" gibi aynı kategori altında tutulmasıdır.

- Birden fazla korelasyon içeren kurallar oluşturulabilmelidir. Örnek senaryo:

  Herhangi bir IP port taraması yapmışsa ve ardından aynı IP ile güvenlik duvarı üzerinde herhangi başarılı trafik olmuşsa ve yine aynı IP ile daha önce başarılı etkileşim kurmuş sistemler varsa, bu sistemlerin diğer sistemlerle etkileşimi olmasının tespit edilebilmesi gerekmektedir.

Bu olaylardan bir alarm oluşturulursa saldırgan çok yüksek ihtimalle tespit edilebilecektir.

3.2.2. Alarm

Güvenlik operasyon merkezi olan SOC (Security Operation Center) ekipleri, sistem yöneticileri ve uygulama sahiplerinin bir problem esnasında anında haberdar olmaları için SIEM üzerinde alarm kuralları bulunmaktadır.

Alarm kuralları ile 1 dakika içerisinde 8 defa yanlış şifre ile oturum açmaya çalışan bir kullanıcı hakkında bildirim alınabilmektedir.

Alarm kuralları oluştururken dikkat edilmesi gereken konu, iyi analiz edilmeden yazılan alarmların çok fazla sayıda alarm üremesine sebep olmasıdır. Örneğin güvenlik duvarı üzerinde "deny" olan her trafiği cep telefonuna kısa mesaj ile bildirim gönderilmesi istenirse, çok fazla sayıda kısa mesaj alınacağı anlamına gelmektedir.

Alarmlar yazılırken kritiklik durumu belirtilmelidir. Bir problem anında alınacak aksiyonun hızı alarmın kritikliğine göre değişecektir. Örneğin " Acil Durum" etiketiyle yazılan bir alarm ürediğinde ilgili ekip hızlıca müdahale etmek zorunda olduğunu anlayacaktır.

SIEM süreçlerinde Alarm ve Korelasyon terimleri sıkça karıştırılabilmektedir. Her üreyen alarm, yazılan bir korelasyon kuralının sonucunda olmamaktadır. Örneğin Ali Akpınar güvenlik duvarında oturum açtığında mail ile bilgilendirilmek istenmesi bir alarmdır. Ancak bir olay zaman ve mantıksal boyutta ilişkilendirilirse korelasyon olmaktadır. Örneğin, bir kullanıcı daha önce hiç bağlantı kurmadığı bir ülkeden VPN (Virtual Private Network) ile iç sistemlere bağlanmışsa ve bu kullanıcı aynı anda Türkiye'de de oturum açmışsa, bu olayın haber verilmesi bir korelasyon örneğidir.

3.2.3. Taksonomi

SIEM çözümleri taksonomi özelliğini logları sınıflandırmak için kullanmaktadır. Gelişmiş bir SIEM çözümünde "Suspicious Traffic", " UnusalTCPTraffic" binlerce sınıflandırma bulunmaktadır.

Taksonomi, olayları sınıflara ayırmaktadır. Örneğin SIEM'e aktarılan logların kaynaklarının çoğunda oturum açma işlemi gerçekleşmektedir. Güvenlik duvarı, Microsoft Server, Linux gibi farklı farklı sistemlerin hepsinde oturum açma işlemi gerçekleştirilmektedir. Bu oturumların tamamı SIEM'de tek bir grup altında tutularak "login" aktivitesi olarak görüntülenmektedir. Bu login aktiviteleri " Uzak bağlantı yapmaya çalışan bir kullanıcı 5 dakika içerisinde 4 başarısız girişin ardından başarılı oturum açtı" gibi korelasyon kuralları içerisinde kullanılabilmektedir.

Örnekler farklı cihazlardaki virüs aktiviteleri, şüpheli trafikler, port taramalar gibi binlerce farklı şekilde çeşitlendirilebilir. Her üründen bu sınıflardaki olayları manuel yapılmak istenirse her bir güvenlik cihaza ait binlerce sayfa log dokümanı okumak gerekmektedir. Bu hem zor hem de ekstra iş yükü olacaktır. SIEM'in taksonomi özelliği sayesinde benzer olaylar sınıflandırılarak raporlama ve korelasyon işlemlerinde görünürlük, analiz etme kolaylığı, esneklik ve kolaylık sağlamaktadır.

3.2.4. Log Kaçırma

Dikkat edilmesi gereken en önemli noktalardan birisi de SIEM ürününün log kaçırmamasıdır. Log kaçırmada dikkat edilmesi gereken noktalar:

- EPS, eşik değerinin üzerine çıkıldığında SIEM üzerine gelen loglar kaybolacaktır. Bu yüzden EPS değerinin aşımı kontrol edilmelidir.
- Her sistemin belli bir kayıt kapasitesi vardır. Eğer bu kapasite aşılırsa iki durum söz konusu olacaktır. Yeni gelen loglar eski logların üzerine yazılacaktır veya yeni loglar depolanmayacaktır. Çözüm depolama alanının iyi ölçeklendirilmesi ve disk doluluğunun takip edilmelidir.
- Bazı formattaki loglar, sisteme uğramadan engellenebilir.
- Bazı ürünler Disk IO problemlerinden dolayı log kaçırmaktadır.

- Sisteme yeterli kaynak verilmediği durumlarda da log kaybı oluşabilmektedir.

3.2.5. Arama Hızı

SIEM yönetiminde önemli hususlardan birisi de bir kaydın raporlanma hızıdır. Bir veri merkezinde çok sayıda cihaz (sunucular, anahtarlar, güvenlik duvarları, yönlendiriciler vb.) bulunmaktadır. Bu cihazların her birinden SIEM'e saniyede binlerce log gelmektedir. Bu logların içerisinde istenen bir logun raporlanmasının hızı da sistem yöneticileri için önemlidir. Bu durumu örneklendirmek gerekirse;

Bir sistemde 10.000 (on bin) EPS değerinde log üremesi demek, 1 dakikada 600.000 (altı yüz bin) log, saatte 3.600.000 (üç milyon altı yüz bin) log, 24 saatte 86.400.000 (seksen altı milyon dört yüz bin) logun oluşması demektir.

Bu değerler incelendiğinde 10.000 (on bin) EPS log akışı olan bir sistemde bir günde 86.400.000 (seksen altı milyon dört yüz bin) log oluşmaktadır. Bu değer yalnızca 1 günlük. Örneğin son 1 ayda Google.com'a bağlanan kullanıcıların sayısı veya son 1 ayda SQL sunucusuna bağlanan kullanıcıların listesi öğrenmek istenildiğinde oluşan log miktarı çok yüksek olacaktır. 24 saatte oluşan log miktarı 86.400.000 (seksen altı milyon dört yüz bin) iken 1 ayda üreyen log miktarı 2.592.000.000 (iki milyar beş yüz doksan iki milyon)'dur. Yani son 1 ayda bir arama yapıldığında bu logun 2.5 milyar log arasında aranması, sayılması ve sıralanması demektir.

3.2.6. Davranış Analizi

Modern bir SIEM, makine öğrenimi, istatiksel analiz ve davranışsal modelleme yoluyla davranışı temel almaktadır. İhtiyaca göre tanımlanan davranışlar ile şüpheli durumlar tespit edilebilmektedir.

Davranış analizi ile normal davranış değerlendirilmekte, olağandışı durumlara risk puanları atanabilmekte ve sonrasında belirli bir eşiği aşan etkinlikler ve davranışlar tespit edilebilmektedir. Örneğin, uzaktan çalışan bir personel bugüne kadar Ankara'dan VPN bağlantısı gerçekleştirirken ve ilk kez Amerika üzerinden VPN bağlantısı yapmışsa, böyle bir anormallik devam eden bir saldırının göstergesi olabilmektedir.

3.2.7. SIEM Çözümlerinde Dikkat Edilmesi Gerekenler

SIEM çözümlerinin yönetimi kadar doğru bir SIEM çözümü tercih etmek de önemlidir. Çeşitli SIEM platformları olsa da, hepsinin farklı kullanım yöntemleri bulunmaktadır. Bazı kritik altyapılar için tercih edilen SIEM çözümü ile küçük ölçekli işletmelerin tercih edeceği çözümler farklı olabilmektedir. Kritik altyapılarda siber saldırı çeşitleri, sistem problemleri karmaşık olabileceği için kullanılacak olan SIEM ürününün gelişmiş korelasyon yeteneklerine sahip olması gerekmektedir [40].

SIEM çözümü tercih edilirken nelere dikkat edilmesi gereken noktalar:

3.2.7.1. Olay Besleme

İyi bir SIEM platformu, kötü niyetli saldırılar ve tehlikeli üçüncü taraflarla ilişkili adresleri, davranışları, IP'leri ve web sitelerini akıllı bir şekilde tanımlayabilir. Etkin siber güvenliğin bir yönü, saldırıları önlemek için güncel verilere ihtiyaç duymaktadır. Bu nedenle etkinlik yönetimi hizmetleri uygulamalarının ayrılmaz bir parçası olarak bu kaliteye sahip olmalıdır.

3.2.7.2. Ek Adli Raporlar

SIEM hizmetlerine yönelik bir diğer olumlu bir yetenek, günlük derlemesinin ötesinde güvenlik olayları hakkında ek veri edinme yeteneğidir. Söz konusu SIEM hizmetinin adli tıp özellikleri, çözümün kendisine göre değişecektir ancak ek raporlar her zaman faydalıdır. Örneğin, söz konusu trafiğin kaynağı gibi fazladan trafik bilgileri veya söz konusu trafiğin nasıl oluşturulduğu ile ilgili ayrıntılar (bir mobil cihaz aracılığıyla mı, konum noktası neredeydi, neye bağlanmaya çalıştı vb.) önemlidir.

3.2.7.3. Uygun Ölçeklendirme

SIEM çözümleri kuruluşun büyüklüğüne göre farklı şekilde çalışmaktadır. Kaynakların en iyi şekilde kullanılabilmesi için (üçüncü taraflar söz konusu olduğunda farklı veri depolama, esnek fiyat planları vb. için birden fazla sunucu sunuyor mu?) nasıl ölçeklendiğini belirlemek önemlidir.

3.2.7.4. Erişilebilir Arayüz

Uygun bir ara yüzün değeri asla hafife alınmamalıdır. Kullanım kolaylığı, yönetim ve BT uzmanlarının karmaşık bir kullanıcı ara yüzüne gitmeden SIEM araçlarına erişmesine olanak tanıyan bir özelliktir. Siber güvenlikte doğru yanıtları zamanında almak gerektiğinden, program araçlarında olabildiğince hızlı ve verimli bir şekilde gezinmek önem taşımaktadır.

3.2.7.5. Raporlama

Kaliteli SIEM hizmetleri aynı zamanda muhasebe veya yönetim için kullanılan sistemler gibi birden çok ağı kapsayan kapsamlı günlük raporları sağlamalıdır. Tüm günlükler okunabilir ve tutarlı bir biçimde olmalıdır. Çünkü ham veriler ile tek başına anlamlı değildir. Bu format, ilgili tüm departmanlar tarafından kullanılabilir olmalıdır. Başka bir deyişle, bir rapor bir BT analisti için ne kadar kolay kullanılırsa kuruluş için o kadar iyidir.

Ayrıca bir SIEM ürününde tehdit raporlaması da önemlidir. Tehdit raporu, kötü niyetli bir saldırının nasıl gerçekleştiğini, ne zaman, nasıl ve neyin kaybolduğunu detaylandırmaktadır. Bunlar, işletmenin hangi alanlarda zayıf olduğunu gösterdiklerinden kritik öneme sahiptir ve gelecekteki saldırıları önlemek için daha iyi stratejiler oluşturmaya olanak tanımaktadır.

3.2.7.6. Log Kaçırma Durumu

Burada log toplama kapasitesi önemlidir. Bunun tespit edilmesi için de kaynakların iyi belirlenmesi gerekir. Örneğin satın alınan SIEM ürünü en fazla 5000 EPS'e kadar çıkabiliyorsa, 5000 eşik değeridir ve bu değer geçildiği zaman log kaçırma söz konusu olacaktır. Log kaçırma durumundan Bölüm 3.2.4.'te detaylı olarak bahsedilmiştir.

3.2.7.7. Geçmiş Logların Yönetimi

Bazı ürünlerde arşivden log aramak çok zordur. Bu yüzden arşive kaldırılacak logların sıklığının belirlenmesi, bu logları arşivde arama hızı gibi testlerin yapılması gereklidir. Arşivden istenilen logların aranmasının maliyeti, çıkardığı iş yükünün tespit edilmesi gerekmektedir. Spesifik bir olay aranırsa iş yükünün hesaplanması gerekmektedir. Örneğin 22 Mart 2020 tarihinde güvenlik duvarı tarafından en çok engellenen IP bilgisini getirmek gibi.

3.2.7.8. Disk ihtiyacının belirlenmesi

Canlıda log tutmak ve arşivlemek için diske ihtiyaç duyulmaktadır. Örneğin canlıdaki ve arşivdeki logların 1,2 veya 3 yıl saklanması için ne kadar disk ihtiyacının olduğu sisteme göre iyi tasarlanmalıdır. Maksimum veriyi minimum boyutta saklayabilen SIEM ürünleri tercih edilmelidir.

3.3. Etkin Korelasyon Örnekleri

SIEM projelerinde kaynakların belirlenmesi, toplanacak log türlerinin belirlenmesi, sistem kaynaklarının kullanımı, EPS ölçeklendirme bunların tamamı önemlidir. Fakat bir SIEM yönetiminde en önemli şey, SIEM kullanımını anlamlandıran unsur korelasyondur. Korelasyonu iyi yapılmayan bir SIEM ürünü log toplama cihazından öteye geçemeyecektir.

Klasik bir log yönetimi ile toplanan loglarda arama yaparak kritik bir güvenlik açıklığının tespit edilmesi çok zordur. SIEM sayesinde birbiri ile ilişkili olmayan olaylar birbiri ile ilişkilendirilir. Korelasyon ile milyonlarca log içerisinde filtreleme yapılır ve gereksiz log incelemek yerine istenilen noktaya odaklanmayı sağlar. SIEM, taksonomi modülü ile milyonlarca log arasında önemli olana odaklanabilmek için süzme işlemi gerçekleştirmektedir [41].

Korelasyon, tamamen korelasyonu yazacak kişinin yaratıcılığı ile doğru orantılıdır. İyi bir korelasyon yazabilmek için, hangi cihazlardan hangi logların alındığı, bu cihazların görevleri ve kapsama alanlarının iyi bilinmesi gerekmektedir. Korelasyon, matematik denklemi gibidir. Doğru sonuç için doğru değerleri vermek gerekmektedir.

3.3.1. Kaba Kuvvet Saldırıları

Kaba kuvvet saldırısı, uygulama programları tarafından parolalar veya Veri Şifreleme Standardı (Data Encryption Standard - DES) anahtarları gibi şifreli verileri, entelektüel stratejiler kullanmaktan ziyade kapsamlı bir çaba (kaba kuvvet kullanarak) çözmek için kullanılan bir deneme yanılma yöntemidir. Kaba kuvvet saldırısı, bir hırsızın para kasasını açabilmek için tüm şifreleri denemesi gibidir [42]. Veri merkezinin sunduğu dış ağ açık servisler, saldırganlar için hedef olabilmektedir. Bu sistemlerin ele geçirilmesi için bu tekniğin kullanılması saldırı yöntemlerinden birisi olacaktır. Sistemlerden birisinin ele

geçirilmesi veri merkezi adına büyük tehlike arz etmektedir. Bu yüzden bu saldırı türlerinin önceden tespit edilmesi, saldırının önüne geçilmesi adına önemlidir.

- Kaba Kuvvet Atağının Tespiti:

Bir cihazda 10 dakika içerisinde hiç başarılı oturum açılmadan 1 dakika içerisinde 2 kez hatalı giriş işlemi yapılması.

Herhangi bir sisteme 1 dakikada en az 10 kez başarısız oturum denemesi.

- Windows Uzak Masaüstü Bağlantısında Kaba Kuvvet Atağının Tespiti:

Bir sunucuya veya çalışan bilgisayarına uzak masaüstü bağlantı protokolünü kullanarak 1 dakikada 5 kez hatalı girişin tespit edilmesi.

- Kaba Kuvvet VPN Atağının Ardından Başarılı Girişin Tespiti:

5 dakika içerisinde 3 kez başarısız VPN oturumunun açılmasının ardından, aynı hesapla başarılı oturum açılması.

Kaba kuvvet saldırıları sonucunda başarılı oturum açılırsa, saldırganın bağlandığı sistem ve o sistemin bağlı olduğu diğer sistemler bu riskle karşı karşıya kalacak ve sistemlerin nelerden etkilenebileceği saldırganın niyetine göre değişecektir. Bu yüzden kaba kuvvet saldırısı yapmaya çalışan bir trafik ürediğinde güvenlik yöneticileri kısa mesaj veya e-posta ile bilgilendirilmeli veya güvenlik duvarı uyarılarak kaba kuvvet saldırısı yapan kaynak IP engellenmelidir.

3.3.2. Hizmet Durdurma Saldırıları

Dağıtılmış hizmet reddi (DDoS - Distributed Denial of Service) saldırısı, hedefin veya çevresindeki altyapının bir Internet trafiği baskısı ile karşı karşıya kalarak, hedeflenen bir sunucunun, hizmetin veya ağın normal trafiğini bozmak için kötü amaçlı bir girişimdir. DDoS saldırıları, saldırı trafiği kaynağı olarak güvenliği ihlal edilmiş birden çok bilgisayar sistemini kullanarak etkinlik sağlar. Sömürülen makineler bilgisayarları ve IoT (Internet of Things) cihazları gibi diğer ağa bağlı kaynakları içerebilir. Yüksek seviyeden, DDoS saldırısı, tıkanmış bir karayolu trafik sıkışıklığına benzemekte ve trafiğin istenen hedefe ulaşmasını engellemektedir [43].

Veri merkezlerinin dış ağa sunmuş olduğu servislerin kalıcı veya geçici olarak durdurulması, hizmetlerin aksatılması ve bu doğrultuda yaşanacak bir itibar kaybı saldırganlar için yine bir başka motivasyon kaynağı olacaktır. Veri merkezlerinin verdiği hizmetlerinin aksatılmaması adına yazılacak olan korelasyonlar bu doğrultuda büyük önem arz etmektedir.

- Web Sayfasına Yönelik Hizmet Durdurma Tespiti:

  Bir web sayfasına aynı kaynak IP'den 1 dakika içerisinde 100'den fazla erişim isteğinin yapılması.

- DNS'e Yönelik Hizmet Durdurma Saldırı Tespiti:

  1 dakikada 100 den fazla DNS isteği üreten IP'nin tespit edilmesi.

3.3.3. Veritabanı Saldırıları

Veritabanı bir uygulamanın kalbidir. Veri tabanları dijital bir biçimde yapılandırılmış bir veri toplamadır. Yapı, şema tanımları, verileri organize bir biçimde saklayan tablolar, sanal tablolar ve performansı iyileştirmek için depolanan sorgular vb. görünümlerden oluşur. Veritabanı, kurumsal bir firmanın kritik görev verilerini içermekte ve bu da onu bilgisayar korsanları tarafından belirgin bir hedef haline getirmektedir. Bilgisayar korsanı web sunucusunun kontrolünü ele geçirdiğinde genellikle erişmek için veritabanı sunucusu adını, kullanıcı kimliğini ve parolasını içeren uygulama yapılandırma dosyalarını aramaktadır.

Veri merkezlerinde önemli bilgileri depolayan veri tabanları kullanılmaktadır. Bu veri tabanlarının saldırıya karşı korunması, saldırıların önceden tespit edilmesi önemlidir. SIEM ile veritabanı saldırılarının önceden tespit edilmesi, anomali hareketlerinin izlenmesi amaçlanmaktadır.

- Bir SQL Kullanıcısının Kullanıcı Hakları Yükseltilmesi:

  Veritabanı kullanıcılarından birisinin yetkileri mesai saatleri dışında yükseltilirse tespit edilmelidir.

- Yetkisi Dışında SQL Sorgusu Atan Kullanıcıların Tespiti:

Bir kullanıcı yetkisi dâhilinde olmayan komutu çalıştırmaya çalışmasının tespit edilmesi.

- Çalışma Saatleri Dışında Yapılan SQL Bağlantısının Tespiti:

  Bir kullanıcının daha önce hiç bağlanmadığı, mesai saati dışında bir saatte SQL bağlantısı ve kritik bir sorgu yapmasının tespit edilmesi.

- SQL Kullanıcısının Şifresinin Değiştirilmesi:

  Bir SQL kullanıcı şifresinin 30 günde 5 defa değiştirilmesinin tespit edilmesi.

- SQL Kullanıcı Hesabının Aktif Edilmesi:

  Aktif olmayan bir SQL kullanıcı hesabı aktif edilmesinin ardından 5 dakika içerisinde bir sorgu çalıştırdıktan sonra aynı hesap tekrar pasif hale getirilirse alarm üretilmelidir.

- Kritik Tablolarda DELETE Komutunun Çalıştırılması:

  Kritik bir SQL tablosunda bir veri silindiğinde alarm üretilmelidir.

- Verilerin Dışarıya Aktarılması:

  SQL verileri "csv" uzantılı olarak dışarıya aktarılırsa ve kopyalama işlemini gerçekleştiren kullanıcı 10 dakika içerisinde dışarıya e-posta gönderirse, harici bir depolama aygıtı veya bulut tabanlı depolar kullanırsa (Google Drive, Yandex Disk vb.) alarm üretilmelidir.

3.3.4. Exploit Tespitleri

Türkçe'de istismar anlamına gelen exploit, bir uygulama veya sistemdeki istenmeyen veya beklenmeyen davranışların ortaya çıkmasına neden olan bir hata veya güvenlik açığından yararlanan bir yazılım, bir veri parçası veya bir komut dizisidir. Temel olarak, bir saldırının hedefinin, insanların ona erişmek için araçlar yaratmasına ve onu kendi yararına kullanmasına izin veren bir tasarım kusurundan muzdarip olduğu anlamına gelmektedir. Genel olarak bilinen ve bilinmeyen istismar olarak ikiye ayrılmaktadır. Sıfırıncı gün denilen Zero-Day güvenlik açıkları, bir yazılımın kritik bir güvenlik açığı içermesi en tehlikeli durumdur. Böyle bir istismar meydana geldiğinde, güvenlik açığını düzeltmek için bir

düzeltme eki yazılana kadar ve düzeltme eki yazılıma uygulanana kadar ilgili yazılımı çalıştıran sistemler bir saldırıya karşı savunmasız kalacaktır.

- Zararlı Powershell Komutları:

  Bir bilgisayar veya sunucu üzerinde şüpheli powershell komutu çalıştırılmışsa tespit edilmelidir. Örneğin (New-Object System.Net.Webclient).DownloadFile() uzak bir sistemden dosya indirme komutunun çalıştırılması gibi.

- Powershell Gizli Komut Saldırısı:

  Powershell komut satırını gizleyen " W Hidden/-WindowStyle Hidden " powershell komutunun tespit edilmesi gibi.

- Şifrelenmiş Powershell Komutları:

  -Enc/-EncodedCommand: base64 komuyu sayesinde powershell komutları şifrelenmektedir ve ne yazıldığı anlaşılmamaktadır. Bu yüzden bu komutun kullanılması şüpheli bir durumdur ve tespit edilmelidir.

- Ransomware WannaCry Saldırı Tespiti:

  WannaCry saldırısında kullanılan dosyaların parmak izi anlamına gelen hash bilgisini içeren bir dosya ile karşılaşıldığında alarm üretilmelidir.

3.3.5. Kötücül Yazılım Tespitleri

Kötücül Yazılımlar, kullanıcı bilgisayarında kötü amaçlı hareket eden yazılımlardır. Kötü amaçlı yazılım yalnızca virüslü bilgisayarı veya cihazı değil, virüslü cihazın iletişim kurabileceği diğer tüm cihazları da etkileyebilir. Kötü amaçlı yazılım, en basit bilgisayar solucanlarından ve Truva atlarından en karmaşık bilgisayar virüslerine kadar her şeyi kapsamaktadır.

Veri merkezi sistemlerinde kötü amaçlı yazılımın bulunması kabul edilemez bir risktir. Bu doğrultuda sistemlere enfekte olmuş virüsler diğer sistemlere zarar vermeden, yayılmadan tedbirlerin alınması gerekmektedir. Bu kapsamda SIEM'de yazılacak alarmlar ile sistem yöneticileri bilgilendirilmelidir. Aşağıda yazılmış olan kurallar da bu doğrultuda katkı verecektir.

- Kötücül Yazılım Olayının Tespiti:

  Kritik sistemlerde kötücül yazılım tespit edilirse alarm üretilmelidir.

- Bir Cihazda Birden Çok ve Birbirinden Farklı Virüs Tespiti:

  Bir cihazda 1 dakika içerisinde 10'dan fazla birbirinden farklı virüs ürerse alarm üretilmelidir.

- Bir virüsün aynı anda en az 5 farklı cihazda tespit edilmesi.

  Bir sunucuda veya kullanıcı bilgisayarında tespit edilen virüs, 5 farklı cihazda daha görülürse tespit edilmelidir.

3.3.6. Keşif Saldırıları

Keşif saldırıları, ağ sistemi ve hizmetleri hakkında hırsızlık yolunda bir tür bilgi toplanmasıdır. Oltalama elektronik postası, şüpheli bağlantı linklerinin kısa mesaj veya başka yollarla kişilere gönderilmesi kullanılan bazı tekniklerdir. Saldırgan ilk olarak port taraması yaparak sistemin savunmasız portlarını keşfetmektedir. Bunun önüne geçilmesi için iyi bir güvenlik duvarı ve saldırı tespit ve önleme cihazı kullanılmalıdır. Güvenlik duvarı hangi portların açıkta ve kime görünür olduklarını kontrol etmektedir. Saldırı önleme sistemi, devam eden bağlantı noktası taramalarını algılayabilir ve saldırgan ağın tam bir haritasını almadan önce bunları kapatabilir. Fakat örneğin belirli bir IP'ye sahip saldırgan kuruma bağlı bir IP için 0-65535 portları arasında port taraması yapmışsa ve güvenlik duvarı kurallarında güvenlik politikalarına bağlı olarak bu trafiklerden bir tanesini dahi geçirir ise, saldırgan için bir yol açılmış olacaktır. SIEM port tarama yapan bir IP'nin engellenmesi için korelasyonlar yazılabilmektedir. Güvenlik duvarı bir IP'nin port tarama yaptıktan sonra başarılı oturum açmasını bir tehdit olarak algılayamayacaktır. Düz mantıkla bakacaktır. Çünkü güvenlik duvarları güvenlik politikalarında, ilgili trafik için erişim varsa gerisine bakmamaktadır. SIEM sayesinde şüpheli hareket eden bir IP, tarama yaptığı zaman tespit edilebilmektedir.

- İç Ağda Yapılan Port Tarama:

  Kurum içerisinde bir cihazdan 1 dakikada bir IP'ye 10 farklı porttan istekte bulunulmuşsa alarm üretilmelidir.

- Dış Ağdan Yapılan DNS Tarama:

  Dış ağda bulunan bir kaynaktan 1 dakika içerisinde DNS 53 portundan 10 defa istekte bulunulmuşsa alarm üretilmelidir.

- Dış Ağdan Yapılan Port Tarama:

  Dış ağdaki bir kaynak IP'den iç ağdaki bir hedef IP'ye 1 dakikada 30 farklı porttan istekte bulunulmuşsa alarm üretilmelidir.

3.3.7. Sistem Olayı Tespitleri

Veri merkezi bünyesinde kullanılan sistemlerde kullanıcı hareketlerinin, servislerin durumu, donanımsal etkinliklerin takip edilmesi gerekmektedir. Çok sayıda sistemin her birinin tek tek kontrol edilmesi zordur. SIEM ile bu loglar merkezi olarak toplanacağından kritik durumlar için alarm yazılarak takip edilmesi gereken noktaları, sistem yöneticilerini anında bilgilendirilebilir.

- Log Silme Aktivitesi:

  Daha önce hiç güvenlik logunun silinmediği bir sunucuda ilk defa bir güvenlik logunun silinmesi durumunda alarm üretilmelidir.

- DMZ Sunucu Üzerinde Servis Durdurma:

  DMZ bölgesinde yer alan kritik bir uygulamanın çalışması için gerekli bir servisin bir kullanıcının kasıtlı olarak durdurması durumunda alarm üretilmelidir.

- Sistem Kayıtlarının Silinmesi:

  Veri merkezi kamera kayıtları, giriş-çıkış bilgileri gibi bilgilerinin tutulduğu kayıtların silinmesi halinde alarm üretilmelidir.

- Veri merkezi sistem odalarına talep olmadan giriş yapılması.

  Giriş bilgilerinin tutulduğu sunucudan loglar alınmalıdır. Veri merkezinde yapılacak çalışmalar için talep açılan sistemin logları alınmalıdır. Bu talepte talep sahibi ve teknikerin ismi yer alacaktır. Veri merkezi odalarına rutin işler dışında giriş

yapmayan personeller haricinde, sistem odasına giriş yapan kişinin adı çağrı kaydında geçmiyor ise alarm üretilmelidir.

3.3.8. Trafik

Bazı trafik etkinlikleri de yakından takip edilmesi gereken önemli noktalardandır. Yüksek boyutta aktarılan verilerin takibi, güvenlik duvarı tarafından sürekli engellenen bir IP'nin kara listeye alınması ve bu sayede diğer sistemlere de enjekte olmasının engellenmesi gibi tedbirler SIEM ile yazılacak korelasyonlar sayesinde alınabilir.

- İç ağdaki bir IP'den dış ağdaki bir cihaza, FTP protokolü kullanarak yapılan yüksek hacimli veri transferinin tespit edilmesi.
- Kuruma ait VPN ile bağlı bir bilgisayar tarafından tespit edilen büyük veri aktarımı.
- SIEM ara yüzünde tanımlı olmayan 514 portundan log aktaran IP'lerin tespit edilmesi.
- İnternet üzerinden bir sunucu üzerine gelen trafik CVE (Common Vulnerabilities and Exposures) kodu içeriyorsa ve bu trafik sunucu üzerinde yakalanmışsa alarm üretilmelidir.

  Dış ağdan yapılan bir trafik CVE (Common Vulnerabilities and Exposures) kodu içeriyorsa uç ağdaki güvenlik çözümlerinin engellemesi beklenir. Ancak güvenlik duvarı, saldırı tespit ve önleme sistemi gibi çözümler engelleyememiş ancak sunucu üzerinde kurulan güvenlik yazılımı Host Based IPS bu kodu fark etmişse alarm üretilmelidir. Trafiği yapan kaynak IP güvenlik duvarı tarafından kara listeye alınmalıdır.

3.3.9. Web Saldırılarına Yönelik Korelasyonlar

Web uygulamaları uygunsuz kodlamalardan kaynaklanan bir dizi güvenlik kaygısı yaratabilmektedir. Ciddi zayıflıklar ve güvenlik açıkları, hassas verilerin çalınması için saldırganların veri tabanlarına erişmesine imkân sağlayabilmektedir. Bu veri tabanlarının birçoğu onları sık sık saldırı hedefi haline getiren değerli bilgiler (Kişisel veriler ve finansal detaylar vb.) içermektedir. Veri merkezlerinin dışarıya açık olan web hizmetlerinin de bu kapsamda korunması, olayların takip edilmesi ve saldırıların önceden tespit edilmesi için

tedbir alınabilmesi gerekmektedir. Aşağıda yer alan örnek korelasyonlar bu bağlamda katkı sağlaması için yazılmıştır.

- İç ağdaki bir kullanıcının aşırı sayıda Web trafik isteklerinin tespit edilmesi.
- Arabellek taşması saldırı olayının tespit edilmesi.
- Aşırı sayıda web yönlendirmelerinin tespit edilmesi.
- Dış ağdan aşırı sayıda yapılan "GET" isteklerinin tespit edilmesi.
- Dış Ağdan aşırı sayıda yapılan "POST" isteklerinin tespit edilmesi.

3.3.10. Geçmiş Loglara Göre Tespit

SIEM yönetiminde log analizini iyi yapmak gerekmektedir. Eğer SIEM'in korelasyon gücü kullanılamazsa SIEM log yığını hale gelecek, analiz yapmak güçleşecektir. Sistemde yaşanan şüpheli hareketleri tespit etmek için kullanıcının geçmiş logları incelenebilir. Bunun için yazılması gereken bazı korelasyon örnekleri aşağıdaki gibidir.

- Bir personelin son 1 ayda oturum açtığı cihazlar ve sayıları:

  Bir kullanıcının bağlandığı cihazlar baz alındığında, o kullanıcıya ait rutin ortaya çıkarılmış olacaktır. Örneğin bir veritabanı yöneticisinin 1 aylık periyotta 10 farklı veritabanında oturum açarken, aniden 15 farklı veritabanına oturum açmaya çalışması gibi. Bunların dışında bir uygulama sunucusuna veya bir ağ cihazına bağlanmaya çalışıyorsa tespit edilmelidir. Örnekler çeşitlendirilebilir. Bunların hepsi şüpheli harekettir ve tespit edilmesi gerekmektedir.

- Bir personelin rutin kullandığı portlar dışında port kullanması:

  Herhangi bir personel rutin kullandığı portlar dışında bir portu kullanmaya başlamışsa bu şüpheli bir durumdur. Örneğin sadece web sayfalarına bağlanmak için 80 ve 443 portlarını kullanan bir personelin bir anda Oracle veritabanı 1521 portunu kullanması normal bir durum değildir.

- Sistemlerde kullanılan portlar dışında bir portun çalışması:

  Bir veri merkezinde cihazların, uygulamaların, servislerin kullandığı portlar bellidir. Eğer herhangi bir cihazın standart kullandığı portlar dışında bir port kullanılmaya başlanmışsa bu durum tespit edilmelidir.

- Rutin saatler/günler dışında yapılan bağlantılar:

  Personellerin, olağan dışı durumlar haricinde çalışma saatleri ve günleri bellidir. Örneğin nöbet sistemi yok ise ve 09:00 – 18:00 saatleri arasında oturum açan bir personelin, o güne kadar hiç oturum açmadığı bir saatte gece 01:00'da bir sisteme başarılı oturum açması olağan dışı bir durumdur. Aynı şekilde cumartesi günleri hiç oturum açmamış bir kullanıcı Cumartesi günü bir sisteme bağlanmışsa da olağan dışı bir durum söz konusudur.

- Yüksek Hacimli Trafik Miktarı:

  Bir web sunucusunda çok büyük miktarda indirme/yükleme işlemi gerçekleşiyorsa ve bu durum daha önce hiç yaşanmamışsa bu durum hiç normal değildir.

Bu örneklerin çeşitlendirilmesi için sistem rutinlerinin ortaya çıkarılması gerekmektedir. Geçmişte yapılan hareketler, şuan yapılan hareketlere referans olacaktır.

3.3.11. KVKK'ya Yönelik Senaryolar

KVKK'nın 17 ana maddelik teknik tedbiri bulunmaktadır. Bu maddelerden birisi de "Log Kayıtları" maddesidir. Bu kapsamda SIEM aracı ile kişisel verilerin ihlal edilmesine yönelik senaryoların yazılabilmesi elzemdir.

KVKK'ya yönelik kural örnekleri [44]:

1. Bir kullanıcı kişisel verilerin bulunduğu bir veritabanında mesai saatleri dışında sorgulama yapmışsa veya mesai saatleri içerisinde günlük yapılan sorgu rutinlerinin dışında sorgulama yapmışsa alarm üretilmelidir.

2. Bir kullanıcı 1 dakikada 3 defa erişim yetkisi olmayan kişisel verilerin bulunduğu bir sunucuya veya veritabanına oturum açmayı denemiş ise alarm üretilmelidir.

3. Bir kullanıcı kişisel verilerin bulunduğu bir cihaza aralıklı zamanlarla erişmeyi deniyor ise alarm üretilmelidir.

4. Bir kullanıcı yetkisi olan bir sunucuya/bilgisayara uzak bağlantı ile bağlandıktan sonra o cihaz üzerinden kişisel veri içeren başka bir makinaya erişim yapar ve başarılı olursa alarm üretilmelidir.

5. Kullanıcı kişisel verilere erişim sağladığı sırada aynı zamanda kurum dışı bir e-posta sitesine de bağlanmış ve ekran görüntüsü uygulaması kullanmışsa alarm üretilmelidir.

6. Bir kullanıcı 1 den fazla kişisel veri içeren ve yetkisi olmayan sistemlere erişirse veya denerse o kullanıcı hesabı pasif hale getirilmelidir.

7. Yetkisi yükseltilen kullanıcılar için alarm üretilmelidir.

8. Yetkisi yükseltilmiş bir kullanıcı aynı zaman diliminde kişisel veri içeren bir sisteme bağlanmayı denerse alarm üretilmelidir.

9. Kişisel verilerin olduğu bir dosya veya veritabanında kopyalama işlemi olursa alarm üretilmelidir.

10. Kişisel verilerin olduğu sisteme bağlanmaya çalışan ve güvenlik duvarı tarafından engellenen bir IP başka sistemlere başarılı oturum açmışsa alarm üretilmelidir.

11. Gönderilen elektronik postanın konusunda ve ekinde kredi kartı, kimlik numarası gibi bilgiler varsa alarm üretilmelidir.

12. Kredi kartı bilgilerinin yazılı olduğu bir dosyaya erişilmişse alarm üretilmelidir.

13. Veritabanı sorgusunda kredi kartı bilgisi veya T.C. kimlik numarası geçiyorsa alarm üretilmelidir.

14. Kişisel verilerin olduğu bir cihaza aynı kullanıcı adı ile farklı IP'lerden erişilmişse alarm üretilmelidir.

15. Daha önce belirli sistemlere erişim hakkı olan fakat pasif hale getirilmiş bir kullanıcının hesabı aktif olur ve aynı zaman diliminde erişim yetkisi olan sistemlere bağlanır ise alarm üretilmelidir.

3.4. Veri Merkezi Mantıksal Güvenlik Tasarımı

Veri merkezlerinde elektronik posta, dosya paylaşımları, internet erişimi, iç ağ portallarrı, web tabanlı uygumalar gibi hizmetler verilebilmektedir. Dış dünya için de çeşitli hizmetler sağlanmaktadır. Bu doğrultuda bu hizmetleri sağlayan uygulamaların barındıracağı güvenlik zafiyetleri veri merkezinde bulunan tüm sistemleri tehdit edecektir. Bu zafiyetlerden faydalanmak isteyen saldırganların motivasyonları farklıdır. Bu motivasyonlardan birisi de ticari veya siyasi itibarı zedeleme olabilmektedir. Bu doğrultuda veri merkezi sistemlerini korumak için katmanlı güvenlik yaklaşımı doğrultusunda hareket edilmelidir.

Gelişmekte olan internet teknolojisi ile birlikte veri merkezi sistemlerinde çalışan uygulamalar ve servislerin riskleri, zafiyetleri, açıklıkları da artış göstermektedir. Bilgi varlıklarına tehdit oluşturacak zafiyetlerin ve mağdur edecek istismarların önüne geçebilmek için sistemler dirençli ve güvenli hale getirilmelidir.

Saldırı türleri her geçen gün artmaktadır. Bundan dolayı ağ güvenliği, veri merkezi yönetiminde büyük bir sorundur. Ağ tasarımında yanlış konumlandırılmış ağ düğümleri, bilgi güvenliği ve iş sürekliliği yöntemlerinin çaresiz kalmasına yol açmaktadır. Ayrıca, bu yanlış konumlandırmalar, ağın başka bölümlerinde konumlandırılmış diğer bilgi varlıklarının istismara uğramasına sebep olmaktadır.

Ağ kaynakları üzerinden erişimleri sağlanan sunucular, uygulamalar servis ve hizmetlerin sayısı gittikçe artmaktadır. Böyle olunca ağ tasarım yapısı da oldukça karmaşıklaşmaktadır. Bu karmaşıklığın önüne geçebilmek, bilgi güvenliğini etkin bir şekilde yönetebilmek için güvenlik gereksinimleri ve sistemde bulunan varlıklar kritiklik düzeyine göre tasarlanmalıdır.

Bilgi güvenliği taktiksel prensiplerinin amacı, BT eko sistemi içerisinde modüler ve esnek bir yapı kurmak, kurulan bu yapıyı risk, tehdit, zafiyet süreçlerini de göz önünde bulundurarak tasarlayıp, daha güvenli operasyonlar elde etmektir.

Kritik sistemlerin korunmasında katmanlı güvenlik mimarisi kullanılmalıdır. Katmanlı güvenlik mimarisi, her fiziksel uygulama katmanı için farklı düzeylerde ağ erişiminin sağlanmasıdır. Hakan Tan ve Prof. Dr. A. Ziya Aktaş'ın "Bir Kuruluşun Bilgi Sistemi Güvenliği İçin Bir Yaklaşım" başlıklı yazısında [45] katmanlı güvenlik, kaynak ve hedef arasına birden fazla güvenlik çözümlerinin konulması olarak tanımlanmıştır. Böylece bir

katmanın koruma sağlayamadığı bir durumda sonraki katman güvenlik önlemleriyle engellenebilmektedir. Katmanlı güvenlik tasarımında işletim sistemleri, uygulamalar ve veri tabanları gibi sistemlerin korunması için güvenlik yapılandırılması derinleştirilmelidir. Bir katmanın uygunsuz çalışması durumu (örneğin, yapılandırma hatası, yazılım hatası, güvenlik işlemi kesintileri vb.), diğer katmanların korunmasını ve güvenliğini tehdit edecektir. BT kaynaklarının kolay bir şekilde saldırıya uğramasına izin verilmemeli, anormalliklerin/tehditlerin hızlı tanımlanmasına ve ortadan kaldırılmasına yönelik derinlik sağlanmalıdır.

Kullanıcılara verilecek yetkiler görevlerin dağılımına göre en az yetki ile verilmelidir. Standart olarak hiçbir kullanıcı yönetici ayrıcalığına sahip olmamalıdır. Uzaktan erişimler iki faktörlü kimlik doğrulaması ile yapılmalıdır.

Kritik veriler, güvenilmeyen açık ağlar üzerinden gönderilirken, oturum dinlemesi ve veri sızıntısı nedeniyle veri kaybını önlemek için katmanlı güvenlik yapısı, şifreleme ve diğer güvenlik kanallarını kullanarak bilgi varlıklarının korunması sağlanmalıdır.

BT eko sisteminde yer alan varlıkların her birinin gereksinimleri ve yetki ihtiyaçları farklıdır. Bu bilgi varlıklarının herhangi bir ihlale uğramaması için en az yetki, görevlerin ayrılığı ve bilinmesi gerekenler prensibi ilkesinin korunması gerekmektedir.

3.4.1. Veri Merkezi Güvenliği

Veri merkezi, bir kuruluşun tüm kritik sistemlerini veya Bilgi Teknolojisi altyapısını barındıran bir bina veya özel bir alandır. Veri merkezlerini etkileyenler de dâhil olmak üzere güvenlik saldırılarının sayısı her geçen gün artmaktadır. Veri merkezleri kuruluşların tüm kritik bilgilerini içermekte ve bu nedenle bilgi güvenliği konusu endişe verici hale gelmektedir. Bir veri merkezi, barındırdığı BT ortamının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için yüksek standartlarda korunmalıdır.

Veri merkezi güvenliği, veri merkezini doğal veya beşeri felaketlerden korunması için veri merkezi altyapıları standartlarında tanımlanan tüm önlemleri ifade etmektedir. Bu doğrultuda veri merkezleri için Telekomünikasyon Altyapısı Standardı [46] ve ISO / IEC 27001: 2005 ve 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Standardı [47] bir veri merkezi güvenliği için kabul edilebilir gereksinimler sunmaktadır.

Bir veri merkezinde en sık rastlanan tehditler:

- Gizli/Kritik bilgilerin ihlal edilmesi
- DoS/DDoS Saldırıları
- Bilgi işlem kaynaklarına yetkisiz erişim ve kullanım
- Kimlik hırsızlığı
- Veri hırsızlığı ve verilerin değişikliğe uğratılması

Veri merkezinde en yaygın güvenlik açıkları:

- Yanlış yazılım tasarımı ve eksik testler neticesinde uygulamalardaki güvenlik açıkları
- Üretici tarafından tanımlanan varsayılan kimlik bilgilerinin kullanılması, sistemlerin güncellenmemesi gibi yapılandırma hataları
- Etkili olmayan güvenlik tasarımı, katmanlı güvenlik mimarisinin kullanılmaması
- Fiziksel erişim denetimlerinin yapılmaması
- Çevre güvenliğinin kontrol edilmemesi

Fiziksel güvenlik kontrolleri:

Bir veri merkezinde fiziksel güvenlik, kuruluşun kritik verilerini depolayan sistemlerde her türlü fiziksel hasarı önleyen protokoller kümesidir. Seçilen güvenlik kontrolleri, doğal afetlerden kurumsal casusluğa, terörist saldırılarına kadar her şeyi denetleyebilmelidir.

Örnek fiziksel güvenlik denetimleri:

- Ağ hizmetleri, telekomünikasyon altyapısı, ulaşım hatlarının, acil durum hizmetleri gibi riskler tanımlanmalıdır.
- Doğal afet riski olmayan yerler tercih edilmelidir.

- Kimlik doğrulama (retina taraması, parmak izi taraması, kart okuyucu vb.) sonrasına yalnızca bir kişinin geçebileceği turnike kapılarının yerleştirilerek fiziksel erişim kontrolünün sağlanması gerekmektedir.
- Tesise tek giriş noktası bulundurmalıdır.
- Veri merkezi içerisinde özel alanlara ek fiziksel erişim kısıtlamaları getirilmelidir.
- Veri merkezi odaları kayıt tutma özelliğine sahip kameralarla kesintisiz olarak gözetilmelidir.
- Güvenlik görevlileri, ağ operasyon merkezi hizmetleri ve teknik ekibin 7/24 veri merkezinde hazır bulunmaları gerekmektedir.
- Kullanılan tüm donanımların düzenli bakımının yapılması gerekmektedir.
- Erişim kontrolleri ve faaliyetleri sürekli izlenmeli ve yetkisiz erişimlerde acil müdahale edilebilmelidir.
- Sıcaklık ve nem oranlarının kontrol edilmesi için ileri teknolojiye sahip klima teknolojileri kullanılmalıdır.
- Sıcaklık, nem gibi unsurların anlık olarak izlenmesi ve ani artış veya inişlerde tedbir alabilmek alarmların oluşturulması gerekmektedir.
- Kesintisiz güç kaynağı (Uninterruptible Power Supply – UPS) kullanılmalıdır.
- Yeni bir yangın anında erken uyarı sağlamak için duman dedektörleri kullanılmalıdır.
- Kablolama güvenliğinin sağlanması için yükseltilmiş döşeme kablolama yapılması gerekmektedir.

Çalışma için gelen teknik personellerin fiziksel üst araması yapılmalı, veri merkezine girerken ve çıkarken kişilerin ağırlıkları ölçülmelidir. Denetimlerin sayısı bunlarla sınırlı değildir. Fiziki konuma bağlı olarak sistemlerdeki, denetimlerin çeşitliliği artacaktır. Ayrıca iç ve dış ağ üzerinden gelebilecek saldırılara karşı koruma sağlayabilmek için ağ güvenlik çözümlerinin de incelenmesi gerekmektedir. John R. Vacca [48] bilgi sistemleri güvenliğini mantıksal, fiziksel ve çevre güvenliği olmak üzere üç ana bölümde ele almaktadır. Fiziksel

güvenliğe yönelik tedbirler Bölüm 3.4.1'e incelenmiştir. Vacca'nın bahsettiği mantıksal güvenlik ise, yazılım ve altyapı güvenliğine odaklanmaktadır. Bu doğrultuda kritik sistemlerin korunması için ihtiyaç duyulan güvenlik çözümlerinin iyi belirlenmesi gerekmektedir.

3.4.2. Güvenlik Bölgeleri

Güvenlik bölgeleri bir ağın güvenlik sınırlarını oluşturmaktadır. Bu bölgeler, ağ ve güvenlik cihazları aracılığı ile politika sınırlamalarına tabi tutulan mantıksal alanlardır. Farklı bölgelerdeki sistemler birbirleri ile doğrudan iletişim kuramamaktadırlar. Dolayısıyla bir bölgede yaşanan istismar, erişim izni olmadıkça diğer bölgedeki sistemleri etkilemeyecektir.

Bir güvenlik tasarımında genel olarak olması gereken güvenlik bölgeleri:

3.4.2.1. İnternet Bölgesi

Güvenilir olmayan bölgedir. İnternet bölgesi, herhangi bir İnternet Servis Sağlayıcısının (Internet Service Provider - ISP) omurga ağlarını içermektedir. İnternet bölgesi, tehdit aktörlerinin barındığı son derece tehlikeli bir bölgedir. Bu bölge kurumsal ağ kontrolünde değildir.

3.4.2.2. DMZ Bölgesi

Harici DMZ, internet bulutundan gelen isteklerin karşılandığı bilişim sistemlerinin barındırıldığı bölgedir. Bu bölge kurumsal bölge ile internetteki sistemler arasında vekil görevi görmektedir. İnternetten gelen veya internet bulutuna doğru giden trafiklerin, bu bölge üzerinden geçirilmesi gerekmektedir. Bölge içerisinde çalışan bilişim sistemlerine yönelik yapılacak saldırıların önlenmesi ve saldırı yüzeylerinin etkisizleştirilmesi için sıkı bir kontrol sağlanmalı ve güvenlik tedbirleri artırılmalıdır. Kritik sunucular burada konumlandırılmamalıdır. Bu bölgede barındırılan bazı sistemler:

- Web sunucular
- E-posta ağ geçidi
- Dosya transfer sunucuları
- Web vekil sunucuları

- Uzaktan erişim servisleri
- Dış DNS sunucuları

3.4.2.3. Test Bölgesi

Test bölgesi, yeni uygulamaların, güvenlik ve ağ cihazlarının ilk defa kurulup test edildiği bölgedir. Yeni kurulan sistemlerde barınacak bir zafiyetin, ağın diğer noktasındaki sistemleri etkilememesi için diğer bölgelerden yalıtılması gerekmektedir. Dolayısıyla yapılan analiz, arama, tarama vb. iş süreçlerinin tüm test aşamaları bu bölgede yapılmalıdır. Test verisi olarak kullanılan hiç bir trafik güvenli bölge içerisine aktarılmamalıdır.

3.4.2.4. Lokal Bölge

Orta ve yüksek riskli sistemler için hassas bilgileri barındıran bir iç bölgedir. Bu bölgede Active Directory, İç DNS, Anti-Virüs, SIEM gibi çözümler bulundurulmalıdır. Bu bölgedeki sunucu ve servislerine internet aracılığıyla erişilmesini engellemek için güvenlik sıkılaştırması yapılmalıdır. Bu bölgede yer alan hiçbir sistem internete erişmemelidir. Yalnızca zaruri bir durumda belirli IP ve portlara erişim tanımlanmalıdır.

3.4.2.5. Kullanıcı Bölgesi

Kullanıcı bölgesi, son kullanıcı bilgisayarları, yazıcılar ve telefonların barındığı yerlerdir. Uç nokta koruma çözümleri, son kullanıcı sistemlerinin kötü amaçlı yazılımlara maruz kalmasını engellemek ve kullanıcıların iç ağdaki diğer sistemlere yetkilendirme tanımlamaları olmadan erişim sağlamalarını önlemek için kullanılmalıdır.

Farklı güvenlik bölgeleri arasındaki bilgi akışı uygun güvenlik politikaları ve güvenlik kontrolleri aşağıdaki operasyonel güvenlik tedbirleri ile yapılabilir:

- Ağ güvenlik bölgeleri, kompartıman usulüne göre tanımlanmalı ve kurulmalıdır.
- Ağ güvenlik bölgeleri arasında, trafiği kontrol etmek ve veri sızıntısını önlemek için mekanizmalara sahip olunmalıdır.
- Ağ güvenlik bölgeleri arasında, güvenlik duvarları üzerinden; port, protokol, uygulama, içerik filtrelemeye dayalı bölgeler arasındaki bilgi akışını güvenli hale getiren kontroller sağlanmalıdır.

- Saldırı önleme sistemleri ile zararlı trafiği kontrol etmek ve anormal trafik akışını belirleyebilmek için konumlandırılmalıdır.
- Ağ güvenlik bölgeleri arasında çalışan, sunucular ve kullanıcılar üzerinde zararlı yazılımların önlenebilmesi için Anti-Virüs uygulaması konumlandırılmalıdır.
- Son kullanıcı cihazları, sunucular ve diğer ortak donanımlar verilerin kritikliğine göre ayrılan farklı bölgelere yerleştirilmelidir.
- Farklı rollere sahip sunucular farklı ağ güvenlik bölgelerine yerleştirilmelidir.
- Diğer bilgi sistemlerine yapılan bağlantılar, bu hizmetler için adanmış güvenlik duvarlarında sonlandırılmalıdır.
- Sistem yönetimi için özel ağ güvenlik bölgeleri kullanılmalıdır.
- Güvenlik uygulamalarının zararlı yazılımı bulabilmesi ve analiz edebilmesi için şifreli web trafiğinin güvenlik uygulamaları üzerinde sonlandırılıp trafik analizinin yapılması sağlanmalıdır.
- Kullanıcı sistemleri üzerinde, kurumsal iş süreçlerimize herhangi bir bilgi güvenliği ihlali ve olayı oluşturmaması için sunucu, servis, uygulama vb. süreçlerin çalıştırılmaması gerekmektedir. Yapılacak analiz ve çalışmalar, sunucu bölgelerinde ve kurumsal iş süreçlerinin profesyonel iş sürekliliği prensiplerine göre yapılmalıdır.
- Tüm gelen ve giden veri paketleri güvenlik duvarları üzerinden; IPS, Anti-Virüs, Web Filter, DNS koruması, SSL sonlandırma vb. güvenlik kontrollerinden geçirilerek analiz edilmeli ve filtrelendirilmelidir.
- Gelen ve giden veri paketlerinin kapasite kontrolleri, güvenlik duvarları üzerinden, yapılmalıdır.
- Her paketin ve kural ve protokol ihlallerinin analizi yapılmalıdır. Uygunsuz ve zararlı trafiklerin kurum bilgi varlıklarına zarar vermesi ve farklı semptomlar göstermesi mutlaka engellenmelidir.

- Güvenlik duvarları üzerinde, kural tabanlı değişiklik yapıldığı zaman kurumsal ağ güvenlik stratejisinin ihlal edilmediğinden emin olunmalıdır. Yapılan bütün değişikliklerin kayıt altına alınması bir zorunluluktur.
- Kötü amaçlı ve şüpheli trafiği tespit etmek ve engellemek için güvenlik uygulamaları üzerinden kural tabanlı operasyonlar sıkılaştırmalıdır.
- Trafik anormalliklerinin tespit edilmesi için IPS kullanılması zorunludur.
- Güvenlik uygulamaları üzerinde, kural tabanlı erişim kontrol listeleri oluşturulmalıdır.
- Güvenlik duvarları üzerinde kullanılmayan servisler devre dışı bırakılmalıdır.
- Kullanıcı bilgisayarları üzerinde herhangi bir bilgi güvenliği istismarı oluşmaması için Open VPN gibi çözümler mutlaka kullanılmalıdır.

Bu tedbirlerin uygulandığı güvenlik çözümleri; Bölüm 3.4.3'te ve güvenlik tasarımı çizimi Bölüm 3.4.5'te incelenmiştir.

3.4.2.6. Dâhili Bölge

Dâhili bölge, iş süreçleri açısından kritik ve hassas bilişim varlıklarını üzerinde barındırmaktadır. Kısıtlı bölge bilgi varlıklarının herhangi birindeki verilerin gizliliği, bütünlüğü veya kullanılabilirliğinin ihlali, kurumsal yapının itibarını olumsuz yönde etkileyebilmektedir. Dâhili bölge, saldırıların tespit edilmesi için en yüksek koruma düzeyine sahip olmalıdır. Bu bölgede bulunan sistemlerin internet erişimi olan herhangi bir sistemle bağlantısı olmamalıdır.

3.4.3. Güvenlik Çözümleri

Bir veri merkezinde sistemlerin korunması için güvenlik cihazlarının ve yeteneklerinin iyi saptanması gereklidir. Son kullanıcıdan ağın uç noktasına kadar güvenliğin sağlanması, hangi güvenlik ürünlerinin kullanılması gerektiği ve bu güvenlik ürünlerinden hangi logların alınması gerektiğinin bilinmesi önemlidir. Bölüm 3.4.3'te bahsedilen güvenlik çözümleri çoğunlukla veri merkezlerinde olan çözümlerdir.

3.4.3.1. DDoS Koruma Cihazı

DDoS (Distributed Denial of Service) dağıtık servis engelleme anlamına gelmektedir. DDoS saldırılarında amaç, hedefteki sistemin erişilebilirliğini engellemektir. Bir DDoS saldırısı, hedefteki sistemin kaldırabileceğinden çok daha fazla anlık istek yollanmasıyla vuku bulmaktadır. Bu istekler farklı kaynaklar üzerinden yapıldığı için, isimdeki "Distributed (Dağıtık)" kelimesi de buradan gelmektedir. Saldırının ardından, hedef sistem yükü kaldıramaz ve sistemlere erişimde sıkıntılar yaşanabilir. Servislerin tamamı veya tamamına yakını hizmet veremez hale gelebilmektedir. İnternet Servis Sağlayıcıları tarafından da bu tarz saldırılar engellenebilmektedir. Fakat katmanlı güvenlik mimarisinde yalnızca servis sağlayıcıdan alınan hizmete bağlı kalınmamalıdır. Ek olarak DDoS koruma cihazı sisteme entegre edilmelidir. Bir DDOS koruma cihazında başlıca olması gereken özellikler:

- Protokol bazlı saldırı formlarına karşı koruma sağlayabilmelidir.

  Örnek saldırılar; smurf, Fraggle, Ping Flood, Ping-of-Death, SYN Flood, Land Attack,TearDrop.

- Web uygulamalarının korunmasını sağlayabilmelidir.

  Örnek saldırılar; HTTP Get/Post taşması, HTTPS taşması, SSL Dos/DDos, Rudy.

- Dinleme saldırılarına karşı koruma sağlayabilmelidir.

- DNS koruması yapabilmelidir.

  DNS sorgu/yanıt taşması, DNS Cache Poisoning saldırılarına karşı koruma sağlayabilmelidir.

- Ağ tipli saldırılara karşı koruma sağlayabilmelidir.

  Örnek saldırılar; SYN/SYN-ACK/ACK taşması, FIN taşması, UDP taşması, IP taşması.

- Kötü ünlü IP koruması yapabilmelidir.

  Daha önce zararlı hareket yapmış kirli IP'lerden gelen saldırılar.

- SIP (Session Initiation Protocol) koruması olmalıdır.

Örnek saldırılar; SIP taşması, kimlik doğrulama taşması.

- Filtreleme olmalıdır.

  IP, protokol (tcp, udp, sip, icmp), DNS ve HTTP paket filtreleme.

- Bölgeye göre filtreleme yapılmalıdır.

  IP adresinin kayıtlı olduğu bölgeye göre trafik engelleme veya sınırlandırma. Örneğin ABD'den (Amerika Birleşik Devletlerinden) gelen trafiklerin engellenmesi.

- İmza tabanlı koruma sağlanmalıdır.

  İmza veritabanındaki imzalara göre koruma sağlamaktadır.

3.4.3.2. Tehdit Önleme Sistemi

Saldırı tespiti, ağda meydana gelen olayları izleme ve olası ihlalleri veya güvenlik politikalarına yönelik olası tehditleri tespit etmek için yapılan analiz işlemidir. İzinsiz giriş önleme, izinsiz giriş tespiti gerçekleştirme ve tespit edilen olayları durdurma işlemidir. Bu güvenlik önlemleri, olası olayları tespit etmek ve durdurmak için ağın bir parçası haline gelen saldırı önleme sistemleri olarak bulunmaktadır.

Tipik bir iş ağının, hem genel hem de özel diğer ağlara çeşitli erişim noktaları vardır. Buradaki zorluk, bu ağların güvenliğini müşterilere açık tutmaktır. Şu anda, saldırılar o kadar karmaşıktır ki, saldırganlar en iyi güvenlik duvarlarını dahi atlatabilmektedirler. Ne yazık ki, bu teknolojiler tek başına günümüzün saldırılarına karşı koymak için yeterli değildir.

Bir IPS çözümü ağı sürekli izler, olası olayları belirler ve bunlar hakkındaki bilgileri günlüğe kaydeder, olayları durdurur ve güvenlik yöneticilerine bildirir. Güvenlik politikalarıyla ilgili sorunları tanımlamak ve saldırganların güvenlik politikalarını ihlal etmelerini engellemek için IPS kullanılmaktadır.

HIPS (Host-Based Intrusion Prevention System) ve NIPS (Network-Based Intrusion Prevention System) olmak üzere iki yöntemle çalışmaktadır. HIPS, dizüstü/masaüstü bilgisayarlara veya sunuculara yüklenen yazılımlar aracılığı ile koruma sağlarken, NIPS ise in-line modda ağ üzerindeki tüm trafiği denetlemektedir.

Ağ Tabanlı IPS özelliğine sahip bir güvenlik duvarı en az iki Ağ Arabirim Kartı (NICs - Network Interface Cards) içermektedir. Bunlardan biri dâhili NIC olarak seçilir ve kuruluşun dâhili ağına bağlanır. Diğer NIC ise harici olarak seçilir ve çoğu durumda internet bağlantısı olan harici ağa bağlanır.

Trafik NIC'lerden birinden alındığında, entegre NIPS'in algılama motoru tarafından derinlemesine denetlenmektedir. NIPS kötü amaçlı bir veri paketi algılarsa, veri paketini anında bırakır ve ağ güvenlik personelini olay hakkında uyarır. Kaynaktan tek bir kötü amaçlı paket algıladıktan sonra, o TCP bağlantısından gelen diğer tüm paketleri derhal atar veya oturumu kalıcı olarak engeller [49].

Bir IPS çözümünde olan diğer özellikler [49];

- Sorun yaratan kaynak IP adreslerinden ağ trafiğini engellemektedir.
- TCP bağlantısını sıfırlamaktadır.
- Parçalanmamış paket akışlarını düzeltmektedir.
- Döngüsel Artıklık Denetimi hatalarını düzeltmektedir.
- TCP sıralama sorunlarını kontrol etmektedir.
- İstenmeyen taşıma ve ağ katmanı seçeneklerini dezenfekte etmektedir.

Saldırı önleme sistemi, genel olarak bir ağda in-line olarak konumlandırılmaktadır. Doğrudan gerçek ağ trafiği yolunda bulunan ve paketler içinden geçerken tüm ağ trafiğini derinlemesine inceleyen bir sensör içermektedir. Sıralı mod, sensörün gerçek zamanlı paket denetimi yaptığı önleme modunda çalışabilmektedir. Koruma için dört yaklaşım ele alınmaktadır:

İmza Tabanlı Yaklaşım: İmza Tabanlı yaklaşımda, önceden tanımlanmış imzalar veya iyi bilinen ağ saldırı kalıpları, satıcıları tarafından IPS aygıtına kodlanmaktadır. Önceden tanımlanmış kalıplar, bir saldırının içerdiği kalıpları IPS'de depolanan kalıplarla karşılaştırarak bir saldırıyı algılamak için kullanılmaktadır. Bu yönteme Kalıp Eşleştirme yaklaşımı da denilmektedir.

Anomali Tabanlı Yaklaşım: Anomali Tabanlı yaklaşımda, ağda herhangi bir anormal davranış veya etkinlik algılanırsa, bir IPS, yöneticiler tarafından tanımlanan kriterlere göre hedef cihaza erişimi engellemektedir. Bu yöntem profil tabanlı yaklaşım olarak da bilinmektedir.

İlke Tabanlı Yaklaşım: İlke Tabanlı yaklaşımda, yöneticiler güvenlik ilkelerini ağ altyapılarına ve kuruluş ilkelerine göre bir IPS aygıtında yapılandırmaktadır. Bir etkinlik yapılandırılmış güvenlik ilkelerini ihlal etmeye çalışırsa, IPS yöneticilerinin kötü amaçlı etkinlik konusunda uyarılması için bir alarm tetiklenmektedir.

Protokol Analiz Tabanlı Yaklaşım: Protokol Analiz Tabanlı yaklaşım, İmza Tabanlı yaklaşıma biraz benzemektedir. İmza Tabanlı yaklaşım ile Protokol Analiz Tabanlı yaklaşım arasındaki tek fark, Protokol Analiz tabanlı sistemde çok daha derin veri paketi denetimi yapılabilmekte ve İmza Tabanlı ile karşılaştırıldığında güvenlik tehditlerini tespit etmede daha esnek olabilmektedir.

3.4.3.3. Yeni Nesil Güvenlik Duvarları

Geleneksel güvenlik duvarları, ağ geçidinde trafiği kaynak ve hedef adreslerine, kullanılan port ve protokole göre izin vermek veya engellemek üzere ayarlanmış cihazlardır. . Yeni nesil güvenlik duvarları klasik güvenlik duvarlarına göre tüm bağlantıların korunmasını sağlamak için veri paketlerini daha derin bir düzeyde analiz etmektedirler.

Yeni nesil güvenlik duvarlarının bazı özellikleri aşağıdaki gibidir:

- Uygulama ve kullanıcı kontrolü
- Derin paket denetim politikası
- İleri kaçırma teknikleri
- Virüs ve kötü amaçlı yazılımlara karşı koruma
- Özelleştirilmiş raporlama
- Dinamik yönlendirme
- URL filtreleme

- Otomasyon ve ürün entegrasyonu
- VPN
- IPS
- Malwere Koruması
- QoS (Quality of Service)

Bilişim güvenliği sektöründe hizmet vermekte olan Beyaz.Net şirketine göre güvenlik duvarı çeşitleri [50]:

Paket filtrelemeli güvenlik duvarları: Ağ trafiği içerisinde gelen ve giden paketlerin başlıkları incelenerek paket kabul edilmekte veya reddedilmektedir.

- Durumlu denetim güvenlik duvarları:

  Ağ trafiğinde verilerin kaynaktan hedefe kadar takip edilerek güvenliğin sağlanmasıdır.

- Uygulama katmanı güvenlik duvarları:

  Gelen ve giden paketlerin sadece başlığı değil paketin veri kısmına kadar kontrol edilerek filtrelenmesi ve kontrol edilmesi sağlanır. En sık kullanılan güvenlik duvarı tekniğidir.

- Devre düzeyli geçit yolu:

  Ağ ile ilk bağlantı yapılırken üç aşamalı el sıkışma sırasında uygulama ve transfer katmanları arasında çalışmaktadır. Veri alışverişi sırasında dışarıdan yapılabilecek bağlantılara karşı bağlantıyı koruyarak güvenliği sağlamaktadır.

Geleneksel güvenlik duvarları yalnızca veri paketini protokollere, bağlantı noktalarına veya adreslere göre analiz ederek paketin ağda engellenmesi veya ağa erişim izni verilip verilmediğini belirlemekte ve VPN yapabilmektedir. Geleneksel veya yeni nesil güvenlik duvarının tercihi tamamen maliyet, yapı ve ihtiyaçlar ile doğru orantılıdır.

3.4.3.4. VPN Concentrator

VPN Virtual Private Network'ün kısaltmasıdır. VPN ile internet gibi halka açık ağlar üzerinden kullanıcıların kendi kurum kaynaklarına güvenli bir şekilde erişmeleri sağlanmaktadır [51].

VPN sayesinde şirketler farklı noktalardaki ofislerini birbirine ya da mobil kullanıcılarını merkeze bağlamaları için kendi ağ omurgalarını kurmalarına gerek kalmamaktadır. VPN ile her lokasyon, diğer lokasyonlarla arasındaki bağlantıyı internet üzerinden kesintisiz ve yüksek hızla gerçekleştirmektedir. VPN, şirketlerin internet omurgasını kendi omurgaları gibi kullanmalarına imkân vermektedir [51].

Üç çeşit VPN bulunmaktadır;

- İntranet VPN:

  Bir işyerinin farklı lokasyonlarda bulunan ek binaları arasında kurulmaktadır.

- Remote Access (Uzaktan Erişim) VPN:

  Gezgin saha çalışanlarının her yerden bağlanabildikleri VPN türüdür.

- Dış Ağ (extranet) VPN:

  Farklı teknolojilere sahip internet tabanlı VPN. IPSec bunlardan birisidir.

Teckopedia'da yayınlanan tanıma göre; VPN concentrator, VPN bağlantılarının güvenli bir şekilde oluşturulmasını ve VPN düğümleri arasında mesajların iletilmesini sağlayan bir tür ağ cihazıdır [52].

VPN iletişim altyapılarını oluşturmak ve yönetmek için özel olarak tasarlanmış bir tür yönlendirici cihazdır. Bir VPN concentrator genellikle bir noktadan bir noktaya VPN mimarileri oluşturmak için kullanılmaktadır. Kısaca VPN çözümlerinin yapabildikleri:

- Tünel kurmak ve konfigürasyonunu sağlamak
- Kullanıcı kimliği doğrulama
- Kullanıcılara tünel/IP atanması

- Veri şifreleme ve şifre çözmek
- Verilerin uçtan uca taşınmasını sağlamak

VPN konusu çok geniş kapsamlı bir konudur. VPN concentrator gibi ürünlerin veri merkezinde kullanılma amacı, farklı lokasyondaki kuruma ait binalarla ve iş ortaklığı yapılan diğer firmalarla verilerin güvenli tünel üzerinden aktarılmasıdır.

3.4.3.5. Web Uygulama Güvenlik Duvarı

Web Uygulama Güvenlik Duvarı (Web Application Firewall - WAF), bir web uygulaması ile internet arasındaki HTTP/HTTPS trafiğini filtreleyerek ve izleyerek web uygulamalarının korunmasına yardımcı olmaktadır. Genellikle web uygulamalarını siteler arası sahtecilik, siteler arası komut dosyası oluşturma, dosya ekleme ve SQL enjeksiyonu gibi saldırılardan korumaktadır. WAF, bir OSI 7. Katman savunmasıdır ve her türlü saldırıya karşı savunmak için tasarlanmamıştır. Yalnızca web saldırılarına odaklanmaktadır. Saldırı hafifletme yöntemi olan WAF, genellikle bir dizi saldırı vektörüne karşı bütünsel bir savunma oluşturan bir takım araçların parçasıdır.

Bir web uygulamasının önüne bir WAF konulduğunda, web uygulaması ile internet arasında bir kalkan yerleştirilmiş olur. Proxy sunucusu bir aracı kullanarak bir istemci makinesinin kimliğini korurken, WAF bir tür ters proxy'dir ve sunucuya ulaşmadan önce istemcilerin WAF'dan geçmesini sağlayarak sunucuyu kötü aktivitelere karşı korumaktadır.

WAF, bazı politikalarla çalışmaktadır. Bu politikalar, kötü niyetli trafiği filtrelemekte ve uygulamadaki güvenlik açıklarına karşı korunmayı amaçlamaktadır. Bir WAF'ın değeri kısmen, politika değişikliğinin uygulanabilme hızı ve kolaylığından kaynaklanır. Bu da değişen saldırı vektörlerine karşı daha hızlı yanıt verilmesini sağlamaktadır. DDoS saldırısı sırasında, hız kısıtlaması (rate limiting) yapılabilmektedir.

Bir WAF, her biri kendi yararları ve eksiklikleri olan üç farklı yoldan biri ile uygulanabilir. Bunlar ağ tabanlı, ana bilgisayar tabanlı, bulut tabanlı ve açık kaynak tabanlı WAF'lardır [53].

Ağ tabanlı WAF genellikle donanım tabanlıdır. Yerel olarak kurulduklarından gecikmeyi en aza indirirler. Ağ tabanlı WAF'lar pahalı bir seçenek olmakla birlikte ca fiziksel ekipmanın

depolanmasını ve bakımını gerektirmektedir. Ağ tabanlı WAF, tüm gelen ve giden trafiğin içinden geçtiği, denetlendiği ve tehlikeli trafiği engelleyen bir WAF motoruna sahiptir.

Ana bilgisayar tabanlı bir WAF, bir uygulamanın yazılımına tam olarak entegre edilebilir. Bu çözüm, ağ tabanlı WAF'dan daha ucuzdur ve daha fazla özelleştirilebilirlik sunmaktadır. Ana bilgisayar tabanlı bir WAF'ın dezavantajı, yerel sunucu kaynaklarının tüketimi, uygulama karmaşıklığı ve bakım maliyetleridir. Bu bileşenler tipik olarak mühendislik süresi gerektirmekte ve maliyetli olabilmektedir.

Bulut tabanlı WAF'lar, uygulanması çok kolay olan uygun fiyatlı bir seçenek sunmaktadır. Genellikle trafiği yönlendirmek için DNS'deki bir değişiklik yeterli olmaktadır. Bulut tabanlı WAF'lar, kullanıcılar hizmet olarak güvenlik için aylık veya yıllık ödeme yaptıkları için minimum bir ön maliyete sahiptir. Bulut tabanlı WAF'lar, kullanıcı tarafında herhangi bir ek çalışma veya maliyet olmadan en yeni tehditlere karşı korumak için sürekli güncellenen bir çözüm de sunabilmektedir. Bulut tabanlı bir WAF'ın dezavantajı, kullanıcıların sorumluluğu üçüncü bir tarafa teslim etmeleridir, bu nedenle WAF'ın bazı özellikleri kendileri için bir kara kutu olabilmektedir.

Açık Kaynak WAF genellikle yapılandırılacak belirli bir bilgi ve deneyime sahip olmayı gerektirir. Ancak açık kaynaklar olduğu için yüksek düzeyde özelleştirmeler sunar ve ücretsizdir.

WAF seçimi yaparken ihtiyaç analizi iyi yapılmalıdır. Veri merkezinde sorumluluğun üçüncü taraflara devredilmesi kabul edilemeyeceği için bulut tabanlı WAF tercih edilmemelidir. Eğer büyük ölçekli bir web hizmeti verilmiyorsa çok fazla kaynak ihtiyacı olmayacağından Host-Based WAF kullanılabilir. Ancak çok fazla sayıda trafik olacaksa güçlü donanım özellikleri sayesinde ağ tabanlı WAF in-line olarak web sunucusu önünde konuşlandırılabilir.

3.4.3.6. Veritabanı Güvenlik Duvarı

Veritabanı güvenlik duvarları, çoğunlukla veri tabanlarında depolanan hassas bilgilere erişmek isteyen veritabanına özgü saldırıları tanımlamak ve bunlara karşı korumak için veri tabanlarını izleyen bir güvenlik duvarı türüdür. Veritabanı güvenlik duvarları, veritabanlarına yapılan tüm erişimi, bunların tuttukları günlükler aracılığıyla izlemeyi ve

denetlemeyi sağlamaktadır. Bir veritabanı güvenlik duvarı, Bölüm 2.4'te de bahsedilen PCI, SOX vb. gibi düzenlemeler için belirli uyumluluk raporları oluşturabilmektedir.

Genel olarak veritabanı güvenlik duvarları, ağ geçidinin yakınında, güvenlik duvarının arkasında, veritabanı sunucusunun önünde konuşlandırılır. Bazı veritabanı güvenlik duvarları ise ajan bazlı çalışmaktadır. Donanım tabanlı güvenlik duvarları, veritabanı sunucularına herhangi bir ek yük olmadan ana bilgisayar/ağ izlemeyi desteklemektedir. Hem donanım cihazı hem de yazılım aracıları aynı anda çalışmak üzere dağıtılabilmektedir.

Veritabanı güvenlik duvarları, bir dizi önceden tanımlanmış, özelleştirilebilir güvenlik denetim ilkeleri içerir ve geçmiş olaylara 'imzalar' adı verilen tehdit kalıplarına göre veritabanı saldırılarını belirleyebilir. Bu nedenle, SQL giriş deyimleri, sorguları, veritabanında bilinen saldırıları tanımlamak için satıcılar tarafından sık sık güncellenen bu imzalarla karşılaştırılmaktadır [55].

Bir sistemdeki en kıymetli varlık veridir. Verilerin korunması da hayati önem taşımaktadır. Bu kapsamda verilerin depolandığı veri tabanları da saldırılardan korunmalı, şüpheli hareketler olduğu zaman anında tespit edilmelidir. Veritabanı güvenlik duvarlarından SIEM'e aktarılacak loglar da bu çalışmanın amacı kapsamında önemli rol oynayacaktır. Çünkü bu çalışmanın amacı, veri merkezlerinde güvenliğin bütüncül olarak sağlanması için SIEM'in en iyi şekilde yapılandırılmasıdır.

3.4.3.7. PROXY Sunucusu

Proxy sunucusu kullanıcı ile internet arasında ağ geçidi görevi görür. Son kullanıcıları göz attıkları web sitelerinden ayıran bir aracı sunucudur. Proxy sunucuları, kullanım durumuna, gereksinimlere veya şirket ilkelerine bağlı olarak değişen düzeylerde işlevsellik, güvenlik ve gizlilik sağlamaktadır.

Proxy sunucusunun olduğu ortamda internet trafiği proxy sunucusundan istenilen adrese gitmektedir. Daha sonra istek aynı proxy sunucusu üzerinden geri dönmektedir ve proxy sunucusu web sitesinden alınan verileri alıcıya iletmektedir.

Modern proxy sunucuları, tümü veri güvenliği ve ağ performansı adına web isteklerini iletmekten çok daha fazlasını yapmaktadır. Proxy sunucuları bir güvenlik duvarı ve web filtresi olarak işlev görmekte, paylaşılan ağ bağlantılarını sağlamakta ve ortak istekleri

hızlandırmak için verileri önbelleğe almaktadır. İyi bir proxy sunucusu, kullanıcıları ve dâhili ağı internette yaşayan kötü aktivitelerden koruyabilmekte, yüksek düzeyde gizlilik sağlayabilmektedir.

Veri merkezi güvenlik tasarımında Proxy kullanılmasının amacı, şifreli trafiklerin (Secure Sockets Layer - SSL) çözülerek kontrolünün sağlanmasıdır. SSL decryption ile SSL paketinin içindeki bilgiler analiz edilebilecektir. Böylece zararlı etkinlikler tespit edilebilecektir. Eğer sistemde proxy sunucusu yoksa ve kullanılan güvenlik duvarı destekliyorsa ssl decryption güvenlik duvarında açılabilmektedir. Gecikmeler (latency) yaşanabilir fakat hiçbir gecikme süresi güvenlikten daha önemli değildir.

3.4.3.8. Anti-Virüs Yazılımları

Virüsler, bilgisayarda yüklü olan diğer programlara benzer şekilde çalışmaktadır. Bununla birlikte, temel fark, programın arkasındaki niyet ve özellikle yazılımın ne yapmak için programlandığıdır. Virüsler cihazlardaki önemli verilere zarar verme, hasat etme, silme, gizlice dinleme, yakalama veya yok etme amaçlıdır.

Her virüs, parmak izi gibi bir imza içermektedir. Parmak izleri sayesinde virüsler bilgisayardaki diğer programlardan ayırt edilebilmektedir. Bu nedenle, bu imzaya sahip kötücül yazılımlar anti-virüs uygulamaları tarafından fark edilebilmektedir.

Virüsten koruma yazılımı, veritabanındaki benzer kalıpları belirleyerek veya bir saldırının ne zaman gerçekleşeceğini tahmin etmeye yardımcı olan araçlar ile çalışmaktadır. Çok yönlü bir yaklaşım kullanmaktadır. Bunun sebebi virüslerin zaman içinde uyum sağlayabilme, dönüşebilme ve güçlenebilme özellikleridir. Maruz kalma riski zamanla azalma göstermemekte aksine, katlanarak artmaktadır.

Virüsten koruma yazılımı, yalnızca virüslerin değil, casus yazılım, rootkit, fidye yazılımı gibi diğer kötü amaçlı tehditlere, tüm yeni ve gelişmiş kötü amaçlı yazılım biçimlerine karşı da koruma içermelidir.

Veri merkezinde kullanılacak anti-virüs yazılımı sistemde olması gereken diğer bir güvenlik aracı olan kum havuzu çözümleri ile entegre edilmelidir. Böylelikle anti-virüs yazılımının tespit edemediği bir zararlı dosya olursa kum havuzu aracılığı ile bunlar analiz edilerek tespit edilebilir.

Bazı anti-virüs yazılımları ek olarak aşağıdaki özellikleri de barındırmaktadır. Derin güvenlik sağlanmak istendiğinde bu özelliklere sahip yazılımlar tercih edilebilir.

İnternet üzerinde güvenli işlemlerin yapılmasına kimlik avı koruması yardımcı olacaktır. DLP (Data Loss Prevention) özelliği var ise veri sızıntılarının önüne geçilmesinde katkı sağlamaktadır. Web koruma özelliği bulunan bir anti-virüs zararlı sitelere erişimleri engellemektedir. Uygulama kontrolü var ise, bilgisayar istenmeyen yazılımların kurulmasını engelleyecektir. Örneğin, oyun kategorisinde bulunan oyunların yüklenmesi ve çalıştırılmasının engellenmesi sağlanabilmektedir.

Bir saldırının son durağı son kullanıcıların bilgisayarları veya sunuculardır. Bu doğrultuda son kalenin korunması hayati önem taşımaktadır. Son kale, içten de fethedilebilir dışardan da. Önemli olan zamanında yapılacak saldırıya hazırlıklı olmaktır.

3.4.3.9. APT Çözümleri

APT (Advanced Persistent Threat) diğer siber saldırı çeşitlerinden farklı olarak sisteme hızlı bir şekilde girmek ya da sistemi tamamen etkisiz hale getirmek yerine yavaş ve fark edilmeden sızarak sistemde olabildiğince uzun süre kalıp, maksimum miktarda değerli veri toplayan hedefli saldırılardır [56].

APT, hedef odaklı karmaşık ve kalıcı tehdit anlamına gelmektedir. Siber dünyada APT saldırılarının artmasıyla APT önleme ürünleri de çıkarılmaya başlamıştır. Siber güvenlik alanında faaliyet gösteren BGA Bilgi Güvenliği şirketine göre [57] APT ürünlerinin seçiminde dikkat edilmesi gereken noktalar aşağıdaki gibidir:

- Yalnızca “exe, .pdf, .doc” uzantılı dosyalar değil tarayıcı ve e-posta üzerinden indirilebilecek tüm çalıştırılabilir dosyaları kontrol edebilmelidir.
- Kullanıcılar oltalama maillerindeki linkleri veya çalıştırılabilir dosyaları indirmeden veya açmadan incelemesi yapılmalıdır.
- Güncel istihbaratları takip edebilmelidir.
- Kum havuzluğu yapabilmeli yani kapalı kutu (İnternete bilgi göndermeden) üzerinde analiz yapabilmelidir.

- In-line konumlandırılabilmelidir. Gelen/giden trafikleri ağ geçidi üzerinde tespit edebilir. Latency ölçeklendirmesi yapılmalıdır.
- Harici disk, dosya paylaşımı gibi yöntemlerle sisteme bulaşmış zararlı yazılımlara ait call-back bağlantılarını yakalayabilmelidir.
- Komuta kontrol bağlantılarını tespit edebilmelidir.
- False pozitif durumlar çok sık olmamalıdır.

Kaspersky güvenlik şirketinin "What IS an Advanced Persistent Threat" başlıklı yazısında [58] ele aldığı APT saldırı aşamaları:

- Aşama 1: Erişim Kazanmak

  Hedef ağa kötü amaçlı yazılım eklemek için güvenlik açıklıklarından faydalanmak.

- Aşama 2: Arka Kapı Oluşturmak

  Tespit edilmeyen sistemlerde hareket etmek için arka kapı kullanılmaktadır. Kötü amaçlı yazılım, genellikle bilgisayar korsanlarının izlerini örtmelerine yardımcı olmak için yeniden kod yazma gibi teknikler kullanmaktadır.

- Aşama 3: Erişimin Derinleştirilmesi

  Bilgisayar korsanları içeri girdikten sonra, yönetici haklarına erişim elde etmek için şifre kırma gibi teknikler kullanırlar. Böylece sistemi daha fazla kontrol edebilir ve daha da fazla erişim elde edebilirler.

- Aşama 4: Kuzey/Güney Yönünde Hareket Etmek

  Güvenlik duvarlarına takılmadan aynı ağda yer alan diğer bölgelere erişim sağlanmaya çalışmaktadır.

- Aşama 5: Bak, Öğren ve Sistemde Kal

  Sistemin güvenlik açıklıklarının tam olarak anlaşılması ve istenilen bilgilerin toplanması aşamasıdır. Bilgisayar korsanları bu süreci devam ettirmeye çalışabilir ve süresiz olarak veya belirli bir hedefe ulaştıklarında geri çekilebilirler. Gelecekte tekrar sisteme erişmek için arka kapıları açık bırakırlar.

Hedefli saldırılar veri merkezinin karşı karşıya kalabileceği en tehlikeli riskler arasındadır. APT saldırılarının en büyük tehlikesi, saldırganların daha sonra kullanabilecekleri bir arka kapı bırakmış olabilmeleridir.

Ayrıca, virüsten koruma ve güvenlik duvarları gibi birçok geleneksel siber savunma her zaman bu tür saldırılara karşı koruma sağlayamamaktadır. APT ürünlerini konumlandırırken geri kalan güvenlik duvarı, IPS, WAF, Anti-virüs, AntiSpam, DLP vs gibi ürünlerin yakalayamayacağı %5'lik küçük ama değerli alanı hedeflemek gerekmektedir [57]. Bu doğrultuda SIEM'e aktarılacak APT engelleme sistemlerinden alınacak loglar iyi analiz edilmelidir.

3.4.3.10. Ağ Erişim Kontrolü

Ağ erişim kontrolü (Network Access Control – NAC), son kullanıcı tarafından kullanılan cihazların ağ kaynaklarına erişimini kısıtlama işlemidir. Ağ erişim denetimleri, erişim için tanımlanmış, kimlik doğrulama ve yetkilendirme gerçekleştiren bir ağ erişim sunucusu tarafından desteklenen bir güvenlik ilkesi uygulamaktadır. Sunucu, her kullanıcının erişebileceği verileri ve son kullanıcı tarafından ağa eriştikten sonra gerçekleştirilebilecek etkinlikleri kısıtlamaktadır.

Beyaz.Net'in "Ağ Erişim Kontrolü " makalesine göre [59] NAC, ağ güvenliğinde ilk adımdır. Erişim denetimi sayesinde ağ üzerinde yalnızca izin verilen istemciler ve kullanıcılar yer alabilir. 802.1x protokolü kullanılarak ağa dâhil olması istenen cihazlar MAC adresleri ile kayıt edilmektedir. Bu yüzden dağıtım ve politika sürecinde ağda ne tür cihazların olduğunu saptamak önemlidir.

Dağıtımda iki yöntem vardır. NAC Pre-Admission ve Post-Admission. Pre- Admission, kullanıcının ön izinle ağa dâhil olup olmayacağına karar verilmesidir. Post-Admission ise kullanıcının ağa dâhil edilmesinin ardından sahip olduğu haklar karşılığında izin verilen uygulamalara erişebilir durumda olmasıdır [59].

Siber güvenlik sitesi SpamLaws'a göre [60] ihtiyaçlara göre değişen dağıtım türleri

Ajan Tabanlı Ağ Erişim Kontrolü: Ajan tabanlı ağ erişim kontrolü, daha yüksek bir güvenlik seviyesi ile birlikte son kullanıcının güvenlik politikalarına uymasını sağlayan uç nokta cihazı (kullanıcının cihazı) aracılığıyla çalışmaktadır. Ünite, güvenlik uyumluluğunu

izlemek için sürekli olarak cihazın arka planında çalışmakta ve ardından ilke sunucusuna periyodik güncellemeler göndermektedir.

Aracısız Ağ Erişim Denetimi: Aracısız ağ erişim denetimi, ek kurulum gerektirmez. Bunun yerine, bu tür ağ erişim denetimi, kullanıcının ağa erişmesine izin vermeden önce her iki uç noktadaki uyumluluğu da değerlendirmektedir. Ağ erişim kontrolüyle ilgili sorun, ağ trafiğinin değerlendirilmesi yoluyla yetkilendirmenin sağlanmasıdır. Bu, uygulamanın ağ sistemine yetkisiz erişim elde etmek için kullanılmasını kolaylaştırmaktadır.

Donanım Tabanlı Ağ Erişim Kontrolü: Donanım tabanlı bir ağ erişim kontrolü, ağa kurulmuş bir cihaz üzerinden ağ trafiğiyle birlikte çalışmaktadır. Bu tür ağ erişim kontrolü, son kullanıcının tanımlanmış erişimine izin vermek için altyapı ve operasyonel uygulamalarda değişiklik yapılmasını gerektirmektedir. Uygulama, önemli sunucu yapılandırma değişiklikleri gerektirdiğinden, hata olasılığı diğer ağ erişim kontrol sistemlerinden daha yüksektir.

Dinamik Ağ Erişim Kontrolü: Dinamik ağ erişim kontrolü, son kullanıcılar tarafından erişimi kontrol etmek için en kolay dağıtım şeklidir. Bunun nedeni, sistemin herhangi bir yazılım veya donanım cihazı kurulumu veya ağ yapılandırmasında değişiklik gerektirmemesidir. Bunun yerine, dinamik ağ erişim denetimi, yerel alan ağına bağlı belirli bilgisayarlarda çalışmakta ve güvenilir sistemler olarak kabul edilmektedir. Yetkisiz bir kullanıcı ağa erişmeye çalıştığında, güvenilen sistemler erişimi kısıtlamakta ve ardından eylemi ana ilke sunucusuna iletmektedir.

Beyaz.Net'e göre [59] NAC'ın sağladığı faydalar:

- ZeroDay saldırılarına karşı önemli rol oynamaktadır.
- Kullanıcı ve cihazların tanınmasını sağlamaktadır.
- Misafir kullanıcıların ağ erişiminin kontrolü için kimlik doğrulaması, kullanıcı kaydı gibi önlemler ile misafir yönetim sayfası gibi servis imkânları sunmaktadır.
- Open/RESTful API yardımıyla diğer güvenlik ve ağ çözümleri ile entegre çalışmaktadır.

- EAP türevi kimlik doğrulama protokolleri kullanılarak 802.1x için kablolu ve kablosuz ağlarda şifreleme yapılmasına izin vermektedir.

Veri merkezinde NAC cihazının olması ağ güvenliğinin ilk adımıdır. Çünkü sistemlere erişimlerin kontrol altına alınmasını sağlayan bir üründür. Bu sayede kötü niyetli birisi binaya girip kablo taktığında otomatik olarak erişimi engellenecektir.

3.4.3.11. İki Faktörlü Kimlik Doğrulama

Bazen iki aşamalı doğrulama veya çift faktörlü kimlik doğrulama olarak da adlandırılan iki faktörü kimlik doğrulaması (Two Factor Authentication - 2FA), kullanıcıların kendilerini doğrulamaları için iki farklı kimlik doğrulama faktörü sağlayan bir güvenlik sürecidir. Bu işlem, hem kullanıcının kimlik bilgilerini hem de kullanıcının erişebileceği kaynakları daha iyi korumak için yapılmaktadır. İki faktörlü kimlik doğrulama, kullanıcının yalnızca bir faktör (şifre) sağladığı tek faktörlü kimlik doğrulamaya (Single Factor Authentication - SFA) bağlı kimlik doğrulama yöntemlerinden daha yüksek bir güvenlik düzeyi sağlamaktadır.

İki faktörlü kimlik doğrulama, internet üzerinden sistemlere erişim sağlarken kullanılmalıdır. Örneğin kurum ağı dışında bir bilgisayardan e-posta, VPN kullanırken kullanıcının kısa mesaj veya kare kod ile oturum açması sağlanabilir.

3.4.3.12. Ağ İzleme

Günümüz dünyasında, ağ izleme terimi BT endüstrisinde yaygındır. Ağ izleme, yönlendiriciler, anahtarlar, güvenlik duvarları, sunucular ve VM'ler (Virtual Machine) gibi tüm ağ bileşenlerinin hata ve performans açısından izlendiği, kullanılabilirliklerini korumak ve optimize etmek için sürekli olarak değerlendirildiği kritik bir BT sürecidir. Ağ izlemenin önemli bir yönü proaktif olması gerektiğidir. Performans sorunlarını ve darboğazları proaktif olarak bulmak, ilk aşamada sorunların tanımlanmasına yardımcı olmaktadır. Etkili proaktif izleme ağ kesintilerini veya arızalarını önleyebilmektedir.

Temel İzleme: Hatalı ağ aygıtları ağ performansını etkilemektedir. Erkentespit ile bu hatalar ortadan kaldırılabilir. Bu yüzden ağın ve ilgili cihazların sürekli izlenmesi önem taşımaktadır. Etkili ağ izlemede ilk adım, izlenecek cihazları ve ilgili performans metriklerini tanımlamaktır. İkinci adım izleme aralığının belirlenmesidir. Masaüstü bilgisayarlar ve yazıcılar gibi aygıtlar kritik öneme sahip değillerdir ve sık sık izleme

gerektirmezken güvenlik cihazları (güvenlik duvarı, IPS, vs.), sunucular, yönlendiriciler ve anahtarlar iş açısından kritik görevleri yerine getirmektedir. Aynı zamanda seçici olarak izlenebilen belirli parametrelere sahiptir.

İzleme Aralığı: İzleme aralığı, performans ve kullanılabilirlik durumunu belirlemek için ağ cihazlarının ve ilgili metriklerinin hangi sıklıkta sorgulanacağını belirtmektedir. İzleme aralıklarını ayarlamak, yükü ağ izleme sisteminden ve kaynaklardan çıkarmaya yardımcı olabilmektedir. Aralık, izlenen ağ cihazının veya parametrenin türüne bağlıdır. Cihazların mevcudiyet durumu, tercihen her dakika en az zaman aralığı ile izlenmelidir. CPU ve bellek istatistikleri her 5 dakikada bir izlenebilir. Disk kullanımı gibi diğer metrikler için izleme aralığı uzatılabilir ve her 15 dakikada bir yoklanması yeterlidir. Her cihazın en az aralıkta izlenmesi tam olarak gerekli olmamakla birlikte ağa sadece gereksiz yük katacaktır

Protokol ve Protokol Türleri: Bir ağı ve cihazlarını izlerken, yaygın ve iyi bir uygulama, ağ performansı üzerindeki etkisini en aza indirmek için güvenli ve bant genişliği tüketmeyen bir ağ yönetim protokolünü benimsemektedir. Ağ aygıtlarının ve Linux sunucularının çoğu SNMP'yi (Simple Network Management Protocol) ve CLI (Command Line) protokollerini ve Windows aygıtları WMI protokolünü desteklemektedir. SNMP, ağ öğelerini yönetmek ve izlemek için yaygın olarak kabul edilen protokollerden biridir. Ağ öğelerinin çoğu bir SNMP aracısıyla birlikte gelmektedir. Sadece ağ yönetim sistemi (Network Management System - NMS) ile iletişim kurmak için etkinleştirilmeleri ve yapılandırılmaları gerekir. SNMP okuma-yazma erişimine izin vermek, cihaz üzerinde tam bir kontrol sağlamaktadır. SNMP kullanarak, cihazın tüm yapılandırması değiştirilebilmektedir. Bir ağ izleme sistemi, SNMP okuma/yazma ayrıcalıklarını ayarlayarak ve diğer kullanıcılar için kontrolü kısıtlayarak yöneticinin ağdan sorumlu olmasına yardımcı olmaktadır.

Proaktif İzleme ve Eşikler: Ağ kesintisi ciddi maliyetlere mal olabilir. Çoğu durumda, son kullanıcı bir ağ sorununu ağ yönetim ekibine bildirir. Bunun nedeni, proaktif ağ izlemeye karşı zayıf bir yaklaşımdır. Gerçek zamanlı ağ izlenirken yaşanan temel zorluk, performans darboğazlarını proaktif olarak tespit etmektir. Bu, eşiklerin ağ izlemede önemli bir rol oynadığı yerdir. Eşik sınırları, kullanım durumuna göre cihazdan cihaza değişmektedir.

Eşik ihlalleri yaşandığı zaman anında uyarı yapılabilmelidir. Eşikleri yapılandırmak, sunucularda ve ağ aygıtlarında çalışan kaynakları ve hizmetleri proaktif olarak izlemeye yardımcı olmaktadır. Her cihazın kullanıcı tercihine ve ihtiyacına göre ayarlanmış bir aralık

veya eşik değeri olabilir. Çok seviyeli eşik, karşılaşılan herhangi bir hatanın sınıflandırılmasına ve parçalanmasına yardımcı olabilir. Eşikler kullanıldığında, cihaz kapanmadan veya kritik duruma ulaşmadan da uyarılar yapılabilmektedir.

Dashboard: Veriler yalnızca doğru kitleye net bir şekilde sunulduğunda faydalı olmaktadır. BT yöneticilerinin ve kullanıcılarının oturum açtıkları anda kritik metrikler hakkında bilgi sahibi olmaları önem taşımaktadır. Bir ağ panosunda, yönlendiricilerin, anahtarların, güvenlik duvarlarının, sunucuların, hizmetlerin, uygulamaların, URL'ler, UPS ve diğer altyapı cihazlarının durumları takip edilebilmektedir. Gerekli özellikleri ve gerçek zamanlı performans grafiklerini izlemek için widget desteği, yöneticilerin sorunları hızla gidermesine ve aygıtları uzaktan izlemesine yardımcı olabilir.

BT alt yapıları sınıflandırılarak görselleştirilebilmelidir. Örneğin güvenlik cihazları, ağ cihazları, sunucular gibi farklı gruplar oluşturulabilmelidir. Ağ izleme aracından alınacak olan loglar da SIEM için önemlidir. Ağ izleme cihazı da diğer cihazlar gibi kendi alarm ve raporunu üretmektedir. Ancak burada logların SIEM'e aktarılmasındaki amaç bu loglara korelasyon yeteneği ile farklı boyut kazandırmaktır.

3.4.3.13. HIPS

"Host Tabanlı İzinsiz Giriş Saptama Sistemi" anlamına gelen HIPS (Host Intrusion Prevention System) bir sunucuya veya bilgisayara yapılması muhtemel tüm kötü niyetli girişleri tespit ederek engellemektedir. Ağ katmanında yer alan güvenlik duvarını veya diğer güvenlik çözümlerini atlatan zararlılara karşı koruma sağlamaktadır.

HIPS, sistem içerisindeki uygulama hareketlerini takip ederek anormallikleri tespit etmekte, sanal yama özelliği ile uygulama ve sistem zafiyetlerini kapatmaktadır.

3.4.3.14. Host-Based Firewall

Ana bilgisayar tabanlı güvenlik duvarı anlamına gelen Host-Based Firewall, tek bir sunucu veya bilgisayar üzerinde yazılım aracılığı ile çalışan ve kurulduğu sunucu veya bilgisayara gelen-giden trafikleri kısıtlayabilmektedir [61].

Host-Based Firewall, ağ segmentinde konumlandırılan güvenlik duvarlarına benzeyen kural setleri bulunmaktadır. Ağ güvenlik duvarları, aynı vlanda yer alan trafikler anahtar üzerinden döndüğü için bu trafikleri güvenlik duvarına gelmeden kontrol edememektedir. Dolayısıyla

aynı ağ segmentinde yer alan iki cihaz kendi aralarında trafik yaptığında güvenlik duvarı bunu fark edemeyecektir. Örneğin 192.168.1.10 IP'li bir sunucudan 192.168.1.20 IP'li sunucuya uzak masaüstü bağlantısı yapıldığında güvenlik duvarı bu trafiği göremeyecek ve engelleyemeyecektir. Fakat bu sunucular üzerinde Host-Based Firewall tanımlı olursa, aynı vlan dahi tüm trafikler denetlenebilecek ve engellenebilecektir. Çünkü Host-Based Firewall sunucuya veya bilgisayarın ağ kartına yapılan tüm trafikleri denetlemektedir.

3.4.3.15. Veri Sızıntısı Önleme Sistemi

Veri sızıntısı önleme sistemi anlamına gelen DLP (Data Lost Prevention), hassas ve önemli verilerin yetkisiz bir şekilde dışarı aktarılmasının takip edilmesini, korunmasını ve veri güvenliğini sağlayan bir teknolojidir [62].

DLP ile e-posta içerisinde, web uygulamalarında, peer-to-peer uygulamaları gibi noktalarda hareket halinde olan ortak alan klasörleri, veri tabanları gibi noktalarda saklanan durağan veriler ve son kullanıcılar tarafından işlenen veriler korunmaktadır.

DLP çözümleri, ağ ve host tabanlı olarak kullanılabilmektedir [62]. Hangi sistemin tercih edileceği maliyet ve ihtiyaçlara göre değişecektir. Ağ tabanlı DLP çözümleri, hareket halindeki veri trafiği içerisinde bir sızma tespit ederse engelleyebilmektedir. Host tabanlı bir DLP çözümü cihaz üzerine ajan vasıtasıyla kurulmaktadır. En önemli kullanım avantajı isekullanılan cihaz bir dizüstü bilgisayar ise kurum ağı dışına çıktığında dahi veri sızıntısının kontrolünü sağlamasıdır [62].

3.4.3.16. Dosya Bütünlük İzleme Sistemi

Dosya bütünlük izleme sistemleri (File integrity monitoring – FIM) hassas bilgileri, hırsızlık, kayıp ve kötü amaçlı yazılımlardan korumaktadır. İşletim sistemleri ve uygulamalar, sistem ve uygulamaların yapılandırma verileri, kurum veya şirketin hassas verileri dosyalarda depolanmaktadır. Bu dosyalardan birisinin değiştirilmesi, silinmesi veya herhangi bir tehlikeye maruz kalması, kuruluşları maddi ve itibar anlamında sarsma tehlikesiyle karşı karşıya bırakabilmektedir. FIM ile bir dosyanın önceki hali karşılaştırılır, yetkisiz değişiklikler ve dosyalarda istenmeyen değişiklikler tespit edilir.

3.4.3.17. Güvenlik Açığı Tarama Sistemleri

Zafiyet tarama sistemi olarak da bilinen güvenlik açığı tarama sistemleri, bilgisayarlar (kişisel bilgisayarlar, sunucular vb.) ağları ve uygulamalar gibi belirli bir sistemin zayıf noktalarını keşfetmek için kullanılmaktadır.

Örneğin Microsoft Windows işletim sistemine sahip bir sunucu üzerinde CVE-2019-0708 "Uzak Masaüstü Hizmetlerinde Uzaktan Kod Yürütme Güvenlik Açığı" gibi kritik bir açıklık [63] var ise, zafiyet tarama sistemi ile bu açıklığı tespit etmektedir.

3.4.3.18. E-Posta Güvenliği

E-posta güvenlik sistemleri kurumu spam, virüs, fidye yazılımı, kötü amaçlı yazılım, kimlik avı gibi e-posta üzerinden gelecek saldırılara karşı korumaktadırlar. Gelen, giden ve dâhili e-posta iletişimlerini kötü amaçlı veya zararlı içerik işaretleri için taramaktadırlar.

Ayrıca, kullanıcıların hassas verileri e-posta yoluyla harici taraflara göndermelerini engellemektedir. Bir e-posta iletisinde güvenliği ihlal edebilecek veya değiştirilebilecek dört ana bileşen bulunmaktadır;

- E-postanın ana gövdesi
- E-posta ekleri
- E-posta içerisinde bulunan URL
- Alıcı/Gönderici bilgisi

3.4.4. Güvenlik Çözümlerinden Alınması Gereken Loglar

SIEM araçları veri güvenliği ekosisteminin önemli bir parçasıdır. Birden fazla sistemden veri toplamakta ve bu verileri anormal davranış veya potansiyel siber saldırılar yakalamak için analiz etmektedir. SIEM araçları, olayları ve uyarıları toplamak için merkezi yönetim sağlamaktadır.

Log yönetimi, gerek yasal şartlar [64] ile zorunlu tutulmakta gerek ise standartlar [65] tarafından önerilmektedir. Gelişmiş saldırıların artmasıyla güvenlik risklerine karşı alınması gereken tedbirler için log yönetiminin önemi sıklıkla vurgulanmaktadır. Log yönetimi ile

personellerin aldığı IP bilgileri, bu IP'ler ile nerelere erişim sağlandığı, uzak bağlantı gerçekleştirildi mi, hangi dosyalara erişildi gibi soruların cevabını nokta atışı raporlamayabilmek ve kısa sürede bulabilmek için log yönetimi sistemi gerekmektedir. SIEM kullanımı durumunda, bu loglar merkezi olarak toplanabilecektir.

Bu kapsamda cihazlardan hangi logların alınması gerektiği belirlenmelidir.

Güvenlik Duvarları: Kurum ağından dışarı ve dışardan kurum ağına doğru olan trafiklerde kaynak IP, hedef IP, port, uygulama, erişim zamanı, erişim durumu bilgileri, konfigürasyon değişiklikleri gibi bilgiler SYSLOG formatında gönderilmektedir.

Bu format içerisinde gelen loglar aşağıdaki gibidir:

- Trafik Logları: Kaynak adres, hedef adres, trafiğin durumu (oturum başlangıç, oturum kapanma, engelleme, izin verme), uygulama (MS-RDP, ping vb.), kuralın adı, trafik paket boyutu gibi bilgiler log içeriğinde yer almaktadır.
- Audit Logları: Güvenlik duvarı kullanıcı denetim loglarıdır. Konfigürasyon değişiklikleri (silme, düzenleme, oluşturma, oturum açma, oturum kapatma), admin rolü gibi bilgiler log içerisinde yer almaktadır.

SIEM'e aktarılacak olan bu loglar olay tespiti, rapor sunma, adli olaylar için delil sunma gibi durumlarda kullanılmaktadır. Bir kullanıcının hangi saatte nerelere eriştiği, kurum personelinin en çok bağlandığı web siteler gibi bilgiler, hem yasal zorunluluktan [64] dolayı saklanabilmesi hem de olay analizi yapılabilmesi için gereklidir.

IPS: Ağ trafiğinin tespiti için güvenlik duvarı önüne veya arkasına konumlandırılan bu cihazlar, ağ trafiği içerisindeki riskli trafikleri tespit etmektedir. Bu cihazlardan karantinaya alınan IP'ler, bir imza koduna takılan trafikler gibi bilgiler SIEM'e aktarılarak, risklerin tespiti, saldırı öncesi tespit, false positive durumların tespitinde kullanılabilmektedir. Alınacak loglar sayesinde hangi saldırıların hangi güvenlik açıklarını kullanmaya çalıştığı tespit edilebilmektedir.

WAF: WAF ile anonim proxy güvenlik açıkları, kaba kuvvet saldırıları, buffer owerflow olayları, çerez kullanılarak yapılan ataklar, Cross Site Scripting açıkları, oltalama atakları gibi saldırılara karşı koruma sağlamaktadır. Bu doğrultuda SIEM'e bu logların aktarılması sayesinde saldırı tespitlerinde, olay analizlerinde kullanılabilmektedir. Ayrıca web

uygulamalarında yapılan saldırı çeşitleriyle ve miktarı ile ilgili raporlar düzenlenebilmektedir.

WEB Sunucusu: Web sunucularında tutulan çerez, hata ve erişim logları SIEM' aktarılmalıdır. SQL enjeksiyon saldırıları veya hizmet reddi saldırıları da dahil olmak üzere en yaygın ve tehlikeli web sunucusu saldırılarının belirlenmesi, sunucunun önemli ve gizli verilerinin saldırılara karşı tepki verebilmek adına bu logların toplanması, üzerinde analiz yapılması önemlidir.

E-Posta Sunucusu: E-postadan alınacak loglar sayesinde, alıcı-gönderici mail bilgisi, mail konu başlığı, mail EK bilgisi gibi bilgiler ışığında olay analizi yapılabilmektedir. Örneğin bir veri sızıntısı var ise adli vakalarda tespit için bu bilgiler faydalı olmaktadır.

E-Posta Gateway: Ağda konumlandırılan e-posta uç nokta sistemleri maillerin içerisinde bulunan zararlıları tespit etmekte ve koruma sağlamaktadır. Bu sistemlerden alınacak loglar sayesinde zararlı mail atan göndericilerin sahip oldukları IP adreslerinin başka noktalardaki trafikleri engellenebilir, zararlı dosyaların bilgileri sistemdeki diğer güvenlik ürünleri (anti-virüs gibi) ile paylaşılabilir ve kullanıcıların bilgisayarlarında bu dosyaların alınması halinde engelleme sağlanabilir. Yazılacak korelasyonlarla kurum ağından dış ağda bulunan harici posta adreslerine atılan mailler tespit edilebilir.

Veritabanı Güvenlik Duvarı: Bu sunuculardan alınacak loglar sayesinde veritabanı kullanıcıları, oturum saatleri, yapılan işlemler (UPDATE, DELETE, INSERT gibi sql sorguları, veritabanı silme, kopyalama vb.) gibi bilgilerin aktarılması, kritik verilerin korunması, saldırı sonrası için delil sunma, saldırı öncesi tedbir alabilmek için gerekmektedir.

Anti-Virüs Yazılımlar: Anti-Virüs yazılımlarında kullanıcıların bilgisayarlarında tespit edilen zararlı dosyaların sayısı ve etkisi SIEM'e aktarılmalıdır. Böylece bir kullanıcı bilgisayarında anormal sayıda virüs bulaşırsa SIEM'de alarm yazılabilmektedir.

Microsoft DHCP: DHCP, ağdaki cihazlara IP adresi, ağ maskesi, ağ geçidi ve dns adresleri gibi bilgileri otomatik olarak atamak için kullanılan servistir. Bu olayların SIEM'e aktarılması bir olay tespiti, problem çözümleri, raporlama için etkili olacaktır.

Sysmon: Sysmon, kullanıcı bilgisayarında gerçekleşen işlemleri izlemeyi sağlayan bir araçtır. Doğru yapılandırılırsa, şüpheli davranışlar Sysmon tarafından algılanabilir. Bu olaylar SIEM'e aktarılarak kritik olaylar (powershell ile şüpheli komutların çalıştırılması gibi) tespit edilebilir.

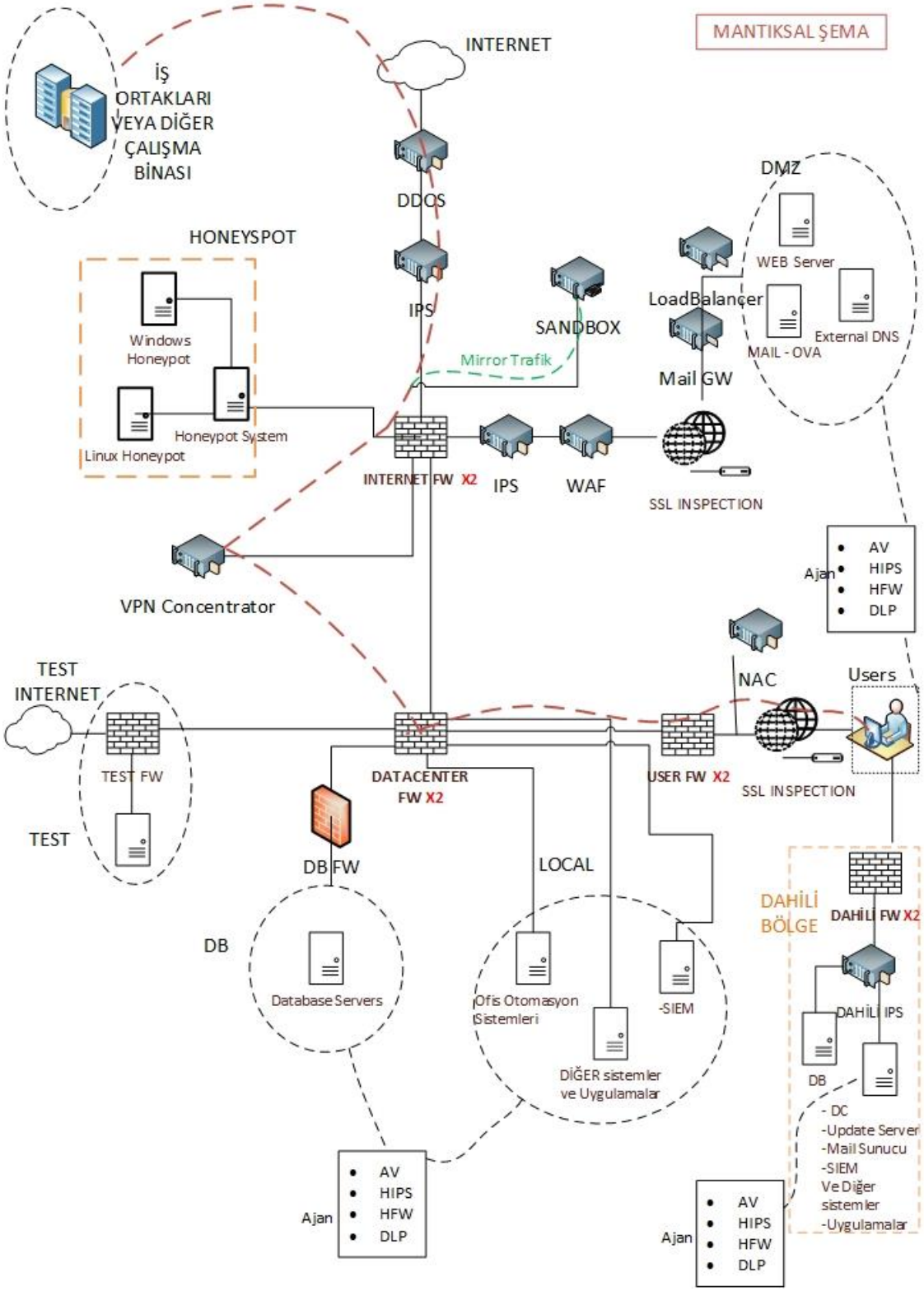
Audit Logları: Denetim günlüğü (Audit Log), bilgi teknoloji sistemindeki bir olayı kaydeden belgedir. Hangi kaynaklara erişildiğini belgelemenin yanı sıra, denetim günlüğü girdileri genellikle hedef ve kaynak adresleri, zaman damgası ve kullanıcı oturum açma bilgilerini içermektedir.

Tüm sistemler (güvenlik duvarları, IPS, WAF, işletim sistemi vb) audit logu üretmektedir. Dolayısıyla tüm sistemlerden hangi kullanıcı, ne zaman oturum açmış gibi bilgilerin edinilmesi olay tespit ve raporlama için önemlidir.

Bazı sistemlerden alınacak log türleri yukarıdaki gibidir. Hangi cihazlardan hangi logların SIEM'e alınacağı tamamen sistemde yer alan cihazlara ve ihtiyaçlara göre değişmektedir. Önemli olan ihtiyaçların ve aktarılacak logların spesifik olarak belirlenmesidir. Bu durumda iki yöntem bulunmaktadır. Birincisi tüm cihazlardan logların filtreleme yapılmadan alınması ve daha sonra ihtiyaçlara göre kısıtlamaya gidilmesidir. Diğer yöntem ise ihtiyaçlar belirlendikten sonra log almaya başlanmasıdır.

3.4.5. Veri Merkezi Mantıksal Güvenlik Tasarımı

Bir güvenlik tasarımına karar verilirken ihtiyaçlar temel alınmalıdır. İhtiyaçtan fazla satın alınan çözümler ek maliyet, ihtiyaçtan az alınan satın alınan çözümler ise güvenlikten taviz verilmesi demektir. Şekil 3.1'de kritik sistemler barındıran kurumlar için örnek güvenlik tasarımı yer almaktadır. Bu tasarım tamamen örnek olması açısından bu çalışma özelinde tasarlanmıştır. Tasarlanan tasarım ve çizimde yer alan ürünler bu çalışma doğrultusunda tasarlanmış olup herhangi bir kurum veya kuruluşta kullanıldığı anlamına gelmemektedir. Her veri merkezinin topolojisi birbirinden farklıdır ve kendisine özeldir. Şekil 3.1'de gösterilen mantıksal çizimdeki amaç, kritik sistemlerin barındığı yerlerde güvenlik noktasında maksimum faydanın sağlanması için örnek teşkil etmesidir.



Şekil 3.1: Örnek Mantıksal Güvenlik Tasarımı

Şekil 3.1'de yer alan tasarımda İnternet, DMZ, Local, DB (Database), Test, Honeypot, Users olmak üzere 7 farklı güvenlik bölgesi yer almaktadır. Bölüm 3.4.3 alt başlıklarında bu

bölgelerde hangi ürünlerin olduğu, bu bölgelerde yer alan sistemlerin hangi güvenlik çözümleriyle korunduğu incelenmiştir.

3.4.5.1. Uç Nokta Güvenliği

Uç noktada, internet üzerinden gelecek tehditlere karşı ilk korumanın sağlandığı, ağa yönelik saldırıların engellendiği bölümdür.

Şekil 3.1'deki tasarıma göre internet üzerinden yapılan sistemlerin çalışmasının durdurulmasına yönelik ataklara karşı korunabilmek için ağın en uç noktasına DDoS (Distributed Denial of Service) cihazı yerleştirilmiştir. DDoS hizmeti ISP (Internet Service Provider) hizmeti olarak da satın alınabilir. Fakat ISP hizmetini atlatabilecek bir saldırının gerçekleşmesi veya ISP hizmetinin bir sebepten devre dışı kalması durumunda ağa yerleştirilen DDoS cihazı sayesinde katmanlı güvenlik sağlanmış olunacaktır.

DDoS cihazının ardından ağın uç noktasında IPS cihazı konumlandırılmıştır. IPS, paketlerin başlıklarını ve yüklerini analiz ederek çalışmakta ve şüpheli davranışlar tespit edilirse o paketleri düşürebilmektedir. Kısacası IPS, tüm ağ paketlerini analiz ederek, güvenlik duvarı kurallarını ihmal etmeyecek olası kötü niyetli davranışları tespit etmekte ve imza veritabanı kullanarak ağdaki zafiyetlerin istismar edilmesine karşı güvenlik sağlamaktadır [66]. IPS, ağın ucunda inline olarak konumlandırıldığında tüm ağ trafiği bu cihazın üzerinden geçeceği için IPS'in gücü çok önemlidir. Ayrıca, false positive durumların yaşanmaması için IPS'in üzerinde bulunan imzalar kontrollü açılmalıdır. Örneğin ilk etapta CVE-2019-0708 - Remote Desktop Services Remote Code Execution Vulnerability [63] gibi kritik imzalar açılmalıdır. Diğer imzalar ilk izleme modunda açılarak takip edilmelidir. İzleme modunda yakalanan trafikler, sunucu/uygulama sahipleriyle de konuşularak false positive bir durum yok ise engelleme modunda ilgili imza açılmalıdır.

Ağın uç noktasına DDoS ve IPS cihazlarının yerleştirilmesinin ardından Şekil 3.1'deki topolojide güvenlik duvarı konumlandırılmıştır. DDoS ve IPS ile ağa gelen giden tüm trafikler denetlenmesi hedeflenmektedir. Veri merkezi ağına giriş/çıkış yapacak trafiklerin belirlenmesi amacıyla IPS cihazı ile güvenlik duvarı entegre edilmiştir. Bu güvenlik duvarında 6 adet bağlantı noktası bulunmaktadır. Bu bağlantı noktalarında, VPN (Virtual Private Network) Concentrator, veri merkezi çıkışında konumlandırılan WAF (Web

Application Firewall), iç ağ güvenlik duvarı, Sandbox cihazı, honeyspot sistemi ve DMZ bölgesi ağını koruyan IPS cihazı bulunmaktadır.

Ağın uç noktasında konumlandırılan VPN Concentrator, VPN bağlantılarının güvenli bir şekilde oluşturulmasını ve VPN düğümleri arasında mesaj gönderilmesini sağlayan bir tür ağ cihazıdır. Veri merkezinin ortak iş yürüttüğü kurum ve kuruluşların kullandıkları servisler, dosya aktarımları gibi süreçler güvenli tüneller üzerinden çalıştırılmalıdır. VPN bağlantıları genellikle güvenlik duvarları üzerinden yapılmaktadır. Ancak bu bağlantıların yalıtılması ve ayrıştırılması katmanlı güvenlik sağlayacaktır.

Ağın uç noktasında honeypot alanı bölgesi tanımlanmıştır. Bu bölgede yer alan honeypot sistemleri, bilgisayar korsanlarının dikkatini dağıtmak ve kritik dosyalardan uzak tutmak için kasıtlı olarak ağa yerleştirilen sahte hedeflerdir. Bir bal küpü uygulamak için birçok yaklaşım bulunmaktadır. En yaygın olanlarını, güvenliği olmayan, güncellemeleri eksik, zayıf parola kullanılmış hesaplara sahip olan çok fazla zafiyet içeren bir PC (personal computer) veya sanal makineler oluşturmaktadır. Amaç, saldırgana gerçek bir sisteme saldırdığını düşündürmek ve hareketlerini takip edebilmektir. Veri merkezlerinde birbirine bağlı çok sayıda honeypot cihazlar kurularak birbirine bağlanabilmekte ve savunmasız bir ağ oluşturulabilmektedir. Çünkü saldırganlar bir sistemi ele geçirdikten sonra ilk hedefi başka sisteme atlamaktır. Saldırganların gerçek ağa erişmesine izin vermemek için ayrı ağda yani farklı bir Vlanda (Virtual Lan Area Network) tutulmalıdır.

Veri merkezi ağının uç noktasında bulunması gereken ve sistemlerin güvenliğini sağlama konusunda yardımcı olabilecek diğer bir güvenlik çözümü de ağda sandbox çözümüdür. Bilinmeyen yazılımların çalıştırılması, bilinmeyen kaynaklardan gelen videoların veya başka dosyaların indirilmesi gibi aktiviteler sistemlere virüs bulaştırabilir ve böylece sistemler her türlü riske açık hale gelebilir. Ağın ucundaki güvenlik duvarına gelip ve giden tüm trafiğin bir kopyası sandbox ürününe yönlendirilmelidir. Mirror trafiğin alınmasının sebebi, sandbox ürünü üzerinde dosyalar taranırken trafiğin ilgili noktaya ulaşmasındaki gecikmeyi azaltmaktır. Böylece ağda akan trafikteki tüm dosyalar sanbox içerisindeki sanal cihazlarda çalıştırılacak ve sonuç dönecektir. Sandbox ürünü bir dosyanın zararlı olduğunu anladıktan sonra tüm sistemlere bu dosyanın zararlı olduğunu bildirebilmeli ve bu dosyanın engellenmesi gerektiğini iletebilmelidir. Ancak buradaki risk, potansiyel zararlı bir dosya sandbox çözümü tarafından taranırken, başka bir güvenlik ürünü bu dosyanın zararlı

olduğunu tespit edemezse bu dosya alıcıya ulaşacaktır. Eğer alıcı üzerindeki anti-virüs tarafından da bu dosyanın zararlı olduğu algılanamazsa veya alıcı üzerinde anti-virüs yok ise zararlı alıcı cihaza bulaşacaktır.

3.4.5.2. DMZ Bölge Güvenliği

DMZ bölgesi, savunmasız bölge olarak adlandırılmaktadır. Veri merkezinin internete açık servisleri burada konumlandırılmaktadır. Bu sayede iç ağdaki sistemleri çok tehlikeye atmadan FTP sunucusu, mail sunucusu, web sunucusu, proxy sunucu, dış dns sunucu gibi dış dünya ile sürekli bağlantı halinde olan sunucular bu bölgede yer almalıdır. Kritik servisler bu sunucular ile aynı ağda hizmet vermemelidir. Aksi takdirde internete bağlı bir sunucu istismara uğradığında, kritik sunucular da bu tehlikeden etkilenebilmektedir.

Bu bölgede ağın uç noktasında bulunan IPS cihazına ek olarak yine bir IPS cihazı konumlandırılmalıdır. Bunun sebebi, hem katmanlı güvenlik sağlamak hem de ağın ucunda yer alan IPS cihazı tüm ağın trafiğini üzerinden geçirmektir. Bu IPS üzerinde yapılan tüm değişiklikler (bir imzayı aktif etmek gibi) tüm ağı etkileyecektir. Dolayısıyla ağın uç noktasında yer alan IPS yapılandırması ile DMZ bölgeisnde bulunan IPS yapılandırmasının aynı olması beklenmemelidir. DMZ bölgesinde uygulamalara yönelik daha sıkı kurallar uygulanabilir. Fakat bu sıkı kurallar ağın uç noktasında da uygulanırsa, iç ağdaki uygulamalar üzerinde false positive durumlar yaşanabilir.

Veri merkezinde hizmet veren web uygulamalarının korunması için WAF cihazı DMZ bölgesinde konumlandırılmalıdır. Bu cihaz güvenlik duvarından sonra ve sunucuların önünde konumlandırılmalıdır. Şekil 3.3'deki örnek topolojide IPS'in arkasında konumlandırılmıştır. En sık rastlanan sorulardan birisi de güvenlik duvarı varken neden WAF kullanılması gerektiğidir. Ağ güvenlik duvarı, port, IP veya uygulama bazlı engellemeler yaparken, WAF sadece web uygulamalarına yönelik saldırılara odaklanmaktadır.

DMZ bölgesinde alınması gereken güvenlik tedbirlerinden birisi de SSL (Secure Socket Layer) Inspection'dır. SSL denetimi tüm trafiği durdurmakta, şifresini çözmekte ve her HTTPS web sitesi üzerinden veri iletildiğinde kötü amaçlı içerik taraması yapmaktadır. Birçok güvenlik çözümü SSL trafiğin içindeki kötü amaçlı yazılımları algılayamaz. Zscaler'a göre, bugünkü kötü amaçlı yazılımların %50'si SSL trafiğinde

saklanmaktadır [67]. Bu nedenle SSL denetimi içeren bir güvenlik çözümü kullanılması önem arz etmektedir. Ancak burada dikkat edilmesi gereken durum, SSL incelemesinin yapılması için Web Filtreleme ve UTM cihazlarının kullanılmamasıdır, aksi halde gecikme süreleri çok artacaktır [67].

Bu bölgede yer alan diğer bir ürün Mail Gateway (e-posta geçiş noktası) ürünüdür. Bir kuruluşun e-posta ağ geçidi, gelen veya giden her e-postanın geçtiği e-posta sunucusudur. Lotus Microsoft Exchange gibi mail sunucu kullanan veri merkezleri gelen ve giden elektronik postalarını kontrol ederek virüs, spy spam içerik gibi taramalardan ya da kurallardan geçirmektedir.

3.4.5.3. Local Bölge Güvenliği

Bu bölgede veri merkezine ait kritik sunucular veya orta dereceli kritik sunucular yer almalıdır. Örneğin, kurum mail sunucusu, anti-virüs, SIEM, SOAR, active directory, güncelleme sunucuları ve diğer kritik sistemler konumlandırılmalıdır. Bu bölgedeki sunucuların internet üzerinden gelecek zararlı aktivitelere karşı dış dünyaya erişimi olmamalıdır. Bu bölgede yer alan tüm sunucular diğer sistemlerden ayrıştırılabilmeleri için farklı sanal yerel alan ağında olmalıdır.

Şekil 3.1'deki genel topolojide merkezi güvenlik duvarı bulunmaktadır. Bu güvenlik duvarında, TEST bölgesi güvenlik duvarı, veritabanı bölgesi, users (kullanıcılar) bölgesi güvenlik duvarı ve local bölgesi sunucularının bağlı olduğu bağlantı noktaları bulunmaktadır.

Örnek topolojideki bu bölgede yeni nesil güvenlik duvarı konumlandırılmıştır. Bir yeni nesil güvenlik duvarı en az üç temel işleve sahip olmalıdır: Kurumsal güvenlik duvarı yetenekleri, izinsiz giriş önleme sistemi ve uygulama kontrolü. Geleneksel güvenlik duvarlarının aksine yeni nesil güvenlik duvarı konumlandırılmasındaki amaç, OSI referans modelinde 7. Katmana kadar güvenlik sağlamaktır.

Güvenlik duvarında uygulanacak güvenlik politikaları sıkılaştırılmış olmalıdır. Örneğin, kullanıcıların DNS (Domain Name System) istekleri için yazılan güvenlik kuralı yalnızca 53. Portundan geçmelidir. Bir web uygulaması 80 veya 443 portlarını kullanıyor ise yalnızca bu portlar üzerinden erişim sağlanmalı ve bu portlar dışında gelen istekler engellenmelidir. Yeni nesil güvenlik duvarlarında port bazlı değil, uygulama bazlı erişimler tanımlanmalıdır.

Örneğin Windows uzak masaüstü bağlantısı yapmak isteyen bir kullanıcı TCP 3389 ve UDP 3389 portlarını kullanmaktadır [68]. Güvenlik kuralında 3389 portuna erişim izni vermek demek 3389 portunu kullanmak isteyen tüm trafiğe erişimi açmak demektir. Bu yüzden yeni nesil güvenlik duvarlarında uygulama bazlı erişim tanımlanarak hangi kaynağın hangi uygulama üzerinden geldiği anlaşılabilmektedir. Örnek kural:

- Kaynak IP: 10.10.10.10
- Kaynak Kullanıcı: akpinar\ali
- Kaynak Bölge: Users
- Hedef IP: 10.10.11.11
- Hedef Bölge: Local
- Uygulama: ms-rdp
- Servis: 3389 veya varsayılan port

Yukarıdaki örnek güvenlik politikasına göre "Users" bölgesinde, kaynak IP'si 10.10.10.10,ve akpinar domainindeki ali kullanıcısı, "Local" bölgesindeki 10.10.11.11 sunucusuna, RDP (remote desktop control) uygulaması kullandığında yalnızca 3389 portunu kullanabilsin. Eğer RDP uygulaması kullanmıyorsa 3389 portundan gelse dahi bu kullanıcının trafiği engellenecektir.

Local bölgede, SIEM ve SOAR gibi ürünler de bulunmalıdır. SIEM ile güvenlik verileri merkezi bir noktada toplanmakta, depolanmakta ve daha sonra işlem yapılabilmesi için istihbarata dönüştürülmektedir. Güvenlik verileri Şekil 3.1'deki gibi bir veri merkezinde yer alan tüm güvenlik sistemlerinin günlükleri, sunucuların günlükleri, uygulama günlükleri, ağ günlüklerini içerebilir. Fakat önemli olan ihtiyaçlar doğrultusunda verilerin toplanmasıdır. Amaç her veriyi almak değil, alınan veriden verim alabilmektir. Verinin toplanmasının ardından bu günlükler analiz edilebilmekte ve uyarı aracı olarak kullanılabilmektedir.

SIEM gibi SOAR sistemi de güvenlik ekiplerinin üretilen alarmları yönetmesine yardımcı olmaktadır. Bununla birlikte, SOAR, kapsamlı bir veri toplama, standardizasyon, vaka yönetimi, iş akışı ve analitiği birleştirerek işletmelerin derinlemesine savunma yeteneklerini uygulamalarına izin vermek için işleri bir adım daha ileri götürmektedir [69]. Özetle, SOAR

tüm güvenlik araçları, uygulamaları ve sistemleri ile entegreli çalışmakta ve güvenlik ekiplerinin sıradan, zaman alan ve tekrarlayan manuel görevlerini otomatikleştirmesini ve düzenlemesini sağlamaktadır. Güvenlik uzmanları, SIEM ve SOAR platformlarının siber tehditlere karşı kolektif bir savunma sağlamak adına birlikte çalışabilmesini önermektedir. Gartner'a göre, beş kişiden daha büyük bir güvenlik ekibine sahip işletmelerin %15'i 2020'nin sonuna kadar SOAR'dan faydalanması beklenmektedir [70].

3.4.5.4. Veritabanı Bölge Güvenliği

Veritabanı bölgesinde kritik verilerin depolandığı veritabanı sunucuları yer almalıdır. Bu verilerin zarara uğramaması için diğer bölgelerden (DMZ, Local vb.) farklı ağda konumlandırılması gerekmektedir. Bu bölgedeki sunucular kritik veriler barındırmakta ve kesinlikle internet bağlantısının olmaması gerekmektedir. İnternet üzerinden gelecek bir saldırı, kritik verilerin tahribata uğramasına, değiştirilmesine veya kaybedilmesine sebep olabilmektedir. Bu doğrultuda sunucular, merkezi güncelleme sunucusu üzerinden çevrimdışı olarak güncellemelerini almalıdır [71].

Veritabanı bölge güvenliğinde yer alan veri tabanlarının korunabilmesi için en etkili yöntemlerden birisi veritabanı güvenlik duvarının kullanılmasıdır. Kullanılan güvenlik duvarı, veritabanı etkinliklerini gerçek zamanlı olarak izleyebilmeli, yetkisiz SQL etkinliğinin yanı sıra, protokol ve işletim sistemi düzeyinde saldırılar arayan veritabanına giden trafiği de analiz edebilmelidir. Uygulama ve kullanıcı yetkisine bakmaksızın bu saldırılara karşı koyabilmelidir. Yetkisiz erişim veya şüpheli sorgular yapan kullanıcıların hakları incelenip onaylanana kadar karantinaya alınabilmelidir. SQL Injection gibi gelişmiş uygulama saldırılarına karşı ek koruma sağlayabilmek için entegre WAF özelliği de bulunmalıdır. Ayrıca sürekli denetim özelliği bulunmalı ve hangi kullanıcı, hangi tabloda hangi sorguyu çalıştırdı gibi bilgileri raporlayabilmelidir. Güvenlik açıklarının istismar edilmesini önlemek için, veritabanında olan açıklıkları sanal yama özelliği ile giderebilmelidir.

Veritabanı güvenlik duvarı kural yapılandırılması yapılırken, veritabanı yöneticileriyle birlikte çalışılmalıdır. Hangi veritabanına hangi kullanıcı erişmeli, hangi tablo kritik, hangi sorgu çalıştırılmamalı gibi bilgiler veritabanı yöneticilerinden alınmalıdır. Alınan bilgiler

ışığında oluşturulan kural politikalarının sonuçlarına göre raporlamalar yine veritabanı yöneticilerine gönderilmelidir.

Veritabanı güvenlik duvarları ağa in-line olarak konumlandırılabilmekte veya veritabanı sunucularına kurulan ajanlar ile çalışabilmektedir. Güvenlik duvarı üzerinde oluşturulacak kurallara dikkat edilmelidir. Aksi takdirde doğru aktivitelerin engellenmesine yol açabilmektedir.

3.4.5.5. Son Kullanıcı Bölge Güvenliği

Şekil 3.1'de yer alan "Users" bölgesinde, çalışan personellerin bilgisayarları, tarayıcılar gibi son kullanıcıya hizmet edecek sistemler bulunmalıdır.

Dış ağdan gelen saldırıların iç ağdaki bir sisteme ulaşması çok zordur. Çünkü saldırganın bir sisteme ulaşması içi arada WAF, IPS, DDoS, güvenlik duvarı gibi güvenlik ürünlerinin her birini atlatması gerekmektedir. Bir sistemin en zayıf halkası insandır. Sisteme sızma çalışmaları başarısız olan saldırganların öncelikli hedefleri veri merkezi personellerinin bilgisayarları olacaktır. Bunu başarmak için oltalama mailleri gibi çeşitli saldırı metotları kullanacaklardır.

Riske Dayalı Güvenlik (RBS- Risk Based Security) 2019 yılı raporunda bir önceki yıla göre veri ihlallerine yönelik saldırılarda %33.3'lük bir artış olduğunu ortaya koyulmuştur [72]. Yaşanan veri ihlalleri incelendiğinde insan hataları ön plana çıkmaktadır.

Kullanıcı kaynaklı zafiyetlerin önüne geçilebilmesi için alınması gereken başlıca tedbirler;

- Kullanıcıların internete çıkışlarında güvenlik duvarında anti-virus, anti-spyware, vulnerability protection, file blocking, url filtreleme, DoS protection gibi filtreleme işlemleri uygulanmalıdır.
- Veri sızıntılarının önüne geçilmesi için güvenlik politikalarında sosyal medya, VPN kullanımı ve peer to peer uygulamaları engellenmelidir.
- Kullanıcı bilgisayarlarında device blocking, vulnerability protection, web reputation gibi gelişmiş özellikleri bulunan anti-virüs yazılımları yüklü olmalıdır.

- Kullanıcıların harici hard disk, USB gibi cihazları kullanımı engellenmelidir. USB cihazı kullanacak kullanıcılara cihaz bazlı erişimler tanımlanmalıdır. Her kullanıcının kullanacağı USB cihaz tanımlı olmalıdır.
- Kullanıcıların bilgisayarlarında gerçekleşen işlemlerin takip edilmesi için Sysmon gibi araçlar kullanılmalıdır.
- Güçlü parolalar kullanılmalı ve bu parolalar 30 günde bir değiştirilmelidir.
- Kullanıcının internet çıkışında HTTPS sayfaların incelenmesi için SSL Inspection yapılmalıdır.
- Veri sızıntılarının önüne geçilebilmesi için DLP (Data Loss Prevention) çözümleri kullanılmalıdır.
- En az yetki prensibine göre hareket edilmelidir. Kullanıcıların sistemlere (veritabanı, uygulama sunucuları vb.) erişimleri denetlenmelidir. Verilen haklar, ihtiyaç kadar olmalıdır.
- VPN erişimlerinde, internet üzerinden kurum mailinin kullanılması gibi durumlarda iki faktörlü kimlik doğrulaması kullanılmalıdır.
- Ağ güvenliğinin en temel yöntemlerinden birisi olan NAC (Network Access Control) kullanılmalıdır. NAC 802.1x protokolü kullanılarak ağa dâhil olmak isteyen kullanıcı bilgisayarlarının MAC adresleri kullanılarak yapılmaktadır.
- Ağ katmanında yer alan güvenlik duvarları haricinde kullanıcı bilgisayarlarında faaliyet gösterebilecek host-based firewall kullanılabilir. Ağ güvenlik duvarları aynı vlanda yer alan trafiklerin kontrolünü sağlayamamaktadır. Host-based firewall sayesinde yatay trafiklerden gelecek tehlikelere karşı koruma sağlanmış olacaktır.
- NAC çözümü ile kurum domaininde olmayan bilgisayarların kurum ağına bağlanmaları engellenebilmektedir. Bunun için güvenlik duvarında bir karantina zone'u (bölgesi) oluşturulmalıdır. Kurum domaini dışında olan bilgisayarlar kurumda bulunan bir internet portuna bağlandıklarında DHCP üzerinden karantina IP'si almalıdırlar. Güvenlik duvarında bu IP'ye sahip tüm cihazların erişimleri her yere kapatılmalıdır.

Bu tedbirlerin kapsamı daha da genişletilebilir. Siber dünyada en zayıf halka insandır. Bu yüzden son kullanıcıların bulunduğu ortamlarda güvenlik tedbirleri en katı şekilde alınmalıdır.

3.4.5.6. TEST Bölgesi Güvenliği

Veri merkezlerinde hayata geçirilecek projelerin, ilk defa kullanılacak güvenlik ürünlerinin, yazılımların veya uygulamaların nasıl bir aksiyon göstereceği tahmin edilemeyebilir. Bu durum canlı sistemlere zarar verebilir. Bu yüzden bu sistemlerin canlı olarak kullanılmadan önce çalışan sistemleri tahribata uğratmamak için test ortamında çalıştırılması gerekmektedir.

Test bölgesi harici bir güvenlik duvarı arkasında konumlandırılmalıdır ve iç ağ ile bağlantısı güvenlik duvarı aracılığı ile kesilmelidir. Test ortamının veri merkezinden ayrı internet çıkışı olmalıdır. Böylece test ortamında meydana gelebilecek bir zafiyetin iç ağdaki sistemlere bulaşmasının önüne geçilebilecektir.

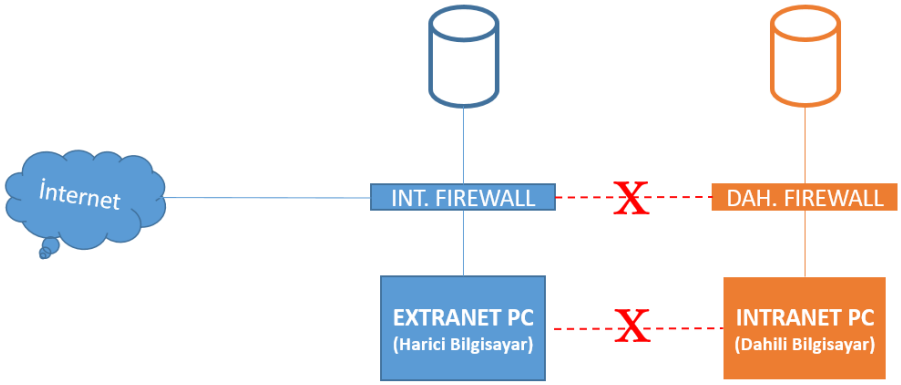
3.4.5.7. Honeypot Bölgesi

Bir bal küpü, çekici bir hedef gibi görünen ancak gerçekte saldırganlar (iç veya dış) için bir tuzak olan ayrı bir sistemdir. Örneğin, finansal veritabanı gibi görünen ancak aslında yalnızca sahte kayıtları olan bir sunucu konumlandırılabilir. Bal küpü alanı ile ilk olarak, aradıklarını bulduklarına inanan saldırganlar, diğer sistemleri en azından bir süreliğine yalnız bırakacaktır. Diğer bir nokta ise, honeypot'lar gerçek sistemler olmadığından, hiçbir meşru kullanıcı ona erişemez ve bu nedenle orada son derece ayrıntılı izleme ve günlük kaydını açılabilir. Bir saldırgan ona eriştiğinde, soruşturmaya yardımcı olacak etkileyici miktarda kanıt toplanabilir. Honeynet, bir honeypot'un bir sonraki mantıksal uzantısıdır ve çok cazip bir hedef gibi görünen sahte bir ağ segmentidir.

3.4.5.8. Dâhili Bölge

Dâhili bölgede bulunan sistemlerin internet bağlantısı ve internet bağlantısı olan herhangi bir sistemle bağlantısı olmamalıdır. Bu bölgede tüm riskler minimize edilmelidir. Bu bağlamda sıkılaştırılmış güvenlik önlemleri alınmalıdır. Güvenlik cihazlarına ek olarak harici disk kullanımı kullanıcılara yasaklı olmalı, Wi-Fi, bluetooth özelliği olmayan (olsa dahi bu özellikler aktif olmamalı ve kullanıcı kullanamamalıdır) bilgisayarlar verilmelidir.

Şekil 3.2'de gösterildiği gibi dâhili bölge sistemlerinin, internet tarafındaki sistemlerle bağlantısı olmamalıdır.



Şekil 3.2: Dâhili Ağın, İnternet Ağından Yalıtılması

3.4.6. Bilgi Güvenliğinde Önemli Noktalar

Kurum ve kuruluşların faaliyetlerinin yürütülmesinde kullanılan verilerin anlam kazanmış haline bilgi denmektedir. Bilginin korunması, ticari ve itibar açısından önemlidir. Bilgi güvenliği de bu doğrultuda önem kazanmaktadır. Bilgi güvenliğinde gizlilik, bütünlük ve süreklilik olmak üzere üç temel yaklaşım bulunur.

Gizlilik: Bilginin yetkisiz kişilerin eline geçmesinin ve yetkisiz erişimlerin önlenmesi

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmesi, tahrip edilmesi

Süreklilik: Bilginin yetkisi olan kişiler tarafından gerektiğinde erişilebilir olmasıdır.

Bilgi güvenliğin sağlanması için çok farklı etkenler bulunmaktadır. Kullanıcının bilgisayarından ağın en ucundaki güvenlik duvarına kadar arada geçen tüm güvenlik cihazları bilgi güvenliğine katkı sağlamaktadır. CyberMag dergisi Ocak 2020 yayınlanan Cemile Denerel Başak'ın "Bilgi Güvenliğinde 7 Önemli Husus" başlıklı makalesine göre bilgi güvenliği 7 sınıfa ayrılmıştır [73]. Her sınıfın kendi altında kullanılan çözümlerle birlikte bu başlıklar nelerdir?

1. Ağ güvenliğinin sağlanması için kullanılabilecek çözümler:
    - İçerik Güvenliği

E-Posta

Web

- Çevresel Güvenlik

  Firewall/UTM

  VPN

  IPS

  NAC

  Wireless

  İzleme

  Yönetilir Servisler

  İzleme

2. Son Kullanıcı Güvenliği için Kullanılabilecek Çözümler

   - Son kullanıcı güvenliği

     Application Device Control

     Anti-Virüs

     Host Firewall

     HIPS (Host-based intrusion detection system)

     Application White List

   - Device Control

     Disk Şifreleme

     Mobil Güvenlik

Uzaktan Erişim

3. Veri Güvenliği için Kullanılabilecek Çözümler:

- Verittabanı Güvenliği
- Veritabanı Değerlendirme
- Veritabanı Aktivite Kontrolü
- Veritabanı Şifreleme
- Veri Sızıntısı Önleme
- DLP çözümleri

  Ağ DLP

  Uç nokta DLP
- İçerik Keşfi
- Erişim Yöntemi

  Yetki Verme

  Dosya Aktivitesi İzleme

4. Uygulama Güvenliği için Kullanılabilecek Çözümler

- Web Uygulama Güvenliği (WAF)
- Uygulama Testi

  Dinamik Uygulama Testi

  Statik Uygulama Testi

  Güvenli Geliştirme

  Tehdit Modelleme

  Geliştirme Süreci

Test Metodolojileri

5. Web Uygulama Değerlendirme
6. Web Güvenlik Açığı Değerlendirmesi
7. Web Penetrasyon Testi
    - Yönetilir Servisler

      Değerlendirme/Testler
    - Yönetilir Web Uygulama Güvenlik Duvarları
8. Kimlik ve Erişim Yönetimi için Kullanılabilecek Çözümler
    - Dizinler
    - Kimlik Doğrulama
    - Hazır Hale Getirme
    - Web erişim yönetimi
9. Güvenlik Yönetimi için Kullanılabilecek Çözümler

    - Uyumluluk/Uygunluk

      PCI

      SOX (Sarbanes-Oxley)

      HIPAA

      Gizlilik/Mahremiyet
    - Güvenlik Operasyonları

      Güvenlik Bilgi ve Olay Yönetimi (SIEM)

      Log Yönetimi
    - Sistem Yönetimi

Yama Yönetimi

Konfigürasyon Yönetimi

- Güvenlik Açığı Yönetimi

  Güvenlik Açığı Değerlendirmesi

  Penetrasyon Testi

- Olay Müdahale

10. Sanallaştırma ve Bulut Güvenliği için Kullanılabilecek Çözümler

- Sanallaştırma Güvenliği

  Sanal Makine Güvenliği

  Sanallaştırma Altyapı Güvenliği

  Bulut Güvenliği

- Bulut Güvenlik Servisleri

  Bulut Güçlendirme

  Bulut Risk Yönetimi

Bahsedilen güvenlik çözümlerinin tamamını satın almak ve kontrol etmek yüklü bir maliyet gerektirmektedir. Kritik ve çok sayıda sistem içeren altyapılarda, veri merkezlerinde bu sistemlerin tamamı tercih edilebilir. Ayrıca, sistemleri kullanacak yetkin personelin de olması gerekmektedir. Hangi sistemin hangi ihtiyacı karşılandığı iyi bilinmeli ve ona göre satın alınmalı ve kullanılmalıdır.

3.4.7. Olay Müdahale Planı

Olay müdahale planı, bir güvenlik ihlali veya siber saldırı sonrasında ele alınacak ve yönetilecek organize yaklaşımları ifade etmektedir. Amaç, bir problem esnasında hasarın boyutunu sınırlandırabilmek ve iyileşme süresi ile maliyeti azaltabilmektir. Bu doğrultuda olay müdahale ekipleri kurulmaktadır. Bu ekipler genellikle BT personelleri, SOC (Security Operation Center) ekipleri [74] ile oluşmaktadır. Ancak ekip hukuk, insan kaynakları ve halkla ilişkiler departmanlarından temsilcileri de içerebilir.

Her kurumun ihlallere karşı olay müdahale planı olmalıdır. Bir olay müdahale planı, müdahale ekibinin bir olay gerçekleştiğinde izlediği talimatlar kümesidir. Bu müdahale planı, bir güvenlik olayının etkilerini tespit etme, bu olaylara müdahale etme ve sınırlama prosedürlerini içermelidir.

SANS Enstitüsü'ne göre [75], bir olay müdahale planının altı temel aşaması bulunmaktadır.

Hazırlık Aşaması: Kullanıcıların ve BT personelinin, ortaya çıkabilecek olası olaylarla başa çıkabilmeleri için hazırlanmaları gerekmektedir.

Olay Kimliğini Belirleme Aşaması: Bir olayın güvenlik olayı olarak nitelenip nitelenmediğinin belirlenmesidir.

Sınırlama Aşaması: Olayın zararını sınırlamak ve daha fazla hasarı önlemek için etkilenen sistemlerin izole edilmesidir.

Eradikasyon Aşaması: Olayın temel nedenini bulma ve etkilenen sistemleri ortamdan çıkarma aşamasıdır.

İyileşme Aşaması: Etkilenen sistemlerin tekrar ortama girmesine izin verilmemesi ve tehdidin tamamen ortadan kaldırılmasının sağlanmasıdır.

Rapor Aşaması: Gerçekleşen olay ile ilgili raporların oluşturulması, gelecekteki benzer olayların yaşanmaması için tedbirlerin alınmasıdır.

Olay yanıtının etkinliğini ölçmek için kullanılan belirli metrikler şunları içerebilmektedir:

- Tespit edilen olay sayısı.
- Kaçırılan olay sayısı.

- Eylem gerektiren olay sayısı.
- Tekrarlanan olay sayısı.
- Düzeltme zaman aralığı.
- İhlale yol açan olay sayısı.

Olay müdahale planları ile bir olay karşısında ekiplerin alacağı tedbirler yer almaktadır. Planlama aşaması kurumlara, sistemlere ve ekibin yeterliliğine göre değişebilmektedir. Bu kapsamda bir olay karşısında ne tür aksiyonlar alınacağı kalem kalem ortaya çıkarılabilmelidir. Böylece belirlenen talimatlar doğrultusunda bir saldırı esnasında ekipler nereye nasıl müdahale edeceğini bilip hızlı çözüm elde edebilecek ve riskin şiddeti azaltılarak önü kesilebilecektir.

3.5. Siber Tehditlerin Tespiti

Teknolojinin gelişimiyle birlikte sistemlerdeki açıklıklar ve tehditlerin sayısı da artmaktadır. Bir saldırıda hedef, BT sistemlerinin sahip olduğu uygulamalar, cihazlar veya bilgi varlıklarına zarar vermek ve sistemleri ele geçirmek olabilmektedir. Bu saldırılar siyasi, ticari ve kişisel sebepler için olabilmektedir. Siber varlıklara yönelik tehditlere bakıldığında siber saldırılara karşı alınması gereken güvenlik önlemlerinin önemi daha iyi anlaşılacaktır.

Kişisel, kurumsal hatta ulusal bilgi varlıkları, bir ülkede en önemli değerdir. Çünkü bilgi varlıklarının istismara uğraması durumu kurumsal veya kişisel imajların zedelenmesi, kurumlara veya kişilere olan güvenin sarsılması, iş gücü ve zaman kaybı, sistemi eski durumuna getirmenin yüksek maliyetlere yol açması, bilgi veya veri kaybı bazen de kaybedilenlerin hiç geri alınamaması gibi ciddi problemleri ortaya çıkaracaktır. Verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması itibar açısından korunmalıdır. Mevcut varlıkları korumak için; yangın ve sel gibi çok farklı kaynaklardan gelen tehlikelere karşı koymanın yanında virüslere, casus ve kötücül yazılımlara, APT saldırılarına, siber saldırılara, bilgisayar korsanlarına, hizmet saldırılarına karşı koyma veri merkezleri için önemlidir.

Siber saldırılar geliştikçe siber savunma araçları da gelişmekte fakat siber artışlar da azalma görülmemektedir. Çok sayıda saldırı türü, kötücül yazılım, saldırı türü bulunmaktadır.

Bunlardan bazıları, APT, casus programlar, açık portların kullanılması, virüs, zararlı e-postalar, oltalama, sosyal mühendislik saldırıları, yapay zekâ saldırı araçlarıdır [76].

Bilgi, her zaman saldırılar için hedeftir. Bir blog sitesi olan Medium.com'da güvenlik analisti Ertuğrul Akbaş'ın kaleminden yayınlanan "Siber Tehditleri Nasıl Tespit Edelim" başlıklı yazıda [77] saldırı tespiti için SIEM'de hangi yaklaşımların incelenmesi gerektiği ele alınmıştır.

3.5.1. Anomali Tespiti

Makine öğrenmesi: Sistemde bir hareketin normal durumun dışında yapılmasıdır. Sistem, gerçekleşen olayları takip etmekte ve hafızasına almaktadır. Öğrendiği olaylar belli bir rutinde sürekli olarak yapılıyorsa normal kabul edilmektedir. Bu normal durumda bir sapma, anormal bir değişikliğinin tespitinde makine öğrenmesi yöntemi kullanılmaktadır. Örneğin her gün 09:00-18:00 saatleri arasında çalışan bir servisin, 18:00'dan sonra çalışması halinde uyarılması gibi.

Eşik değerlemesi: Statik olarak belirlenen bir değerin aşılması durumlarının tespiti için kullanılmaktadır.

3.5.2. Davranış Analizi

Bir saldırı, ardışık davranış sergiliyorsa bunun tespitine yönelik bir metottur.

Örnek bir senaryo:

- Bir veritabanına arka arkaya 2 defa yanlış şifre girildikten sonra 5 dakika içerisinde başarılı bir oturum açılır ise
- Başarılı oturumun ardından 5 dakika içerisinde yeni bir kullanıcı oluşturulur ve özel yetkiler tanımlanırsa
- 5 dakika içerisinde özel yetki tanımlanmasının ardından oluşturulan yeni kullanıcı ile oturum açılırsa
- Yeni kullanıcıyla açılan oturumun ardından 5 dakika içinde kritik bir tabloda "SELECT", "DELETE" gibi SQL sorguları çalıştırılırsa

- Yapılan işlemin ardından 2-3 dakika içerisinde bu kullanıcı hesabı silinirse anormal bir durum söz konusudur.

Yukarıdaki senaryoda da görüldüğü gibi ardışık senaryolar oluşabilmekte ve bu senaryolar ile analiz yapılabilmektedir. Bu tür tespitler esnek ve ardışık aşamalardan oluşan senaryoları kapsamaktadır.

3.5.3. Referans liste analizi:

Bu analiz metodunda sistem bileşenlerinin anomali davranışları tespit edilmektedir. Örneğin bir uygulama yalnızca 80 portunu kullanmaktadır. Örneğin, 80 portu dışında bir porttan hizmetin tespit edilmesi gibi.

3.5.4. İstihbarat ile Tespit

Tehdit istihbaratı sağlayan kaynaklardan gelen IP veya URL'ler ile sistemde izlenen logların eşleşmesiyle oluşan tespit yöntemidir.

3.5.5. Verilerin Korunması

Üstünlük yarışı içerisinde olan devletler, istihbarat sağlamak isteyenler, ticari kaygısı olanlar, siyaset veya din amaçlı inançlara yönelik hacktivistler, hizmet durdurmaya yönelik saldırı yapan siber korsanlar veya intikam duygusu besleyen eski personel gibi kötü niyetli kişiler, devletler, kurumlar vs. bir veri merkezinin en değerli varlığı olan bilgi varlığına karşı saldırı yapmak isteyebilirler. Veri merkezleri içerisinde büyük veri barındırdığı için bir ekosistem yaratmaktadır. Güvenlik bakış açısıyla bu ekosistemin bütüncül şekilde ele alınıp, risklere karşı gerekli tedbirlerin alınması gerekmektedir.

Saldırılara karşı koyabilmek için temel olarak dört adım vardır [76].

1. Saldırı tespit ve koruma sistemi
2. Tehdit saptama sistemi
3. Saldırının ne zaman, hangi yolla, kim tarafından yapıldığının tespiti
4. Saldırılara karşı aksiyon alma

SIEM ile bu dört koruma adımına katkı sağlanabilmektedir. Korelasyonlar ile saldırı tespiti önceden yapılabilir, bir tehdidin nereden geldiğini, hangi sistemlere bulaştığı tespit edilebilir, tüm kaynaklarda log analizi yapılarak saldırıyı kimin yaptığı tespit edilebilir, yazılan alarmlar ile bir saldırı esnasında erken müdahale yapılabilir veya saldırıyı engellemek adına saldırıyı başlatan IP'nin tüm sistemlerde engellenmesi için sistemler uyarılabilir.

3.6. En Çok Bilinen Siber Saldırı Çeşitleri

Bir siber saldırı, veri veya bilgi sistemlerini çalmak, değiştirmek veya yok etmek için çeşitli yöntemler kullanarak bilgisayar bilgi sistemlerini, altyapılarını, bilgisayar ağlarını veya kişisel bilgisayar cihazlarını hedefleyen herhangi bir saldırı eylemidir.

Netwrix bloğunda yayınlanan en sık rastlanan 10 siber saldırı türü [78]:

3.6.1. Hizmet Durdurma Saldırısı

DDoS saldırıları olarak bilinen hizmet durdurma saldırıları, bir sistemin kaynağını tüketmek ve verdiği hizmeti kesintiye uğratmak için kullanılmaktadır. Bu saldırı, doğrudan sistem kaynaklarına yapılmaktadır.

Saldırıda, birçok farklı kaynak IP adresi aynı hedef IP adresini hedeflemekte ve yüksek bir hızda hizmet istemektedir. Hedef sistem bu meşru olmayan isteklere hizmet vermeye çalışırken bunalmakta, meşru taleplere hizmet veremez hale gelmektedir. DDoS saldırısının sistemik göstergesi, bir sunucu için bağlantı noktası veya protokolde aşırı yüksek bir talep oranını veya bir eşiği ihlal eden, bir uyarıyı tetikleyen davranışsal IDS (Intrusion Detection System) sensörü tarafından sağlanabilmektedir.

Farklı DoS ve DDoS saldırıları türleri vardır; en yaygın olanları TCP SYN sel saldırısı, gözyaşı saldırısı, şirin saldırısı, ölüm pingi saldırısı ve botnet'lerdir [78].

3.6.2. Ortadaki Adam Saldırısı

Man-in-the-middle (MitM) olarak da bilinen bu saldırıda saldırgan, istemci ile sunucu arasındaki iletişim dinlenmekte ve istenilen bilgiler ele geçirilmektedir. Ortadaki adam saldırısının bazı yaygın türleri;

Oturum Çalma: Bu tür MitM saldırısında, bir saldırgan güvenilir bir istemci ile ağ sunucusu arasındaki bir oturumu ele geçirir. Saldırı yapan bilgisayar IP adresini güvenilir istemci yerine geçerken, sunucu oturumu devam ettirerek istemci ile iletişim kurduğuna inanır. Örneğin, saldırı şu şekilde ortaya çıkabilir:

- İstemci bir sunucuya bağlanır.
- Saldırganın bilgisayarı istemcinin kontrolünü ele geçirir.
- Saldırganın bilgisayarı istemcinin sunucu ile olan bağlantısını keser.
- Saldırganın bilgisayarı, istemcinin IP adresini kendi IP adresiyle değiştirir ve istemcinin sıra numaralarını taklit eder.
- Saldırganın bilgisayarı sunucuyla iletişim kurmaya devam eder ve sunucu hala istemciyle iletişim kurduğuna inanır.

IP Spoofing: IP kimlik sahtekârlığı, bir saldırgan tarafından bir sistemi bilinen, güvenilir bir varlıkla iletişim kurduğuna ikna etmek ve saldırganın sisteme erişimini sağlamak için kullanılır. Saldırgan, hedef ana bilgisayara kendi IP kaynak adresi yerine bilinen, güvenilir bir ana bilgisayarın IP kaynak adresine sahip bir paket gönderir. Hedef ana bilgisayar paketi kabul edebilir ve ona göre hareket edebilir.

DNS Spoofing: Bu saldırıda kullanıcı, saldırganın istediği IP adresine erişmektedir ve bu sayede kullanıcı istediği siteye giriş yaptığını düşünürken aslında saldırganın IP adresine giriş yapmaktadır.

3.6.3. Oltalama Saldırısı

Kimlik avı saldırısı, kişisel bilgiler edinmek veya kullanıcıları bir şeyler yapmak için etkilemek amacıyla güvenilir kaynaklardan gelen e-postalar gönderme uygulamasıdır. Sosyal mühendislik ve teknik hileyi birleştirmektedir. Bilgisayarınıza kötü amaçlı yazılım yükleyen bir e-posta eki içerebilir. Ayrıca, kullanıcının kötü amaçlı yazılım indirmesi veya kişisel bilgilerini aktarması için aldatıcı gayri meşru bir web sitesine ait bağlantı olabilir.

3.6.4. Drive-by download

Drive-By Download saldırıları, hackerların bir web sitesi kullanıcılarının bilgisayarlarına gizlice kötü amaçlı yazılım yüklemelerine olanak sağlayan saldırı türüdür. Hacker kendi oluşturduğu veya sızdığı bir sitenin kaynak kodlarını değiştirerek veya tarayıcı eklentilerini değiştirerek zararlı yazılımları oluşturur. Bu zararlı yazılımlar sitenin kaynak kodunda bulanabilir. Bu site, kullanıcı için tamamen normal gözükmektedir.

3.6.5. Parola Saldırısı

Parolalar, kullanıcıların bilgi sisteminde kimliklerini doğrulamaları için en yaygın kullanılan mekanizma olduğundan, parola edinmek yaygın ve etkili bir saldırı yaklaşımıdır. Bir kişinin parolasına erişim, kişinin masasının etrafına bakarak, şifrelenmemiş parolaları elde ederek, sosyal mühendisliği kullanarak, bir parola veritabanına erişim veya doğrudan tahmin elde etmek için ağ bağlantısını izleme gibi yollarla sağlanabilmektedir.

3.6.6. SQL Injection Saldırısı

SQL enjeksiyonu, veritabanı odaklı web sitelerinde yaygın bir sorun haline gelmiştir. Bir malefactor, istemciden sunucuya girdi verileri aracılığıyla veritabanına bir SQL sorgusu yürüttüğünde oluşmaktadır. SQL komutları, önceden tanımlanmış SQL komutlarını çalıştırmak için veri düzlemi girişine (örneğin, oturum açma adı veya parola yerine) eklenir. Başarılı bir SQL enjeksiyon açığı, hassas verileri veritabanından okuyabilir, veritabanı verilerini değiştirebilir (ekleyebilir, güncelleyebilir veya silebilir), veritabanında yönetim işlemlerini yürütebilir (kapatma gibi), belirli bir dosyanın içeriğini kurtarabilir ve bazı durumlarda, işletim sistemine komutlar verebilir.

SQL enjeksiyonu (SQLi), mevcut SQL ifadelerine kötü amaçlı kod enjekte etmek için kullanılan bir tekniktir.

Bu enjeksiyonlar, kötü niyetli kullanıcıların mevcut güvenlik kontrollerini atlamasını ve müşteri kayıtları, fikri mülkiyet veya kişisel bilgiler de dâhil olmak üzere veri elde etmek, değiştirmek ve çıkarmak için yetkisiz erişim elde etmelerini mümkün kılmaktadır. Saldırganlar yöneticilerin kimlik bilgilerini bulmak ve etkilenen web siteleri, uygulamalar ve veritabanı sunucuları üzerinde tam kontrol elde etmek için bu tekniği kullanabilmektedir. SQL enjeksiyon saldırıları, SQL veritabanı kullanan ve web siteleri, masaüstü bilgisayarlar ve telefon uygulamaları da dâhil olmak üzere verileri son derece ciddi sonuçlarla işleyen tüm uygulamaları etkileyebilmektedir.

En yaygın kullanılan SQL Injection türü Union-Based SQL Injection'dır. Bu tür SQL enjeksiyonu, saldırganlar tarafından gerçekleştirilen en popüler yöntemdir. Bu enjeksiyon tekniği, kötü aktörlerin sonuçları orijinal sorgudan uzatarak veritabanından veri çıkarmasına olanak tanımaktadır. İki SELECT deyimini tek bir sonuca entegre etmek için UNION SQL operatörünü kullanır ve ardından yanıtın bir parçası olarak döndürür.

Diğer SQL Injection Türleri:

Blind SQL Injection: Tipik olarak, diğer enjeksiyon çeşitlerinden daha karmaşık ve gerçekleştirilmesi zordur. Saldırganlar, hedeften genel hata mesajları alındığında kör SQL enjeksiyonlarını gerçekleştirmektedir. Kör SQL enjeksiyonları, kendilerini veritabanından bilgi aldıkları yöntemdeki normal SQL enjeksiyonlarından ayırmaktadır. Bu teknikte, kötü aktörler veritabanını doğru veya yanlış sorular için sorgulamaktadır. Ardından yanıtı ve yanıtı zaman tabanlı saldırılarla kullanırken sunucu yanıtını almak için geçen süreyi belirlemektedir.

Boolean-Based SQL Injection: Bu saldırı türü, sorgunun mantığını ve koşullarını kendi üzerine yazmaktadır. Veritabanında izinleri yükseltmek veya doğru kimlik bilgileri olduğunu düşünmeleri için kandıkları izin veya kimlik doğrulama sorgularında yaygın olarak kullanılmaktadır. Boolean tabanlı SQL enjeksiyonları, veritabanından veri ayıklamak için eleme yoluyla ilerledikleri kör SQL enjeksiyonlarında da kullanılır. Saldırganlar her biri emsallerden biraz farklı bir koşula sahip tonlarca istek göndererek, operasyonun sonucuna göre depolanan verilerin ne olduğunu anlayabilmektedir.

Error-Based SQL Injection: Hata tabanlı bir SQL enjeksiyonunda saldırganlar, bir web sayfasından veya uygulamadan, onaylanmamış girdiler tarafından tetiklenen veritabanı hatalarından yararlanmaktadır. Saldırı sırasında bu teknik, tam sorgu sonuçlarını döndürmek ve veritabanından gizli bilgileri göstermek için hata mesajlarını kullanır. Bu yöntem, bir web sitesinin veya web uygulamasının savunmasız olup olmadığını belirlemek, kötü amaçlı sorguları yeniden yapılandırmak adına ek bilgi edinmek için de kullanılabilir.

Time-Based SQL Injection

Normal bir SQL enjeksiyonu sırasında, kötü aktörler metni döndükçe okuyabilirler. Ancak saldırganlar bir veritabanı sunucusundan bilgi alamadığında, sonuçlarına ulaşmak için genellikle zamana dayalı SQL enjeksiyonları kullanırlar. Bu, tamamlanması uzun süren ve çoğu zaman birkaç saniye süren işlemleri kullanarak çalışmaktadır. Zaman tabanlı SQL enjeksiyonları, bir web uygulamasında veya web sitesinde güvenlik açıklarının bulunup bulunmadığını belirlerler. Ayrıca, Kör SQL enjeksiyonları sırasında Boole tabanlı tekniklerle birlikte kullanılmaktadırlar.

SQL enjeksiyonlarının tespit edilmesi oldukça zordur. Siteler arası komut dosyası oluşturma, uzaktan kod yerleştirme ve diğer bulaşma türlerinden farklı olarak, SQL enjeksiyonları sunucuda iz bırakmayan güvenlik açıklarıdır. Bunun yerine, istismar veritabanında gerçek sorgular yürütmektedir. Sonuç olarak, saldırganların çoğu, bir saldırganın kötü amaçlı eylemler gerçekleştirmek için güvenlik açığını kullandığında veya yönetim erişimi kazandığında algılanır.

3.6.7. Cross-site Scripting (XSS) Saldırısı

XSS saldırıları, kurbanın web tarayıcısında veya yazılabilir uygulamasında komut dosyaları çalıştırmak için üçüncü taraf web kaynaklarını kullanmaktadır. Özellikle, saldırgan bir web sitesinin veritabanına zararlı JavaScript içeren bir yük yüklemektedir. Mağdur, web sitesinden bir sayfa istediğinde web sitesi, saldırganın HTML gövdesinin bir parçası olan ve yükünü içeren sayfayı kötü niyetli komut dosyasını çalıştıran kurbanın tarayıcısına iletmektedir. Örneğin, kurbanın çerezini saldırganın sunucusuna gönderebilir, saldırgan onu çıkarabilir ve oturumun ele geçirilmesi için kullanabilir. En tehlikeli sonuçlar, XSS ek güvenlik açıklarından yararlanmak için kullanıldığında ortaya çıkmaktadır. Bu güvenlik açıkları, bir saldırganın yalnızca çerezleri çalmasını değil, aynı zamanda tuş vuruşlarını

günlüğe kaydetmesini, ekran görüntülerini yakalamasını, ağ bilgilerini keşfedip toplamasını, kurbanın makinesine uzaktan erişmesini ve bunları kontrol etmesini sağlayabilir.

XSS, VBScript, ActiveX ve Flash içinde yararlanabilirken, en yaygın istismar JavaScript'tir. XSS saldırılarına karşı savunmak için, geliştiriciler bir HTTP isteğinde bulunan kullanıcıların veri girişini geri yansıtmadan önce dezenfekte edebilirler. Arama sırasında sorgu parametrelerinin değerleri gibi kullanıcıya herhangi bir şey geri göndermeden önce tüm verilerin doğrulandığından, filtrelendiğinden veya kaçtığından emin olunmalıdır. “ ?, &, /, <,> “ ve boşluklar gibi özel karakterleri ilgili HTML veya URL kodlu eşdeğerlerine dönüştürülmelidir. Kullanıcılara istemci tarafı komut dosyalarını devre dışı bırakma seçeneği verilmelidir.

3.6.8. Dinleme Saldırısı

Gizlice dinleme saldırıları ağ trafiğinin kesilmesi ile gerçekleşmektedir. Gizlice dinleyerek, bir saldırgan kullanıcının ağ üzerinden gönderebileceği şifreleri, kredi kartı numaralarını ve diğer gizli bilgileri elde edilebilir. Gizlice dinleme pasif veya aktif olabilmektedir.

3.6.9. Doğum Günü Saldırısı

Doğum günü saldırısı kriptografik bir saldırıdır. İki veya daha fazla nokta arasındaki iletişimi kötüye kullanmak için kullanılmaktadır. Doğum günü saldırısı ile aynı mesaj özetini üreten farklı iki mesajı bulmaktadır. Eğer saldırgan, kurbanın mesajıyla aynı mesaj özetini hesaplayabilirse, kurbanın mesajını değiştirebilmektedir.

3.6.10. Malware Saldırıları

Kötü amaçlı yazılımlar, kullanıcının izni olmadan sisteme yüklenen istenmeyen yazılımlar olarak tanımlanabilir. Kendini meşru koda ekleyebilir ve çoğaltabilir, yararlı uygulamalarda gizlenebilir veya kendini internet üzerinden çoğaltabilir. Trojanlar, adware, spyware, ransomware en yaygın kötü amaçlı yazılım türlerinden bazılarıdır.

Siber saldırılar elbette bu 10 saldırı ile sınırlı değildir. Teknoloji ve hizmet alanları genişledikçe saldırı türleri de doğru orantılı olarak çeşitlenmektedir. Saldırganlar oltalama yöntemleri, sistem açıkları gibi zayıflıklardan yararlanarak gizli, kritik bilgileri elde etmek, onları bozmak veya ifşa etmek isteyeceklerdir. Bunların önlenmesi için sistemlerin

güçlendirilmesi ve önlemlerin alınması gerekmektedir. Bu tehditleri azaltmaya yönelik önlemler değişebilir ancak güvenlik temelleri aynı kalacaktır. Bu saldırıların önlenmesi için temelde; sistemler ve virüsten koruma veri tabanları güncel tutulmalı, çalışanlar güvenlik konusunda bilinçlendirilmeli, güvenlik duvarları yalnızca ihtiyaç olan belirli bağlantı noktalarına ve ana bilgisayara erişecek şekilde yapılandırılmalı, şifreler güçlü olmalı, kullanılan BT ortamında en az yetki prensibi uygulanmalı, düzenli yedeklemeler yapılmalı ve BT sistemleri şüpheli etkinlik açısından sürekli denetlenmelidir.

3.7. Kritik Kurumlara Yapılan Saldırı Örnekleri

Bu bölümde 2014-2019 yılları arasında yaşanan siber saldırılar ele alınmıştır.

3.7.1. Almanya Kamu Kurum ve Özel Sektör İşletmelerine Yönelik Saldırılar

Aralık 2018 tarihinde Almanya'da 1000 kamu kurum ve özel sektör işletmeleri siber saldırıya maruz kalmıştır. Bu saldırganın ismi Almanya Devleti tarafından açıklanmamıştır. The Guardian'da yayınlanan habere göre, [79] 20 yaşındaki saldırgan, adli mercilere verdiği ifadede yaklaşık 1000 kamu ve özel sektör firmalarının sistemlerini ele geçirdiğini ve hem kurumsal hem de kişisel verileri sızdırdığını itiraf etmiştir. Saldırganın kurbanlarının arasında Alman siyasetçilerinin ve bürokratlarının da kişisel verileri olduğu tahmin edilmektedir.

Saldırgan, casusluk yapmak, veri sızdırmak ve kişisel verilerin mahremiyetinin bozulmasına neden olmakla suçlanmaktadır. Yetkililer, saldırganın yakalanmaması halinde daha fazla kamu networklerine sızacağı ve daha fazla bilgiyi kazıp çıkarmayı deneyeceğini ifade etmişlerdir. Hangi kamu kuruluşlarının etkilendiği ulusal güvenlik kaygısı ile paylaşılmamaktadır.

3.7.2. NASA Sistemlerine Yönelik Saldırı

Ulusal Havacılık ve Uzay Dairesi (The U.S. National Aeronautics and Space Administration- NASA), Jet Propulsion Laboratuarı'nın (JPL) geçtiğimiz yıl saldırıya uğradığını doğrulamıştır. Saldırgan, ucuz bir Pi bilgisayarı kullanarak uzay ajansının görevleri ile ilgili 500 MB'lik verileri çaldığını aktarmıştır [80].

NASA, Haziran 2019'da yayınlanan denetim raporunda [81] , Nisan 2018'de JPL'nin harici kullanıcıya ait bir hesabın tehlikeye atıldığı ve başlıca görev sistemlerinden birinden yaklaşık 500 MB'lık verileri çalmak için kullanıldığı açıklanmıştır.

3.7.3. Amerika Personel Yönetim Ofisine Yönelik Saldırı

Bloomberg Ht ekonomi kanalının 5 Haziran 2015'te yayınladığı habere göre [82] Amerika Personel Yönetim Ofisi, 4 milyon civarındaki eski ve mevcut federal çalışanın bilgilerinin çalınmış olduğunu bildirmiştir. Amerikalı yetkililer, ilgili saldırının Aralık 2014 tarihinde meydana geldiğini aktarmıştır.

CSOnline web sitesinde yayınlanan habere göre, kurum eksik ve katmanlı güvenlik önlemleri alınmadan internete açmış oldukları veritabanı sunucusunun etkilendiğini, veritabanı sunucusu ele geçirildikten sonra SP-86 form içeriklerinin dışarıya sızdığını tespit etmiştir. Saldırganların OPM sistemine giriş yapmak için OPM sistemlerinde çalışan bir uygulamanın üretici hesabı ile giriş yaptıkları kötü amaçlı yazılım yükledikleri ve ağa erişmek için bir arka kapı (backdoor) bıraktıkları tespit edilmiştir [83].

4. DEVLET KURUMUNA AİT VERİ MERKEZİNDE SIEM UYGULAMASI

SIEM ile belirli kaynaklardan toplanan loglar ile ağ, sistem ve uygulamalar üzerinde anomali hareketler, saldırılar gibi zararlı davranışlar tespit edilebilmektedir. Bu çalışmanın desteklenmesi amacıyla bir devlet kurumuna ait veri merkezinde SIEM uygulaması gerçekleştirilmiştir. Bu doğrultuda örnek uygulamanın yapıldığı veri merkezine ait sistemlerden loglar toplanarak çeşitli korelasyon kuralları yazılmıştır.

Veri merkezinde yapılan çalışmada logların toplanabilmesi ve SIEM çözümünün yönetilebilmesi için 3 adet fiziksel sunucu kurulmuştur. Veri merkezinde bulunan sistemlerden, syslog ve WMI (Windows Management Instrumentation) olmak üzere 2 farklı yolla loglar toplanmıştır. Güvenlik, ağ cihazları ve Linux tabanlı işletim sistemlerinden, syslog, Windows işletim sistemine sahip cihazlardan ise WMI aracılığı ile loglar toplanmıştır. Bilinmeyen sunucular tarafından kasıtlı veya kasıtsız olarak syslog formatında gönderilen loglar, disk kullanımını artıracağından log kaçırmaya sebep olacaktır. Bu yüzden güvenlik duvarında güvenlik politikası yazılarak yalnızca bilinen sunucuların IP'lerine erişim tanımlanmıştır. Veri merkezinde yer alan sistemlerden alınan loglar 3 ay süreyle izlenmiştir.

Gizlilik politikaları gereğince kurum ismi ve kurulumu yapılan SIEM uygulamasının markası belirtilmemiştir.

4.1. Korelasyon Nasıl Tanımlanır?

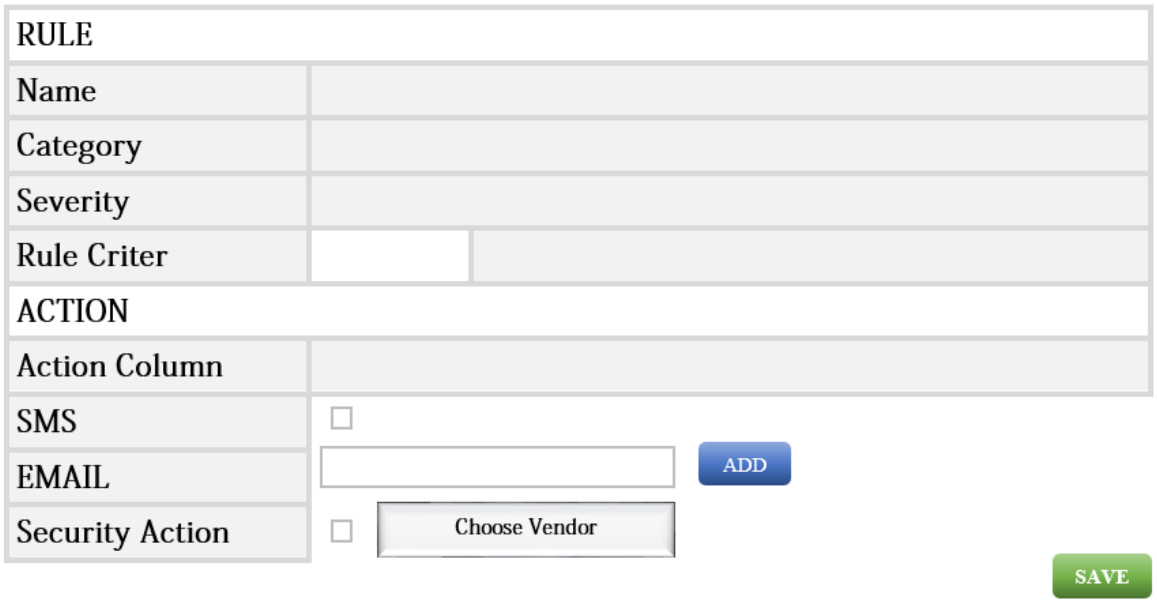
Korelasyon, veriler arasındaki ilişkiyi ve bu ilişkinin etkisini inceleyen bir yöntemdir. Amaç, SIEM ürünlerinde bulunan korelasyon motoru sayesinde, korelasyon çıktısını, siber tehdit bağlamında incelemek, yöneticileri bilgilendirmek, bu tehdidi önlemek ve tehditler için farkındalık yaratmaktır.

Bir korelasyon kuralı yazılırken bazı önemli noktalar bulunmaktadır. Bunlar risk seviyesinin belirlenmesi, kural setinin tanımlanması, nasıl bir aksiyon alınacağı, alarm yöntemi, liste yazılması gibi adımlardır. Bu kural tanımlamaları üreticiden üreticiye farklılık göstermektedir.

Risk Seviyesi: Kural yazarken risk değerlendirmesinin belirlenmesi gerekmektedir. Örneğin, Brute force atağının tespit edilmesi kuralı " Kritik" seviye, şüpheli icmp trafiğinin tespit edilmesi " Uyarı" seviyesi, bir sistem servisinin başlamasının tespiti " Bilgilendirme" gibi seviyeler atanmalıdır. Kritiklik seviyesini kuralı oluşturan kişi belirlemelidir. Böylece alarmlar seviyesine göre incelenebilir. Kritik seviyedeki bir alarm ürerse acilen tedbir almak gerektiği anlaşılmalıdır.

Kural Seti: Kural oluştururken kural setinin belirlenmesi en önemli noktadır. Burası incelenmesi istenen olayın tanımlandığı noktadır. Burada dikkat edilmesi gereken nokta, kuralın sağlanması verilen bilgilerin hedefi doğrultusunda doğrulanmasına bağlıdır. Örneğin kaynak IP 1.1.1.1 ise kural tetiklensin. Alarmın çalışacağı koşullar, nesneler ve kurallar burada tanımlanmaktadır.

Aksiyon: Aksiyon bölümünde ise kural bölümünde tanımlanan koşullar sağlandığında, hangi aksiyonun alınacağı, kimlerin hangi yollarla bilgilendirileceği tanımlanmaktadır. Örneğin, alarm ürerse istenilen kişiye e-posta veya kısa mesaj atılması durumu burada tanımlanmaktadır. Ayrıca güvenlik duvarı ile entegrasyon var ise şartın sağlandığı kaynak IP'si engellenebilmektedir.



Şekil 4.1: Korelasyon Tanımlama Ekranı

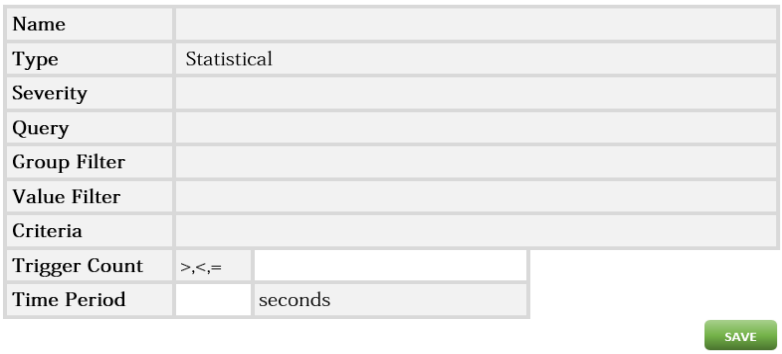
Kural bölümünde bir veya birden fazla kural seti oluşturulabilmektedir. Birden fazla kural seti tanımlandığında şartların tamamının sağlanması gerekmektedir. Bu kısımda şartların gerçekleşmesi için IS, IS NOT, CONTAINS, BEHAVIOR gibi şartlı ifadeler bulunmaktadır. Kural tanımlanırken bu ifadelere ihtiyaç duyulmaktadır. Örneğin "Source.IP IS 1.1.1.1" kural cümleciği, kaynak IP yalnızca 1.1.1.1 ise yazılan kuralın tetiklenmesi anlamındadır. BEHAVIOR kural şartı ise liste kullanımında yazılmaktadır. Liste sayesinde de statik ve dinamik olmak üzere belirli adımlar için listeler oluşturulmaktadır. Böylece olay eşiği belirlenebilmekte, birden fazla nesne için aynı kural girişi uygulanabilmektedir.

Liste tanımlamasında genellikle isim, tür ve içeriğin tanımlandığı alanlar bulunmaktadır. "Type" kısmında liste tipleri belirlenmektedir. Liste tanımlamalarında "Static" ve "Statistical" tipleri kullanılmaktadır. Eğer tanımlı olan verinin (örneğin bir gruba üye olan kullanıcı isimleri) bir kolerasyon içinde kullanılması istenirse "Static" liste türünü seçmektedir. Fakat belli şartların sağlandığı (örneğin 25 portuna istek yapan source ip lerin bilgisi) tespitler için "Statistical" liste türü seçilmektedir.

Name	
Type	Static / Statistical
Severity	Emergency/Alert/Warning/Information
Data Type	

Şekil 4.9: Liste Tanımlama Ekranı

Liste tanımlamasında istatistik türü seçildiğinde, belli kural deyimleri, belli kriterlere göre gruplama, eşik değeri, zaman periyodu gibi ayarlar yapılmaktadır. Örneğin 1 dakika içerisinde 5 defa başarısız oturum hareketlerinin tespiti için liste, zaman ve olayın belirli sayıda tetiklenmesini içerdiğinden istatistik türünde tanımlanması gerekmektedir.



Şekil 4.10: İstatistik Liste Tanımlama Ekranı

Korelsayon kuralı içerisinde listenin kullanılması için "BEHAVIOR" şartlı ifadesi kullanılmaktadır. Liste sayesinde kural içerisinde çok sayıda komut yazılmasının önüne geçilmektedir.

4.2. Veri Merkezi Uygulamasında Yazılan Korelasyonlar

Bölüm 4.2'de veri merkezi bünyesinde kurulan SIEM uygulamasında yazılan bazı korelasyon kuralları incelenmiştir.

4.2.1. Veritabanı Güvenliğine Yönelik Korelasyonlar

Veritabanı, verinin hassasiyet derecesine de bağlı olarak, kritiklik seviyesi kurumdan kuruma değişmektedir. Örneğin bankalarda müşterilerin hesapları, veri merkezinde dışa açık bazı servislerde kullanıcıların kimlik bilgileri gibi verilerin tutulduğu veri tabanlarında güvenlik çok önemlidir. Bir kurumu ticari zarara uğratmak ve itibarını zayıflatmak, saldırganlar için motivasyon kaynağıdır. Bu doğrultuda SIEM'e aktarılacak loglar üzerinde iyi bir korelasyon yapılarak bazı anomali durumlar tespit edilebilir.

4.2.1.1. Kural 1: Dışarıya Veri Aktarılması

Eğer bir veritabanında kullanıcı erişim yetkisi olan/olmayan verileri dışarı çıkartmak (export) isterse ve bu hareketi rutin işleri arasında değilse, rutin çalışma saatlerinde yapılmamışsa riskli ve incelenmesi gereken bir durumdur.

Veri merkezinin gizlilik politikaları gereğince kullanılan veritabanına ait ürün ismi paylaşılamayacağı için örnek olması adına en yaygın bilinen veritabanları MongoDB, MSSQL ve Oracle sql sorguları kullanılmıştır.

Oracle veritabanında “spool” komutu, sorgu sonuçlarını bir dosyada depolamakta veya isteğe bağlı olarak dosyayı bir yazıcıya göndermektedir [84]. Aşağıda yazılan korelasyon “spool” komutunu kullanan kullanıcıların tespitini yapmaktadır. Aşağıda gösterilen komutta, veritabanı yöneticisinden alınan gizli veya kritik bir tablodaki bilgilerin dışarıya aktarılması sağlanmaktadır.

- spool runme.sql
- 'select * from dba_tables' where table_name like 'gizli_bir_tablo%';
- spool off;
- @runme

Eğer veritabanı olarak ORACLE kullanmakta ise Şekil 4.4’teki korelasyon kuralı yazılmalıdır.

RULE		
Name	Oracle DB Uzerinde Spool Komutu Calistirildi	
Category	Database	
Severity	Critical	
Database.Query	CONTAINS	Spool
Database.Query	IS	“ Select * from dba_tablo where sart”
ACTION		
Action Column	Source.IP	
SMS	■	
EMAIL		ADD
Security Action	■ Choose Vendor	

SAVE

Şekil 4.11: Oracle Veritabanında Spool Komutu Çalıştırılmasının Tespiti

Kural seti bölümünde iki kural tanımlandı. Birincisi ”Database.Query CONTAINS spool “ ikincisi ise “Database.Querty IS “select * from dba_tablo where şart “ kurallarıdır. Burada “şart” kısmı veritabanı yöneticisinden alınacak bilgiye göre yazılması gerekmektedir.

Contains, seçilmesinin sebebi, sorgu içerisinde “spool runtime” ve “spool off” komutları olmasından dolayı, bu kural içerisinde “SPOOL” kelimesi geçen tüm sorguları

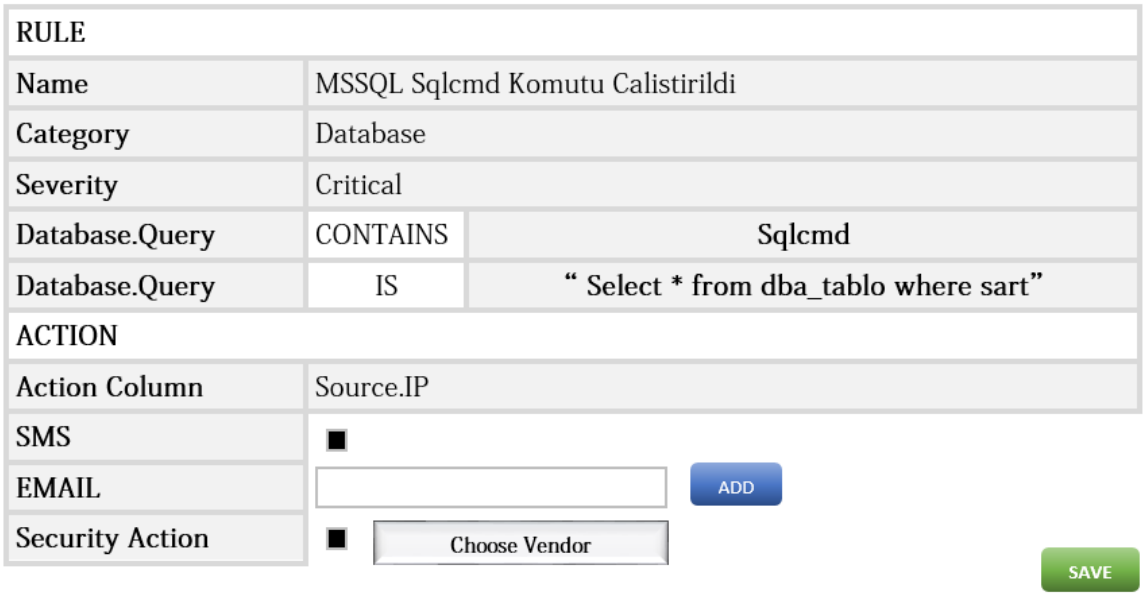
kapsamaktadır. “IS” şartlı ifadesinin seçilmesinin sebebi, girilen değerin birebir sağlanması gerektiğidir.

Yapılan bu kural tanımlamaları sonucunda, veritabanı sorgusu içerisinde hem “spool” komutu geçiyor hem de veritabanı yöneticisi tarafından bildirilen tablo üzerinde “select” sorgusu geçiyor ise bu alarmın kısa mesaj, e-posta ile bilgilendirilmesi ve aynı zamanda güvenlik duvarı tarafından ilgili kaynak IP’nin trafiği kesilmesi beklenmektedir.

Aynı şekilde MSSQL kullanılan bir ortam için örnek sorgu;

- sqlcmd -S localhost -d AdventureWorks2012 -E -Q “SELECT * FROM db_tablo” -o “CSVData.csv” -W -w 1024 -s”,”

Bu komutu çalıştıran bir kullanıcı şekil 4.5’teki SIEM kuralı ile tespit edilebilmektedir.



Şekil 4.12: MSSQL Veritabanında Sqlcmd Komutu Çalıştırılmasının Tespiti

Kural bölümünde export işlemi için kullanılan “sqlcmd” komutu ve veritabanı yöneticisi tarafından iletilen “SELECT” ifadesi aynı anda çalışır ise alarm, kısa mesaj, e-posta yolu ile iletilmesi ve bu hareketi yapan kullanıcıya ait trafiğin güvenlik duvarı tarafından engellenmesi beklenmektedir.

Başka bir veritabanı olan MongoDB’de de verilerin dışarıya aktarılması için **“**mongoexport**”** komutu kullanılmaktadır. MongoDB veritabanında bir JSON veya CSV dosyasına veri

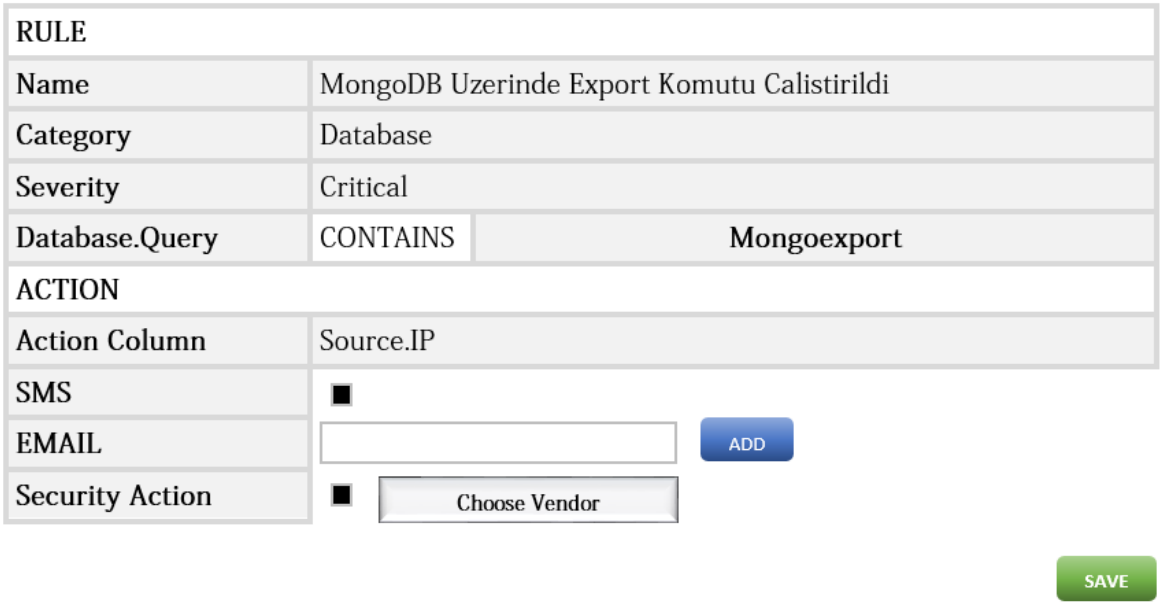
aktarmak için “mongoexport” yardımcı programı kullanılmaktadır. Yardımcı program MongoDB “bin” dizininde bulunmaktadır (örn. /Mongodb/bin). Yardımcı program çalıştırıldığında, veritabanının adı, koleksiyonu ve dışa aktarılması istenilen dosya sağlanmalıdır. Aşağıdaki komutlarla json formatına veya csv formatında veriler dışarı aktarılmaktadır.

- Mongoexport --db VERİTABANI ADI --collection KOLEKSİYON ADI --out /data/dump/bir_klasor/ornekdosya.json

Burada, bir koleksiyonu bir CSV dosyasına aktarmak için mongoexport'u kullanılmaktadır. _id ve sutun1 ve sutun2 alanlarını dışa aktarılmaktadır. Ayrıca dosya adına bir .csv uzantısı verilmiştir.

- mongoexport --db veritabani_adi --collection kolekysiyon_adı --type=csv --fields _sutun1,sutun2 --out /data/dump/music/ornekdosya.csv

Mongo veri tabanlarında kullanılan export komutunun çalıştırılması halinde oluşacak alarm için yapılan tanımlamalar Şekil 4.6’daki gibidir;



Şekil 4.13: Mongo Veritabanında Mongoexport Komutu Çalıştırılmasının Tespiti

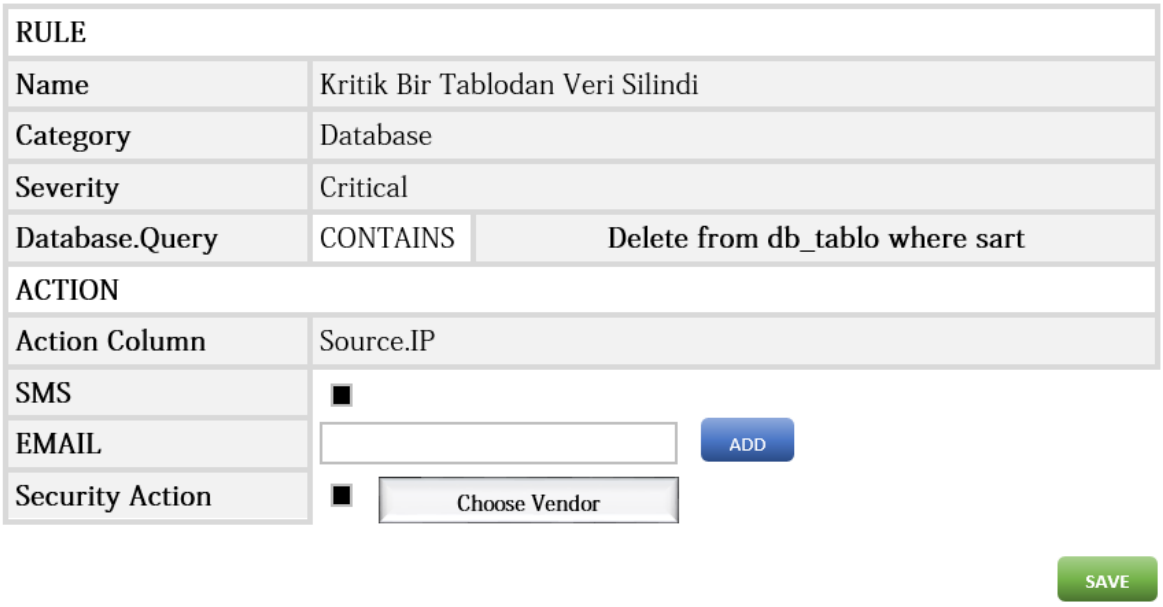
Kural bölümünde sql sorgusu “mongoexport” komutunu içeriyorsa (CONTAINS) bu alarm ilgili kişilere iletilmesi ve güvenlik duvarı tarafından ilgili trafiğin engellenmesi beklenmektedir.

Bu üç veritabanı için kullanılan komutlar için SIEM korelasyonu yazıldığı zaman, veritabanında yer alan bilginin dışarı aktarıldığı tespit edilebilmektedir.

4.2.1.2. Kural 2: DELETE Komutunun Çalıştırılması

Bir veritabanında kritik bir veri kasıtlı olarak silinmek istenebilmektedir. O yüzden DELETE komutu kullanan kullanıcıların bunu çalışma saatlerinde mi yaptığı, hangi veritabanı, hangi sütunu üzerinde yaptığı, görevi gereği mi yaptığı tespit edilmelidir.

Kritiklik durumu veritabanı yöneticisiyle birlikte çalışarak öğrenilebilir. Veritabanı yöneticisi SIEM'de alarm üretilmesi gereken tabloları, DB (Database) isimlerini paylaştıktan sonra SIEM'de bu bilgiler ışığında korelasyonlar yazılmalıdır.



Şekil 4.14: Kritik Bir SQL Tablosunda Delete Komutu Çalıştırılmasının Tespiti

Şekil 4.7'de tanımlanan korelasyon kuralında aşağıdaki tanımlamalar yapılmıştır.

Name: Kuralın adı "Veritabanindan Kritik Bir Verinin Silinmesi " olarak tanımlanmıştır.

Category: Alarm "Database" kategorisine atanmıştır.

Severity: Risk seviyelendirmesi "Critical" olarak belirlenmiştir.

Rule: Kural seti, "Database.Query IS delete from db_tablo where şart" olarak tanımlanmıştır. Veritabanı sorguları, SIEM ekranlarına düşen log içeriğinde "Database.Query" altında görüntülenmektedir.

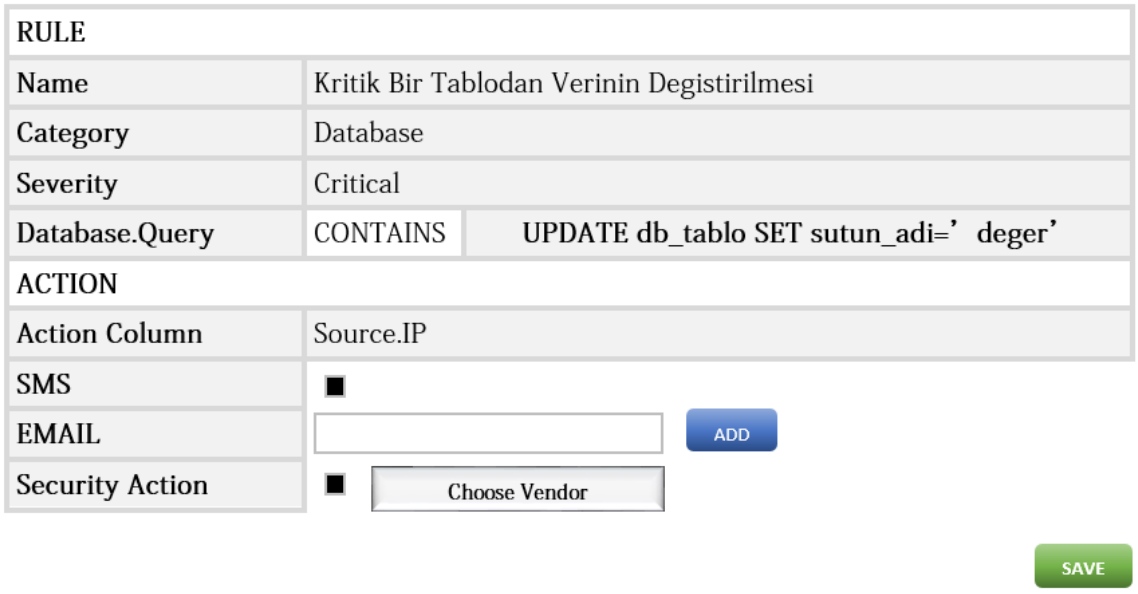
Action**:** Bu bölümde Delete komutunu yapan kaynak IP, E-posta ile ilgili veritabanı yöneticisine iletildi. Durum kritik olduğu için kısa mesaj ile de bilgilendirme yapılabilir. Ayrıca durumun kritikliği açısından bu kaynağın IP'nin güvenlik duvarı tarafından engellenmesi ayarlanmıştır.

Yapılan bu korelasyon ile veritabanı yöneticisinin silinmesini istemediği bir verinin veritabanından silinmesi halinde alarm üremesi beklenmektedir.

4.2.1.3. Kural 3: UPDATE Komutunun Çalıştırılması

UPDATE komutu, veritabanında bulunan verileri değiştirmektedir/güncellemektedir. Veritabanı yöneticisinin kesinlikle değiştirilmemesi gereken bir veri sütun/satır bilgisini vermesi halinde, SIEM ile yazılabilir ve bir veri değişikliğine uyarı alınabilir.

Veritabanı yöneticisinin belirteceği tablo üzerinde UPDATE komutu çalıştırılması kritik olarak kabul edilerek ve Şekil 4.8'de yer alan korelasyon tanımlanmıştır.



Şekil 4.15: Kritik Bir SQL Tablosunda Update Komutu Çalıştırılmasının Tespiti

Kural bölümünde "Database.Query IS UPDATE db_tablo SET sütun_adı="değer"" tanımı yapılmıştır. İlgili veritabanının belirtilen değeri değiştirildiği zaman kısa mesaj, e-posta ile yönetici bilgilendirilmesi, güvenlik duvarı tarafından ilgili trafiğin engellenmesi beklenmektedir.

4.2.2. Web Saldırılarına Yönelik Korelasyonlar

Her gün yeni web tabanlı saldırı türleri ve vektörler çıkmakta, bu da işletmelerin, toplulukların ve bireylerin güvenliği geçmişte olduğundan daha fazla ciddiye almasına neden olmaktadır. Bu durum, World Wide Web için büyük bir kazanç olmakla birlikte teknolojiyi daha sağlam ve güvenli bir şekilde geliştirilmiş web uygulamalarına doğru iten bir eğilimdir.

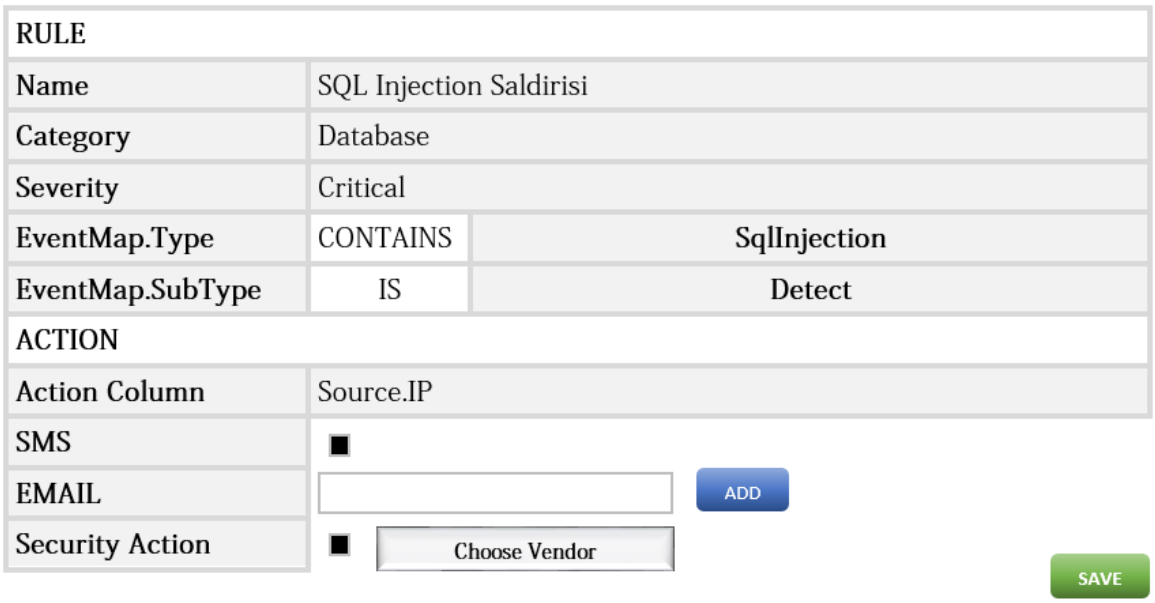
SIEM uygulamasının yapıldığı veri merkezinin sahip olduğu itibar, saldırganların hedefine girmesine neden olmaktadır. Bu yüzden çeşitli varyasyonlar ile her saniye saldırılar düzenlenmektedir. Unutulmamalıdır ki ne kadar güçlü savunma sistemi olursa olsun, aşılamayacak bir sistem yoktur. Bu bölümde SIEM ile dış ağ üzerinden gelecek saldırı türlerine yönelik korelasyonlar ile veri merkezi bünyesinde istismara sebep olabilecek zafiyetlerin tespit edilmesi amaçlanmaktadır. Bu bağlamda WAF, güvenlik cihazları, IPS ve web sunucuları ve uygulamalarından alınan loglara göre korelasyon kuralları geliştirilmelidir.

4.2.2.1. Kural 4: SQL Injection Saldırı Tespiti

SQL enjeksiyonu (SQLi), mevcut SQL ifadelerine kötü amaçlı kod enjekte etmek için kullanılan bir teknik olduğundan Bölüm 3.6.6'da bahsedilmiştir.

Güvenlik önlemleri alarak ve veritabanı ve sorguları aktif olarak izlenerek, bir saldırganın web sitesinde kötü amaçlı enjeksiyonlar yapıp yapmadığı tespit edilebilir.

Bu doğrultuda Şekil 4.9'daki korelasyon kuralı yazılmıştır.



Şekil 4.16: SQL Injection Saldırısı Korelasyon Kuralı

"SQL Injection Saldırısı" adındaki alarmı "Database" kategorisine atanmış ve risk seviyesi "Critical" olarak konfigüre edilmiştir. Kural seti "Event.Type CONTAINS SqlInjection" ve "EventMap.Subtype IS Detect" olarak ayarlanmıştır. Kural setindeki bu tanımlamanın anlamı; Event.Type, oluşan logun türünü tanımlamaktadır. Örneğin, bir kullanıcının web erişim trafikleri "Web" türünde kaydedilmektedir. Bu kuralda SqlInjection tanımlanmıştır. "EventMap.SubType" ise üretilen loga karşı alınmış aksiyonu göstermektedir. Örneğin güvenlik duvarında bir trafik engellenmişse "Deny" olarak SIEM'e aktarılan log içerisinde görüntülenecektir. Bu kuralda da "Detect" olarak tanımlanmıştır. "Action Column" ile logun içerisinde hangi bilgiye göre aksiyon alınacağı gösterilmektedir. Burada kaynak IP seçilmiştir. Özet olarak, türü "Sql Injection" ve aksiyonu "Detect" olan logları için alarm üretilmiştir.

SQL sorgularını sürekli takip etmek dikkat ve zaman gerektirmektedir. SIEM ile yapılan sorgular için korelasyon kuralı yazılabilmekte ve sorgular takip edilebilmektedir. Ayrıca, güvenlik açıklarından faydalanıldığı için uygulamalar ve sistemler sürekli güncellenmelidir.

Bu örnekler genişletilebilir. SIEM korelasyonları tamamen kuralı yazacak kişinin yaratıcılığına ve sistemin ihtiyaçlarına göre değişmektedir.

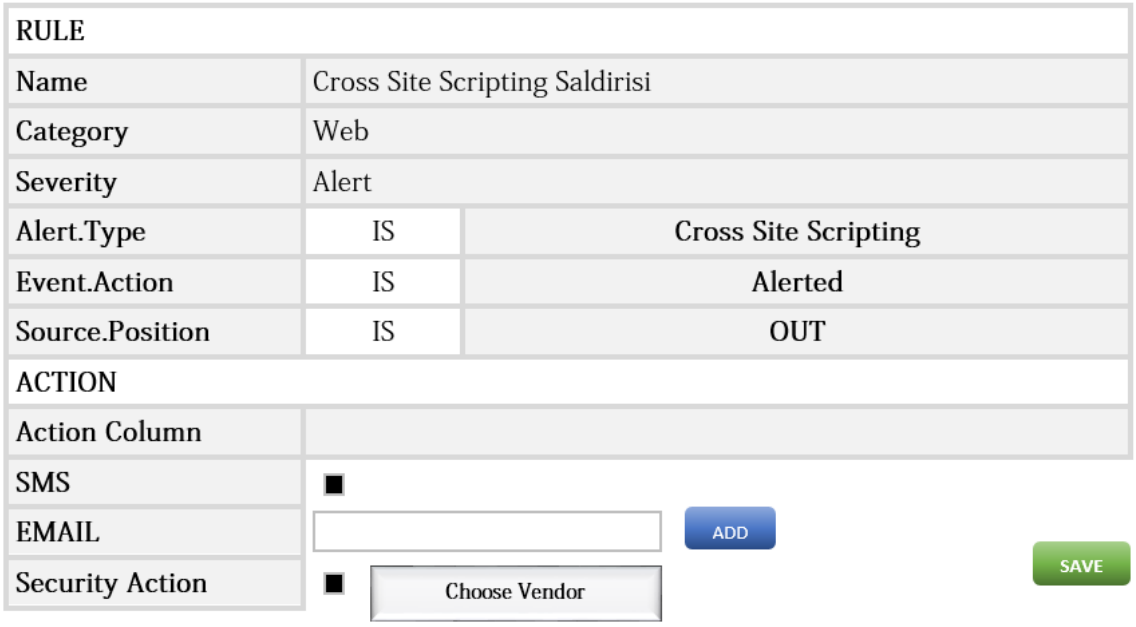
4.2.2.2. Kural 5: Cross Site Scripting Saldırıları

Cross Site Scripting, bir saldırganın kullanıcıların savunmasız bir uygulamayla olan etkileşimlerini tehlikeye atmasına izin veren bir web güvenlik açığıdır. Saldırganın, farklı web sitelerini birbirinden ayırmak için tasarlanan aynı başlangıç politikasını atlamasını sağlamaktadır. Siteler arası komut dosyası oluşturma, bir saldırganın kurban kullanıcı olarak maskelenmesine, kullanıcının gerçekleştirebileceği tüm eylemleri gerçekleştirmesine ve kullanıcının verilerine erişmesine izin verir. Mağdur kullanıcının uygulama içinde ayrıcalıklı erişimi varsa, saldırgan uygulamanın tüm işlevselliği ve verileri üzerinde tam kontrol sahibi olabilir.

Siteler arası komut dosyası oluşturma, güvenlik açığı bulunan bir web sitesini kullanıcılara kötü amaçlı JavaScript döndürmesi için işleyerek çalışır. Kötü niyetli kod kurbanın tarayıcısında yürütüldüğünde, saldırgan uygulama ile etkileşimlerini tamamen tehlikeye atabilir.

Mağdur kullanıcı olarak kimliğe bürünmek veya maskelenmek. Kullanıcının gerçekleştirebileceği tüm işlemleri gerçekleştirmek. Kullanıcının erişebildiği tüm verileri okumak. Kullanıcının oturum açma kimlik bilgilerini yakalamak. Web sitesine trojan işlevselliği enjekte etmek gibi amaçları bulunmaktadır.

Bu tarz saldırıların tespiti SIEM ile mümkündür. Yazılan konfigürasyonun detayları Şekil 4.10'daki gibidir;



Şekil 4.17: Cross Site Scripting Korelasyon Kuralı

Alarm isminin girilmesinin ardından, alarmı Web kategorisine atanmıştır. Risk seviyesi "Alert" olarak tanımlanmıştır. Kural bölümünde;

Alert.Type'ı Cross Site Scripting (XSS) ise

Event.Action "alerted" ise

Source.Position yani saldırı kaynağı dışarıdan geliyorsa yani out ise bu alarm çalışmalıdır.

Bu alarm tetiklendiğine ne gibi aksiyon alınacağı Action and Notification bölümünde tanımlanmıştır. Yapılan tanımlamada bu alarm tetiklendiğinde mail olarak ilgili kişilere mail gönderilecektir. E-posta içeriğinde tespit edilen IP bilgisi ve saldırı türü olacak ve ilgili entegrasyon varsa kısa mesaj gönderimi de yapılacaktır.

4.2.2.3. Kural 6: Buffer Overflow Saldırıları

Arabellek taşması (Buffer Overflow), bir arabelleğe veri yazarken arabellek kapasitesini aştığında, bitişik bellek konumlarının üzerine yazılmasına neden olan bir anormalliktir. Arabellek taşmaları, saldırganlar tarafından program yürütmesini zayıflatmak veya kontrolünü ele geçirmek için bilgisayarın belleğini değiştirmek amacıyla kullanılabilmektedir. Şekil 4.11'deki örnekte kullanıcı adı için ayrılmış 8 byte'lık alanın taşması gösterilmektedir.

Buffer (8 Bytes)								OVERFLOW	
U	S	E	R	N	A	M	E	1	2
0	1	2	3	4	5	6	7	8	9

Şekil 4.18: 8 Byte'lık Arabellek Kapasitesinin Aşılması

Web uygulamalarına Buffer Overflow saldırı gerçekleştiğince güvenlik ekiplerinin bilgilendirilmesi için Şekil 4.12'deki alarm yazılmıştır. Bu alarmın kural setinde "EventMap.Type IS BufferOverflow komutu" komutu kullanılmıştır.

RULE		
Name	BufferOverflow Saldirisi	
Category	Web	
Severity	Alert	
EventMap.Type	IS	BufferOverflow
EventMap.SubType	IS	detect
ACTION		
Action Column		
SMS	■	
EMAIL		ADD
Security Action	■ Choose Vendor	

SAVE

Şekil 4.19: BufferOverFlow Korelasyon Kuralı

4.2.2.4. Kural 7: Command Execution Saldırısı

Bir saldırgan sunucular üzerinde rasgele kod yürütebilirse, sistemler çok büyük ihtimalle tehlikeye girecektir. Kod yürütme saldırısı, büyük bir güvenlik atlamasıdır ve sistem devralma işlemini tamamlamak için yoldaki son adımdır. Erişim kazandıktan sonra, bir saldırgan sunucudaki ayrıcalıklarını artırmaya, kötü amaçlı komut dosyalarını yüklemeye veya sunucuyu daha sonraki bir tarihte kullanılacak bir botnet'in parçası yapmaya çalışacaktır.

Şekil 4.13'de gösterilen Command Execution saldırısına karşı alarm kuralına göre, atak türü "Command Execution" olan, uygulama adı "HTTPS" olan, kaynak dışı ağdan bir IP olan log ürediğinde alarmın çalışması beklenmektedir.

RULE		
Name	Comman Execution Saldirisi	
Category	Reconnaissance	
Severity	Alert	
Attack.Type	IS	Command Execution
DataType	IS	log
Application.Name	IS	HTTPS
Source.Position	IS	out
ACTION		
Action Column		
SMS	■	
EMAIL		ADD
Security Action	■ Choose Vendor	

SAVE

Şekil 4.20: Command Execution Saldırısı Korelasyonu

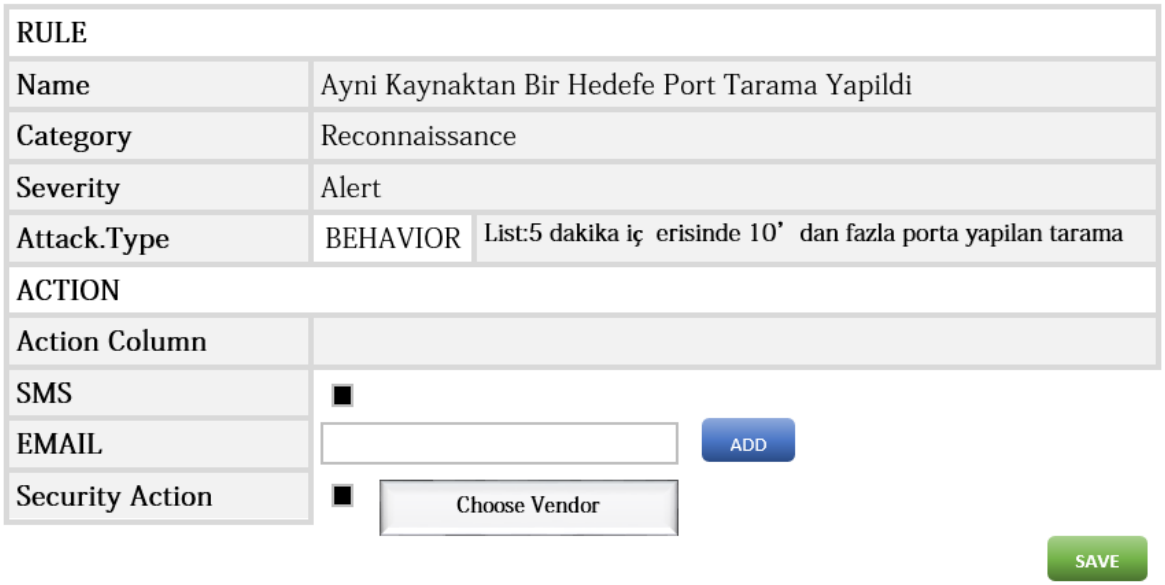
4.2.3. Reconnaissance Saldırılarına Yönelik Korelasyonlar

Bağlantı noktası taramaları (port scan), bağlantı noktası kullanılabilirliğini bir hedef bilgisayara bağlantı istekleri göndererek ve hangi bağlantı noktalarının nasıl ve nasıl yanıt verdiğini kaydederek belirler. Hangi bağlantı noktalarının kullanımda olduğunu belirlemek, bilgisayar korsanlarının hedef aygıtın hangi uygulamaları ve hizmetleri çalıştırdığını belirlemesine olanak tanır. Bu aşaman sonra bilgisayar korsanı güvenlik açıklarını test edebilir ve bir saldırı planlamaya başlayabilir.

4.2.3.1. Kural 8: Port Tarama Saldırısı

SIEM uygulamasının yapıldığı veri merkezi sistemlerinde kullanılan uygulamalarda gözden kaçan açık portlar, güvenlik duvarı üzerinden engellenememiş port tarama trafikleri var ise bunların tespit edilebilmesi Şekil 4.14'teki korelasyonda tanımlanmıştır.

Kural tanımlaması:



Şekil 4.21: Port Tarama Saldırısının Tespit Edilmesi

Name: Aynı Kaynaktan Aynı Hedef IP'ye 5 Dakika İçerisinde 10'dan Fazla Porta Tarama olarak yazılmıştır.

Category: Alarm kategorisi "Reconnaissance" olarak seçilmiştir.

Severity: Risk seviyesi "Alert" tanımlanmıştır.

Rule Set: Bu kuralın çalışması için eşik değerinin tanımlanma ihtiyacı bulunmaktadır. Belirli bir eşik değerine göre kuralın çalışması için liste tanımlamasının yapılması gerekmektedir. Aşağıdaki liste tanımlamasına göre, üretilen verinin türü "log" olan, olay türü "Session" olan aksiyonu "Allow" olan log, EventTrack.ID verisine göre gruplandırılarak, 5 dakika içerisinde 10 kez tetiklenirse bu alarm çalışacaktır.

Liste tanımlaması:

Name	List:5 dakika içerisinde 10’ dan fazla porta yapilan tarama	
Type	Statistical	
Severity	Alert	
Query	DataType:” log” EventMap.Type:Session EventMap.SubType:” Allow”	
Group Filter	Event.TrackID	
Value Filter	Destination.Port	
Criteria	Unique Count	
Trigger Count	>	10
Time Period	300	seconds

SAVE

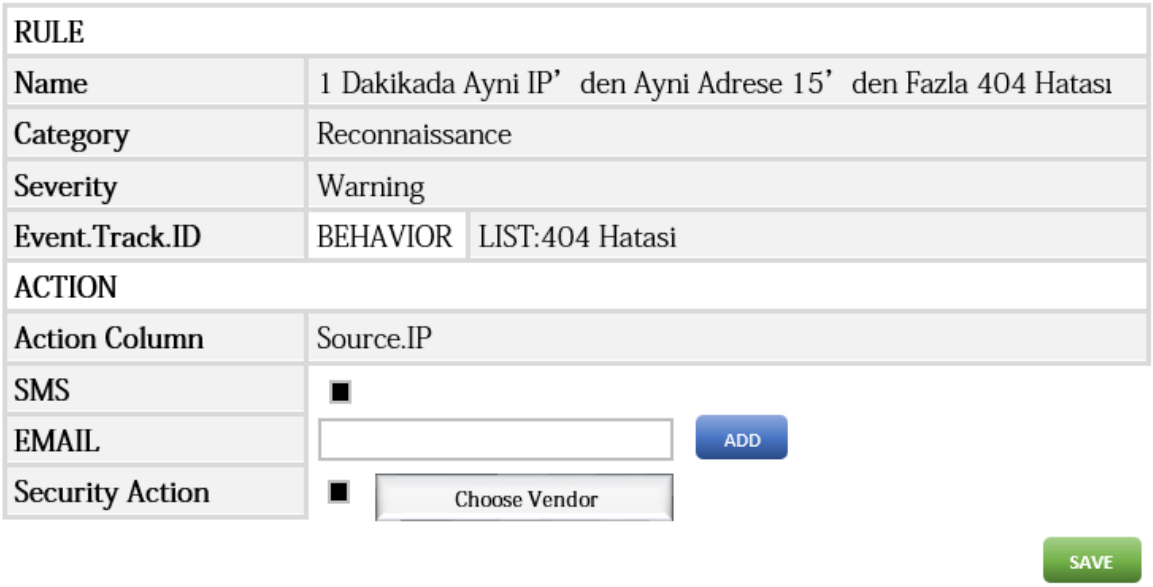
Şekil 4.22: Port Tarama Saldırısının Tespit Edilmesinde İstatistiksel Liste Tanımlaması

4.2.3.2. Kural 9: Çok Sayıda 404 Hatası

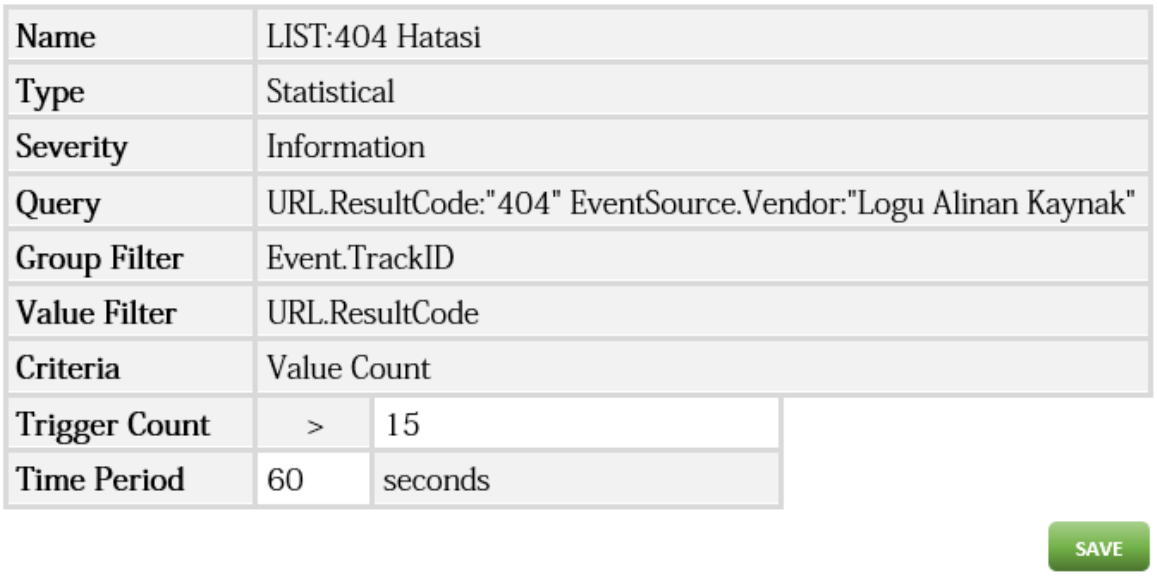
Web sunucularında istenen dosya bulunamadığında "HTTP 404 - Dosya bulunamıyor" hata iletisi döndürülmektedir [85]. Web sayfalarına yönelik keşif saldırılarında, web sayfasına ait çok alt domainleri ve yönetici sayfalarını tespit etmeyi amaçlayabilmektedir. Yapılan web sorguları legal olduğu için herhangi bir güvenlik ürününe takılmayacaktır. Ancak sorgulanan web sayfası eğer yok ise sonuç olarak 404 hatası döndürülmektedir. Bu doğrultuda belirli bir sürede IP'de çok sayıda 404 hatasının olması bir saldırıyı işaret edebilmekte ve bu saldırıyı başlatan kaynağın acilen engellenmesi gerekmektedir.

SIEM uygulamasının yapıldığı veri merkezi bünyesinde çok sayıda dış ağa açık web sayfası bulunmaktadır. Şekil 4.16’daki korelasyon sayesinde bu web sayfalarına yapılan yoğun isteklerin sonucunda çok sayıda 404 hatasının tespit edilebilmesi amaçlanmıştır.

Şekil 4.16’daki kural setinde aşağıdaki olayların tamamı gerçekleştiğinde alarmın çalışması beklenmektedir;



Şekil 4.23: Alt Domain Saldırılarının Tespit Edilmesi



Şekil 4.24: Alt Domain Saldırılarının Tespit Edilmesinde İstatistiksel Liste Tanımlaması

Şekil 4.17'de tanımlanan listeye göre web isteklerinin alındığı log içerisinde bir kaynaktan yapılan isteklerde 404 hatası varsa ve bu olay 1 dakikada 15'ten fazla gerçekleşmişse bu bilgiler listeye eklenecektir. Şekil 4.16'da tanımlanan kural listenin sonucuna göre çalışacaktır. Böylece bir IP çok sayıda 404 hata mesajı döndürmüşse şüpheli kabul edilip engellenecektir.

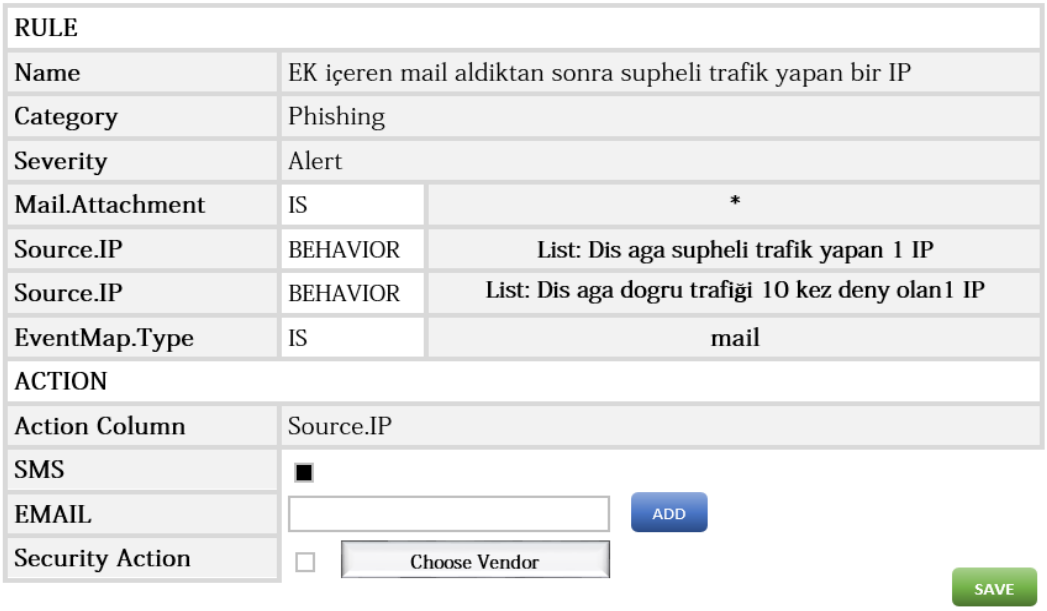
4.2.4. Oltalama Saldırılarına Yönelik Korelasyonlar

Kimlik avı, belirli bir kişiyi potansiyel olarak tanımlayabilen herhangi bir veri olan giriş bilgileri veya diğer kişisel kimlik bilgileri gibi hassas bilgileri elde etmeye yönelik sahte bir girişimdir. Saldırganlar zararlı EK içeren e-posta atabilir ve kullanıcının bilgisayarını köle olarak kullanabilir. Köle, komuta kontrol sunucularına hizmet eden bilgisayar demektir.

Bu olayın tespiti için SIEM'de yazılan korelasyon kuralı Bölüm 4.2.4.1'de tanımlanmıştır.

4.2.4.1. Kural 10: Oltalama Saldırı Tespiti

Bu korelasyon ile, kullanıcı EK içeren mail aldıktan sonra (Mail.Attachment:* AND EventMap.Type:"Mail") , eğer iç ağdaki bir kullanıcı bilgisayarı şüpheli IP'lere istek yapıyor ise ((Source.Position:"in" Event.Category:"Suspicious Traffic") ve 1 dakika içerisinde 10'dan fazla IP'ye yaptığı istek güvenlik duvarı tarafından engelleniyorsa (Source.Position:in AND Destination.Position:out AND ((EventMap.Info:"Network Connection Deny" AND EventSource.Category:"Firewall") OR (Event.Action:("reset-both" OR "drop"))) alarm üremesi beklenmektedir.



Şekil 4.25: Oltalama Saldırısına Yönelik Korelasyon

Korelasyonun kural bölümünde logun içeriğinin mail olması ve aynı zamanda güvenlik duvarı üzerinden alınan loglar üzerinden yazılan korelasyonda iki adet liste tanımlaması yapılmıştır.

Şekil 4.19'da tanımlanan sorgu ile güvenlik duvarı tarafından engellenen iç ağdan dış ağa yapılan trafiklerin logları filtrelemesi beklenmektedir.

Query:Source.Position:in Destination.Position:out ((EventMap.Info:"Network Connection Deny" EventSource.Category:"Firewall") OR (Event.Action:("reset-both" OR "drop")))

Group Column ile filtrelenen loglar kaynak IP'sine göre gruplandırılacak.

Trigger Level 10 seçilmesinin sebebi, bu olayın 10 kez tekrarlanması şartını sağlamaktır. Time Period 60 seconds seçilmesinin sebebi ise, 10 kez tekrarlanacak bu querynin 1 dakika içerisinde gerçekleşmiş olması şartının sağlanmasıdır.

Name	List: Dis aga dogru trafiği 10 kez deny olan1 IP	
Type	Statistical	
Severity	Alert	
Query	Source.Position:in Destination.Position:out ((EventMap.Info:"Net	
Group Filter	Source.IP	
Value Filter	Source.IP	
Criteria	Value Count	
Trigger Count	>	10
Time Period	60	seconds

SAVE

Şekil 4.26: İç Ağdan Dış Ağa 10'dan Fazla Trafiği Engellenen IP'nin Tespiti

Tanımlanan şüpheli trafiklerin tespiti için yazılan ikinci listede ise **(**Source.Position:"in" Event.Category:"Suspicious Traffic") query'si yazılmıştır. Filtrelenen bu olayın 1 dakika içerisinde en az 1 kere tekrarlanması şartıyla çalışması beklenmektedir. Bu yüzden Trigger Level yani tetiklenme sayısı 1, check events ins last ise 60 seconds seçilmiştir.

Description	List: Dis aga supheli trafik yapan 1 IP	
Type	Statistical	
Severity	Alert	
Query	Source.Position:"in" Event.Category:"Suspicious Traffic"	
Group Filter	Source.IP	
Value Filter	Source.IP	
Criteria	Value Count	
Trigger Count	>	1
Time Period	60	seconds

SAVE

Şekil 4.27: Şüpheli Bir IP'ye Trafik Yapan IP'nin Tespit Edilmesi

Son duruma göre; 1 dakika içerisinde iç ağda 1 kere şüpheli trafik yapan IP 1 dakika içerisinde iç ağdan dış ağa doğru 10'dan fazla deny logu yaratmışsa ve bu IP EK içeren mail almışsa alarm üretilmesi beklenmektedir.

4.2.5. Custom Korelasyonlar

4.2.5.1. Kural 11: Sahte DHCP Sunucu Tespiti

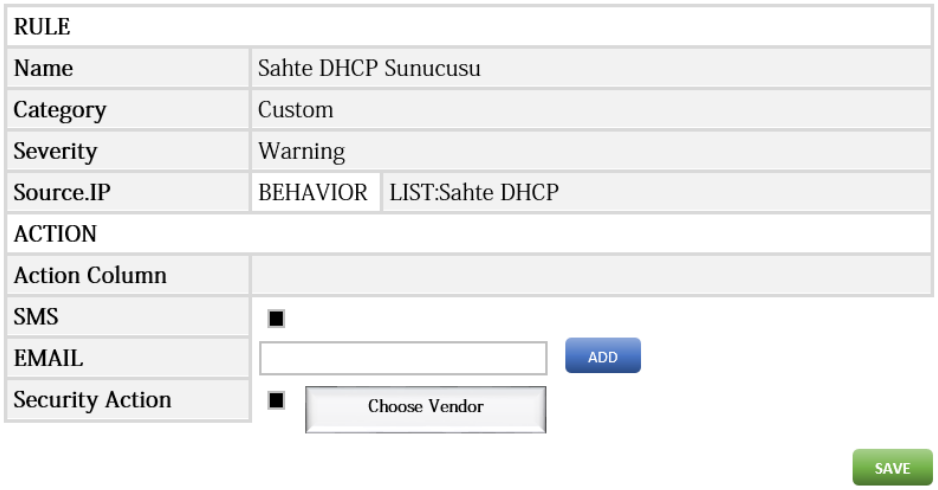
Dinamik Ana Bilgisayar Yapılandırma Protokolü anlamına gelen DHCP (Dynamic Host Configuration Protocol), bir ağ içindeki IP adreslerinin dağıtımı için hızlı, otomatik ve merkezi yönetim sağlayan bir protokoldür. DHCP aygıttaki alt ağ maskesini, varsayılan ağ geçidini ve DNS sunucusu bilgilerini yapılandırmak için de kullanılmaktadır. Ayrıca, DHCP, UDP 67 ve 68. Portlarını kullanmaktadır.

DHCP açlık saldırısı ise, DHCP sunucularını hedefleyen, sahte DHCP isteklerinin, DHCP sunucusu tarafından ayrılabilen tüm kullanılabilir IP adreslerini tüketmek amacıyla bir saldırgan tarafından hazırlanan saldırıdır. Dolayısıyla kurum içerisinde kullanılan DHCP sunucuları dışında başka bir IP'ye istek yapılıyorsa şüpheli bir durum olduğu anlaşılmalıdır. Bu bağlamda sahte dhcp sunucusunun tespit edilmesi için yazılacak korelasyonda ihtiyaç duyulan bilgiler;

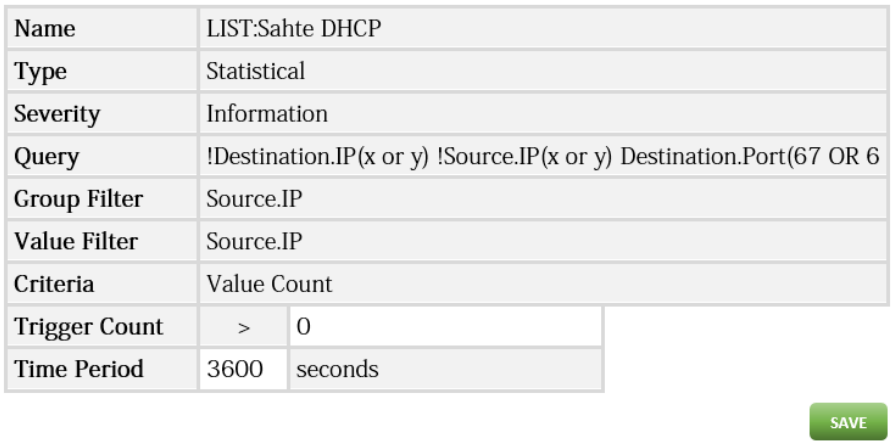
- Kurumda kullanılan DHCP sunucularının IP'leri

- Kullanılan portlar
- Trafik yönü (in, out)

Sahte DHCP sunucusunun tespit edilebilmesi için yazılan korelasyon kuralı Şekil 21'de gösterilmiştir.



Şekil 4.28: Sahte DHCP Sunucusunun Tespitine Yönelik Korelasyon



Şekil 4.29: Sahte DHCP Sunucusun Tespitine Yönelik Liste Tanımlaması

Şekil 4.21'de yazılan kuralda, Şekil 4.22'de gösterilen listeden gelen bir kaynak IP olursa alarm üretilecektir. Yazılan liste tanımlamasında;

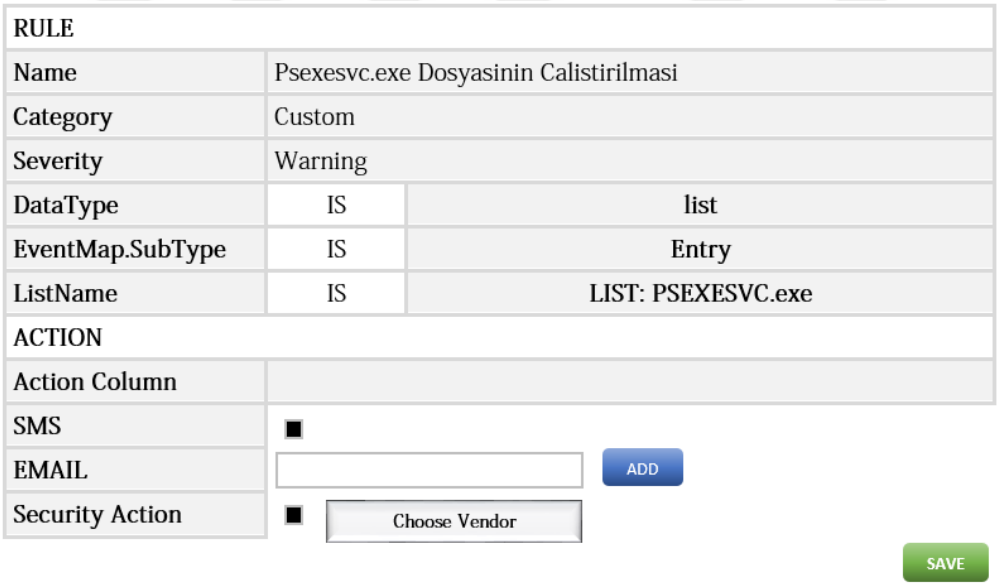
- x or y: kurum içerisindeki DHCP server IP'si
- !Destination.IP:(x or y) !Source.IP:(x or y) Destination.Port:(67 OR 68) Protocol.Name:(UDP OR TCP) Destination.Position:in Source.Position:in

Yazılan listeye göre; 67 veya 68 portlarını kullanan, istek yapan kaynağın pozisyonu veya istek yapılan hedef pozisyon iç ağ olan bir Kaynak IP veya hedef IP kurumda kullanılan DHCP sunucusu dışında bir IP ise ve bu IP 1 dakika içerisinde en az 1 kere trafik yapmışsa liste oluşturmaktadır. Elde edilen bu IP Şekil 4.21'deki kuralda göründüğü gibi BEHAVIOR komutuyla listeden çekilmiştir.

4.2.5.2. Kural 12: Uzaktan İşlem Yürütme Dosyası PSEXESVC.EXE'nin Çalıştırılması

PsExec, tıpkı telnet gibi konsol üzerinden çalıştırılan manuel olarak yüklemeye gerek kalmadan çalışmaktadır. Diğer sistemlerde uzaktan kod yürütmeyi sağlamaktadır.

Bu uygulama sayesinde aynı ağda bulunan bir bilgisayara kolaylıkla sızılabilir ve istenilen işlemler gerçekleştirilebilir. Bu uygulama her ne kadar yasal olsa da kötü amaçlar için kullanılabilmektedir. Bu yüzden bu uygulamanın kurum içerisinde çalıştırılması ve PSEXESVC.exe dosyasının kullanılması risk teşkil etmektedir. Bu riske karşı tedbir alabilmek için uygulamayı çalıştıran kullanıcılar SIEM ile tespit edilebilmektedir.



Şekil 4.30: Psexesvc.Exe Dosyasının Çalıştırılmasının Tespitine Yönelik Korelasyon

Şekil 4.23'de oluşturulan korelasyon kuralında 3 kural tanımlanmıştır;

- DataType IS List: Veri türü liste ise
- EventMap.SubType IS Entry

- ListName IS LIST:PSEXESVC.exe: Şekil 4.24'te tanımlanan listedeki kural çalışmasını ifade etmektedir.

Şekil 4.24'te yapılan liste tanımlamasında;

Query bölümüne aşağıdaki komut girilmiştir;

- Event.VendorID:1 (Process.Name:(*cmd* OR *powershell* OR *rundll32* OR *wscript* OR *scrcons* OR *scripts* OR *bash* OR *sh*) OR Process.Command:(*cmd* OR *powershell* OR *rundll32* OR *wscript* OR *scrcons* OR *csripts* OR *bash* OR *sh*)) Process.ParentCommand:PSEXESVC.exe

Bu komuta göre SIEM'e aktarılan loğlarda çalışan komut veya process içerisinde cmd, powershell, rundll32, wsciprt, scrcons, scripsts, bash, sh geçiyorsa ve PSEXESVC.exe komutu 180 saniye içerisinde en az 1 kere çalıştırılırsa listenin oluşması beklenmektedir.

Name	LIST:PSEXESVC.exe	
Type	Statistical	
Severity	Information	
Query	Event.VendorID:1 (Process.Name:(*cmd* OR *powershell* OR *ru	
Group Filter	EventSource.HostName	
Value Filter	EventSource.HostName	
Criteria	Value Count	
Trigger Count	>	0
Time Period	180	seconds

SAVE

Şekil 4.31: Psexecsvc.exe Dosyasının Çalıştırılmasının Tespitine Yönelik Liste Tanımlaması

cmd: CMD, Microsoft komut yorumlayıcısıdır [86].

powershell: NET üzerinde oluşturulmuş görev tabanlı bir komut satırı kabuğu ve betik dilidir [87].

rundll32: Rundll32 komutuyla çalıştırılan belirli bir DLL için yardım bilgileri saklanmaktadır [88].

wscript: Windows Komut Dosyası (Windows Script Host) Ana Bilgisayarı, kullanıcıların görevleri gerçekleştirmek için çeşitli nesne modellerini kullanan çeşitli dillerde komut dosyaları yürütebileceği bir ortam sağlamaktadır [89].

scrcons: Microsoft'un yürütülebilir dosya kaynağıdır [90].

scripts: Linux tabanlı sistemlerde çalıştırılan komutlar.

bash: Bash GNU işletim sistemi için bir kabuk ya da başka bir deyişle komut dili yorumlayıcısıdır [91].

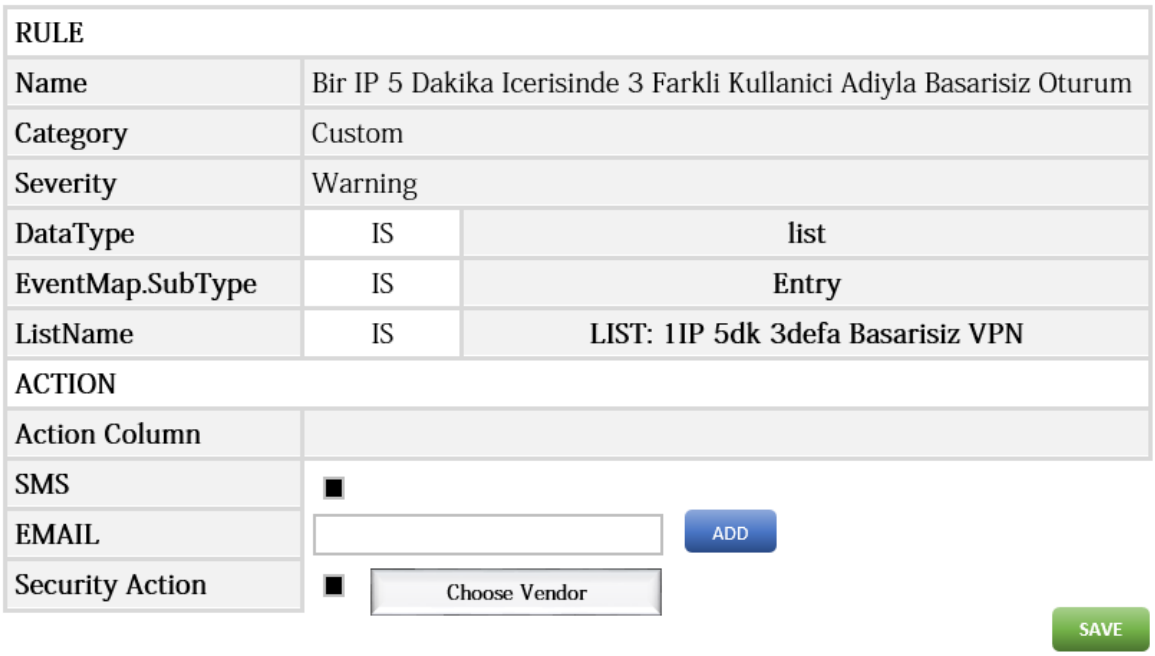
sh: Linux tabanlı sistemlerde çalıştırılan komut dosyasıdır [92].

4.2.5.3. Kural 13: Bir IP 5 Dakika İçerisinde 3 Farklı Kullanıcı İsmiyle VPN Oturum Denemesi

VPN hizmetleri ile internet erişiminin olduğu her yerden kurum içerisindeki sistemler, uzaktan yönetilebilmektedir. Siber saldırganlar bir kurumun VPN erişimleri ile sistemlere sızmak isteyebilirler. Benzer şekilde kurum içerisinde çalışan kötü niyetli kişiler de sistemler üzerinde kendi kullanıcısı haricinde özel yetkiye sahip başka kullanıcı isimlerini kullanarak VPN erişimi sağlamak istiyor olabilirler.

Şekil 4.25'de yazılan korelasyon kuralına göre 1 IP 5 dakika içerisinde 3 farklı kullanıcı adıyla başarısız oturum açmaya çalışırsa tespit edilmesi beklenmektedir.

Kural tanımlamasında süre ve tetiklenme olayı olduğu için liste tanımlaması yapılması gerekmektedir. Bu kural tamamen liste özelliği ile çalışmaktadır. O yüzden ListName içerisinde Şekil 4.26'da yazılan listenin adı girilmiştir.



Şekil 4.32: 3 Farklı Kullanıcı Adıyla VPN Denemesinin Tespitine Yönelik Korelasyon

Şekil 4.26'da tanımlanan listede tetiklenme söz konusu olduğu için ve zaman tanımlaması yapıldığı için liste türü "Statistical" olarak tanımlanmıştır. Yazılan Query;

- EventSource.Vendor:" kullanilan urun" EventMap.Info:"VPN User Deny"

  EventMap.SubType:"Deny" Event.Action:"globalprotectportal-auth-fail"

Query'de tanımlanan alanların belirlenmesi için öncelikle SIEM ekranına düşen loglar içerisinde herhangi başarısız VPN logu tespit edilmelidir. Tespit edilen loglar detay bölümünde EventMap.SubType, Event.Action, EventSource.Vendor alanlarının içeriği not alınmalıdır.

EventSource.Vendor: VPN ürünü hangi markaya ait ise o seçilmelidir.

EventMap.SubType: Bu kısımda deny olan trafikler seçilmelidir. "Deny" değeri atanmalıdır.

Event.Action: Gelen loglar içerisinde Event.Action incelendiğinde authentication fail gibi bir log görüntülenecektir. Event.Action kısmı bu olmalıdır.

EventMap.Info:"VPN User Deny" şekilde kullanıcı erişiminin başarısız olduğuna yönelik bir log seçilmelidir.

Name	LIST:1IP 5 dk 3defa Basarisiz VPN	
Type	Statistical	
Severity	Information	
Query	EventSource.Vendor:" kullanilan urun" EventMap.Info:"VPN User	
Group Filter	Source.IP	
Value Filter	Source.UserName	
Criteria	Unique Count	
Trigger Count	>	3
Time Period	300	seconds

SAVE

Şekil 4.33: 3 Farklı Kullanıcı Adıyla VPN Denemesinin Tespitine Yönelik Liste Tanımlaması

Yazılan listede, çıkan sonuçlar kaynak IP'ye göre gruplandırılacak (Group Filter:SourceIP) ve değer filtresi kullanıcı adı (Source.UserName) seçilmiştir. Çıkan sonuçlardan benzersiz (Unique Count) olan sonuçlar listelenecek ve query bölümünde yazılan olay ve 300 saniye içerisinde en az 3 defa tekrarlanması şartı ile liste oluşacaktır.

4.2.5.4. Kural 14: Windows Komut Satırı ile Uzaktan Bağlantının Tespiti

Powershell ve CMD.exe uygulamaları, Windows işletim sistemlerinde komut satırı yorumlayıcısı olarak kullanılmaktadır. İşletim sistemleri üzerinde çeşitli işlemler komut satırı ile de yapılabilmektedir.

PowerShell, Microsoft tarafından Windows komut satırı cmd.exe [86] alternatif olarak geliştirilen yeni nesil bir komut satırı uygulamasıdır [87].

Standart bir kullanıcının, uzaktan erişimleri ya web tarayıcıları üzerinden ya da uzak masaüstü araçları ile yapması beklenmektedir. Ancak bir kullanıcı powershell veya cmd uygulamaları üzerinden uzaktan bağlantı sağlıyor ise şüpheli bir durum söz konusudur.

Şekil 4.27'de yazılan korelasyonda Windows komut satırı ile uzak bağlantı sağlayan kullanıcılar tespit edilmektedir. Korelasyon tanımında liste kullanılmıştır. Şekil 4.28'de yazılan liste ListName kural bölümünde belirtilmiştir. Ayrıca kuralın türünün liste olduğu ve bu liste şartı sağlandığında alarmın çalışacağı DataType ile belirtilmiştir.

RULE		
Name	Windows Komut Satiri Ile Uzak Baglanti Yapilmasi	
Category	Custom	
Severity	Warning	
DataType	IS	list
EventMap.SubType	IS	Entry
ListName	IS	LIST: Windows Komut Satiri Uzak Baglanti
ACTION		
Action Column		
SMS	■	
EMAIL		ADD
Security Action	■	Choose Vendor

SAVE

Şekil 4.34: Komut Satırı ile Uzak Bağlantıların Tespit Edilmesine Yönelik Korelasyon

Şekil 4.28'de yazılan listede yarım saat içerisinde en az 1 kere powershell veya cmd komut yorumlayıcısı üzerinde yazılan komut içerisinde "http" veya "https" protokolü veya "username" veya "password" kelimeleri geçiyorsa liste oluşacaktır.

Name	LIST: Windows Komut Satiri Uzak Baglanti	
Type	Statistical	
Severity	Information	
Query	Process.Name:(*powershell* OR *cmd*) Process.CommandLine:(*	
Group Filter	EventSource.HostName	
Value Filter	EventSource.HostName	
Criteria	Unique Count	
Trigger Count	>	0
Time Period	1800	seconds

SAVE

Şekil 4.35: Komut Satırı ile Uzak Bağlantıların Tespit Edilmesinde Liste Tanımlaması

Bu şartın sağlanması için yazılan sorgu;

- Process.Name:(*powershell* OR *cmd*) Process.CommandLine:(*http* OR *https* OR "username" OR "password")

4.3. Gösterge Tablosu Yapılandırma

Bir veri merkezini yönetmek çok fazla koordinasyon gerektirmektedir. Anlık olarak, gösterge tablolarına, güç tüketimine ve sistem erişimlerinin kontrol edilmesi için izleme ekipleri kurulmaktadır.

SIEM, daha gelişmiş izleme için veri merkezlerine başka bir güvenlik katmanı eklemektedir. Verimli bir SIEM ortamı için, hangi olayların manuel müdahale gerektirdiği ve günlük, haftalık veya aylık olarak hangi raporlara ihtiyaç duyulduğunun planlanması gerekir.

Gösterge tabloları (dashboard), ağdaki güvenlik durumunu izlemek için izleme ve raporlama metrikleri sunmaktadır. Kullanıcıların grafikler ve tablolar kullanarak mevcut ağ altyapısı verilerinin bir özetini okumalarına olanak tanımaktadır. İyi bir SIEM aracında, kullanıcılar ihtiyaçlarına yönelik yapılandırabilmelidir.

Bölüm 4.3'ün alt başlıklarında SIEM uygulamasının yapıldığı veri merkezi örnekleminde oluşturulan dashboard tasarımları bulunmaktadır. Dashboard üzerinde oluşturulan Widget'lar bulunmaktadır. Her bir Widget istenilen verinin gösterildiği araçlardır.

4.3.1. Atak, Malware, Virüs ve Spam Aktiviteleri

Tespit edilen atak, malware, virüs ve spam aktivitelerinin canlı olarak takip edilmesi için yazılan gösterge konfigürasyonu aşağıdaki gibidir;

Oluşturulan Widget'ta hangi bilginin gösterileceği Query bölümünde yazılan kurala bağlıdır. Query bölümünde yapılan atakların gösterilmesi için "DataType:"log" EventMap.Type:"Attack" " sorgusu yazılmıştır. Bu sorguya göre, veri tipi "log" olan ve olay tipi "Attack" olan olaylar gösterilecektir. Aynı şekilde Malware için yazılacak sorgu; "DataType:"log" EventMap.Type:Malware", virüs için "DataType:"log" EventMap.Type:Virus", Spam aktiviteleri için ise "DataType:"log" EventMap.Type:Spam" olması gerekmektedir.

+ADD WIDGET	
Name	Tespit Edilen Atak Aktiviteleri
Time Column	Time.Generated
Query Type	○Count ○Unique ○Value
Refresh Time	1 min.
Query	DataType:" log" EventMap.Type:" Attack"
Index Time	6 Hour

SAVE

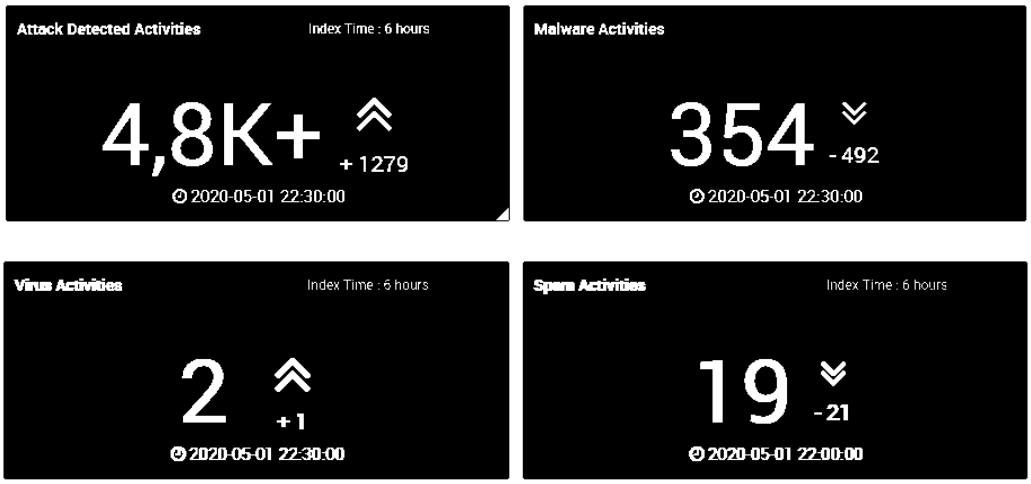
Şekil 4.36: Atak Aktivitelerinin Takibi için Gösterge Tablosunun Yapılandırılması

+ADD WIDGET	
Name	Tespit Edilen Atak Aktiviteleri
Time Column	Time.Generated
Query Type	○Count ○Unique ○Value
Refresh Time	1 min.
Query	DataType:" log" EventMap.Type:" Malware"
Index Time	6 Hour

SAVE

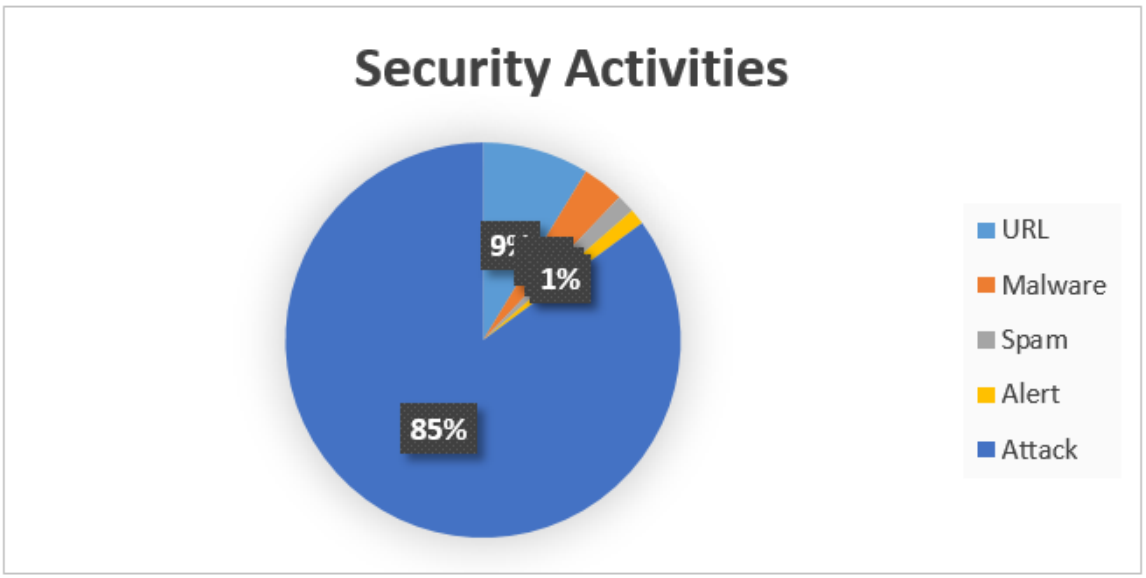
Şekil 4.30: Malware Aktivitelerinin Takibi için Gösterge Tablosunun Yapılandırılması

Widget'lar eklendikten sonra görüntülenecek ekran Şekil 4.31'de olduğu gibidir;



Şekil 4.31: Atak ve Malware Aktivitelerinin Gösterge Tabloları

Örnek veri merkezine ait sistemlerin içerisinde güvenlik olaylarının kategorize edilerek dashboard üzerinde gösterilmesi için Şekil 4.31'deki çıktı elde edilmiştir. Bu çıktının elde edilebilmesi için kural setinde *" DataType:"log" EventMap.Context:"Security" "* komutu kullanılmıştır. Grafiğe gösterimi her 1 dakikada bir yenilenmektedir. Loglar ise 6 saatte bir çekilmektedir.

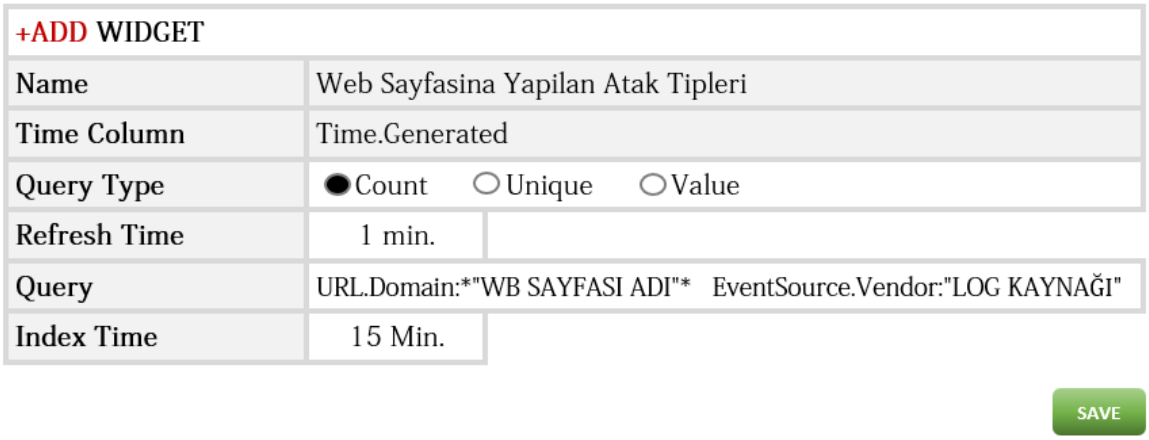


Şekil 4.32: Güvenlik Aktiviteleri Gösterge Tablosu

Şekilde 4.32'de görüldüğü üzere en sık rastlanan güvenlik olayının "Attack" kategorisinde olduğu anlaşılmaktadır. Bu rapor sayesinde güvenlik olayları için farkındalık yaratılmaktadır.

4.3.2. Web Sayfalarına Yapılan Atak Türleri

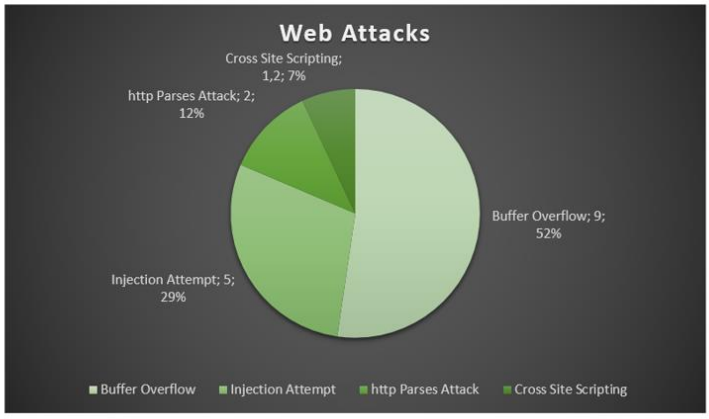
Dış ağa açık web sayfalarına yönelik yapılan saldırı türlerinin canlı olarak izlenmesi için Şekil 4.33'de yer alan konfigürasyon ile Şekil 4.34'deki dashboard tasarımı gerçekleştirilmiştir.



Şekil 4.33: Web Atak Tiplerinin Gösterge Tablosunun Yapılandırılması

Yapılandırma ekranında URL.Domain:*"WB SAYFASI ADI"* EventSource.Vendor:"LOG KAYNAĞI"komutu kullanılmıştır. EventSource.Vendor kısmında log alınan güvenlik cihazının yani üreticinin adı, URL.Domain'de ise atak yapılan sayfaların adı yazılmalıdır. İki yıldız (* *) arasında tanımlama yapılması, domain ve alt domainleri de kapsamaktadır. Eğer tek bir web sayfasına yönelik atakların tanımlanması isteniyorsa iki tırnak (" ") arasına ilgili web sayfası yazılabilir. Grafikte gösterilen veriler her 15 dakikada aranacak ve her 1 dakika da grafik verileri yenilenecektir.

Attack Type	Attack Count
Buffer Overflow	9
Injection Attempt	5
http Parser Attack	2
Cross Site Scripting	1



Şekil 4.34: Web Saldırı Türlerinin Gösterge Tablosu

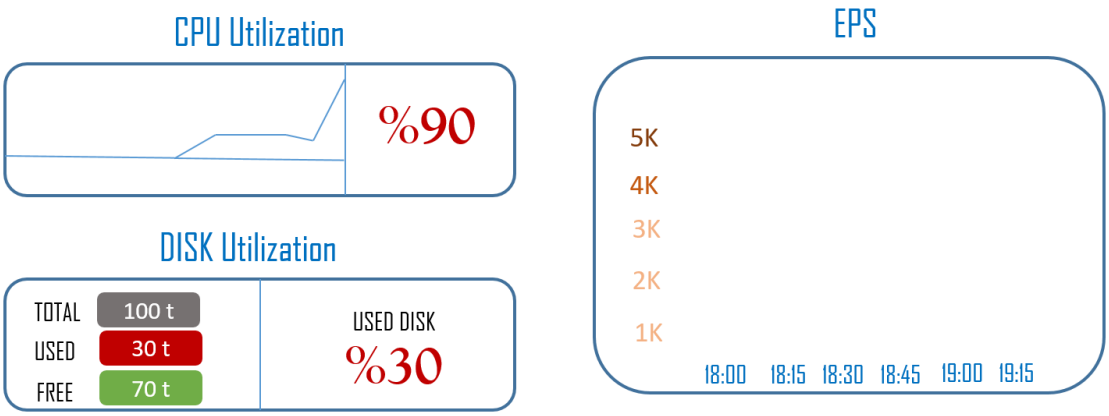
Bu tasarımların dışında aşağıdaki dashboardların tanımlanması;

- EPS değerlerinin takip edildiği,
- Ağ trafik yoğunluğunun takip edildiği,
- Yazılan alarmların takip edildiği,
- SIEM kaynaklarının (disk, ram vb) takip edildiği,
- Kritik sistemlerde açılan oturumların takip edildiği gibi durumların izlenmesi iyi bir izleme, problemlerin erken tespiti için önemlidir.

4.3.3. SIEM Sistem Olayları

Aşırı kaynak kullanımlarının, anormal artışların takip edilebilmesi için sistem olaylarının görüntüleneceği dashboard tasarımı bulunmalıdır. Bu tasarımlar genel olarak SIEM çözümlerinde varsayılan olarak gelmektedir.

Dashboard'da Şekil deki gibi CPU, DISK, EPS gibi sistem olayları takip edilebilmektedir. Böylece log kaçırma, yavaşlık gibi sistemsel olaylara müdahale edilebilir. Örneğin disk değeri %90'a ulaşmışsa acil müdahale edilmesi gerektiği anlaşılmaktadır.



Şekil 4.35: Sistem Olaylarının Gösterge Tablosunda Gösterimi

4.4. Raporlama

Raporlama ile belirli zaman diliminde gerçekleşen olaylara görünürlük kazandırmaktadır. Raporlama sayesinde sistem ve güvenlik olayları hakkında yöneticilere düzenli bilgilendirme sağlanmaktadır.

Bu raporların oluşturulması ihtiyaca ve o anlık duruma göre değişmektedir. Raporlar, verilen ölçütlere göre oluşturulmaktadır. Örneğin kritik sistemlere bağlantı sağlayan IP ve kullanıcı bilgilerinin haftalık kontrol edilebilmesi için rapor oluşturulabilmektedir. Bunun için kritik sistemin IP bilgisi, zaman bilgisi ölçüt olarak seçilmelidir.

Raporlama sayesinde çok sayıda güvenlik olayı, sistemde yaşanan bir problemin kök nedeninin tespiti gibi durumlar raporlanabilmekte ve üst yönetime sunulabilmektedir. Bu sayede, hem güvenlik tedbiri alınması sağlanmış olacak hem de üst yönetimin bilgilendirilmesi konusunda spesifik raporlar oluşturulabilecektir.

Örnek olarak kullanılabilecek bazı raporlar:

Kullanıcı İnternet trafik raporu: Bu raporda kurum içerisinde en çok internet kullanımını gerçekleştiren personellerin listesi alınabilir.

Sosyal Medya Kullanım Raporu: Bu raporda kurum içerisinde sosyal medya (Instagram, Youtube vb.) kullanan kullanıcılar tespit edilebilir.

İnternet Erişimi olan sunucu Raporu: Bu rapor ile internet erişimi olmaması gereken sunuculardan birisi internete erişiyor ise raporlanabilir.

Anti-Virus Yüklü olmayan kullanıcılar: Bilgisayarında anti-virüs yüklü olmayan kullanıcılar raporlanabilir. Bu rapor aslında SCCM çözümünün görevidir. Ancak SCCM haricinde böyle bir rapor çıkartılmak istenirse, SIEM üzerinde son 2 haftada antivirüs sunucusuna ilgili porttan hiç istek yapmayan kullanıcılar raporlanabilmektedir.

Raporlama, SIEM sürecinin kritik noktalarından birisidir. Bu raporlar tamamen ihtiyaca göre belirlenmektedir. Her olayın raporlanması, çok sayıda raporun oluşmasına sebep olacak ve bu raporların incelenmesini güçlendirecektir. Bu yüzden spesifik olarak önemli durumların raporlanması, raporlar içerisinde istenen tüm bilgilerin sağlanabilmesi önem taşımaktadır.

4.4.1. Rapor 1: Eşler Arası Uygulamaları Kullanan Kullanıcıların Raporu

Eşler arası uygulamalar (P2P – Peer-to-Peer), her bir tarafın aynı özelliklere sahip olduğu ve her iki tarafın da bir iletişim oturumu başlatabildiği merkezi olmayan bir iletişim modelidir. İstemcinin bir hizmet isteği yaptığı ve sunucunun isteği yerine getirdiği istemci/sunucu modelinin aksine, P2P ağ modeli her düğümün hem istemci hem de sunucu olarak çalışmasına izin vermektedir.

P2P üzerinden iki eş arasında dosya paylaşımları yapılabilmektedir. Bu da bazı tehlikeleri beraberinde getirmektedir. P2P kullanmanın getirdiği bazı riskler:

Kötü amaçlı yazılım riskleri: P2P uygulamaları ile indirilen bir dosya zararlı yazılım olabilir. Bu da bağlı olunan ağ ve o ağdaki sistemlerin de tehlikeye girmesi demektir.

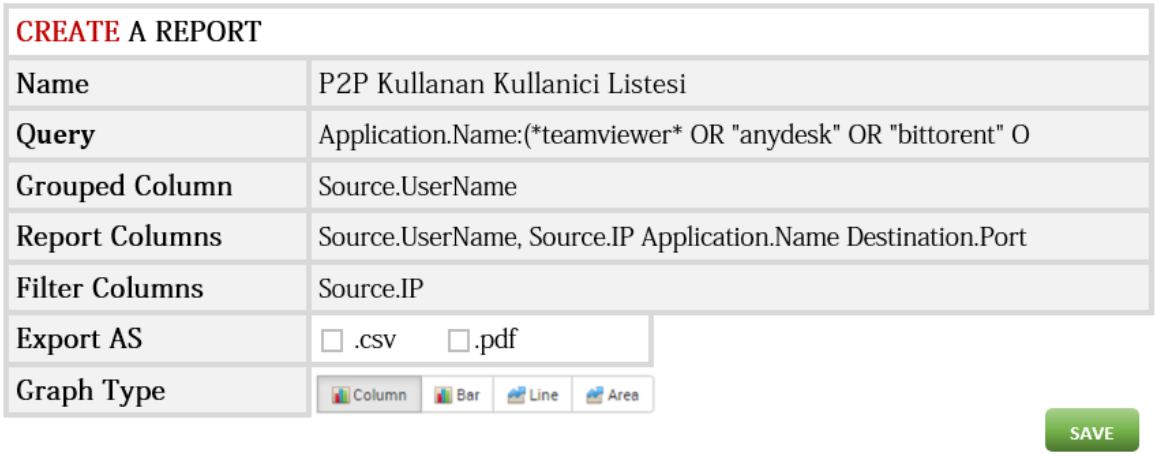
Veri Güvenliği: Kuruluşun kritik iş bilgilerine yetkisiz erişimler söz konusu olabilmektedir.

SIEM uygulamasının yapıldığı veri merkezi bünyesinde bu riskler kabul edilemez. Bu doğrultuda bu riskleri taşıyan bazı uygulamaları kullanan kullanıcıların farkında olabilmek için aşağıdaki rapor tanımlanmıştır.

P2P rapor tanımlamasında, teamviewer, anydesk, bittorrent, ultrasurf, tunnelbear, Freegate, ipvanish uygulamalarını kullanan kullanıcıların trafiği güvenlik duvarından geçiyorsa bu kişilerin kaynak IP'si, kullanıcı adı, hedef IP, kullandığı uygulama bilgileri yer almaktadır.

Rapor kural seti olarak " Application.Name:(*teamviewer* OR "anydesk" OR "bittorent" OR "ultrasurf" OR "tunnelbear" OR "freegate" OR "ipvanish") EventMap.SubType:Allow " kuralı girilmiştir. Bu komut kullanılan uygulamaların tespitini sağlamaktadır. Filter

Columns bölümünde ise Source.IP bilgisine göre filtreleme yapılmakta olup, Report Columns bölümünde girilen bilgiler ise raporda görüntülenecek alanlardır. Şekil 4.36'daki rapor tanımlamasına göre; kullanıcının adı, kullanıcının IP'si, kullanılan uygulamanın adı, hedef port bilgileri görüntülenecektir.



Şekil 4.36: Peer-to-Peer Uygulama Kullanan Kullanıcıları Tespit Raporu

Oluşturulan bu rapor .pdf, .csv uzantılarıyla dışarı aktarılabilmekte ve mail yolu ile istenilen kişilere iletilebilmektedir. Böyle bir rapor sayesinde bilgi güvenliği ekibi ve yöneticiler P2P uygulamalarını kullanan kullanıcıların listesini elde etmiş olacaktır. Eğer bu raporlar Schedule edilir ise günlük, haftalık veya aylık olarak yöneticilere e-posta yoluyla otomatik olarak iletilmesi sağlanabilir.

4.4.2. Rapor 2: Karantina Bölgesinden Yapılan Erişimlerin Tespiti

Antivirüs yazılımı, bireysel bilgi işlem cihazlarında, ağlarda ve BT sistemlerinde kötü amaçlı yazılım bulaşmalarını önlemek, tespit etmek ve kaldırmak için tasarlanmış yazılımlardır [93]. USB, e-posta gibi yöntemlerle bir şekilde kullanıcı bilgisayarına zararlı dosya bulaştığında kişilerin bilgisayarları ve o bilgisayarların bağlı olduğu sistemler tehlike altındadır. Bu bağlamda kullanıcıların bilgisayarlarında anti-virüslerin yüklü olması önemlidir.

Kullanıcı bilgisayarlarında anti-virüs yüklü olmayan kullanıcıların tespitini sistem ekibi active directory, SCCM (System Center Configuration Manager) vb. sistemler üzerinden alabilmektedirler. Ayrıca NAC sistemi kullanılarak bilgisayarlarında AV yazılımı olmayan

kullanıcılar güvenlik duvarı üzerinde karantina bölgesine alınarak erişimleri kısıtlanabilmektedir.

NAC üzerinden SIEM'e alınacak loglar ile olası yanlış konfigürasyon ile karantina bölgesinden yapılacak erişimler için Şekil 4.37'deki gibi alarm tanımlanabilir.

Şekil 4.37: Karantina Bölgesinden Başarılı Erişimin Tespitine Yönelik Korelasyon

Bu kurala göre kaynak bölgesindeki bir cihaz karantina bölgesinde ise ve herhangi bir hedef adrese doğru gitmeye çalışmışsa ve bu trafik güvenlik duvarı üzerinden geçmişse alarm üretilmesi beklenmektedir. Bu olayın raporlanması için Şekil 4.38'deki rapor tanımlaması yapılmalıdır.

Şekil 4.38: Karantina Bölgesinden Başarılı Erişim Sağlayan IP'nin Tespit Raporu

5. SONUÇ ve TARTIŞMA

Bu çalışmada etkin SIEM yönetimi ve bir veri merkezinde güvenlik yaklaşımı üzerine incelemeler yapılmıştır. Çalışmada, bir veri merkezinde hangi güvenlik çözümlerinin olması gerektiği, etkin SIEM yönetiminin sağlanması ve devlet kurumuna ait bir veri merkezi sistemleri üzerinde gerçekleştirilen uygulama ile örnek korelasyonlar, raporlar ve dashboard tasarımları gerçekleştirilmiştir.

Örnek veri merkezi bünyesinde gerçekleştirilen SIEM uygulamasında güvenlik ve ağ cihazları ile sunuculardan loglar alınmıştır. Alınan bu loglar üzerinden korelasyon kuralları ve raporlar tanımlanmıştır. Bu sayede örnek veri merkezi uygulamalarına yönelik gerçekleşen saldırı türleri ve ağ içerisindeki şüpheli hareketlere yönelik farkındalık yaratılmıştır.

Siber güvenlik ekipleri, bir güvenlik olayı, anında, öncesinde ve sonrasında sorumluluklarını ve alacakları aksiyonları net bir şekilde anlamalıdırlar. Her kurumun bir olay karşısında playbook olarak adlandırılan ve Türkçe karşılığı başucu kitabı olarak geçen eylem planı olmalıdır. Bir olay karşısında temel eylem adımları; olay tespiti, olaya yanıt ve iletişimdir. Burada en büyük problem, olaylara güvenlik ekibinin çok hızlı tepki vermesi gerektiğidir. Bir olay karşısında ne kadar hızlı tepki verilirse tehdidin şiddeti ve maliyeti o derece azalacaktır. Yapılan bu çalışma ile SIEM çözümleri ile olay tespitlerinin yapılabildiği anlaşılmıştır. Ancak tespit edilen olaylara müdahale edebilmek için yazılan korelasyon kuralları ve alarmlar ile yaşanan olayın güvenlik ekiplerine iletilmesi gerekmektedir. Güvenlik ekibinin kendilerine kısa mesaj veya e-posta yoluyla gelen bu alarmları en hızlı şekilde görmesi ve anında müdahale edebilmeleri gerekmektedir. Bu alarmların görülmesinde geç kalınır veya hızlı müdahale edilemezse tehdidin etkisi ve maliyeti artacaktır.

Bu tez çalışması ile:

- Kurumlarda SIEM ürünleri için özel personel bulundurulması (ayrı bir SIEM ekibinin olması) ile olaylara tepki sürelerinin azaltılacağı ve diğer tehditlerin tespitinde güç kazandırılacağı anlaşılmıştır.

- Gece saatlerinde nöbetçi personelin olmaması, doğru yazılmamış veya eksik korelasyon ve alarm kurallarının tanımlanması gibi durumlarda siber olayların farkına varılamadığı, müdahale edilemediği veya geç müdahale edilebildiği görülmüştür.
- Aynı aynıda çok sayıda farklı saldırılar geldiğinde ekip sayısının yetersiz olması durumunda saldırılara odaklanma ve müdahale probleminin yaşanabileceği anlaşılmıştır.

Örnek veri merkezi SIEM uygulamasında yazılan bazı korelasyonlar sayesinde aşağıdaki faydaların sağlandığı görülmüştür:

5.1. Veri Merkezi Uygulamasında Yazılan Korelasyonlar ve Çıktıları

Bölüm 4.2'de yer alan veri merkezi bünyesinde uygulanan korelasyon neticesinde bir takım bulgular elde edilmiştir. Yazılan korelasyonların çıktıları aşağıdaki gibidir:

Tablo 5.1: Uygulama Bölümünde Yazılan Korelasyon Bulgularının Değerlendirilmesi

BULGULAR	**SONUÇ**
Kural 1: Dışarıya Veri Aktarılması Tespit Edilen Olay Sayısı: 0	Kural 1'de veritabanı yöneticisi tarafından belirtilen kritik tablolardan dışarıya veri aktarıldığında olayı gerçekleştiren kişiyi tespit edebilmek ve olayın yaşandığı anda müdahale edebilmek için korelasyon kuralı yazılmıştır. Kural 3 ay boyunca izlenmiş, bir bulguya rastlanılmamıştır. Bunun sebebi, 5237 sayılı TCK (Türk Ceza Kanunu), "Bilişim Alanında İşlenen Suçlar" başlıklı kanun ve 6698 sayılı KVKK kanununa göre hukuki yaptırımları caydırıcı unsur olabilir.

Tablo 5.1 (devam): Uygulama Bölümünde Yazılan Korelasyon Bulgularının Değerlendirilmesi

Kural 2 ve 3: DELETE / UPDATE Komutunun Çalıştırılması Tespit Edilen Olay Sayısı: 0	Kural 2 ve 3 ile veritabanı yöneticisi tarafından belirtilen kritik tablolarda SQL "DELETE" ve "UPDATE" komutunun çalıştırılmasının tespit edilmesi amaçlanmıştır. Korelasyon kuralının yazıldığı günden itibaren 3 ay süreyle loglar izlenmiş olup herhangi bir bulguya rastlanılmamıştır. Bunun sebebinin personellerin karşılaşacağı hukuki yaptırımlar olabileceği tahmin edilmektedir.
Kural 4: SQL Injection Saldırı Tespiti Tespit Edilen Olay Sayısı: 5	3 aylık süre zarfında 5 adet injection saldırısı tespit edilmiş olup, bu saldırıların güvenlik çözümleri tarafından engellendiği anlaşılmıştır.
Kural 5: Cross Site Scripting Saldırıları Tespit Edilen Olay Sayısı: 1	Bölüm 4.2.2'de yazılan 5. kurala göre 3 aylık izleme süresinde veri merkezinin web uygulamalarına yönelik 1 adet Cross Site Scripting atağının yapıldığı tespit edilmiştir. Atağı yapan kaynak IP'sinin yurt dışı kaynaklı olduğu tespit edilmiş olup ilgili atağın güvenlik cihazları tarafından engellendiği görülmüştür.
Kural 6: Buffer Overflow Saldırıları Tespit Edilen Olay Sayısı: 9	3 aylık süre zarfında 9 adet buffer overflow saldırısı tespit edilmiş olup, bu saldırıların güvenlik çözümleri tarafından engellendiği anlaşılmıştır.

Tablo 5.1 (devam): Uygulama Bölümünde Yazılan Korelasyon Bulgularının Değerlendirilmesi

Kural 7: Command Execution Saldırısı Tespit Edilen Olay Sayısı: 0	7. kural neticesinde veri merkezinin web uygulamalarına yönelik 3 aylık periyotta Command Execution saldırısına rastlanmamıştır. Ancak bu durum ile daha sonra karşılaşılmayacağı anlamına gelmemektedir. Bu olaya yönelik korelasyon kuralının aktif olarak çalışmaya devam etmesi gerekmektedir.
Kural 8: Port Tarama Saldırısı Tespit Edilen Olay Sayısı: 0	Yazılan kuralın 3 aylık izleme sürecinde güvenlik duvarını aşan başarılı port taramalarına rastlanmamıştır. Çok fazla başarısız olan port atakları tespit edilmiş olup bu atakların veri merkezi sistemlerine özel olmadığı, rastgele yapılan port tarama atakları olduğu anlaşılmıştır.
Kural 9: Çok Sayıda 404 Hatası Tespit Edilen Olay Sayısı: 220	3 aylık izleme sürecinde Kural 9'da tanımlanan korelayon kuralı sayesinde 220 IP'nin bu kuralı tetiklediği tespit edilmiştir. 215 IP'nin Çin, Amerika ve Rusya kökenli olduğu ve kurum web sayfasında sürekli farklı subdomainleri kontrol ettiği anlaşılmıştır. 5 IP'nin ise yalnızca bir sefer trafik yaptığı görülmüş ve şüpheli bir hareketine rastlanmamıştır.
Kural 10: Oltalama Saldırı Tespiti Tespit Edilen Olay Sayısı: 0	Şüpheli e-postaların personeller tarafından açılmadığı, bilgi güvenliği

	farkındalık eğitimlerinin katkı sağladığı anlaşılmıştır.

Tablo 5.1 (devam): Uygulama Bölümünde Yazılan Korelasyon Bulgularının Değerlendirilmesi

Kural 11: Sahte DHCP Sunucu Tespiti [0] Tespit Edilen Olay Sayısı: 0	Bu olayı gerçekleştirmek için iç ağa bağlı olunmalıdır. Kurum çalışanlarından veya dış dünyadan bu olayı gerçekleştirecek bir saldırı girişimi tespit edilememiştir.
Kural 12: Uzaktan İşlem Yürütme Dosyası PSEEXESVC.EXE'nin çalıştırılması Tespit Edilen Olay Sayısı: 0	Herhangi bir bulguya rastlanılmamıştır. Bunun sebebi, saldırı girişiminin olmamasından veya kullanıcı bilgisayarlarının tamamından log toplanmaması olabilir.
Kural 13: Bir IP 5 Dakika İçerisinde 3 Farklı Kullanıcı İsmiyle VPN Oturum Denemesi Tespit Edilen Olay Sayısı: 0	Korelasyon kuralında tanımlanan süre içerisinde ve korelasyon kuralında tanımlanan eşik değerlerine uygun bir olay gerçekleşmemiş olabilir.
Kural 14: Windows Komut Satırı ile Uzaktan Bağlantının Tespiti Tespit Edilen Olay Sayısı: 0	Herhangi bir bulguya rastlanılmamıştır. Bunun sebebi, saldırı girişiminin olmamasından veya kullanıcı bilgisayarlarının tamamından log toplanmamasından kaynaklı olabilir.

Yazılan korelasyonların her zaman bir çıktı vermesi beklenmemelidir. Bir çıktının elde edilebilmesi için verilen şartların sağlanması gerekmektedir. Her olay için bir korelasyon kuralı yazılmamalıdır. Aksi takdirde çok fazla sayıda e-posta, kısa mesaj bildiriminin önüne geçilemeyecek olup, çok sayıdaki alarmın arasında analiz yapılması güçleşecektir. Ayrıca

bu çalışma içerisinde örnek olarak gösterilmemiş ancak bazı noktalarda sağlanan faydalar aşağıdaki gibidir:

- Kurumdan ayrılmış eski çalışanların sistemlerde açık kalan oturumları tespit edilmiş ve ilgili sistemlerde oturumlar sonlandırılmıştır.
- Mobil e-posta uygulamalarında eski şifresi kayıtlı kalmış kullanıcıların çok sayıda yanlış şifre uyarısı ürettiği tespit edilmiş ve bu kullanıcılar uyarılmıştır. SIEM sayesinde bu hesapların kilitlenmesinin önüne geçilmiştir.
- Birbirleriyle haberleşmek zorunda olan servisler arasındaki bağlantı problemleri anlık olarak tespit edilebilmiştir. Örneğin, güvenlik duvarında yapılan yanlış değişiklik sonrası DHCP'nin yaptığı DNS trafiğinin kesilmesi alarm olarak güvenlik ekiplerine bildirilmiştir. Alarm olmasaydı kurum içerisindeki kullanıcılar otomatik IP alamayacaktı. Windows DHCP üzerinde Dynamic DNS update özelliği bulunmaktadır. DHCP kullanıcılara IP atadıktan sonra DNS'e güncelleme göndermektedir. Bu problem sonrası güncelleme gönderilemediği için kullanıcılar otomatik IP alamamışlardı. Eğer SIEM'de alarm yazılmasaydı sorunun kök çözümü için DHCP sunucusu, DNS sunucusu, güvenlik duvarı gibi sistemlerin her birinin üzerinde logları incelemek gerekecekti. SIEM'de yapılan tespit sonrası erken müdahale edilebilmiştir.

Bölüm 4.4'te yer alan raporlar neticesinde aşağıdaki bulgular elde edilmiştir:

Tablo 5.2: Uygulama Bölümünde Yazılan Raporların Değerlendirilmesi

BULGULAR	**SONUÇ**
Rapor 1: Peer to Peer Uygulamaları Kullanan Kullanıcıların Raporlanması:	Oluşturulan rapor 3 ay süreyle haftalık olarak takip edilmiştir. Özel erişim izni olmayan kullanıcılar dışında peer to peer uygulaması kullanmaya çalışan personellerin IP ve kullanıcı isimleri tespit edilmiş olup, bu uygulamaları çalıştırma girişimleri güvenlik ürünleri ile engellendiği anlaşılmıştır.

Tablo 5.2 (devam): Uygulama Bölümünde Yazılan Raporların Değerlendirilmesi

Rapor 2: Karantina Bölgesinden Yapılan Erişimlerin Tespiti	Rapor 2'de anti-virüs yüklü olmayıp başarılı trafik yapan kullanıcı tespit edilememiştir. Yapılan incelemelerde anti-virüs yüklü olmayan kullanıcıların trafiklerinin engellendiği için rapora yansımadığı anlaşılmıştır.

SIEM kullanımında aşağıdaki durumlara dikkat edilmesi gerekildiği tespit edilmiştir:

- Dikkat edilmeden ve iyi analiz edilmeden yazılan korelasyonların çok sayıda yanlış alarm oluşturduğu tespit edilmiştir.
- Veri merkezi web sistemlerine yapılan saldırı çeşitleri haftalık olarak raporlanarak bu saldırılara karşı güvenlik sıkılaştırmaları yapılmıştır.
- Log miktarı arttıkça disk kullanımının da hızla arttığı gözlemlenmiştir. Logların SIEM'e aktarılmasından önce kullanılacak disk ihtiyacının iyi hesaplanması gerektiği tespit edilmiştir. Disk alanında optimum yararın sağlanabilmesi için öncelikli olarak log kaynağından gönderilmemesi gereken, sistemi yoracak, incelenmesinin bir güvenlik olayına katkısı bulunmayacak logların filtrelenmesi, eğer bu olay log kaynağında yapılamıyor ise, SIEM ürününde bu işlemlerin yapılması gerektiği anlaşılmıştır.
- Parse olmayan logların fark edilebilmesi için alarm yazılması gerektiği anlaşılmıştır.
- Güvenlik duvarı üzerinde SIEM log toplama sunucusuna yalnızca log aktaracak kaynağın IP'si için erişim izni tanımlanmalıdır. Aksi takdirde bu durum kötü niyetli bir kişi tarafından suiistimal edilerek, SIEM'e çöp log olarak tabir edilen çok sayıda gerçek olmayan log gönderebileceği ve SIEM sisteminin çalışmasını engelleyebileceği riskinin olduğu anlaşılmıştır.

- Çok sayıda logların takip edilebilmesinin zorlaştığı ve SIEM'de yaratılan alarmların, gösterge panellerinin, sistem kaynaklarının takip edilebilmesi için ayrı bir izleme ekibinin kurulması gerektiği anlaşılmıştır.

Veri merkezi SIEM uygulaması sürecinde, log kaynakların sayısı ve toplanacak log miktarı iyi hesaplanmadığı durumlarda log kaçırma, performans problemlerinin yaşandığı ve log yönetiminin zorlaştığı anlaşılmıştır. SIEM için kaynak ihtiyaçlarının iyi belirlenebilmesi, doğru ve etkili korelasyon kurallarının yazılabilmesi için SIEM'i kullanacak personellerin SIEM konusunda uzman olmaları gerektiği anlaşılmıştır. Ayrıca, örnek veri merkezinde her geçen gün veri hacminin genişlediği görülmüştür. Veri miktarının artması, SIEM'de kaynak kullanımının (EPS, DISK vb.) artmasına da sebep olmuştur. Örnek SIEM uygulamasının yapıldığı veri merkezi gibi sürekli büyüyen veya büyüme ihtimali olan sistemlerde, ileriye dönük genişleme imkânı olan modüler yapıların kullanılması gerektiği anlaşılmıştır.

Yasa ve standartlara uyum, logların merkezi olarak toplanması, saklanması ve analiz edilmesi noktalarında SIEM'in katkı sağladığı görülmüştür. Gelişmiş korelasyonlar sayesinde şüpheli aktiviteler takip edilerek saldırı öncesi tespitin yapılabileceği, gerekli yerlere alarm olarak iletim sağlanabileceği anlaşılmıştır.

5.2. ÖNERİ

Bir siber olay karşısında müdahalenin erken yapılabilmesi için sistemlerin 7/24 izlenmesi, güvenlik ekibinin yetkinliği ve sayısı hayati rol oynamaktadır. Ancak siber olaylar karşısında her kurumun kendi iş akışına uygun hazırladıkları playbooklar kapsamında yapılan müdahaleler insan inisiyatifine bırakılmaz ise, kısacası dinamik playbook kullanan çözümler kullanılırsa, bu siber olaylara anında müdahale edilebilecek ve riskler bertaraf edilebilecektir. Bu doğrultuda olaylara karşı otomatik aksiyon alan güvenlik orkestrasyonu, otomasyon, ve yanıt anlamına gelen SOAR (Security Orchestration, Automation and Response) çözümleri bulunmaktadır.

SOAR kelimesi, ilk olarak araştırma şirketi olan Gartner tarafından icra edilmiştir [94]. Kurumların eylem planları SOAR üzerinde tanımlanarak otomatik aksiyon alınabilmesi sağlanmaktadır. Olay müdahale planları genellikle veri ihlalleri, servis reddi / dağıtılmış servis reddi saldırıları, ağ müdahaleleri, kötü amaçlı yazılım salgınları veya içeriden gelen tehditler de dâhil olmak üzere potansiyel saldırı senaryolarına nasıl yanıt verileceğine dair

talimatlar içermektedir. SOAR bu olaylara karşı nasıl müdahale edileceğine karar veren merkezi otomasyon sistemidir. Ayrıca Gartner'a göre SOAR'ın kullanım örnekleri arasında SIEM alarm işleme de bulunmaktadır [95].

Bu çalışma kapsamında SIEM çözümlerinin, aktif izleme, pasif önleme cihazları olduğu görülmüştür. SIEM ile siber olayların tespitinin yapılabildiği, alarmlar üretilerek güvenlik ekiplerinin bilgilendirilebildiği anlaşılmıştır. Hızlı tespitlerin nasıl yapılacağı anlaşılabilmesine rağmen bu çalışma ile siber güvenlik olaylarına karşı hızlı ve otomatik müdahalelerin nasıl yapılacağı konusu eksik kalmıştır. Bu çalışma siber güvenlik kapsamında kritik sistemlerin korunmasına yönelik SOAR çözümlerinin kullanılmasını önermektedir. Kritik sistemlerde kullanılacak SIEM ürününün ihtiyaç olduğunda farklı SOAR ürünleri ile entegrasyonu destekleyecek alt yapıya sahip olmasının faydalı olacağı anlaşılmıştır. Bu çalışma ile hazırlanan korelasyon kuralları, SOAR çözümlerinde kullanılması noktasında fayda sağlayacaktır. Yapılan araştırma, incelenen güvenlik yaklaşımları ve SIEM kabiliyetleri, siber güvenlik kapsamında kritik sistemlerin korunmasına yönelik yapılacak benzer çalışmalarda SIEM ile SOAR çözümlerinin beraber etkili kullanılabilmesine ışık tutacaktır.

6. KAYNAKÇA

[1]. Başaranoğlu, E., 2016, Bilgi Güvenliği Unsurları (CIA ve Diğerleri), https://www.siberportal.org/blue-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/, [Ziyaret Tarihi: 1 Şubat 2020].

[2]. Security Event Management, https://www.siberportal.org/blue-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/, [Ziyaret Tarihi: 1 Şubat 2020].

[3]. Teknoloji Okulu, Günümüzde En Çok Kullanılan İşletim Sistemleri, 2020, https://www.teknolojioku.com/donanim/gunumuzde-en-cok-kullanilan-isletim-sistemleri-5a29050b18e54078fb1631dc?p=5, [Ziyaret Tarihi: 1 Şubat 2020]

[4]. GeeksforGeeks, 2017, Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter), https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/, [Ziyaret Tarihi: 1 Şubat 2020].

[5]. Melnick, J., 2019, Network Security Devices You Need to Know About, https://blog.netwrix.com/2019/01/22/network-security-devices-you-need-to-know-about/, [Ziyaret Tarihi: 1 Şubat 2020].

[6]. Leskiw, A., 2020, Syslog: Servers, Messages & Security – Tutorial & Guide to this System Logs, https://www.networkmanagementsoftware.com/what-is-syslog/, [Ziyaret Tarihi: 1 Şubat 2020].

[7]. Sparanberg, K., 2018, Top 10 Log Sources You Should Monitor, https://www.dnsstuff.com/top-10-log-sources-you-should-monitor/, [Ziyaret Tarihi: 1 Şubat 2020].

[8]. Exabeam, 2020, SIEM Architecture: Technology, Process and Data, https://www.exabeam.com/siem-guide/siem-architecture/, [Ziyaret Tarihi: 2 Şubat 2020]

[9]. Broadcom, 2020, Types of Log Collection Methods, https://knowledge.broadcom.com/external/article/150665/mss-ts-types-of-log-collection-methods.html, [Ziyaret Tarihi: 2 Şubat 2020].

[10]. Wikipedia, UDP, https://tr.wikipedia.org/wiki/UDP, [Ziyaret Tarihi: 3 Şubat 2020].

[11]. Exabeam, 2019, Log Aggregation, Processing and Analysis for Security, https://www.exabeam.com/siem-guide/events-and-logs/, [Ziyaret Tarihi: 4 Şubat 2020].

[12]. Crawley, K., 2018, How SIEM Correlation Rules Work, https://cybersecurity.att.com/blogs/security-essentials/how-siem-correlation-rules-work/, [Ziyaret Tarihi: 4 Şubat 2020].

[13]. Can, S., 2017, Bakanlıkta Kullanılan Log Sistemlerinin Merkezileştirilmesi Ve Yönetimi Uzmanlık Tezi, T.C Çevre ve Şehircilik Bakanlığı.

[14]. Allen, S., 2020, Importance of Understanding Logs from an Information Security Standpoint, https://www.sans.org/reading-room/whitepapers/logging/paper/200, [Ziyaret Tarihi: 5 Şubat 2020].

[15]. Akbaş, E., 2013, Log Yönetiminde Cihaz Sayıları & Eps Değerleri Arasındaki İlişki, https://www.slideshare.net/anetertugrul/log-yonetiminde-cihaz-sayilari-ile-eps-degerleri-arasindaki-iliski/, [Ziyaret Tarihi: 6 Şubat 2020].

[16]. Türk Standartları Enstitüsü, 2013, Veri Merkezi Bilgi Güvenliği Standardı, https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2222/17032015164359-3.pdf, [Ziyaret Tarihi: 7 Şubat 2020].

[17]. Kent, K. And Souppaya, M., 2006, Guide to Computer Security Log Management, National Institute of Standards and Technology, United States of America.

[18]. Miller, D. And Harris, S. And Harper, A. And VanDyke, S. And Blask, C., 2011, Security Information and Event Management Implementation, The McGraw-Hill Companies, United States of America, ISBN: 978-0-07-170108-2.

[19]. Akbaş, E., 2013, Bilgi Güvenliği ve Log Yönetimi Sistemlerinin Analizi, https://www.slideshare.net/anetertugrul/ertugrul/, [Ziyaret Tarihi: 7 Şubat 2020].

[20]. Microsoft, 2018, W3C Logging, https://docs.microsoft.com/en-us/windows/win32/http/w3c-logging/, [Ziyaret Tarihi: 7 Şubat 2020].

[21]. Microsoft, 2016, ODBC Logging, https://docs.microsoft.com/en-us/iis/configuration/system.webserver/odbclogging/, [Ziyaret Tarihi: 8 Şubat 2020]

[22]. Türkiye Cumhuriyeti Resmi Gazete, 2007, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.

[23]. Türkiye Cumhuriyeti Resmi Gazete, 2016, 6698 Sayılı Kişisel Verilerin Korunması Kanunu.

[24]. Kişisel Verileri Koruma Kurumu, 2017, Açık Rıza, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf, [Ziyaret Tarihi: 9 Şubat 2020].

[25]. Barış, K., 2018, Kişisel Verileri Koruma Kanunu nedir, şirketlerin ne yapması gerekiyor, https://medium.com/peoplebox-ats/kisisel-verileri-koruma-kanunu-kvkk-nedir-sirketlerin-ne-yapmasi-gerekiyor-cd8c4b93a235/, [Ziyaret Tarihi: 9 Şubat 2020].

[26]. Kişisel Verileri Koruma Kurumu, 2020, Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Gratis İç ve Dış Tic. A.Ş., https://www.kvkk.gov.tr/Icerik/6691/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Gratis-Ic-ve-Dis-Tic-A-S-/, [Ziyaret Tarihi: 9 Şubat 2020].

[27]. Türk Standartları Enstitüsü, 2006, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, Ankara.

[28]. Sentor, 2018, Accelerate ISO 27001 Compliance With SIEM, https://www.sentor.se/wpcontent/uploads/2018/06/Accelerate_ISO_compliance_with_SIEM.pdf, [Ziyaret Tarihi: 10 Şubat 2020].

[29]. PCI Security Standards Council, 2004, Payment Card Industry Data Security Standards, United States of America.

[30]. Simpson, M., 2017, PCI DSS Requirement 12: Leverage Policy To Improve Security, https://www.securitymetrics.com/blog/pci-dss-requirement-12-leverage-policy-improve-security/, [Ziyaret Tarihi: 15 Şubat 2020].

[31]. Johnson, B., 2013, How Data Centers Work, https://computer.howstuffworks.com/data-centers2.htm, [Ziyaret Tarihi: 17 Şubat 2020].

[32]. Google, Discover our data center locations, https://www.google.com/about/datacenters/locations/, [Ziyaret Tarihi: 17 Şubat 2020].

[33]. AFL HyperScale, Understanding Different Types Of Data Center, https://www.aflhyperscale.com/understanding-different-types-of-data-center/, [Ziyaret Tarihi: 17 Şubat 2020].

[34]. Ayvaz, T., Co-location nedir?, https://www.mediaclick.com.tr/blog/co-location-nedir/, [Ziyaret Tarihi: 17 Şubat 2020].

[35]. Radore, Colocation, https://radore.com/co-location-sunucu-barindirma, [Ziyaret Tarihi: 17 Şubat 2020].

[36]. Andrews, P., 2014, Retail vs. Wholesale Colocation, https://www.markleygroup.com/blog/retail-vs-wholesale-colocation/, [Ziyaret Tarihi: 17 Şubat 2020].

[37]. Sampera, E., 2019, Enterprise vs Edge Data Center, https://www.vxchnge.com/blog/enterprise-vs-edge-data-center, [Ziyaret Tarihi: 18 Şubat 2020].

[38]. Cyberciti, 2011, Data Center Standard, https://www.cyberciti.biz/faq/data-center-standard-overview/, [Ziyaret Tarihi: 18 Şubat 2020].

[39]. Aspire Tech, EPS Calculator, http://www.aspiretss.com/tools, [Ziyaret Tarihi: 19 Şubat 2020].

[40]. Cyberdefenses INC., 2019, What Is SIEM And How To Choose The Right Tool, https://cyberdefenses.com/what-is-siem-and-how-to-choose-the-right-tool/, [Ziyaret Tarihi: 20 Şubat 2020].

[41]. Akbaş, E., 2015, Gerçek SIEM Nedir? Olmazsa Olmazları! Ve Gerçek SIEM Ürünü ile Güvenlik Analiz Senaryoları, https://www.slideshare.net/anetertugrul/gerek-siem-nedir-olmazsa-olmazlar-ve-gerek-siem-rn-ile-gvenlik-analiz-senaryolar, [Ziyaret Tarihi: 21 Şubat 2020].

[42]. Rouse, M., 2019, Brute Force Attack, https://searchsecurity.techtarget.com/definition/brute-force-cracking, [Ziyaret Tarihi: 22 Şubat 2020].

[43]. CloudFlare, What is a DDoS Attack, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/, [Ziyaret Tarihi: 22 Şubat 2020].

[44]. Akbaş, E., 2019, KVKK SIEM Senaryo ve Kuralları, https://medium.com/@eakbas/kvkk-siem-senaryo-ve-kurallar%C4%B1-5fd8f3fe8077, [Ziyaret Tarihi: 23 Şubat 2020].

[45]. Tan, H. Ve Aktaş, Z., 2011, Bir Kuruluşun Bilgi Sistemi Güvenliği İçin Bir Yaklaşım, http://www.emo.org.tr/ekler/906558234de5822_ek.pdf?dergi=, [Ziyaret Tarihi: 24 Şubat 2020].

[46]. TIA 942, 2013, About Data Centers, http://www.tia-942.org/content/162/289/About_Data_Centers, [Ziyaret Tarihi: 25 Şubat 2020]

[47]. International Organization for Standardization, 2013, ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements, Switzerland.

[48]. Vacca, J., 2009, "Computer and Information Security Handbook" Morgan Kaufmann, United States of America, ISBN-10: 0123743540.

[49]. Spiceworks, 2013, How Intrusion Prevention Systems IPS Work in Firewall?, https://community.spiceworks.com/topic/362007-how-intrusion-prevention-systems-ips-work-in-firewall, [Ziyaret Tarihi: 26 Şubat 2020].

[50]. Beyaz.Net, 2018, Ağ Mimari Tasarımı, https://www.beyaz.net/tr/network/cozumler/ag_mimari_tasarimi.html, [Ziyaret Tarihi: 28 Şubat 2020].

[51]. Düyen, S., 2015, VPN (Virtual Private Network / Özel Sanal Ağ), http://www.elektrik.gen.tr/2015/08/vpn-virtual-private-network-ozel-sanal-ag/589, [Ziyaret Tarihi: 1 Mart 2020].

[52]. Techopedia, 2014, VPN Concentrator, https://www.techopedia.com/definition/30748/vpn-concentrator, [Ziyaret Tarihi: 1 Mart 2020].

[53]. CloudFlare, 2017, Web Appliation Firewall- WAF, https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/, [Ziyaret Tarihi: 2 Mart 2020].

[54]. Beyaz.Net, 2017, Veri Tabanı Güvenliği Nasıl Sağlanır, https://www.beyaz.net/tr/guvenlik/makaleler/veri_tabani_guvenligi_nasil_saglanir.html, [Ziyaret Tarihi: 2 Mart 2020].

[55]. Rajesh, K., 2011, What are Database Firewalls Why are They Required and How Do They Protect Databases, https://www.excitingip.com/1933/what-are-database-firewalls-why-are-they-required-how-do-they-protect-databases/, [Ziyaret Tarihi: 3 Mart 2020].

[56]. Kayar, E.,2014, Advanced Persistent Threat- APT, https://lostar.com.tr/2014/11/advanced-persistent-threat-apt.html, [Ziyaret Tarihi: 4 Mart 2020].

[57]. BGA Security, 2014, APT (Advanced Persistent Threats) Ürün Seçim Kriterleri ve Test/Demo Prosedürü, https://www.bgasecurity.com/2014/10/aptadvanced-persistent-threats-urun/, [Ziyaret Tarihi: 4 Mart 2020].

[58]. Kaspersky, 2018, Advanced Persistent Threats, https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats, [Ziyaret Tarihi: 4 Mart 2020].

[59]. Beyaz.Net, 2019, Ağ Erişim Kontrolü (Network Access Control –NAC) Nedir?, https://www.beyaz.net/tr/guvenlik/makaleler/ag_erisim_kontrolu_network_access_control_nac_nedir.html, [Ziyaret Tarihi: 5 Mart 2020].

[60]. SpamLaws, 2009, How Network Access Controls Work?, https://www.spamlaws.com/how-network-access-controls-work.html, [Ziyaret Tarihi: 6 Mart 2020].

[61]. IT Law Wiki, 2005, Host-Based Firewall, https://itlaw.wikia.org/wiki/Host-based_firewall, [Ziyaret Tarihi: 6 Mart 2020].

[62]. Pesen, M., 2015, Bir Bakışta Veri Sızıntısı Önleme (DLP), http://www.egisbilisim.com.tr/bir-bakista-veri-sizintisi-onleme-dlp/, [Ziyaret Tarihi: 6 Mart 2020].

[63]. Microsoft, 2019, CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708, [Ziyaret Tarihi: 7 Mart 2020].

[64]. Resmi Gazete, 2007, İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm, [Ziyaret Tarihi: 7 Mart 2020].

[65]. CTR Uluslararası Belgelendirme ve Denetim, 2013, ISO 27001 Bilgi Güvenliği Yönetim Sistemi Nedir?, https://belgelendirme.ctr.com.tr/iso-27001.html, [Ziyaret Tarihi: 7 Mart 2020].

[66]. Zomaya, D., 2018, 6 Best Intrusion Prevention Systems & Intrusion Detection Tools, https://www.itprc.com/intrusion-prevention-detection-tools/, [Ziyaret Tarihi: 7 Mart 2020].

[67]. Avast, 2019, SSL Inspection, https://smb.avast.com/answers/ssl-inspection, [Ziyaret Tarihi: 8 Mart 2020].

[68]. Wikipedia, 2020, Remote Desktop Protocol, https://en.wikipedia.org/wiki/Remote_Desktop_Protocol, [Ziyaret Tarihi: 8 Mart 2020].

[69]. Froehlich, A., 2019, SOAR vs. SIEM: What's the difference?, https://searchsecurity.techtarget.com/answer/SOAR-vs-SIEM-Whats-the-difference, [Ziyaret Tarihi: 8 Mart 2020].

[70]. Williams, S., 2018, Gartner SOAR report: "Innovation Insight for Security Orchestration, Automation and Response", https://swimlane.com/blog/gartner-soar-report/, [Ziyaret Tarihi: 10 Mart 2020].

[71]. Microsoft, 2017, Windows Server Update Services (WSUS), https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus, [Ziyaret Tarihi: 10 Mart 2020].

[72]. RiskBasedSecurity, 2019, Number of Records Exposed Up 112% in Q3, https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/, [Ziyaret Tarihi: 10 Mart 2020].

[73]. H Başak, C., 2020, Bilgi Güvenliğinde 7 Önemli Husus, CyberMag, Sayı 48, 14-17.

[74]. Muniz, J. and Mclntyre, G. and Alfardan, N., 2016, Security Operations Center: Building, Operating, and Maintaining your SOC, Cisco Press, United States of America, ISBN-13:978-0-13-405201-4.

[75]. Kral, P. 2011, The Incident Handlers Handbook, https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901, [Ziyaret Tarihi: 15 Mart 2020].

[76]. Sağıroğlu, Ş. ve Alkan, M. Ve Samet R. ve Diğerleri, 2018, Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Grafiker Yayınları, Ankara, ISBN: 978-605-2233-22-1

[77]. Akbaş, E., 2019, Siber Tehditleri Nasıl Tespit Edelim?, https://medium.com/@eakbas/siber-tehditleri-nas%C4%B1l-tespit-edelim-51339d9c8d2c, [Ziyaret Tarihi: 17 Mart 2020].

[78]. Melnick, J., 2018, Top 10 Most Common Types of Cyber Attacks, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/, [Ziyaret Tarihi: 17 Mart 2020].

[79]. The Guardian, 2019, German cyber-attack: man admits massive data breach, say poliçe, https://www.theguardian.com/world/2019/jan/08/germany-data-breach-man-held-in-suspected-hacking-case, [Ziyaret Tarihi: 17 Mart 2020].

[80]. Mamiit, A., 2019, NASA hacked: 500 MB of mission data stolen through a Raspberry Pi computer, https://www.digitaltrends.com/computing/hackers-steal-500-mb-nasa-data-raspberry-pi/, [Ziyaret Tarihi: 18 Mart 2020].

[81]. Office of Inspector General, 2019, Cybersecurıty Management And Oversıght At The Jet Propulsıon Laboratory, https://oig.nasa.gov/docs/IG-19-022.pdf, [Ziyaret Tarihi: 18 Mart 2020].

[82]. BloomBerght, 2015, ABD'de federal çalışanlarının bilgileri hacklendi, https://www.bloomberght.com/haberler/haber/1795723-abdde-federal-calisanlarinin-bilgileri-hacklendi, [Ziyaret Tarihi: 19 Mart 2020].

[83]. Fruhlinger, J., 2020, The OPM hack explained: Bad security practices meet China's Captain America, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html, [Ziyaret Tarihi: 19 Mart 2020].

84]. Oracle, 2011, Spool,

https://docs.oracle.com/cd/E11882_01/server.112/e16604/ch_twelve043.htm#SQPUG126, [Ziyaret Tarihi: 20 Mart 2020].

[85]. http 404, 2020, https://tr.wikipedia.org/wiki/HTTP_404, [Ziyaret Tarihi: 21 Mart 2020].

[86]. Microsoft, 2017, CMD (Command), https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cmd, [Ziyaret Tarihi: 22 Mart 2020].

[87]. Microsoft, 2018, Powershell, https://docs.microsoft.com/tr-tr/powershell/scripting/overview?view=powershell-7, [Ziyaret Tarihi: 22 Mart 2020].

[88]. Microsoft, 2017, Rundll32, https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/rundll32, [Ziyaret Tarihi: 22 Mart 2020].

[89]. Microsoft, 2018, WScript, https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wscript, [Ziyaret Tarihi: 22 Mart 2020].

[90]. Geater, J., 2020, https://www.exefiles.com/tr/exe/scrcons-exe/, [Ziyaret Tarihi: 22 Mart 2020].

[91]. Belgeler.org, 2006, Bash Nedir?,

http://www.belgeler.org/bashref/bashref_what.is.bash.html, [Ziyaret Tarihi: 23 Mart 2020].

[92]. Reviversoft, 2013, .SH Dosya Uzantısı Nedir?, https://www.reviversoft.com/tr/file-extensions/sh, [Ziyaret Tarihi: 23 Mart 2020].

[93]. Rouse, M., 2017, https://searchsecurity.techtarget.com/definition/antivirus-software, [Ziyaret Tarihi: 23 Mart 2020].

[94]. Gartner, 2019, Security Orchestration, Automation And Response (SOAR), https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar, [Ziyaret Tarihi: 24 Mart 2020].

[95]. Ahlm, E. and Barros, A. And Clark, M. , SOAR: Assessing Readiness Through Use-Case Analysis, https://www.gartner.com/en/documents/3981938, [Ziyaret Tarihi: 24 Mart 2020].

[96]. Akbaş, E., 2017, SIEM Çözümlerinde Taxonomy Ne İşe Yarar?, https://www.slideshare.net/anetertugrul/siem-cozumlernde-taxonomy-ne-ise-yarar, [Ziyaret Tarihi: 3 Nisan 2020].

ÖZGEÇMİŞ

Kişisel Bilgiler		
Adı Soyadı	Ali AKPINAR	
Doğum Yeri	YAHYALI	
Doğum Tarihi	28.07.1989	
Uyruğu	T.C.	
Telefon	0536 065 48 45	
E-Posta Adresi	Ali.akpinar@hotmail.com.tr	

Eğitim Bilgileri	
Lisans	
Üniversite	Erciyes Üniversitesi
Fakülte	Mühendislik Fakültesi
Bölüm	Bilgisayar Mühendisliği
Mezuniyet Yılı	2016

Eğitim Bilgileri	
Yüksek Lisans	
Üniversite	Ahi Evran Üniversitesi
Enstitü Adı	Fen Bilimler Enstitüsü
Anabilim Dalı	İleri Teknolojiler Anabilim Dalı
Programı	İleri Teknolojiler Anabilim Dalı
Mezuniyet Yılı	Hala okuyor

Yabancı Dil	
İngilizce	
Okuma	İyi
Yazma	İyi
Konuşma	Orta