
GAZİ ÜNİVERSİTESİ
Gazi
1926

GÜVENLİK BİLGİLERİ VE OLAY YÖNETİMİ (SIEM) SİSTEMLERİ KULLANILARAK ADLİ BİLİŞİM OLAYLARININ TESPİT YÖNTEMLERİNİN İNCELENMESİ

Mustafa Çağrı FANUSCU

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Ocak 2023

Mustafa Çağrı FANUSCU tarafından hazırlanan GÜVENLİK BİLGİLERİ VE OLAY YÖNETİMİ (SIEM) SİSTEMLERİ KULLANILARAK ADLİ BİLİŞİM OLAYLARININ TESPİT YÖNTEMLERİNİN İNCELENMESİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Mustafa ALKAN

Gazi Üniversitesi Adli Bilişim Ana Bilim Dalı

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ...……

Başkan: Prof. Dr. Olgun DEĞİRMENCİ

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ……...

Üye: Prof. Dr. Ercan Nurcan YILMAZ

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ……...

Tez Savunma Tarihi: ...../……/……

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..……

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Mustafa Çağrı FANUSCU

...../……/……

GÜVENLİK BİLGİLERİ VE OLAY YÖNETİMİ (SIEM) SİSTEMLERİ KULLANILARAK ADLİ BİLİŞİM OLAYLARININ TESPİT YÖNTEMLERİNİN İNCELENMESİ

(Yüksek Lisans Tezi)

Mustafa Çağrı FANUSCU

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ocak 2023

ÖZET

Günümüzde siber saldırı tipleri ve yoğunluğu artmıştır, bu durum saldırı tespit yöntemlerinin önemini artırmaktadır. Saldırı tespiti için yıllar boyunca birçok farklı araç ve yöntem geliştirilmiştir. SIEM sistemleri bu amaç için kullanılan araçlardan biridir. Bu sistemler, düzgün bir yapılandırma ve yönetim ile saldırıların tespit edilmesi ve olaya müdahale edilmesi aşamalarında güvenlik analistlerinin işlerini kolaylaştırmaktadır. Ayrıca bu sistem, gerçekleşen bir siber suçun ardından delillerin bulunmasını kolaylaştırmakta ve delil toplama süresini kısaltmaktadır.

Kurumsal altyapılarda yaşanan adli bilişim olaylarının hızlı bir şekilde tespiti büyük önem arz etmektedir. Yaşanan olay sonrasında hangi personelin ne gibi aksiyonları alacağının belirlenmesi de olay müdahale sürelerini kısaltmaktadır. Ortaya çıkan delillerin güvenli bir şekilde saklanması ve ihtiyaç halinde ilgili mercilerle hızlı bir şekilde paylaşılması da önemlidir. Yapılan bu çalışma ile kurumsal bir altyapıda SIEM sistemleri kullanılarak adli bilişim olay tespitinin nasıl yapılabileceği uygulamalı örnekler üzerinden incelenmiştir. Bu inceleme işlemi için gerekli iz kayıt kaynakları ve bu kaynakların özellikleri detaylı bir şekilde aktarılmıştır. Bu kaynaklardan gelen iz kayıtları içerisinde korelasyon kurallarında kullanılabilecek parametrelerin elde edilme yöntemleri ve bu parametrelerin anlamları üzerine araştırmalar yapılmıştır. İz kayıtlarının işlenebilmesi için SIEM sistemine aktarımı gereklidir. Bu çalışmada iz kayıtlarının aktarım yöntemleri hakkında da bilgiler verilmiştir. Tüm bu bilgilerin ışığında örnek olarak seçilen bir SIEM uygulaması üzerinde iz kayıt kaynakları oluşturulmuş, bu kayıtlar üzerinde ayrıştırma ve normalizasyon çalışmaları yapılmış ve korelasyon kuralları yazılarak örnek adli bilişim olaylarının tespitine yönelik çalışmalar yapılmıştır. Ortaya çıkan sonuçlar değerlendirilmiştir. Son olarak yapılan tüm işlem adımları bir şablon üzerinde gösterilmiştir. Bu şablon üzerinde bir siber olayın tespiti için gerekli adımlar ve tespit sonrasında bilişim personelinin olaya müdahale yöntemleri belirlenerek taslak halinde gösterilmiştir.

Bilim Kodu	:	92401
Anahtar Kelimeler	:	Bilgi Güvenliği ve Olay Yönetimi, Adli Bilişim, Olayların korelasyonu, siber güvenlik
Sayfa Adedi	:	126
Danışman	:	Prof. Dr. Mustafa ALKAN

INVESTIGATION OF DETECTION METHODS OF FORENSICS INCIDENTS USING SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SYSTEMS

(M. Sc. Thesis)

Mustafa Çağrı FANUSCU

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

January 2022

ABSTRACT

Today, the types and intensity of cyber attacks have increased, which increases the importance of attack detection methods. Many different tools and methods have been developed over the years for intrusion detection. SIEM systems are one of the tools used for this purpose. These systems make it easier for security analysts to detect attacks and respond to incidents with proper configuration and management. In addition, this system facilitates the discovery of evidence after a cybercrime and reduces evidence collection times.

The rapid detection of forensic incidents in institutional infrastructures is of great importance. Determining which personnel will take what actions after the incident also shortens the incident response times. It is also important that the resulting evidence is kept securely and shared quickly with the relevant authorities in case of need. In this study, how to make forensic incident detection using SIEM systems in an institutional infrastructure has been examined through applied examples. The trace recording resources required for this review process and the characteristics of these resources are explained in detail. Research has been carried out on the methods of obtaining parameters that can be used in correlation rules within the trace records from these sources and the meanings of these parameters. Trace records must be transferred to the SIEM system in order to be processed. In this study, information about the transfer methods of trace records was also given. In the light of all this information, trace recording sources were created on a SIEM application selected as an example, decomposition and normalization studies were carried out on these records, and the results were evaluated by writing the correlation rules and working on the determination of sample forensic events. Finally, all the processing steps were shown on a template. On this template, the necessary steps for the detection of a cyber incident and the intervention methods of the IT personnel after the detection were determined and shown in a draft.

Science Code	:	92401
Key Words	:	SIEM, Security Information and Event Management, Cybersecurity, forensics, Events correlation, Alert correlation
Page Number	:	126
Supervisor	:	Prof. Dr. Mustafa ALKAN

TEŞEKKÜR

Yüksek lisans eğitimim süresince benden desteklerini esirgemeyen, bu tezin yazım aşamasında görüş ve önerileri ile bakış açımı geliştiren saygıdeğer danışanım Prof. Dr. Mustafa ALKAN'a, zorlandığım her aşamada bana sabırla yardımcı olan Arş.Gör. Aynur KOÇAK'a, yüksek lisans sürecim boyunca bana tüm desteği sağlayan yöneticim Necati ÖZGEN ve tüm çalışma arkadaşlarıma, bugünlere gelmemi sağlayan biricik aileme ve son olarak tüm bu süreçte motivasyonumu korumamı sağlayan sevgili eşim Aybüke FANUSCU'ya sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

ÖZET…… iii
ABSTRACT……. iv
TEŞEKKÜR……. v
SİMGELER VE KISALTMALAR…….. xii
1. GiRİŞ…… 1
2. LİTERATÜR ARAŞTIRMASI…… 3
2.1. SIEM…….. 4
2.2. SIEM Çalışma Prensibi…….. 6
2.3. İz Kayıt Çeşitleri…… 10
2.3.1.Microsoft Windows security event logs……... 11
2.3.2. IIS (Internet Information Services) web sunucu iz kayıtları…… 18
2.3.3. Linux denetim iz kayıtları…… 21
2.3.4. Aix (Advanced Interactive Executive) denetim iz kayıtları……. 23
2.3.5. Apache HTTP sunucu iz kayıtları…… 25
2.3.6. Güvenlik duvarı iz kayıtları……. 29
2.3.7. IDS/IPS (Intrusion Detection System/ Intrusion Prevention System) iz kayıtları…….. 36
2.3.8. Antivirüs iz kayıtları……. 39
2.3.9. VPN (Virtual Private Network) iz kayıtları……. 43
2.3.10. DNS (Domain Name System) iz kayıtları…….. 45
2.3.11. WAF (Web Application Firewall) iz kayıtları…… 47
2.3.12. NAC (Network Access Control) iz kayıtları…… 55
2.3.13. Web proxy iz kayıtları……. 58
2.4. İz Kayıt Toplama Yöntemleri……. 60
2.4.1. Ajan ile iz kayıt toplama…… 60
2.4.2. Syslog ile iz kayıt toplama…… 61
2.4.3. JDBC (Java Database Connectivity) protokolü ile iz kayıt toplama…… 63

2.4.4. OPSEC (Open Platform for Security) LEA (Log Export API) ile iz kayıt toplama…… 64
2.4.5. MSRPC protokolü ile iz kayıt toplama……. 64
3. MATERYAL VE METOT……. 67
3.1. Qradar SIEM Üzerinde İz Kayıtlarının Anlamlandırılması……. 67
3.2. Qradar SIEM Üzerinde İz Kayıt Kaynaklarının Oluşturulması……... 74
3.3. Qradar SIEM Üzerinde Kural Oluşturma…… 76
3.4. Kurallar İçin Oluşturulan Use Case Örneği……. 80
4. BULGULAR VE TARTIŞMA……... 81
4.1. Ele Geçirilen Kurumsal E-Posta Hesaplarının Tespiti…… 81
4.1.1. Zimbra iz kayıtlarının SIEM sistemine aktarımı…….. 82
4.1.2. Qradar SIEM üzerinde zimbra iz kayıtlarının anlamlandırılması…… 86
4.1.3. Qradar SIEM üzerinde mail sunucu kaynağının oluşturulması…… 86
4.1.4. Ele geçirilen e-posta hesaplarının tespiti için oluşturulan kurallar……... 87
4.1.5. Tespit için oluşturulan kural ve use case örneği……... 87
4.2. Bilgi İşlem Cihazı Üzerinde Zararlı Yazılım Aktivitelerinin Tespiti…….. 90
4.2.1. Tespit için gerekli iz kayıtlarının toplanması…… 91
4.2.2. Qradar SIEM üzerinde yapılan işlemler…… 91
4.2.3. Tespit için oluşturulan kural ve use case örneği…… 94
4.3. Karşı Adli Bilişim Faaliyetlerinin Tespiti…… 102
4.3.1. Tespit için gerekli iz kayıtlarının toplanması…… 102
4.3.2. Tespit için oluşturulan kural ve use case örneği…….. 105
4.4. Kurum Dışına Doğru Yapılan Yüksek Boyutlu Veri Çıkışının Tespiti…….. 110
4.5. Kurum Ağında Veri tabanı Taraması Yapan Lokal IP Adresi Tespiti…… 113
4.6. Web Sayfalarına Yapılan Saldırıların Tespiti…….. 114
5. SONUÇLAR VE ÖNERİLER……. 119
KAYNAKLAR…… 122
ÖZGEÇMİŞ…… 126

ŞEKİLLER LİSTESİ

Sayfa

Şekil 2.1 Standart bir SIEM Mimarisi..... 7
Şekil 2.2 Olay ID 4625..... 13
Şekil 2.3 Olay ID 4738..... 16
Şekil 2.4 Olay ID 4688..... 17
Şekil 2.5 Olay ID 1100..... 17
Şekil 2.6 Olay ID 4724..... 18
Şekil 2.7 IIS Web Sunucu Örnek İz Kayıtları..... 19
Şekil 2.8 Linux OS Örnek Denetim İz Kayıtları..... 22
Şekil 2.9 Palo-Alto Güvenlik Duvarı Trafik Sonlandı İz Kayıt Tipi..... 31
Şekil 2.10 Palo-Alto Güvenlik Duvarı Tarafından Engellenen Trafik Örneği..... 33
Şekil 2.11 Zararlı Paket Tespiti Sonucu Oluşan İz Kaydı..... 35
Şekil 2.12 SQL Injection Saldırı Denemesine İlişkin iz Kayıt Örneği..... 36
Şekil 2.13 TeamViewer Trafiğinin Tespiti..... 38
Şekil 2.14 Zararlı Dosya Tespiti..... 38
Şekil 2.15 Blind SQL Injection Saldırı Tespiti..... 39
Şekil 2.16 Windows Kernel Yetki Yükseltme Saldırısı Tespiti..... 39
Şekil 2.17 Zararlı Bulaşan Dosyanın Silinmesi..... 40
Şekil 2.18 Güncelleme Hatası..... 41
Şekil 2.19 Zararlı Olarak Tespit Edilen Dosyanın Silinememesi..... 41
Şekil 2.20 Zararlı Olay Tespit Edilen Dosyanın Silinmesi..... 42
Şekil 2.21 Cisco ASA VPN Örnek İz Kayıtları..... 45
Şekil 2.22 Microsoft Windows DNS Sunucu Debug İz Kayıt Örnekleri..... 46
Şekil 2.23 F5 ASM HTTP-GET İsteği..... 49
Şekil 2.24 F5 ASM HTTP-POST İsteği..... 50
Şekil 2.25 F5 ASM XSS Saldırısı Örneği..... 51
Şekil 2.26 F5 ASM SQL Injection Saldırısı Örneği..... 52
Şekil 2.27 F5 ASM Server Side Code Injection Saldırısı Örneği..... 53
Şekil 2.28 Kaçınma Tekniği Saldırı Örneği..... 54
Şekil 2.29 Scopnet İz Kayıt Örnekleri..... 57
Şekil 2.30 McAfee Web Gateway Örnek İz Kayıtları..... 59

Şekil 2.31: Syslog Paket Yapısı..... 62
Şekil 2.32: Syslog Facility Değerleri..... 62
Şekil 2.33: Syslog Severity Değerleri..... 63
Şekil 3.1: Yeni Kaynak Tipi Oluşturma..... 68
Şekil 3.2: Event ID ve Event Category Parametreleri..... 69
Şekil 3.3: Yeni Bir Event Mapping Oluşturma..... 70
Şekil 3.4: Yeni Bir QID Kaydı Oluşturma..... 71
Şekil 3.5: DSM Editor'un Açılması..... 72
Şekil 3.6: DSM Editor Ekranları..... 73
Şekil 3.7: Custom Property seçme ekranı..... 73
Şekil 3.8: Yeni Custom Property Oluşturma Ekranı..... 74
Şekil 3.9: İz Kayıt Kaynağı Oluşturma Ekranına Giriş..... 75
Şekil 3.10: Kural Listesi..... 77
Şekil 3.11: Yeni Kural Oluşturma Ekranına Giriş..... 77
Şekil 3.12: Kurala Filtrelerin Eklendiği Bölüm..... 78
Şekil 3.13: Kural Tetiklendiğinde Alınacak Aksiyonların Belirlendiği Ekran..... 79
Şekil 3.14: Dispatch New Event Aksiyonu..... 79

TABLOLAR LİSTESİ

Sayfa

Tablo 2.1 Olay ID Listesi..... 12
Tablo 2.2 Oturum Açma Türü Listesi..... 14
Tablo 2.3 Status Kod Örnekleri..... 15
Tablo 2.4 W3C Extended Log File format Parametreleri..... 20
Tablo 2.5 Syslog Denetim Kayıtlarındaki Parametreler..... 22
Tablo 2.6 Hata İz Kayıtları Format Parametre Tablosu..... 26
Tablo 2.7 Erişim İz Kayıtları Format Parametre Tablosu..... 27
Tablo 2.8 Palo-Alto Güvenlik Duvarı İz Kayıt İçeriğinde Bulunan Parametreler ve Açıklamaları..... 32
Tablo 2.9 McAfee Antivirus İz Kayıt Parametre ve Açıklamaları..... 42
Tablo 2.10 Microsoft Windows DNS Sunucu İz Kayıt Parametreleri..... 46
Tablo 2.11 F5 ASM İz Kayıt Parametre ve Açıklamaları..... 55
Tablo 2.12 Scopnet İz Kayıt Parametre ve Açıklamaları..... 57
Tablo 2.13 McAfee Web Gateway İz Kayıt Parametre ve Açıklamaları..... 60
Tablo 3.1:Zimbra Mail Uygulası İz Kayıt Örneği..... 68
Tablo 3.2: Kaynak tanımı için gerekli parametreler..... 75
Tablo 3.3: Use Case şablonu..... 80
Tablo 4.1: Rsyslog Konfigürasyon Örneği..... 82
Tablo 4.2: Zimbra Mail Uygulaması İz Kayıt Örneği..... 85
Tablo 4.3: Zimbra Mail İz Kayıt Parametreleri..... 86
Tablo 4.4: Zimbra Mail Sunucusu Kaynak Tanımı..... 86
Tablo 4.5 Ele Geçirilen Kurumsal Hesapların Tespiti..... 87
Tablo 4.6: McAfee EPO Kaynak Tanımı..... 92
Tablo 4.7: McAfee EPO İz Kayıt Parametreleri..... 93
Tablo 4.8 Bilgi İşlem Cihazı Üzerinde Zararlı Yazılım Aktivitelerinin Tespiti..... 94
Tablo 4.9 Bilgi İşlem Cihazı Üzerinde Silinemeyen Zararlı Yazılım Tespiti..... 97
Tablo 4.10 Komuta ve Kontrol Merkezleri İle Haberleşen Bilgi İşlem Cihazlarının Tespiti..... 99
Tablo 4.11 Kurum Ağında Port Taraması Yapan Lokal IP Adreslerinin Tespiti..... 100
Tablo 4.12: Anti-Forensics faaliyetlerinin tespiti için gerekli iz kayıt örnekleri..... 102
Tablo 4.13 Olay ID 1102 İz Kayıt Örneği için Regex Örnekleri..... 105

Tablo 4.14 İşletim Sistemi Üzerindeki İz Kayıtlarının Silinmesi..... 105
Tablo 4.15 İşletim Sistemi Üzerindeki İz Kayıt Servislerinin Kapatılması..... 107
Tablo 4.16 İşletim sistemi üzerinde disk wipe işlemi için kullanılan işlemlerin çalıştırılması..... 108
Tablo 4.17 Kurum Dışına Doğru Yüksek Boyutlu Veri Transferinin Tespiti..... 110
Tablo 4.18 Kurum Ağında Veri tabanı Taraması Yapan Lokal IP Adresi Tespiti..... 113
Tablo 4.19 HTTP 200 Web Erişim İz Kayıt Örneği..... 115
Tablo 4.20 Web Sayfalarına Yapılan Saldırıların Tespiti..... 115

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	**Açıklamalar**
AIX	Advanced Interactive eXecutive
API	Application Programming Interface
ASA	Adaptive Security Appliance
ASCII	American Standard Code for Information Interchange
CLI	Command Line Interface
CPU	Central Process Unit
DNS	Domain Name System
DPI	Deep packet inspection
DSM	Device Support Module
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HTTP	Hyper Text Transfer Protocol
IIS	Internet Information Services
IP	Internet Protocol Address
JDBC	Java DataBase Connectivity
KVKK	Kişisel Verileri Korunması Kanunu
LEA	Log Export API
MAC	Media Access Control
MSRPC	Microsoft Remote Procedure Call
NAC	Network Access Control
NCSA	National Center for Supercomputing Applications
NGFW	Next Generation Firewall
NIDS	Network-based Intrusion Detection System

NTLM	New Technology LAN Manager
OPSEC	Open Platform for Security
PCI/DSS	Payment Card Industry/Data Security Standard
RAM	Random Access Memory
RIPE	Regional Internet Registry for Europe
RPC	Remote Procedure Call
SIEM	Security information and event management
SMB	Server Message Block
SMLI	Stateful multi-layer inspection
SOAR	Security Orchestration Automation and Responce
SOC	Security Operation Center
SOX	Sarbanes Oxley
SQL	Structured Query Language
SSH	Secure Shell
TBMM	Türkiye Büyük Millet Meclisi
TCP	Transmission Control Protocol
TTL	Time to live
URI	Uniform Resource Identifier
VPN	Virtual private network
WAF	Web Application Firewall
WEF	Windows Event Forwarding
XSS	Cross Site Scripting
OSI	Open Systems Interconnection
RR	Resource Records

1. GİRİŞ

Günümüzde bilgi güvenliği, pek çok kurum ve kuruluş yöneticileri için endişe kaynağı olan başlıca konulardan biridir. Siber güvenlik firmaları her yıl raporlar yayınlamaktadır ve bu raporlar endişelerin yersiz olmadığını göstermektedir. Bu raporlar belirtmektedir ki, 2020 yılında dünya genelinde her gün yaklaşık yüz bin kötücül web sitesi yayınlanmaktadır, on bin kötücül dosya internette dolaşıma girmektedir. Bu zararlı web sayfaları ve dosyalar bilişim sistemine zarar verme, bilgi hırsızlığı, dolandırıcılık gibi işlemler için kullanılmaktadır ve kurumların %46'sında en az bir çalışanın bahsi geçen zararlı dosyaları kişisel bilgisayarlarına indirdiği ya da bu zararlı web sayfalarını ziyaret ettiği aynı raporlarda anlatılmaktadır. Buna ek olarak kurumlara minimum bir kez mevcut bir zafiyetinin sömürülmesi yoluyla saldırı girişiminde bulunulması oranının %87 olduğu bildirilmiştir [1].

Her yıl yayınlanan bu raporlar ve araştırmalar göstermektedir ki dışarıdan ve içeriden gerçekleşebilecek saldırılara karşı hazırlıklı olmak ve adli bilişim incelemelerinin etkili ve hızlı şekilde yapılması oldukça önemlidir. Bu çalışmada, oluşabilecek siber saldırı örnekleri modellenecek ve SIEM sistemleri kullanılarak bu saldırıların nasıl tespit edilebileceği incelenecek, siber güvenlik analistlerinin ve bilgi işlem çalışanlarının bu olaylara nasıl tepki verebilecekleri üzerinde çalışmalar yapılacaktır.

Bu çalışmanın ikinci bölümünde literatür araştırmasına yer verilmiştir. Kurumsal altyapılarda bulunması muhtemel sistemlerin iz kayıt tipleri incelenmiştir. Bu iz kayıtlarından korelasyon kurallarında kullanılmak üzere elde edilebilecek parametreler açıklamaları ile birlikte verilmiştir. Son olarak bu iz kayıtlarının SIEM sistemine aktarım amacıyla kullanılan yöntemler incelenmiştir.

Çalışmanın üçüncü bölümünde örnek SIEM uygulaması üzerinde olay tespiti için yapılan işlemler adım adım aktarılmıştır. Uygulama üzerinde iz kayıt kaynaklarının oluşturulması, iz kayıtlarının anlamlandırılması, korelasyon kurallarının yazılımı ve oluşturulan şablonun açıklamaları ekran görüntüleri ile birlikte verilmiştir.

Çalışmanın dördüncü bölümünde örnek olarak seçilen adli bilişim olayları için ilk üç bölümde anlatılan bilgiler ve uygulamalar kullanılarak tespit işlemi uygulanmıştır. Yapılan uygulama çalışması sonucunda yapılan işlem adımları şablonlar üzerinde gösterilmiştir.

Çalışmanın son bölümünde yapılan uygulama çalışmasının sonuçları değerlendirilmiş ve ilerideki çalışmalarda neler yapılabileceği üzerine bilgiler aktarılmıştır.

2. LİTERATÜR ARAŞTIRMASI

Siber saldırıların önlenmesi, tespiti ve bu saldırılara karşı konulması konusunda hayli güçlü olan SIEM (Security Information and Event Management) sistemleri adli bilişim alanında birçok çözüm sağlamaktadır. Bu çözümler, yüksek riskli alanlarda görünürlüğü artırarak siber suçların etkilerinin görülmesinden önce engel olmaya çalışan bir perspektif ile sürekli gelişmekte ve bu doğrultuda adım adım büyük veri analitiği araçlarına dönüşmektedir [2]. SIEM sistemleri, bilgi güvenliği konusunda bilinç düzeyini artırmak amacıyla orta ve büyük ölçekli şirketlerin çoğunun Güvenlik Operasyon Merkezlerinde kullanmaktadır. Günümüzde kullanılan SIEM ürünlerinin analizine yönelik çalışmalar mevcuttur. Bu çalışmalar, kullanıcıların SIEM'i genel hatları ile anlaması, yazılım modüllerinin yeniden kullanımınının desteklenmesi ve yeni sistemlerin geliştirilmesi konularında yol göstericidir [3].

Žgela ve Penga'nın yaptığı çalışmada araştırmacılar, farklı sistemlerden elde edilen verileri merkezi bir yapıda bir araya getirerek analiz etmenin, olay yönetiminin sağlanması üzerindeki etkisini araştırmışlardır. Bu çalışma kapsamında bir buçuk ay boyunca, bir banka altyapısındaki 10 farklı platformdan 3.462.187 adet olay kaydı toplanmıştır. Bu farklı bilişim sistemlerinden elde edilen verileri analiz ederek farklı ekosistemlerde olayların nasıl değişkenlik gösterdiği incelenmiştir. Farklı ortamlardan gelen bu kayıtların birbiri ile nasıl ilişkilendirilmesi, anlamlandırılması ve anomalilerin tespit edilmesi gerektiği bilgi güvenliğini iyileştirme amacıyla sunulmuştur [4]. Benzer bir çalışmada, SIEM sistemlerinin korelasyon özelliği incelenmiş ve saniyede 15 bin olay kaydını işleyerek gerçekleşen siber saldırıyı üzerinde yazılan kurala göre bir dakikanın altında tespit edebilecek yeni bir bir korelasyon motoru tasarımı yapılmıştır. Bu tasarım üzerinde, yaşanan performans sorunları ile mücadele yöntemlerini göstermiş ve korelasyon sistemi ile son kullanıcı arasında daha kolay anlaşılabilecek bir korelasyon dilini tasarımına entegre etmiştir [5].

Gökçeoğlu'nun korelasyon kural yazılımı üzerine yaptığı çalışmada, bir takım güvenlik cihazlarının ve işletim sistemlerinin iz kayıtları incelenmiştir. Bu kayıtlar IBM Qradar platformu üzerinde toplanarak korelasyon kurallarının yazımı hakkında bilgiler verilmiştir. Örnek siber saldırı senaryoları uygulama üzerinde bu korelasyon kuralları ile gösterilmiştir [6].

Irfan ve ark.'ın yaptığı çalışmada, bulut ortamlarda bilgi güvenliğinin sağlanması ve adli bilişim vakalarında delil toplama aşamasında yaşanan zorluklar incelenmiştir. Bu çalışmada çerçeve bir sistem tasarımı yapılmıştır. Bu tasarım, bulut ortamlarında merkezi bir olay yönetimi sisteminin kurularak tüm altyapıda gelişen olaylar üzerinde görünürlüğün artırılması ve yaşanan siber olaylarda saldırganların izinin takip edilerek adli bilişim süreçlerinin kolaylaştırılması ve saldırıların proaktif bir şekilde önüne geçilmesini amaçlamaktadır [7].

Yapılan bu çalışmalar incelendiğinde, SIEM sistemlerinin iki yönden araştırıldığı görülmektedir. Birincisi, teorik olarak geniş perspektiften SIEM sistemlerinin siber olay müdahalede kullanımı, ikincisi ise uygulamalar ile örnek saldırı senaryoları için korelasyon kurallarının nasıl oluşturulabileceğidir. Literatürde, adli bilişim olay tespiti sürecinin uçtan uca detaylı olarak anlatıldığı bir çalışmaya rastlanmamıştır.

Bu tez çalışmasında, bir bilgi işlem merkezinde karşılaşılabilecek bilişim sistemlerinin oluşturduğu iz kayıtları uçtan uca incelenmiştir ve bu iz kayıtlarının SIEM sistemlerine aktarımı için kullanılan yöntemler ele alınacaktır. Aynı zamanda bu iz kayıtlarından elde edilebilecek veriler anlamlandırılarak belirlenen saldırı senaryoları için oluşturulan korelasyon kuralları ile yaşanabilecek saldırıların tespiti yapılacaktır. Bu tespit sonrası bilişim personelinin alması gereken aksiyonlar bir şablonu üzerinde gösterilecektir. Bununla birlikte literatürde bu çalışmada kullanılan şablon benzeri bir yapıya rastlanmamıştır. Bu şablon sayesinde herhangi bir SIEM kullanıcısı aynı yöntemi kendi sisteminde uygulayarak aynı sonuca ulaşabileceklerini düşünmekteyiz.

2.1. SIEM

İz kayıtları, kurum bünyesinde çalışan sistemlerin içerisinde veya kurum ağında yaşanan olayları gösteren kayıtlardır. Her ne kadar önceleri sistemsel problemlerin çözümü için kullanılmış olsalar da günümüzde sistemlerin performans optimizasyonu, kullanıcı işlem kayıtlarının tutulması, zararlı veya şüpheli aktivitelerin takibi gibi konular için de kullanılmaktadır. Bilgi teknolojilerinin hayatın her alanına girmesi ve günlük kullanımlarındaki artışın yanında bu sistemlere karşı yapılan saldırıların da artması ile güvenlik iz kayıtlarının miktarında ve çeşitliliğinde ciddi bir artış olmuştur [8, 9]. Tüm iz kayıtlarının incelenmesi, anlamlandırılması, başka iz kayıtları ile anlamlı bağlantılar kurulması ve alarm haline getirilmesi sürecini bir güvenlik analistinin herhangi bir yardımcı araç kullanmadan yapabilmesi imkansıza yakındır. Bu nedenle iz kayıtlarını

anlamlandıracak ve sadece gerekli kayıtları güvenlik analistinin önüne getirerek hem efor hem de zamandan kazanç sağlayacak bir sistem ihtiyacı ortaya çıkmıştır. Bu ihtiyacı karşılayan sistemler SIEM olarak adlandırılan sistemlerdir [10].

SIEM, temelde güvenlik bilgilerinin yönetimi işlemlerinin yapıldığı SIM (Security Information Management) sistemleri ile güvenlik olay yönetiminin yapıldığı SEM(Security Event Management) sistemlerinin tek bir çatı altında birleştirilmesinden oluşmuştur [11]. Bu sistemlerin gelişmesinin ve üretilmesinin arkasındaki birçok motivasyon kaynağı mevcuttur. Bu sistemlerin gelişmesine en çok etki eden motivasyon kaynağı regülasyonlar ve yasal zorunluluklardır [12]. Ulusal ve uluslararası birçok regülasyon ve kanun gereksinimi SIEM sistemleriyle karşılanabilmektedir. Ülkemizde 2016 yılında TBMM tarafından kabul edilen Kişisel Verilerin Korunması Kanunu (KVKK) ile kişisel veri barındıran tüm kurumların uyması gereken kurallar belirlenmiştir. Kişisel verilerin saklanması, işlenmesi ve yok edilmesi aşamalarının tümünde SIEM sistemlerinin büyük bir rolü bulunmaktadır. Örnek olarak kişisel verilerin saklandığı veri tabanlarına kimlerin erişim sağladığı, yetkisiz kişilerin bu verilere ulaşıp ulaşmadığı gibi kontroller SIEM sistemleri aracılığı ile yapılabilmektedir. Kontrol mercilerinin denetimlerinde bu kayıtlar delil olarak da sunulabilmektedir [13]. Buna benzer olarak ISO 27001 ve PCI/DSS gibi global olarak kabul görmüş bir çok standardın maddeleri incelendiğinde bu standart maddelerinin bir kısmının sağlanabilmesi için SIEM sistemlerine ihtiyaç duyulduğu anlaşılmaktadır [14] .

Kurumların SIEM sistemlerini kullanmasında bir diğer önemli motivasyon ise iç tehditlerin tespiti ve önlenmesi ihtiyacıdır. İç tehdit, bir bilgi sistemine herhangi bir düzeyde yetki verilmiş herhangi bir kişi olarak tanımlanabilir [15]. Bu kişiler isteyerek veya istemsiz olarak bilişim sistemleri üzerinden kuruma zarar verecek faaliyetlerde bulunabilirler. Yapılan araştırmalar iç tehditlerin kurumlar için başlıca risk faktörleri olduğunu göstermektedir. Bu durumun başlıca sebebi kurumun personeline olan güveni ve personelin kurum hakkında dışardaki herhangi birinden daha fazla bilgi sahibi olmasıdır. 2020 yılında yapılan bir araştırmaya göre 2018 ve 2020 yılları arasında iç tehdit kaynaklı olaylar %47 oranında artmıştır [16]. İç tehdit faktörlerinin harekete geçmesi durumunda veya güvenlik ihlal olayının yaşanmasının ardından kanıtların elde edilmesi noktasında SIEM sistemleri kullanılmaktadır.

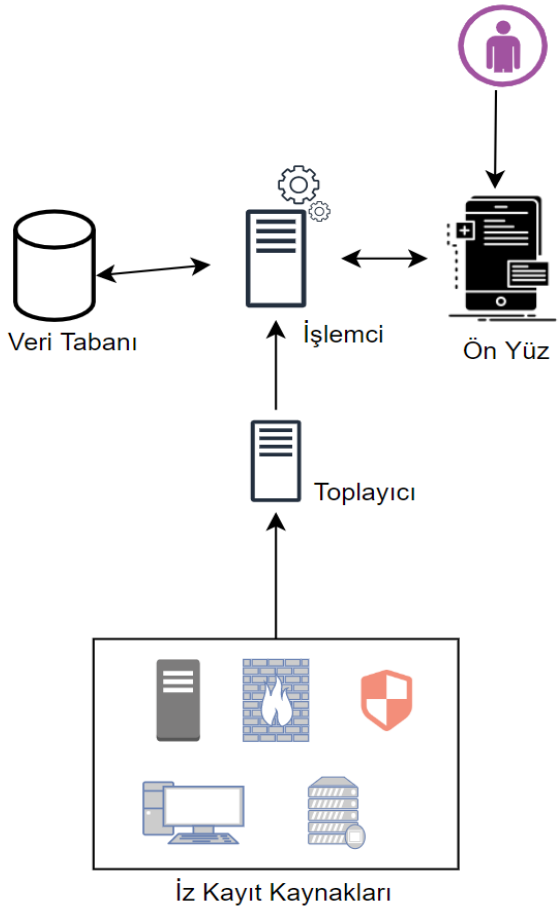
Bir diğer motivasyon kaynağı bilgi güvenliği ihlal olaylarının kurumlara hem maliyet olarak hem de kuruma olan güvenin zedelenmesi noktasında büyük zararlar vermesidir. Bu gibi

siber saldırı durumlarının henüz başlangıçta tespit edilmesi ve saldırganlar ile ilgili delil toplanması noktasında SIEM sistemleri aktif olarak kullanılabilmektedir.

Son motivasyon kaynağı olarak güvenlik izleme ve analiz aşamalarında ihtiyaç duyulan insan kaynağını azaltması ve olaylara müdahale süresini kısaltması gösterilebilir. Bilgi teknolojileri alanındaki gelişmeler ile birlikte üretilen sistemlerin ve cihazların artışı beraberinde üretilen güvenlik iz kayıtlarının miktarını da arttırmaktadır. Bu durumda kayıtları inceleyecek ve güvenlik olaylarını tespit edecek personelin sayısında da artışa ihtiyaç duyulmaktadır. Ancak ne kadar personel çalışırsa çalışsın farklı kaynaklardan elde edilen iz kayıtlarının anlamlı olarak birleştirilmesi ve güvenlik olayının tespit edilmesi yine de oldukça zordur. SIEM sistemleri bu noktada hem zamandan hem de personel sayısından tasarruf edilmesine olanak sağlamaktadır [17].

2.2. SIEM Çalışma Prensibi

İlk geliştirilen SIEM sistemleri veri akışının her aşamasında, politikaların uygulanmasında, alarmların incelenmesi ve analiz edilmesinde detaylı ve titiz bir yönetime ihtiyaç duymaktaydı. Ancak bu sistemler geliştikçe daha akıllı hale gelmiştir. İz kayıtlarının toplanması, bunların tanımlanması ve alarm haline getirilmesi aşamaları her geçen gün daha otomatize hale gelmiştir. Bu durumun sonucu olarak daha karmaşık saldırı senaryoları ve davranış tabanlı analizler yapay zeka uygulamaları kullanılarak yapılmaya başlanmıştır [18]. Standart bir SIEM sistemi mimarisi Şekil 2.1'de gösterilen bileşenlerden oluşur. Her bir bileşen özelleştirilmiş bir işlevi yerine getirmek için tasarlanmıştır. Önyüz olarak isimlendirilen kısım kullanıcıların etkileşime girdiği arayüzdür. Bu arayüz üzerinden güvenlik alarmları takip edilebilir, iz kayıtları üzerinde belirlenen kurallara göre aramalar yapılabilir, raporlar oluşturulabilir ve sistem yönetimi gibi işlemler yapılabilir. İşlemci olarak isimlendirilen kısımda toplayıcıdan gelen iz kayıtları belirlenen kurallara göre işlenerek veri tabanına yazılır. Sistem yöneticisinin yazdığı kurallara göre farklı kaynaklardan toplanan iz kayıtları bu kısımda korelasyona sokularak anlamlı güvenlik alarmları oluşturulur. Toplayıcı ismiyle anılan kısımda kaynaklardan iz kayıtları toplanır, normalize edilir ve anlamlı parçalara ayrılarak etiketlenir. Veri Tabanı, iz kayıtlarının ve korelasyon sonucu oluşturulan alarmların saklandığı kısımdır. Log kaynakları olarak isimlendirilen kısımda ise birbirinden farklı ağ ekipmanı, sunucu veya bilgisayar bileşeni bulunmaktadır. Bu bileşenlerden her biri kendine özgü iz kaydı tutma ve gönderme özelliklerine sahiptir.



Şekil 2.1 Standart bir SIEM Mimarisi

Bir SIEM sisteminden temel olarak beklenebilecek özelliklerin bir kısmı aşağıda verilmiştir.

Veri Toplama

Bir SIEM sisteminden beklenen temel özelliklerin başında güvenlik cihazları ve ağ ekipmanlarından iz kayıtlarının toplanması ve bu ham kayıtların istatistiksel analizler için özet biçiminde ifade edilmesi gelmektedir [19].

Siber İstihbarat Kaynakları

SIEM sistemlerinin bir diğer özelliği üçüncü parti uygulamalardan aldığı veriler ile iç verilerini karşılaştırıp güvenlik analizleri yapabilmesidir. SIEM sistemlerinden en yaygın kullanılan üçüncü parti verisi Threat Intelligence verisidir. Threat Intelligence kelime anlamı olarak tehdit istihbaratı olarak çevrilebilir. Tehdit istihbaratı, saldırganın hedeflerini, amaçlarını ve saldırı yöntemlerini anlamak için toplanan, işlenen ve analiz edilen verilerdir.

Bu veriler kullanılarak daha hızlı, daha bilinçli, veri destekli güvenlik kararlarının alınmasını ve tehdit aktörlerine karşı mücadelede güvenlik cihazlarının davranışlarını reaktiften proaktif hale getirmesini sağlar [20].

Korelasyon ve güvenlik izleme

Korelasyon işlemi farklı kaynaklardan oluşan iz kayıtlarının bir saldırıyı veya güvenlik olayını ortaya çıkarmak için anlamlı bir şekilde bir araya getirilmesidir. Bunlar olaylar ve bağlantılı veriler ile tehditler, güvenlik olayları ve adli bilişim bulguları arasında bağlantı kurmayı kolaylaştıran işlemlerdir. Korelasyon işleminde bir saldırının ne olduğunu veya saldırının gerçekte olup olmadığını anlayabilmek için gelişmiş ve yoğun veri işleme uygulamaları kullanılmaktadır. [21].

Analiz Yapma

Veri parçaları arasında daha derinlemesine ilişkiler kurmak ve anlamlı sonuçlar elde edebilmek için birçok üretici ürünlerine istatistiksel model çıkarma veya makine öğrenme yetenekleri eklemektedir.

Uyarı Oluşturma

SIEM ürünleri iz kayıtlarının toplanması, işlenmesi ve analiz edilmesi sonucunda güvenlik analistini uyaracak bir bilgilendirme mesajı oluşturular. Bu sayede analist sadece belirli uyarıları inceleyerek olayları tespit edebilir.

Gösterge Panelleri

Birçok SIEM ürününde olayların takip edilmesinde kullanılan bir arayüz bulunmaktadır. Bu arayüz üzerinde ayrıca istatistiksel veriler ve grafikler ile zenginleştirilmiş alanlar da bulunabilir.

Standart ve Regülasyonlara Uyum

Kurumlar bağımlı oldukları standartlar veya regülasyonların kontrolü ve denetimi için SIEM sistemlerini kullanabilirler. Bu sistemler üzerinden PCI/DSS, SOX, GDPR veya ISO27001 standartları/regülasyonları için raporlar üretilebilir. Bu sayede hem kurumun standartlara uyum durumu görülebilir hemde denetimlerde istenen verilere daha kolay bir ulaşım sağlanmış olunur.

Veri Tutma

Çoğu ülkede veri tutulması kanuni bir zorunluluk haline gelmiştir. Ülkeler, kamu güvenliğini garanti altına alabilmek için yasalar üretir ve kanuni müdahale politikaları uygulayarak veri inceleme veya takip işlemlerini gerçekleştirir. Kurumlar bu yasalara uyabilmek için belirlenen özellikteki verilerini belirlenen süreler boyunca tutmak ve gerektiğinde bunu ilgili kurumlar ile paylaşmak için SIEM sistemlerini kullanabilir [9].

Adli Bilişim Analizi

Adli bilişim sürecini daha iyi anlayabilmek için, dört katmanlı bir yapı kullanabilir. Bu katmanlar veri, içerik tarama, veri analizi ve uygulama katmanı olarak ayrılabilir. Veri katmanında delillerin toplanması işlemleri yapılır. İçerik tarama katmanında aranan veriye daha hızlı ulaşabilmek için verilerin sınıflandırılması işlemleri gerçekleştirilir. Veri analizi kısmında taranan içerikler üzerinde yapılan incelemeler ile olay ile ilişkili bilgilere ulaşılıp rapor haline getirilmesi adımları uygulanır. Son olarak uygulama aşamasında kanıtlar simüle edilerek toplama işlemi ve filtreleme adımları gözden geçirilir. Bu dört katmanlı yapıda veri toplama ve analiz işlemlerinde SIEM sistemlerinin kullanımı birçok açıdan fayda sağlamaktadır [22].

Tehdit Avcılığı

Siber saldırıları engellemek ya da müdahale sürelerini minimum seviyeye düşürmek için siber güvenlik farkındalığı bulunan kurumlar güvenlik operasyonlarına siber istihbarat hizmetini de katmaktadır. Siber saldırıların karmaşıklığı, saldırı aktörlerinin motivasyonu ve atik yapıları arttıkça kurumların bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumaları da zorlaşmaktadır. Bu gibi nedenlerden dolayı tehdit istihbaratı tek başına yeterli olmamaktadır. İz kayıtları üzerinde tehdit aktörlerinin izini sürecek bir SIEM sistemi ile bu sistem üzerinde düzgün konfigürasyon sayesinde daha başarılı bir tehdit avcılığı çalışması yapılabilir [23].

Olay Müdahale

Siber Güvenlikte olay müdahale kurumlarda sürekli devam eden ve hiç durmayan bir süreçtir. Bu süreç hazırlık, tespit, önleme, soruşturma, kurtarma ve öğrenme gibi farklı alt başlıkların bir arada değerlendirilmesi ile uygulanabilir. Güvenlik olaylarına karşı etkili, sistematik ve hızlı bir şekilde müdahale edilebilmesi için olay müdahale sürecinin kurumlarda uygulanması önem arz etmektedir. Bu süreçlerin işletilememesi durumunda

kurumun tüm faaliyetinin durmasına yol açabilecek durumlar ile karşılaşılabilir. Bununla birlikte kurumların bağlı bulunduğu kanun ve regülasyonlara uyamama durumları da ortaya çıkabilir. Olay müdahale sürecinin tespit ve analiz aşamalarında SIEM ürünlerinin kullanımı olayların tespiti ve müdahale sürelerinin kısaltılması konularında yardımcı olmaktadır [24].

SOC Otomasyonu

Modern teknolojilerin gelişmesi ile birlikte çoğu kurum iş süreçlerini bilgi teknolojileri üzerinden yürütmeye ve hassas verilerini kendi içlerinde saklamaya başlamıştır. Ancak bu kritik altyapıların ve verilerin güvenliğini sağlamak, özellikle internete açık yapılarda kolay değildir. Bu noktada kurumların ihtiyacı karşılayan yapı Güvenlik Operasyon Merkezleridir (SOC). Tipik bir SOC merkezinde her gün binlerce güvenlik olayı tespit edilir ve analizden geçer. Bu sayı büyük yapılarda milyonları bulabilir. Güvenlik analistleri çok sayıda güvenlik olayını manuel olarak inceleyecek durumda değildir. Bu durumun önüne geçmek için SIEM sistemleri kullanılır. Ancak bu durumda tespit edilen bir olayın farkedilmesi ve aksiyon alacak personele bir güvenlik alarmı olarak iletmesi, aksiyon alacak personelin bu alarmı görerek ilgili cihaz üzerinde gerekli önleme faaliyetini gerçekleştirme süreci uzun sürmektedir. Bu süreçlerin iyileştirilmesi adına SIEM sistemleri ile aksiyon alacak güvenlik cihazları arasında entegrasyonlar yapılarak daha kısa müdahale sürelerine ulaşmak mümkündür. Örnek olarak SIEM ve güvenlik duvarı arasında kurulacak bir entegrasyon ile kuruma yönelik yapılan bir siber saldırının kaynak IP adresi SIEM sistemleri tarafından tespit edilerek güvenlik duvarı üzerinde bu IP adresinin otomatik olarak engellenmesi sağlanabilir. SIEM ile aktif güvenlik cihazları arasında entegrasyonu sağlayan bu gibi sistemlere SOAR (Security Orchestration Automation and Responce) adı verilir [25].

2.3. İz Kayıt Çeşitleri

İz kayıtları kurumun sistemleri ve ağında meydana gelen olayların kayıtlarıdır. Bu kayıtlar içerisinde sistem ve ağ hakkında çeşitli yönlerden bilgi verecek çok sayıda parametre bulunmaktadır. Çalışmanın bu aşamasında güvenlik iz kayıtları incelenecektir.

Her sistemin ve cihazın ürettiği iz kayıtları aynı değildir. Farklı üreticiler ihtiyaçları veya tasarımlarını göz önüne alarak farklı yapılarda iz kayıtları oluşturmuştur [8]. Bu sistemlerden en yaygın kullanılanlar aşağıda incelenmiştir.

2.3.1.Microsoft Windows security event logs

Windows, Microsoft firması tarafından üretilmiş, günümüzde kurumların birçoğunda son kullanıcı bilgisayarlarında kullanılan bir işletim sistemidir. Windows, kendi içinde gerçekleşen aktiviteleri kaydetmektedir. Bu kayıtlar iki kategoriye ayrılabilir. Birincisi, sistem olay kayıtlarıdır ve daha çok operasyonel işlemlerin kayıtlarından oluşmaktadır. Örnek vermek gerekirse servis başladı, durduruldu, sistem kapandı, vb. İkincisi ise denetim kayıtlarıdır ve güvenlik olay bilgilerinden oluşmaktadır. Bu kayıtlara örnek; dosya erişimleri, başarısız veya başarılı oturum açma denemeleri, hesap işlemleri (kullanıcı oluşturuldu, silindi, vb.), güvenlik politika değişimleri, yetki kullanımları gösterilebilir [8, 26].

Security Auditing, Windows güvenlik olaylarının oluşturulması için kullanılan araçtır. Bu araç, işletim sistemi üzerinde gereken seviyede denetim kayıtlarının oluşturulmasını ve saklanmasını sağlamaktadır. Temelde iki düzeyde iz kayıtları tutulmaktadır. Bunlar *Gelişmiş ve Basit Güvenlik Denetimi'*dir [26].

Basit Güvenlik Denetiminde aşağıdaki kategorilerde denetim gerçekleştirilebilir;

- Ayrıcalık kullanımını,
- Dizin hizmeti erişimini,
- Hesap oturumu açma olaylarını,
- Hesap yönetimini,
- İlke değişikliğini,
- İşlem izlemeyi,
- Nesne erişimini,
- Oturum açma olaylarını,
- Sistem olaylarını denetle.

Bu denetimleri aktif ve pasif hale getirme işlemleri, Windows'da "Yerel Güvenlik İlkesi" aracı üzerinden "Denetim İlkesi" klasörü altından yapılır.

"Gelişmiş Güvenlik Denetimleri" ise "Yerel Güvenlik İlkesi" aracı üzerinden Güvenlik Ayarları > Gelişmiş Güvenlik İlkesi Yapılandırması > Sistem Denetim İlkeleri altında yer almaktadır. *Olay Görüntüleyici* isimli araç, bu olay kayıtlarının işletim sistemi üzerinden takibi ve incelemesini sağlamaktadır [26].

Windows'da gerçekleşen her güvenlik olayı tipi bir ID ile eşleştirilmiştir. Microsoft'un takip edilmesini önerdiği bir dizi ID değeri Tablo 2.1'de yer almaktadır [27].

Tablo 2.1 Olay ID Listesi

Olay ID	**Olay Adı**	**Açıklama**
4740	Account Lockouts	Kullanıcı hesabı kilitlendi.
4648	Account Login with Explicit Credentials	Oturum açan hesap haricinde başka bir hesap bilgisi kullanılarak işlem yapıldı.
4781	Account Name Changed	Hesap ismi değiştirildi.
4733	A member was removed from a security-enabled local group	Yerel bir gruptan hesap çıkarıldı.
4776	The computer attempted to validate the credentials for an account.	NTLM otantikasyon yöntemi kullanılarak hesap doğrulama denemesi yapıldı.
5376	Credential Manager credentials were backed up	Kimlik Yönetici Veritabanının yedek alma işlemi başarılı olarak gerçekleşti.
4625	An account failed to log on	Başarısız oturum açma denemesi yapıldı.
4720	A user account was created	Yeni kullanıcı hesabı oluşturuldu.
4782	The password hash of an account was accessed	Bir hesabın parola geçişi sırasında, hesabın parola hash bilgisine erişildi.
4624	An account was successfully logged on	Hesap ile başarılı oturum açıldı.
1100	The event logging service has shut down	Windows Event Log servisi kapandı.
1102	The audit log was cleared	Windows güvenlik olay kayıtları silindi.
1000	Application error	Uygulama hatası alındı.

Her bir olay ID'si yaşanan durumla ilgili birçok bilgi sağlamaktadır. Bu bilgilerin ne olduğu ve hangi durumları işaret ettiği şekil 2.2'de Olay ID 4625 üzerinden incelenmiştir.

Olay ID 4625 başarısız bir oturum açma isteği yapıldığında oluşan olay kaydıdır. Bu olay oluştuğunda üretilecek iz kaydının örneği aşağıdaki gibidir.

Jan 09 16:32:32 hostname01.deneme.com AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.0.41 Source=Microsoft-Windows-Security-Auditing Computer=hostname01.deneme.com OriginatingComputer=10.10.10.10 User= Domain= EventID=4625 EventIDCode=4625 EventType=16 EventCategory=12544 RecordNumber=534168 TimeGenerated=1640933936 TimeWritten=1640933936 Level=Log Always Keywords=Audit Failure Task=SE_ADT_LOGON_LOGON Opcode=Info Message=An account failed to log on. Subject: Security ID: NT AUTHORITY\SYSTEM Account Name: hostname01$ Account Domain: DENEME Logon ID: 0x3E7 Logon Type: 2 Account For Which Logon Failed: Security ID: NULL SID Account Name: user01 Account Domain: DENEME Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x7b8 Caller Process Name: C:\Windows\System32\svchost.exe Network Information: Workstation Name: hostname01 Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0

Şekil 2.2 Olay ID 4625

Bu kayıt içerisindeki alanlar ve anlamları aşağıdaki gibidir.

Computer: Olayın gerçekleştiği cihazın adıdır.

EventID: Olay ID numarası.

Account Name: Oturum açma isteğini yapan hesabın adıdır. Eğer ismin sonunda dolar işareti bulunuyorsa bu bilgisayar ismi olduğu anlamına gelmektedir.

Account Domain: Hesabın bulunduğu domainin adıdır.

Failure Reason: Olayın meydana gelme sebebi ile ilgili açıklamadır.

Logon Type: Bu parametre oturum açma isteğinin çeşidi hakkında bilgi verir. Bu oturum açma çeşitlerinin anlamları Tablo 2.2'de verilmiştir [28].

Tablo 2.2 Oturum Açma Türü Listesi

Oturum Açma Türü	**Oturum Açma Başlığı**	**Açıklama**
2	Etkileşimli	Klavye kullanarak ekran üzerinden oturum açma isteğinin yapıldığı ifade eder.
3	Ağ	Ağ üzerinden bir oturum açma isteğinin yapıldığını ifade eder. (paylaşımlı dosyalara erişim vb.)
5	Servis	Servis kontrol yönetici tarafından bir servisin başlatıldığını ifade eder.
7	Kilit açma	Ekran kilidinin açılması sırasında oturum açma denemesinin yapıldığını ifade eder.
8	Ağ açık metin	Ağ üzerinden parolanın açık metin olarak gönderilerek oturum açma isteğinin yapıldığını ifade eder.
10	Uzaktan etkileşimli	Uzak masaüstü veya terminal sunucu kullanılarak sistem üzerinden oturum açma denemesinin yapıldığını ifade eder.

Status: Oturum açma işleminin neden başarısız olduğu ile ilgili bilgi veren bir koddur. Bu kodların birkaçının anlamı Tablo 2.3'de verilmiştir [28].

Tablo 2.3 Status Kod Örnekleri

Status Kodu	Açıklama
0XC000005E	Oturum açma isteğine cevap verecek bir oturum açma sunucusu bulunmuyor.
0xC0000064	Yanlış yazılmış veya hatalı hesap ismi ile oturum açma isteği.
0xC000006A	Yanlış yazılmış veya hatalı parola ile kullanıcı oturum açma isteği.
0XC000006D	Hatalı kullanıcı adı veya kimlik doğrulama bilgisi.
0xC000006F	Yetkili saatler dışında oturum açma isteği.
0xC0000070	Yetkisiz iş istasyonu üzerinden oturum açma isteği.
0xC0000071	Son kullanma tarihi geçmiş parola ile oturum açma isteği.
0xC0000072	Admin kullanıcısı tarafından pasif duruma getirilmiş bir hesap ile oturum açma isteği.

Windows güvenlik olay kayıtlarının örnekleri aşağıda verilmektedir.

Olay ID 4738: Kullanıcı hesabıyla ilgili herhangi değişiklikte bu olay ID oluşmaktadır. Şekil 2.3'de gösterilen örnekte *Changed Attributes* kısmında değiştirilen değerler görünmektedir. Bu kısımdan hesabın parolasının değiştirildiği anlaşılmaktadır.

Jan 09 20:11:58 hostname01.deneme.com AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.0.41 Source=Microsoft-Windows-Security-Auditing Computer=hostname01.deneme.com OriginatingComputer=10.10.10.10 User= Domain= EventID=4738 EventIDCode=4738 EventType=8 EventCategory=13824 RecordNumber=563497 TimeGenerated=1641752236 TimeWritten=1641752236 Level=Log Always Keywords=Audit Success Task=SE_ADT_ACCOUNTMANAGEMENT_USERACCOUNT Opcode=Info Message=A user account was changed. Subject: Security ID: NT AUTHORITY\SYSTEM Account Name: hostname01$ Account Domain: DENEME Logon ID: 0x3E7 Target Account: Security ID: S-1-5-21-1764262681-222222111212-1111111111-500 Account Name: Cagri Fanuscu Account Domain: hostname01 Changed Attributes: SAM Account Name: Cagri Fanuscu Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: 9.01.2022 20:17:16 Account Expires: <never> Primary Group ID: 513 AllowedToDelegateTo: - Old UAC Value: 0x210 New UAC Value: 0x210 User Account Control: - User Parameters: - SID History: - Logon Hours: All Additional Information: Privileges: -

Şekil 2.3 Olay ID 4738

Olay ID 4688: İşletim sistemi üzerinde yeni bir işlem (process) oluştuğunda üretilen iz kaydıdır. Şekil 2.4'de verilen örnekte "user01" tarafından oluşturulan işlemin bilgileri görünmektedir.

Jan 09 20:28:37 hostname01.deneme.com AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.0.41 Source=Microsoft-Windows-Security-Auditing Computer=hostname01.deneme.com OriginatingComputer=10.10.10.10 User= Domain= EventID=4688 EventIDCode=4688 EventType=8 EventCategory=13312 RecordNumber=143924768 TimeGenerated=1641749227 TimeWritten=1641749227 Level=Log Always Keywords=Audit Success Task=SE_ADT_DETAILEDTRACKING_PROCESSCREATION Opcode=Info Message=A new process has been created. Creator Subject: Security ID: deneme\user01 Account Name: user01 Account Domain: deneme Logon ID: 0x1AFBF1 Target Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Process Information: New Process ID: 0x3c58 New Process Name: C:\Windows\System32\conhost.exe Token Elevation Type: %%1936 Mandatory Label: Mandatory Label\Medium Mandatory Level Creator Process ID: 0xf9ec Creator Process Name: C:\Windows\System32\cmd.exe Process Command Line: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Şekil 2.4 Olay ID 4688

Olay ID 1100: Olayların kayıt edilmesini sağlayan servisin kapanması durumunda oluşan olay ID'sidir. Şekil 2.5'da gösterilen örnekte olayın hangi makine üzerinde hangi tarih ve saatte olduğu yer almaktadır.

Jan 09 20:10:05 hostname01.deneme.com AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.0.41 Source=Microsoft-Windows-Eventlog Computer=hostname01.deneme.com OriginatingComputer=10.10.10.10 User= Domain= EventID=1100 EventIDCode=1100 EventType=4 EventCategory=103 RecordNumber=319384 TimeGenerated=1641305176 TimeWritten=1641305176 Level=Informational Keywords=AuditSuccess Task=el:Shutdown Opcode=Info Message=The event logging service has shut down.

Şekil 2.5 Olay ID 1100

Olay ID 4724: Bir hesabın başka bir hesabın parolasını resetlemeye çalışması durumunda bu olay kaydı oluşmaktadır. Şekil 2.6'de verilen örnekte *Cagri Fanuscu* isimli hesabın parolasının değiştirilmeye teşebbüs edildiği görülmektedir.

Jan 09 20:11:58 hostname01.deneme.com AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.0.41 Source=Microsoft-Windows-Security-Auditing Computer=hostname01.deneme.com OriginatingComputer=10.10.10.10 User= Domain= EventID=4724 EventIDCode=4724 EventType=8 EventCategory=13824 RecordNumber=563498 TimeGenerated=1641752236 TimeWritten=1641752236 Level=Log Always Keywords=Audit Success Task=SE_ADT_ACCOUNTMANAGEMENT_USERACCOUNT Opcode=Info Message=An attempt was made to reset an account's password. Subject: Security ID: NT AUTHORITY\SYSTEM Account Name: hostname01$ Account Domain: deneme Logon ID: 0x3E7 Target Account: Security ID: S-1-5-21-1111111111-1212121212-1212121212-500 Account Name: Cagri Fanuscu Account Domain: hostname01

Şekil 2.6 Olay ID 4724

2.3.2. IIS (Internet Information Services) web sunucu iz kayıtları

IIS, Microsoft tarafından Windows işletim sistemleri üzerinde çalışması amacıyla tasarlanmış bir web sunucusudur. IIS sunucusu web uygulamaları veya internet siteleri barındırılabilir. TLS (Transport Layer Security) sertifika yöneticisi sayesinde https ve sftp özellikleri de kullanabilir [29].

IIS Web Sunucusu üzerinde oluşan HTTP bağlantı iz kayıtları varsayılan olarak *%SystemDrive%\inetpub\logs\LogFiles* dizini altına yazılmaktadır.

IIS Web sunucusu iz kayıtları IIS Log File, W3C Extended Log File, ODBC Logging ve NCSA Common Log File gibi farklı formatlarda kayıt altına alınabilir. Bu çalışmada W3C Extended Log File formatına göre kayıt altına alınan iz kayıtları incelenecektir. W3C Extended Log File formatı farklı değerlerde özelleştirilebilen bir ASCII biçimidir. İstenmeyen özellik alanlarını atlanarak iz kayıt boyutunu sınırlarken sistem yöneticisi için

önemli olan özellikleri kaydetmenize olanak sağlar. İz kayıt içerisindeki özellik alanları boşluklarla birbirinden ayrılır ve saat UTC formatında kaydedilir. Şekil 2.7'de farklı http kodlarına göre seçilmiş örnek iz kayıtları bulunmaktadır.

HTTP Kod 200
Jan 11 21:21:47 WebSrv01 AgentDevice=MSIIS AgentLogFile=W3SVC261\u_ex220111_x.log PluginVersion=7.3.0.41 AgentLogFormat=W3C AgentLogProtocol=W3C date=2022-01-11 time=18:21:37s-ip=10.10.10.10 cs-method=GET cs-uri-stem=/duyurular cs-uri-query=- s-port=80 cs-username=- c-ip=10.10.10.20 cs(User-Agent)=Mozilla/5.0+(Linux;+Android+10;+M2003J15SC)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/96.0.4664.104+Mobile+Safari/537.36 cs(Referer)=https://testwebserver.deneme.com/ sc-status=200 sc-substatus=0 sc-win32-status=0 time-taken=2810 XFF-Header=10.10.10.30
HTTP Kod 404
Jan 11 21:21:47 WebSrv01 AgentDevice=MSIIS AgentLogFile=W3SVC70\u_ex220111_x.log PluginVersion=7.3.0.41 AgentLogFormat=W3C AgentLogProtocol=W3C date=2022-01-11 time=18:21:23s-ip=10.10.10.10 cs-method=GET cs-uri-stem=/Font/MyriadPro-Regular.woff2 cs-uri-query=- s-port=80 cs-username=- c-ip=10.10.10.20 cs(User-Agent)=Mozilla/5.0+(Linux;+Android+6.0.1;+Nexus+5X+Build/MMB29P)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/97.0.4692.71+Mobile+Safari/537.36+(compatible;+Googlebot/2.1;++http://www.google.com/bot.html) cs(Referer)=- sc-status=404 sc-substatus=0 sc-win32-status=2 time-taken=10 XFF-Header=10.10.10.30
HTTP Kod 302
Jan 11 21:21:47 WebSrv01 AgentDevice=MSIIS AgentLogFile=W3SVC292\u_ex220111_x.log PluginVersion=7.3.0.41 AgentLogFormat=W3C AgentLogProtocol=W3C date=2022-01-11 time=18:21:35s-ip=10.10.10.10 cs-method=GET cs-uri-stem=/eft-para-yatirma cs-uri-query=- s-port=80 cs-username=- c-ip=10.201.60.5 cs(User Agent)=Mozilla/5.0+(Linux;+Android+8.1.0;+SM J710FQ)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/97.0.4692.70+Mobile+Safari/537.36 cs(Referer)= https://testwebserver.deneme.com/eft-havale-para-yatirma sc-status=302 sc-substatus=0 sc-win32-status=0 time-taken=24 XFF-Header=10.10.10.30

Şekil 2.7 IIS Web Sunucu Örnek İz Kayıtları

Yukarıda gösterilen her üç örnekteki alanların açıklamaları Tablo 2.4'da verilmiştir. Bu alanlarda "s-" ile başlayanlar sunucu aksiyonları, "c-" ile başlayanlar istemci aksiyonları, "cs-" ile başlayanlar istemciden sunucuya doğru olan aksiyonlar ve "sc-" ile başlayanlar ise sunucudan istemciye doğru olan aksiyonları belirtir [30].

Tablo 2.4 W3C Extended Log File format Parametreleri

Parametre	**Açıklama**
date	Olayın gerçekleşme tarihi
time	Olayın gerçekleşme saati
c-ip	IIS sunucuya erişen istemcinin ip adresi(Şekil 2.7'da gösterilen örneklerde yük dengeleyici arkasında birden fazla IIS sunucusunun olduğu senaryo görülmektedir. Bu durumda c-ip yük dengeleyicinin ip adresini ifade eder.)
cs-username	Sunucuya erişen kimliği doğrulanmış kullanıcının adı
s-ip	IIS web sunucusunun ip adresi
s-port	İstemcinin bağlandığı port numarası
cs-method	İstemcinin gerçekleştirmeye çalıştığı http metodunu gösterir. Örneğin GET, POST veya PUT vb.
cs-uri-stem	İstemcinin erişmeye çalıştığı asıl URL bilgisi
cs-User-Agent	İstemcinin kullandığı tarayıcı bilgisi gösterir
sc-status	İşlemin http cevap kodunu gösterir.Örneğin http-200 veya http-404 vb.
cs(Referer)	İstemcinin ziyaret ettiği bir önceki web sayfasının bilgisini içerir
XFF-Header	Yük dengeleyici kullanıldığını durumda istemcinin gerçek ip adresini gösterir.
cs-uri-query	Eğer kullanıldıysa istemcinin yaptığı sorgu bilgisini gösterir

2.3.3. Linux denetim iz kayıtları

Linux açık kaynak kodlu geliştirilmiş bir işletim sistemidir. Linux işletim sistemi, uygulamaların CPU, RAM ve depolama birimi gibi donanım parçalarının doğrudan yönetmeyi sağlar. Yazılım ve donanım arasında bir köprü kurarak haberleşmeyi ve istenen işi yerine getirmeye olanak tanır. Linux, Unix'e benzer şekilde dizayn edilmiştir ancak farklı olarak akıllı telefonlardan arabalara kadar çok farklı alanlarda kendine kullanım alanı bulmuştur. Linux, birbirinden farklı ihtiyaçları ve zevkleri olan kullanıcılar için farklı varyasyonlara ayrılmıştır. Bu duruma dağıtım adı verilir. Örneğin Debian, ubuntu ve Fedora bu dağıtımlardan bazılarıdır. Bu çalışmada Centos isimli dağıtım ve bu dağıtım üzerine geliştirilen Redhat işletim sistemi üzerine çalışmalar yapılacaktır [31].

Redhat işletim sisteminde denetim iz kayıtları */var/log/audit/* dizini altında *audit.log* isimli dosyanın içerisinde bulunmaktadır. Bu kayıtlardan özetle aşağıdaki veriler elde edilebilir.

- Bir olayın tarihi ve saati, türü ve sonucu,
- Yaşanan olayın kritiklik seviyesi,
- Olayın, olayı tetikleyen kişi ile ilişkilendirilmesi,
- Denetim yapılandırmasındaki tüm değişiklikler ve denetim iz kayıt dosyalarına erişme girişimleri,
- SSH ve kerberos gibi kimlik doğrulama mekanizmalarının tüm kullanım bilgileri,
- Kritik veri tabanlarında yapılan değişiklik kayıtları (örneğin /etc/passwd)
- İşletim sisteminden ve işletim sistemine veri alış verişi işlemleri [32].

Audit.log dosyası içerisinde oluşan örnek iz kayıtları Şekil 2.8'de verilmiştir. Bu kayıtlar üzerinden elde edilebilecek bilgiler Tablo 2.5'de açıklamaları ile birlikte verilmiştir.

SYSCALL Kayıt Tipi
"type=SYSCALL msg=audit(1364481363.243:24287): arch=c000003e syscall=2 success=no exit=-13 a0=7fffd19c5592 a1=0 a2=7fffd19c4b50 a3=a items=1 ppid=2686 pid=3538 auid=500 uid=500 gid=500 euid=500 suid=500 fsuid=500 egid=500 sgid=500 fsgid=500 tty=pts0 ses=1 comm="cat" exe="/bin/cat" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="sshd_config"
CWD Kayıt Tipi
type=CWD msg=audit(1364481363.243:24287): cwd="/home/shadowman"
PATH Kayıt Tipi
type=PATH msg=audit(1364481363.243:24287): item=0 name="/etc/ssh/sshd_config" inode=409248 dev=fd:00 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0
DAEMON_START Kayıt Tipi
type=DAEMON_START msg=audit(1363713609.192:5426): auditd start, ver=2.2 format=raw kernel=2.6.32-358.2.1.el6.x86_64 auid=500 pid=4979 subj=unconfined_u:system_r:auditd_t:s0 res=success
USER_AUTH Kayıt Tipi
type=USER_AUTH msg=audit(1364475353.159:24270): user pid=3280 uid=500 auid=500 ses=1 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res=failed'

Şekil 2.8 Linux OS Örnek Denetim İz Kayıtları

Tablo 2.5 Syslog Denetim Kayıtlarındaki Parametreler

Parametre	**Açıklaması**
type	İz kaydının tipini belirtir. Örneğin "SYSCALL" tipi çekirdeğe yapılan sistem çağrılarını ifade eder.
msg	Zaman damgası ve benzersiz bir ID değerinden oluşan alandır. Eğer aynı olay ile ilgili oluşmuş kayıtlar varsa aynı zaman damgası ve ID değerini paylaşabilirler. Örnek: msg=audit(1364481363.243:24287)
success	Yapılan sistem çağrısının başarılı olup olmadığı hakkında bilgi verir. Örnek: success=yes

exit	Sistem çağrısına karşılık gelen cevap kodunu ifade eder. Bu kodun okunabilir şeklinin görüntülenmesi için işletim sistemi üzerinde "ausearch --interpret --exit –[kod değeri]" komutu çalıştırılır.
acct	Kullanıcının hesap ismini gösterir. Örnek: acct="root"
addr	Ipv4 veya Ipv6 olarak kayıt adresi bulunur. Kaynak sunucu adına karşılık gelen ip adresi değeridir.
auid	Oturum açıldığında kullanıcıya atanan ID değeridir. Bu değer oturum süresi boyunca değişmez. Örneğin kullanıcı "su - username" komutu ile başka bir kullanıcı hesabına geçiş yapsa bile bu id değeri sabit kalır.
uid	İşlemi başlatan kullanıcıya karşılık gelen ID değerini ifade eder.
gid	İşlemi başlatan kullanıcı grubuna karşılık gelen ID değerini ifade eder.
comm	İşlem sırasında kullanılan komutun adını verir. Örnek: comm="cat"
exe	İşlemi gerçekleştiren komutun dizin değerini gösterir. Örnek: exe="/bin/cat"
name	Sistem çağrısında iletilen dosya veya klasörün tam dizin yolunu gösterir.
hostname	Bilgisayar/sunucu adını gösterir.
key	İşlemin gerçekleştirildiği hedef dosya veya obje adıdır.

2.3.4. Aix (Advanced Interactive Executive) denetim iz kayıtları

AIX, IBM firması tarafından geliştirilmiş UNIX tabanlı bir işletim sistemidir. Kurumsal müşterilere hizmet verir ve UNIX tabanlı sunucu sistemleri pazarının yaklaşık %58'ine sahiptir. Diğer işletim sistemlerinden öne çıkan özellikleri güvenli ve stabil bir çalışma sergilemesidir [33].

AIX işletim sisteminin denetim kayıtları sunucu işletim sistemi içerisinde */etc/security/audit/events* dizini altında bulunmaktadır. CLI (Command Line Interface) üzerinde yapılan basit bir komut bir çok farklı denetim izi oluşturur. Örnek olarak CLI üzerinde *cat* veya *more* komutları çalıştırıldığında aşağıdaki kayıtların oluştuğu görülebilir [34].

- FILE_Open (Dosya açıldı)
- FILE_Read (Dosya okundu)
- FILE_Write (Dosya standart çıktıya yazıldı)

- PROC_Create (Cat veya more komutu için işlem oluşturuldu)
- PROC_Execute (Komut çalıştırıldı)
- PROC_Delete (Süreç tamamlandı)

Mümkün olan tüm denetim iz kayıtlarının kayıt altına alınması yüksek boyutlarda disk ihtiyacını meydana getirir. Bu durumdan kaçınmak için konfigürasyon dosyalarında yapılacak değişiklikler ile ihtiyaç duyulan iz kayıtları seçilebilir. Denetim iz kayıtları sınıflara ayrılmıştır. Hangi olay kaydının hangi sınıf içinde olacağı belirlenebilir. Sınıf adları isteğe bağlı olsa da, denetim alt sistemi etkinken bireysel olay adları yerine kullanıcı kimlikleriyle ilişkilendirilirler [34].

AIX işletim sisteminde iki farklı veri toplama yöntemi mevcuttur. Eğer büyük miktarlarda veri uzun süreli olarak saklanmak istenirse bu durumda *Bin Collection* adı verilen metot kullanılmalıdır. Eğer veri oluştuğu anda işlenecek ise *Stream Collection* adı verilen metot kullanılmalıdır. Bu iki metot bir arada da kullanılabilmektedir [34].

Aşağıda AIX işletim sistemi denetim kayıtlarından bazı örnekler ve açıklamaları paylaşılmaktadır.

PROC_Delete: Çağrılan işlemin sona erdiğini ifade eder.

PROC_Delete awk mustafa root OK 14 Nov 2021 21:00:06.091179 No associated roles exited child process 19334524, rc: 0, filename: awk

PROC_Create: Yeni bir işlemin oluşturulduğunu ifade eder.

PROC_Create ksh mustafa root OK 14 Nov 2021 21:00:06.085346 No associated roles forked child process 21759164

PROC_Execute**:** CLI üzerinde çalıştırılan komutu gösterir.

PROC_Execute netstat mustafa root OK 14 Nov 2021 21:00:06.028641 No associated roles euid: 0 egid: 0 epriv: ffffffff:ffffffff name netstat -ni

S_PASSWD_READ: Passwd dosyasının okunduğunu ifade eder.

S_PASSWD_READ sudo mustafa mustafa OK 14 Nov 2021 20:59:58.375971 No associated roles audit object read event detected /etc/security/passwd

USER_Login: İşletim sisteminde kullanıcının oturum açtığını gösterir.

USER_Login sshd root root OK 14 Nov 2021 20:01:05.559994 No associated roles user: mustafa tty: ssh

FILE_Rename: Dosyanın adının değiştirildiğini ifade eder.

FILE_Rename extract mustafa oracle OK 14 Nov 2021 00:00:00.858851 oracle_devmgmt frompath: /backup/silvergate/dirrpt/abcS10.rpt topath: / /backup/silvergate/dirrpt/abcBS11.rpt

FS_Chdir: Çalışılan mevcut klasörün değiştirildiği gösterir.

FS_Chdir sshd mustafa mustafa OK 14 Nov 2021 20:59:58.059999 No associated roles change current directory to: /home/mustafa

2.3.5. Apache HTTP sunucu iz kayıtları

Apache http sunucu projesi, The Apache Software Foundation tarafından UNIX ve Windows gibi işletim sistemlerine açık kaynak kodlu http sunucu geliştirilmesi ve desteğinin verilmesini için kurulmuştur. Bu projenin amacı güncel http standartlarına uygun, güvenli, verimli ve esnek http servisleri geliştirmektir. Apache, 1996'dan günümüze kadar en popüler http sunucusu olmuştur [35].

Apache sunucusunun kendi üzerinde hataların takibi veya yapılan işlemlerin incelenebilmesi için gelişmiş bir günlükleme özelliği vardır. Bunlardan bir tanesi hata kayıtlarının işlendiği *Error Log*'dur. Bu kayıtlar UNIX işletim sistemlerinde varsayılan olarak */var/log/httpd/error_log* dizini altındaki dosyalarda tutulurlar. Hata iz kayıtlarının hangi düzende tutulacağı format ayarlaması ile belirlenir. Formatı belirlerken kullanılan parametreler ve bunların anlamları Tablo 2.6'de verilmiştir [36].

Tablo 2.6 Hata İz Kayıtları Format Parametre Tablosu

Parametre	Anlamı
%%	Yüzde imi
%a	İstekte bulunan IP adresi ve port numarası
%a	Bağlantının emsal IP adresi and portu
%A	Yerel IP adresi ve portu
%e	İstek ortam değişkeni isim
%E	PR/OS hata durum kodu ve iletisi
%F	Günlük çağrısının kaynak dosya ismi ve satır numarası
%i	İstek başlığı isim
%k	Bağlantıdaki keep-alive isteklerinin sayısı
%l	İletinin günlük seviyesi
%L	İsteğin günlük kimliği
%m	İletiyi günlükleyen modülün ismi
%M	Asıl günlük iletisi
%P	Geçerli sürecin süreç kimliği (PID)
%T	Geçerli evrenin evre kimliği
%t	Geçerli zaman
%v	Geçerli sunucu adı

Tabloda verilen değerlere istenen sırada ve istenen verilere göre konfigürasyon dosyasına yazılan örnek bir format aşağıdaki gibidir.

```
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\
referer\ %{Referer}i"
```

Bu formata göre oluşan örnek hata iz kaydı aşağıdaki gibidir.

```
[Thu May 12 08:28:57.652118 2011] [core:error] [pid 8777:tid 4326490112] [client
::1:58619] File does not exist: /usr/local/apache2/htdocs/favicon.ico
```

Apache'de bir diğer önemli iz kayıt türü *Access* (erişim) kayıtlarıdır. Erişim kayıtları web sunucusuna gelen istekler hakkında bilgiler içerir. Bunlar isteğin durum kodu, istekte bulunan web sayfasının adı, sunucunun tepki süresi, istekte bulunan IP adresi gibi bilgiler içerebilir. Error iz kayıtlarında olduğu gibi access iz kayıtları da belirlenen format biçiminde oluşur. Bu format için kullanılabilecek parametre değerleri Tablo 2.7'de verilmiştir [37].

Tablo 2.7 Erişim İz Kayıtları Format Parametre Tablosu

Parametre	**Anlamı**
%a	Uzak IP adresi ve isteğin portu
%A	Yerel IP adresi
%B	Yanıtın byte cinsinden uzunluğu (HTTP başlıkları hariç)
%D	İsteği sunmak için harcanan zaman (Mikrosaniye)
%f	Dosya ismi
%h	Sunucu ismi veya ip adresi
%H	İsteğin protokol bilgisi
%k	Bu bağlantıda işlenen isteklerin sayısı
%l	Uzak kullanıcı kimliği
%m	İstek yöntemi
%p	Sunucunun isteği sunduğu port bilgisi
%t	[18/Sep/2011:19:18:28 -0400] biçiminde isteğin alındığı tarih ve saat. Sondaki sayı zaman diliminin GMT'ye uzaklığıdır
%T	İsteği sunmak için harcanan zamanın saniye cinsinden karşılığı
%u	Uzak kullanıcı kimliği
%U	Herhangi bir sorgu dizgesi içermeksizin istenen URL yolu
%v	İsteği sunan sunucu adı
%I	Request ve header dahil olmak üzere alınan verinin byte cinsinden değeri
%O	Header dahil olmak üzere gönderilen verinin byte cinsinden değeri
%S	Request ve header dahil olmak üzere gönderilen ve alınan verinin byte cinsinden değeri
\"%r\"	İstek yapılırken kullanılan metod, istek yapılan url
%X	Yanıt tamamlandığında bağlantı durumu:

	X :Yanıt tamamlanmadan önce bağlantı koptu. + :Yanıt gönderiminden sonra bağlantı canlı kalabilir. - :Yanıt gönderiminden sonra bağlantı kapatılacak.
%>s	Yapılan http isteğinin durum kodu

Aşağıda örnek olarak oluşturulan bir format konfigürasyonu ve bu konfigürasyona göre oluşan örnek iz kayıtları görünmektedir.

Format Örneği:

```
%h %t %v \"%r\" %>s %b %D %X %{env}e %{X-Forwarded-For}i %{SESSIONID}C
```

HTTP-200 Örneği: Bu durum kodu istemci tarafından yapılan isteğin başarılı bir şekilde sunucuya iletildiğini, işlendiğini ve kabul edildiğini ifade eder. Aşağıdaki örnekte görülen POST ifadesi bir HTTP istek metodudur. POST metodu, belirtilen kaynağa bir girdi iletir ve genellikle durum değişkenlerinde veya sunucuda değişikliklere neden olur. Daha özet şekilde sunucuya veri gönderirken kullanılan metottur. Örnek olarak bir web sayfasında bulunan form alanını doldurup gönderdiğinizde bu bilgi bir POST metodu ile gönderilir [37].

```
“10.10.10.10 [20/Jan/2022:20:04:51 +0300] deneme.test.com.tr "POST
/main/jsp/esatis/getTekliflerim_brd.ajx HTTP/1.1" 200 35 9733 + deneme.test:9123
10.10.10.20 0000tD19s474fa7”
```

HTTP-302 Örneği: HTTP-302 yönlendirme durum kodudur. Erişim isteği gönderilen kaynağın geçici olarak başlıkta belirtilen lokasyona taşındığını ifade eder. Kullanılan tarayıcı İstemciyi bu sayfaya yönlendirir ancak arama motorları mevcut link bilgisini kısa süreli taşınan link bilgisi ile değiştirmez [37].

```
10.10.10.10 [20/Jan/2022:18:24:14 +0300] deneme.test.com.tr "POST
/BilgiBankasiIstemciWeb/pf/sorgula.xhtml HTTP/1.1" 302 - 2926 + hostname01:9157
10.10.10.20 0000H1eaumqvq5
```

HTTP-404 Örneği:

```
10.10.10.10 - - [20/Jan/2022:20:04:24 +0300] deneme.test.com.tr "GET /esatis/index.jsp
HTTP/1.1" 404 2278 1341 + hostname01:9149 10.10.10.10
0000zdKTosxW0g7CYVum1ot0z_v:1eaujecpl
```

2.3.6. Güvenlik duvarı iz kayıtları

Güvenlik duvarı, bulunduğu ağa giren ve çıkan veri trafiğini analiz ederek üzerinde bulunan kural setine göre hangi trafiğin üzerinden geçip geçmeyeceğine karar veren, yazılım veya donanım tabanlı sistemdir. Yaklaşık 25 yıldan bu yana ağ güvenliğinin en dış katmanını oluşturur ve ilk savunma hattıdır. Yıllar boyunca yeni özellikler eklenerek güvenlik duvarı sistemlerinin kabiliyetleri arttırılarak farklı özelliklerde güvenlik duvarı tipleri ortaya çıkmıştır. Güvenlik duvarı çeşitleri aşağıda incelenmiştir [38].

Proxy Güvenlik Duvarı: Ağ trafiğini uygulama katmanında filtreleyen bir güvenlik duvarı çeşididir. Geleneksel güvenlik duvarlarının aksine, iki uç sistemin arasında bulunan vekil sunucu bir aracı görevindedir. İstemcinin güvenlik duvarına gönderdiği istek, bu sistem üzerinde bir takım güvenlik kurallarına göre değerlendirilir. Değerlendirme sonucuna göre bloklanır veya izin verilir. Bu güvenlik duvarı tipinin önemli özelliklerinden birisi de vekil sunucunun güvenlik duvarlarının FTP ve HTTP gibi OSI'nin yedinci katmanında bulunan protokoller için trafiği izlemesi ve kötü amaçlı trafiği tespit etmek için derin paket denetleme özelliklerini kullanmasıdır [39].

Yeni Nesil Güvenlik Duvarları: Geçmişten bugüne kullanılan güvenlik duvarı teknolojisini ele alarak bu teknolojiyi antivirus, saldırı önleme sistemleri, şifreli trafik inceleme ve buna benzer pek çok ek özellikle birleştirir. Ayrıca "Derin Paket Denetleme (DPI)" özelliğine sahiptirler. Geleneksel güvenlik duvarları sadece paketin başlık bilgisi ile ilgilenirken, derin paket denetleme, paketin içeriğinde bulunan verileri denetler ve kullanıcıların kötücül veri içeren paketleri daha etkili bir şekilde tespit etmesini, kategorilere ayırmasını veya engellemesini sağlar [39].

Çok Katmanlı Durum İncelemeli Güvenlik Duvarı: Paketleri uygulama, ağ ve aktarım katmanlarında filtreleyerek güvenli olduğu önceden bilinen paketlerle karşılaştırır. Next Generation Firewall (NGFW)güvenlik duvarlarına benzer olarak SMLI güvenlik duvarları da paketin hem gövde hem de başlık kısmını denetler ve ancak her bir katmandan olumlu sonuç alındığında geçmesine izin verir. Bu güvenlik duvarları, başlatılan tüm oturumların

güvenilir kaynaklarla gerçekleştirildiğinden emin olmak üzere iletişimin durumunu saptamak amacıyla paketleri incelemeden geçirir [39].

Stateful Inspection Güvenlik Duvarı: Geleneksel güvenlik duvarı tipi olarak da bilinir. Trafiğin durumuna, port ve protokol bilgisine bakarak bloklar veya izin verir. Oturumun açılışından kapanana kadar oluşan tüm aktiviteyi izler. Filtreleme kararları, hem yönetici tanımlı kurallara hem de önceki bağlantılardan gelen bilgilerin ve aynı bağlantıya ait paketlerin kullanılmasına atıfta bulunan bağlama göre verilir [38].

Bu çalışmada iz kayıtları incelenecek olan güvenlik duvarı cihazı, Palo Alto firmasının PA-5250 model yeni nesil güvenlik duvarı cihazıdır.

İzin Verilen Trafik: İz kaydına konu olan trafik hiçbir güvenlik duvarı kuralına takılmaz ve makine öğrenme veya benzeri güvenlik önlemlerinden geçer ise oluşan iz kayıt tipidir. Bir örneği şekil 2.9'de verilmiştir. Bu iz kaydının içerisinde bulunan önemli alanlar ve anlamları Tablo 2.8'de verilmiştir.

<14>Feb 5 15:50:59 Panorama-1 LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|10.0.8-h8|allow|cat=TRAFFIC|

ReceiveTime=2022/02/05 15:50:59|SerialNumber=013101010824|Type=TRAFFIC|Subtype=end|devTime=$cef-formatted-receive_

time|src=192.168.150.10|dst=10.10.20.20|srcPostNAT=192.168.150.10|dstPostNAT=10.10.20.250|RuleName=web_sayfasına_erişim|usrName=|

SourceUser=|DestinationUser=|Application=web-browsing|VirtualSystem=vsys1|SourceZone=INTERNET|

DestinationZone=LAN|IngressInterface=ae3|EgressInterface=ae1|

LogForwardingProfile=Panorama|SessionID=3780358|RepeatCount=1|srcPort=49315|dstPort=443|

srcPostNATPort=49315|dstPostNATPort=443|Flags=0x140001c|proto=tcp|action=allow|

totalBytes=15656|dstBytes=10601|srcBytes=5055|totalPackets=34|StartTime=2022/02/05 15:50:36|

ElapsedTime=18|URLCategory= |sequence=7054213674134852735|ActionFlags=0x8000000000000000|

SourceLocation=Turkey|DestinationLocation=Turkey|dstPackets=21|srcPackets=13|

SessionEndReason=tcp-fin|DeviceGroupHierarchyL1=911|

DeviceGroupHierarchyL2=0|DeviceGroupHierarchyL3=0|

DeviceGroupHierarchyL4=0|vSrcName=vsys1|DeviceName=PA-5250-1|

ActionSource=from-policy|SrcUUID=|DstUUID=|TunnelID=0|

MonitorTag=|ParentSessionID=0|ParentStartTime=|

TunnelType=N/A

Şekil 2.9 Palo-Alto Güvenlik Duvarı Trafik Sonlandı İz Kayıt Tipi

Tablo 2.8 Palo-Alto Güvenlik Duvarı İz Kayıt İçeriğinde Bulunan Parametreler ve Açıklamaları

Parametre	**Açıklama**
ReceiveTime	Olayın tarih ve saati
Type	İz kaydının tipini ifade eder. Örneğin traffic, ağ trafiği ile ilgili olayları ifade eder. Threat, tespit edilen bir siber güvenlik tehdidi ile ilgili iz kaydıdır. System ise güvenlik duvarı uygulamasının sisteminin işleyişi ile ilgili oluşan iz kayıtlarına verilen isimdir.
src	Trafiği başlatan cihazın IP adresidir.
dst	Hedef IP adresidir.
srcPostNAT	Kaynak IP adresine NAT işlemi uygulanmış ise NAT IP adresidir. Bu işlem uygulanmamış ise kaynak IP adresi bu alanda da yazılıdır.
dstPostNAT	Hedef IP adresine NAT işlemi uygulanmış ise NAT IP adresidir. Bu işlem uygulanmamış ise hedef IP adresi bu alanda da yazılıdır.
RuleName	Engellenen veya izin verilen trafiğe hangi kurala göre işlem yapıldığı bilgisini verir.
Application	Layer-7 güvenlik duvarı cihazları uygulama katmanında çalışabildiği için gelen trafiğin hangi uygulamadan yapıldığı bilgisi bu alanda yazar. Örneğin:ssl, dns, ldap, kerberos, google-play, gmail-base vb.
SourceZone	Güvenlik duvarı üzerinde kural yazımı sırasında oluşturulan kaynak ağ zone adıdır. Zone tanımının amacı, kural yazılırken her seferinde tek tek ip adresi yazmak yerine ön tanımlı olarak bu IP'lerin belirlenmesi ve kullanım kolaylığı olmasıdır.
DestinationZone	Güvenlik duvarı üzerinde kural yazımı sırasında oluşturulan hedef ağ zone adıdır. Zone tanımının amacı, kural yazılırken her seferinde tek tek ip adresi yazmak yerine ön tanımlı olarak bu IP'lerin belirlenmesi ve kullanım kolaylığı olmasıdır.
srcPort	Kaynak port bilgisi
dstPort	Hedef port bilgisi
action	Güvenlik duvarının aldığı aksiyonu gösterir. Örneğin allow, drop, alert, reset-both vb.
totalBytes	Toplam paket boyutunun byte cinsinden değeridir.

usrName	Cihaz üzerinde veya domain entegrasyonu sayesinde belirlenen kullanıcı adı bilgisidir.

Engellenen Trafik: Güvenlik duvarına ulaşan trafik yazılan allow kurallarının hiçbirine değmiyor veya bu trafik için özel olarak deny kuralı yazılmış ise Şekil 2.10'da verilen örnekte gösterildiği gibi bir iz kaydı oluşur. Burada dikkat edileceği üzere *action* parametresi *drop* değerini almıştır. Bu trafiğin güvenlik duvarı üzerinden geçmediğini ve paketlerin düşürüldüğünü ifade eder.

<14>Feb 5 15:23:58 Panorama-1 LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|10.0.8-h8|drop|cat=TRAFFIC|

ReceiveTime=2022/02/05 15:23:58|SerialNumber=013101010824|Type=TRAFFIC|Subtype=drop|devTime=$cef-formatted-receive_

time|src=192.168.150.10|dst=192.168.140.10|srcPostNAT=0.0.0.0|dstPostNAT=0.0.0.0|RuleName=Son_Engel|usrName= |

SourceUser= |DestinationUser=|Application=not-applicable|VirtualSystem=vsys1|SourceZone=LAN|

DestinationZone=INTERNET|IngressInterface=ae1|EgressInterface=|

LogForwardingProfile=Panorama|SessionID=0|RepeatCount=1|srcPort=65239|dstPort=443|

srcPostNATPort=0|dstPostNATPort=0|Flags=0x0|proto=tcp|action=drop|

totalBytes=66|dstBytes=0|srcBytes=66|totalPackets=1|StartTime=2022/02/05 15:23:56|

ElapsedTime=0|URLCategory=any|sequence=7054213674131663087|ActionFlags=0x8000000000000000|

SourceLocation=10.0.0.0-10.255.255.255|DestinationLocation=United States|dstPackets=0|srcPackets=1|

SessionEndReason=policy-deny|DeviceGroupHierarchyL1=911|

DeviceGroupHierarchyL2=0|DeviceGroupHierarchyL3=0|

DeviceGroupHierarchyL4=0|vSrcName=vsys1|DeviceName=PA-5250-1|

ActionSource=from-policy|SrcUUID=|DstUUID=|TunnelID=0|

MonitorTag=|ParentSessionID=0|ParentStartTime=|

TunnelType=N/A

Şekil 2.10 Palo-Alto Güvenlik Duvarı Tarafından Engellenen Trafik Örneği

Zararlı Paket Tespiti: Yeni nesil güvenlik duvarı cihazları üzerinde farklı bir çok güvenlik özelliği bulunmaktadır. Örneğin güvenlik duvarı cihazı üzerinde bulunan imzalardan yola çıkarak gelen trafik içerisinde zararlı yazılım olup olmadığını tespit edebilir. Şekil 2.11'de Petya ransomware zararlısının tespitine istinaden oluşan iz kaydının örneği verilmiştir. Bu örnekte category değerinin THREAT olduğu görülmektedir. Örnekteki *Miscellaneous* parametresinin aldığı değerler incelendiğinde trafik içerisinde bulunan *625877-1644063699.exe* isimli dosyanın ransomware ailesinden Petya türevi bir zararlı yazılım olduğu anlaşılmaktadır.

<12>Feb 5 15:21:46 Panorama-1 LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|10.0.8-h8|Ransom/Win32.petya.g(153902535)|

ReceiveTime=2022/02/05 15:21:46|SerialNumber=013101010824|cat=THREAT|Subtype=virus|devTime=$cef-formatted-receive_

time|src=192.168.150.10|dst=10.10.20.20|srcPostNAT=0.0.0.0|dstPostNAT=0.0.0.0|RuleName=Malware|usrName=|

SourceUser=|DestinationUser=|Application=web-browsing|VirtualSystem=vsys1|SourceZone=INTERNET|

DestinationZone=LAN|IngressInterface=ae1|EgressInterface=ethernet1/20|

LogForwardingProfile=Panorama|SessionID=2368386|RepeatCount=1|srcPort=15805|dstPort=80|

srcPostNATPort=0|dstPostNATPort=0|Flags=0x2000|proto=tcp|action=reset-server|

Miscellaneous="625877-1644063699.exe"|ThreatID=Ransom/Win32.petya.g(153902535)|URLCategory=AllStar|sev=3|Severity=medium|

Direction=server-to-client|sequence=7054213669038043903|ActionFlags=0xa000000000000000|SourceLocation=10.0.0.0-10.255.255.255|

DestinationLocation=172.16.0.0-172.31.255.255|ContentType=|PCAP_ID=0|FileDigest=|

Cloud=|URLIndex=1|RequestMethod=|Subject=|

DeviceGroupHierarchyL1=911|DeviceGroupHierarchyL2=0|

DeviceGroupHierarchyL3=0|DeviceGroupHierarchyL4=0|

vSrcName=vsys1|DeviceName=PA-5250-1|SrcUUID=|DstUUID=|

TunnelID=0|MonitorTag=|ParentSessionID=0|

ParentStartTime=|TunnelType=N/A|ThreatCategory=pe|

ContentVer=Antivirus-3983-4494

Şekil 2.11 Zararlı Paket Tespiti Sonucu Oluşan İz Kaydı

Saldırı Tespiti: Yeni nesil güvenlik duvarı cihazları üzerlerinden geçen trafikte gönderilen istekleri analiz ederek saldırı paternlerine uyan trafikleri tespit ederek bunları engelleyebilirler. Şekil 2.12'de örnek bir saldırı girişiminin engellendiğine yönelik iz kaydı bulunmaktadır. Bu örneğin kategorisi THREAT'dir. 80 portundan yapılan bir web

trafiğinde saldırı tespit edilmiştir. *Miscellaneous* parametre değerleri incelendiğinde saldırı tipinin *HTTP SQL Injection Attempt* olarak belirlendiği görülmektedir.

<12>Feb 5 15:22:58 Panorama-1 LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|10.0.8-h8|HTTP SQL Injection Attempt(54608)|

ReceiveTime=2022/02/05 15:22:58|SerialNumber=013101010824|cat=THREAT|Subtype=vulnerability|devTime=$cef-formatted-receive_

time|src=192.168.150.10|dst=10.10.20.20|srcPostNAT=0.0.0.0|dstPostNAT=0.0.0.0|RuleName=web_erisim|usrName=|

SourceUser=|DestinationUser=|Application=web-browsing|VirtualSystem=vsys1|SourceZone=INTERNET|

DestinationZone=LAN|IngressInterface=ethernet1/20|EgressInterface=ae1|

LogForwardingProfile=Panorama|SessionID=33963839|RepeatCount=1|srcPort=41753|dstPort=80|

srcPostNATPort=0|dstPostNATPort=0|Flags=0x2000|proto=tcp|action=reset-both|

Miscellaneous=""|ThreatID=HTTP SQL Injection Attempt(54608)|URLCategory=AllStar|sev=3|Severity=medium|

Direction=client-to-server|sequence=7054213669038047942|ActionFlags=0xa000000000000000|SourceLocation=172.16.0.0-172.31.255.255|

DestinationLocation=10.0.0.0-10.255.255.255|ContentType=|PCAP_ID=0|FileDigest=|

Cloud=|URLIndex=1|RequestMethod=|Subject=|

DeviceGroupHierarchyL1=911|DeviceGroupHierarchyL2=0|

DeviceGroupHierarchyL3=0|DeviceGroupHierarchyL4=0|

vSrcName=vsys1|DeviceName=PA-5250-1|SrcUUID=|DstUUID=|

TunnelID=0|MonitorTag=|ParentSessionID=0|

ParentStartTime=|TunnelType=N/A|ThreatCategory=sql-injection|

ContentVer=AppThreat-8523-7225

Şekil 2.12 SQL Injection Saldırı Denemesine İlişkin iz Kayıt Örneği

2.3.7. IDS/IPS (Intrusion Detection System/ Intrusion Prevention System) iz kayıtları

IDS sistemleri iki çeşide ayrılırlar HIDS (Host Intrusion Detection System) ve NIDS (Network Intrusion Detection System). NIDS ağ trafiğini izleyerek saldırı tespiti yaparken NIDS bilgi işlem cihazları üzerinde konumlanır ve bu cihaz üzerinde saldırı tespiti yapmaya

odaklanır. Saldırı tespiti imza tabanlı veya anomali tabanlı olabilir. İmza tabanlı yöntemde bilinen ağ saldırılarının desenleri ağ üzerinden geçen trafik akışı ile karşılaştırılarak saldırı tespit edilir. Anomali tabanlı yöntemde ise davranış analizi ve buluşsal yaklaşımlar uygulanarak saldırı olabilecek durumlar tespit edilir. IPS sistemleri ise ağ trafiğini kendi üzerinden geçirerek IDS tarafından tespit edilen saldırıları engellemek için kullanılır. Bu sistemler ilk ortaya çıktıkları dönemlerde ayrı birer sistem iken günümüzde bu sistemler bütünleşik olarak ağ trafiğinde konumlanmaktadır [40].

Bu çalışmada McAfee firmasının IPS ürünü olan Network Security Platform iz kayıtları incelenecektir. İncelenen ürünün modeli NS9500'dür.

Farklı atak tiplerine ilişkin IPS sisteminde oluşan iz kayıtlarından örnekler şekil 2.13'da görülmektedir. Bu şekilde görülen iz kaydı TeamViewer uygulamasının kullanımının tespitine yöneliktir. Bu kayıt incelenecek olursa bilgisayarın *ping3.teamviewer.com* web sayfasına istekte bulunulduğu ve bu nedenle IPS sistemine takıldığı görülebilir. IPS sisteminin bu duruma karşı aldığı aksiyon *Inconclusive* olarak görülmektedir. Bunun anlamı trafiği engellemek için yeterli şüphenin olmadığı veya bu durumun bilinen saldırı tiplerinden hiçbiri ile eşleşmediğidir. İz kaydının sonunda yer alan *signature* ifadesi tespit yönetiminin imza tabanlı olduğunu ifade eder. Şekil 2.14'de yer alan saldırı tipi ağ üzerinde zararlı dosya transferinin tespit edildiğine yöneliktir. İz kaydı içerisindeki *Attack Blocked* ifadesi saldırının IPS tarafından engellendiğini ve son kısımdaki *signature* ifadesi imza tabanlı bir tespit olduğunu ifade eder. *HTTP URI* parametresinde geçen *378211-1644146656.exe* ifadesi zararlı yazılımının tespit edildiği çalıştırılabilir dosya adıdır. Şekil 2.15'de yer alan iz kaydında SQL Injection yöntemlerinden Blind SQL Injection tipinde bir saldırı girişiminin olduğu ve bu saldırının engellendiği ifade edilmektedir. Şekil 2.16'da CVE-2020-1566 koduyla bilinen bir zafiyeti sömürmeye yönelik saldırının tespit edildiği ve engellendiği görülmektedir.

TeamViewer Traffic Detected
<164>Feb 6 14:14:06 SyslogAlertForwarder: |7008815687028393828|Signature|2022-02-06 14:14:05 TRT|"P2P: TeamViewer Traffic Detected"|0x42c05f00|Medium|teamviewer_conn|Low|My Company|CLUSTER|Wan|192.168.150.10|56152|192.168.150.20|80|Inbound|restricted-application|Inconclusive HTTP Request Method == CONNECT ;;; HTTP URI == ping3.teamviewer.com:443;;; HTTP User-Agent == Mozilla/4.0 (compatible; MSIE 6.0; DynGate);;; HTTP Return Code == 407;;; HTTP Host == ping3.teamviewer.com:443;;; HTTP Response Content Type == text/html;;; signature

Şekil 2.13 TeamViewer Trafiğinin Tespiti

Malicious File Detected
<162>Feb 6 14:23:48 SyslogAlertForwarder: |7008815687028398045|Malware|2022-02-06 14:23:47 TRT|"MALWARE: Malicious File Detected by GTI"|0x4840c900|High|malware|Medium|My Company|CLUSTER|Internet|192.168.150.10|80|192.168.150.20|15572|Inbound|GTI-File-Reputation|Attack Blocked HTTP Request Method == GET ;;; HTTP URI == /378211-1644146656.exe;;; HTTP User-Agent == Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3;;; HTTP Return Code == 200;;; HTTP Host == 172.29.0.20;;; HTTP Response Content Type == application/octet-stream;;; signature

Şekil 2.14 Zararlı Dosya Tespiti

Blind SQL Injection – Timing Detected
<164>Feb 6 13:05:48 SyslogAlertForwarder: |70088156870283629 37|Signature|2022-02-06 13:05:47 TRT|"HTTP: Blind SQL Injection - Timing"|0x40272600|Medium|Sig5|Low|My Company|CLUSTER|Internet|192.168.150.10|41033|192.168.150.20|80|Inbound|privileged-access|Attack Blocked HTTP Request Method == POST ;;; HTTP URI == /page360133.htm;;; HTTP User-Agent == Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36;;; HTTP Host == 10.201.156.254:80;;; signature

Şekil 2.15 Blind SQL Injection Saldırı Tespiti

Windows Kernel Elevation of Privilege Vulnerability
<164>Feb 6 13:29:41 SyslogAlertForwarder: |70088156870283735 69|Signature|2022-02-06 13:29:39 TRT|"HTTP: Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1566)"|0x45282400|Medium|sig1|Medium|My Company|CLUSTER|Internet|192.168.150.10|80|192.168.150.20|15293|Inbound|code-execution|Attack Blocked HTTP Request Method == GET ;;; HTTP URI == /365560-1644143409.exe;;; HTTP User-Agent == Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3;;; HTTP Return Code == 200;;; HTTP Host == 172.29.0.20;;; HTTP Response Content Type == application/octet-stream;;; signature

Şekil 2.16 Windows Kernel Yetki Yükseltme Saldırısı Tespiti

2.3.8. Antivirüs iz kayıtları

Antivirüs yazılımlarının ilk kullanım amaçları bilgisayarlara bulaşan virüsleri tespit etmek, virüsü bilgisayardan silmek veya başka bilgisayarlara bulaşmasını engellemek iken günümüzde zararlı yazılımların çeşitliliğindeki ve kullanım tekniklerindeki artış nedeniyle birçok gelişmiş özelliği içerisinde barındırmaya başlamıştır. Bu sayede casus yazılımlar, kimlik bilgisi hırsızlığı, fidye yazılımları, istenmeyen e-postalar ve kripto para madenciliği gibi birçok farklı saldırı tipini engelleyecek kapasiteye ulaşmışlardır. İlk geliştirilen antivirus yazılımları imza tabanlı çalışırken modern yazılımlar davranış analizleri, sezgisel tespit gibi yöntemlerle ilk kez kullanılan ve henüz tanınmayan zararlı yazılımları da tespit edip silmeyi amaçlamaktadır [41].

Bu çalışmada iz kayıtları incelenecek olan ürün McAfee firmasının McAfee Endpoint Security yazılımıdır. Bu ürünün oluşturduğu iz kayıtlarından bazı örnekler aşağıdaki şekillerde gösterilmektedir. Bu iz kayıtları içerisindeki parametrelerin bazıları ve açıklamaları Tablo 2.9'de [42] gösterilmektedir.

Şekil 2.17'de verilen ilk olay kaydında *hostname01* isimli ve MAC adres değeri *30-e3-7a-df-c8-ed* olan bilgisayarın *C:\ProgramData\zararli\yazilim\Threats* dizininde *152704-1644007553.exe* isminde trojan tipinde bir zararlı yazılımın tespit edildiği sonrasında bu zararlı dosyanın silinerek tehdidin ortadan kaldırıldığı bilgisi yer almaktadır. Şekil 2.18'de bulunan olay kaydında aynı bilgilere sahip bilgisayarın üzerindeki ajanın güncelleme alamadığının bilgisi yer almaktadır. Şekil 2.19'da görünen olay kaydında ise zararlı yazılımın tespit edildiği ancak silinemediği için tehdidin ortadan kaldırılamadığının bilgisi yer almaktadır. Şekil 2.20'de görülen olayda zararlı yazılımın ilgili bilgisayarda tespit edildiği ancak silinirken hata aldığı sonraki denemede silindiği bilgisi yer almaktadır.

1 - Infected file deleted

AutoID: "2480924069" AutoGUID: "D7BF50C2-D776-48FF-9060-30878086C254" ServerID: "HANDLER01" ReceivedUTC: "2022-02-04 20:58:47.26" DetectedUTC: "2022-02-04 20:48:09.0" AgentGUID: "DB1C27CC-6322-11EC-2513-005056A10423" Analyzer: "ENDP_AM_1070" AnalyzerName: "McAfee Endpoint Security" AnalyzerVersion: "10.7.0.2522" AnalyzerHostName: "hostname01" AnalyzerIPV4: "10.10.10.10" AnalyzerIPV6: "XXXXXXXXXXXXX" AnalyzerMAC: " 30e37adfc8ed" AnalyzerDATVersion: "4699.0" AnalyzerEngineVersion: "6400.9594" AnalyzerDetectionMethod: "On-Access Scan" SourceHostName: " hostname01" SourceIPV4: "-123456789" SourceIPV6: " XXXXXXXXXXXXX" SourceMAC: "null" SourceUserName: "null" SourceProcessName: "C:\Program Files\zararli\yazilim\Agent.Service.exe" SourceURL: "null" TargetHostName: " hostname01" TargetIPV4: "10.10.10.10" TargetIPV6: " XXXXXXXXXXXXX" TargetMAC: "null" TargetUserName: "TEST\cagri" TargetPort: "null" TargetProtocol: "null" TargetProcessName: "null" TargetFileName: "C:\ProgramData\zararli\yazilim\Threats\152704-1644007553.exe" ThreatCategory: "av.detect" ThreatEventID: "1027" ThreatSeverity: "2" ThreatName: "Generic.dfu" ThreatType: "trojan" ThreatActionTaken: "IDS_ALERT_ACT_TAK_DEL" ThreatHandled: "true" TheTimestamp: "0000000320F76CF5" TenantID: "1"

Şekil 2.17 Zararlı Bulaşan Dosyanın Silinmesi

2 - Update Failed

AutoID: "2483179514" AutoGUID: "A187C0B6-9E7E-4B23-B31E-F0084E13D624" ServerID: "HANDLER01" ReceivedUTC: "2022-02-06 14:42:45.363" DetectedUTC: "2022-02-06 14:33:14.0" AgentGUID: "6143DDDE-DB0E-11EA-382D-000000000000" Analyzer: "ENDP_GS_1070" AnalyzerName: "McAfee Endpoint Security" AnalyzerVersion: "10.7.0.2174" AnalyzerHostName: " hostname01" AnalyzerIPV4: "10.10.10.10" AnalyzerIPV6: " XXXXXXXXXXXXX " AnalyzerMAC: "30e37adfc8ed" AnalyzerDATVersion: "" AnalyzerEngineVersion: "" AnalyzerDetectionMethod: "" SourceHostName: "null" SourceIPV4: "10.10.10.10" SourceIPV6: " XXXXXXXXXXXXX " SourceMAC: "null" SourceUserName: "null" SourceProcessName: "null" SourceURL: "null" TargetHostName: "null" TargetIPV4: "10.10.10.10" TargetIPV6: " XXXXXXXXXXXXX " TargetMAC: "null" TargetUserName: "null" TargetPort: "null" TargetProtocol: "null" TargetProcessName: "null" TargetFileName: "null" ThreatCategory: "ops.update.end" ThreatEventID: "1119" ThreatSeverity: "5" ThreatName: "_" ThreatType: "" ThreatActionTaken: "none" ThreatHandled: "true" TheTimestamp: "0000000321413C9B" TenantID: "1"

Şekil 2.18 Güncelleme Hatası

3 - file infected. Undetermined clean error, delete failed

AutoID: "2482974829" AutoGUID: "B47A35B4-1AD7-400B-9A86-9EEADD64CD35" ServerID: "HANDLER02" ReceivedUTC: "2022-02-06 09:51:58.573" DetectedUTC: "2022-02-04 13:04:51.0" AgentGUID: "81D17C40-F018-11EA-2695-000000000000" Analyzer: "ENDP_AM_1070" AnalyzerName: "McAfee Endpoint Security" AnalyzerVersion: "10.7.0.2298" AnalyzerHostName: " hostname01" AnalyzerIPV4: "10.10.10.10" AnalyzerIPV6: " XXXXXXXXXXXXX" AnalyzerMAC: "30e37adfc8ed" AnalyzerDATVersion: "4699.0" AnalyzerEngineVersion: "6400.9594" AnalyzerDetectionMethod: "On-Access Scan" SourceHostName: " hostname01" SourceIPV4: "10.10.10.10" SourceIPV6: "XXXXXXXXXXXXX" SourceMAC: "null" SourceUserName: "null" SourceProcessName: "C:\Windows\System32\wscript.exe" SourceURL: "null" TargetHostName: " hostname01" TargetIPV4: "10.10.10.10" TargetIPV6: "XXXXXXXXXXXXX" TargetMAC: "null" TargetUserName: "TEST\cagri" TargetPort: "null" TargetProtocol: "null" TargetProcessName: "null" TargetFileName: "G:\ .lnk" ThreatCategory: "av.detect" ThreatEventID: "1284" ThreatSeverity: "1" ThreatName: "LNK/Autorun.worm.aajr" ThreatType: "trojan" ThreatActionTaken: "IDS_ALERT_ACT_TAK_DEN" ThreatHandled: "false" TheTimestamp: "000000032137E38F" TenantID: "1"

Şekil 2.19 Zararlı Olarak Tespit Edilen Dosyanın Silinememesi

4 - file infected. Undetermined clean error, deleted successfully
AutoID: "2480924075" AutoGUID: "5A772EFF-57F8-41ED-9907-4071A32F4F1B" ServerID: "HANDLER01" ReceivedUTC: "2022-02-04 20:58:47.283" DetectedUTC: "2022-02-04 20:48:23.0" AgentGUID: "DB1C27CC-6322-11EC-2513-005056A10423" Analyzer: "ENDP_AM_1070" AnalyzerName: "McAfee Endpoint Security" AnalyzerVersion: "10.7.0.2522" AnalyzerHostName: " hostname01" AnalyzerIPV4: "10.10.10.10" AnalyzerIPV6: " XXXXXXXXXXXXX" AnalyzerMAC: "30e37adfc8ed" AnalyzerDATVersion: "4699.0" AnalyzerEngineVersion: "6400.9594" AnalyzerDetectionMethod: "On-Access Scan" SourceHostName: " hostname01" SourceIPV4: "10.10.10.10" SourceIPV6: " XXXXXXXXXXXXX " SourceMAC: "null" SourceUserName: "null" SourceProcessName: "C:\Program Files\zararli\yazilim\Agent.Service.exe" SourceURL: "null" TargetHostName: " hostname01" TargetIPV4: "10.10.10.10" TargetIPV6: " XXXXXXXXXXXXX " TargetMAC: "null" TargetUserName: "TEST\cagri" TargetPort: "null" TargetProtocol: "null" TargetProcessName: "null" TargetFileName: "C:\ProgramData\zararli\yazilim\Threats\153020-18525\ppt\embeddings\oleObject1.bin\office.gif" ThreatCategory: "av.detect" ThreatEventID: "1280" ThreatSeverity: "2" ThreatName: "Artemis!3A620A95026B" ThreatType: "trojan" ThreatActionTaken: "IDS_ALERT_ACT_TAK_DEL" ThreatHandled: "true" TheTimestamp: "0000000320F76CF6" TenantID: "1"

Şekil 2.20 Zararlı Olay Tespit Edilen Dosyanın Silinmesi

Tablo 2.9 McAfee Antivirus İz Kayıt Parametre ve Açıklamaları.

Parametre	**Açıklama**
ReceivedUTC	Ajan tarafından tespit edilen durumun merkezi sunucuya ulaşma tarih ve saatidir.
DetectedUTC	Yaşanan olayın tespit edilme tarih ve saatidir.
AgentGUID	Sistem üzerinde kurulan her antivirus ajanına benzersiz olarak verilen ID değeridir.
AnalyzerVersion	Antivirus ajanı üzerinde çalışan analyzer versiyonudur.
AnalyzerHostName	Ajanı kurulu olduğu makinenin adıdır.
AnalyzerIPV4	Ajanın kurulu olduğu makinenin IPV4 adresidir.
AnalyzerIPV6	Ajanın kurulu olduğu makinenin IPV6 adresidir.

AnalyzerMAC	Ajanın kurulu olduğu makinenin MAC adresidir.
SourceProcessName	Tespit edilen tehdidin kaynak process adıdır.
SourceURL	Tehdidin kaynak URL adresidir.
TargetUserName	Tehdit hedefi kullanıcı adı veya e-posta adresidir.
TargetFileName	Tespit edilen hedef dosya adıdır.
ThreatCategory	Tehdit kategorisidir.
ThreatEventID	Yaşanan olayın ID değeridir. Üretici tarafından her olay tipi için oluşturulmuş benzer bir değerdir.
ThreatName	Tespit edilen tehdidin ismidir.
ThreatType	Tespit edilen tehdidin tipidir. Örneğin: Trojan, worm, virus vb.
ThreatActionTaken	Ajan tarafından tespit edilen tehdide karşı alınan aksiyondur.
ThreatHandled	Tehdidin bertaraf edilip edilmediği bilgisinin yer aldığı parametredir.

2.3.9. VPN (Virtual Private Network) iz kayıtları

Kurum ağına uzaktan yapılan erişimlerin güvenliğini sağlamak her zaman zor bir problem olmuştur. VPN teknolojisi internet üzerinden güvenli iletişim problemine çözüm olarak ortaya çıkmıştır. VPN, kurumun private ağına bağlanmak için public ağ kaynaklarını kullanır. VPN haberleşmesi içerisinde gizliliği, bütünlüğü ve erişim kontrolünü sağlayabilmek için güvenlik mekanizmaları bulunmaktadır. Bu sayede uzak istemciler kurum ağına güvenli bir şekilde bağlanabilmektedir. İdeal bir VPN servisi aşağıdaki özellikleri garanti altına almalıdır [43].

- Güvenlik: Bağlantı süresince gizliliği, bütünlüğü, inkar edilemezliği sağlamalıdır.
- Bağlantı: Uzak istemciler istedikleri her an kurum private ağına bağlanabilmedir.
- Servis Kalitesi: Public ağ sağlayıcısıyla yapılan anlaşmaya göre VPN bağlantılarına yeterli public ağ kaynağı verilmelidir.
- Ağ İzleme: Kurum merkezi, VPN bağlantılarını izleyebilmeli ve gerektiğinde müdahale edebilmelidir [43].

Bu çalışmada Cisco firmasının Adaptive Security Appliance(ASA) ürünü üzerindeki VPN servisinin iz kayıtları incelenecektir. Örnek iz kayıtları şekil 2.21'de gösterilmektedir. Bu

şekildeki ilk kayıtta iki host arasında TCP bağlantısının kurulduğu anlaşılmaktadır. Bu kayıtta VPN sırasında kullanıcıya atanan IP adresinden (192.168.150.10) kurum private ağı içerisinde bulunan başka bir bilgisayarın IP adresine (10.10.10.10) 3389 portundan bağlantı yapıldığı ve bağlantı yapan kişinin *cagri* kullanıcısı olduğu görülmektedir. İkinci sıradaki olay kaydında birinci kayıtta TCP bağlantısı kurmuş olan iki host arasındaki bağlantının sonlandığı anlaşılmaktadır. Burada fazladan bilgi olarak bağlantının ne kadar süre devam ettiği HH:mm:ss formatında görülmekte ve bağlantı süresince yapılan veri alışverişinin byte cinsinden büyüklük bilgisi yer almaktadır. Üçüncü sırada yer alan iz kaydı ilk VPN tünelleme bağlantısı gerçekleştiğinde oluşur. VPN bağlantısı yapan kullanıcının otantikasyon sırasında kullandığı hesap adı ve VPN bağlantısını gerçekleştirdiği public IP adresi bilgisi de bu iz kaydı içerisinde görülebilir. Dördüncü kayıtta ürünün VPN bağlantısını gerçekleştirmek için kullandığı Any Connect isimli ajanı üzerinden otantikasyonun sağlandığı anlaşılmaktadır. Bu iz kaydı içerisinde kullanıcı hesap adı, kullanıcı public IP adresi, kullanılan ajanın versiyonu ve işletim sistemi bilgileri yer almaktadır. Son sırada bulunan iz kaydı kullanıcıya public IP adresi yerine kurum ağında kullanacağı private IP adresinin atamasının yapıldığını göstermektedir. Bu kayıtta kullanıcı hesap adı, pulic IP adresi, IPV4 private IP adresi ve kullanılıyorsa IPV6 private IP adresi bilgisi yer almaktadır.

1- Built TCP connection
<182>%ASA-6-302013: Built inbound TCP connection 65883914 for outside:192.168.150.10/62474 (192.168.150.10/62474)(LOCAL\cagri) to outside:10.10.10.10/3389 (10.10.10.10/3389) (cagri)
2 - Teardown TCP connection
<182>%ASA-6-302014: Teardown TCP connection 65883299 for outside: 192.168.150.10/62474 (LOCAL\cagri) to outside: 10.10.10.10/3389 duration 0:09:47 bytes 430916 TCP Reset-0 from outside (cagri)
3 - First TCP SVC connection established for SVC session
<181>%ASA-5-722033: Group <GroupPolicy_ADMINRDP_TNL> User <cagri> IP <XXX.XXX.XXX.XXX> First TCP SVC connection established for SVC session.
4 - User connection with the user-agent
<182>%ASA-6-722055: Group <GroupPolicy_ADMINRDP_TNL> User <cagri> IP < XXX.XXX.XXX.XXX > Client Type: Cisco AnyConnect VPN Agent for Windows 3.1.04072
5 - Address assigned to session
<180>%ASA-4-722051: Group <GroupPolicy_ADMINRDP_TNL> User <cagri> IP < XXX.XXX.XXX.XXX > IPv4 Address <192.168.150.10> IPv6 address <::> assigned to session

Şekil 2.21 Cisco ASA VPN Örnek İz Kayıtları

2.3.10. DNS (Domain Name System) iz kayıtları

DNS dağıtılmış, tutarlı, güvenilir, özerk ve hiyerarşik yapıda bir veri tabanıdır. İnternetin halen ilk zamanları olan 1980'lerin başında IP sayılarının artması ile birlikte ana bilgisayar adlarını IP adreslerine çevirme işlemi zorlu bir süreç olmaya başlamıştır. DNS sistemi bu duruma bir çözüm üreterek dünya çapında internetin yaygınlaşmasında kilit teknolojilerden birisi olmuştur. DNS sistemi ağaç yapısındadır ve her bir node'un bir parent node'u bulunur. Bu yapının en tepesinde root node'ları bulunmaktadır. Node'lar bir araya gelerek zone'ları oluşturur. Her node içerisinde hostname'e karşılık gelen IP adres bilgilerini barındıran kayıtları tutar. Bu kayıtlara *resource records* (RR) adı verilir. Her bir RR içerisinde isim, sınıf, tip, TTL(time to live) ve veri alanları bulunur [44].

Bir DNS kaydının temel elementleri ve örnekleri Microsoft DNS sunucusunun Debug Logging özelliği ile elde edilen veriler üzerinden incelenmiştir. Bu yöntem sunucu üzerinde performans kayıplarına sebep olacağı için sadece gerekli görülen durumlarda açılması

önerilmektedir [45]. Microsoft Windows DNS Sunucu Debug iz kayıt örneklerini şekil 2.22'de verilmiştir. İz kayıtları içerisinde geçen verilerin anlamları Tablo 2.10'de gösterilmektedir.

İz Kayıt Örnekler
6.7.2018 14:48:37 1290 PACKET 00000029F1C121B0 UDP Rcv 192.168.150.2 8fdd Q [0001 D NOERROR] AAAA (6)shava(4)prot(6)mozaws(3)net(0)
6.7.2018 14:48:37 1290 PACKET 00000029F1C121B0 UDP Rcv 192.168.150.2 b69e Q [0001 D NOERROR] A (5)a1294(3)w2(6)akmai(3)net(0)
6.7.2018 14:48:37 1290 PACKET 00000029EED7A250 UDP Rcv 192.168.150.2 722b Q [0001 D NOERROR] SRV (5)_ldap(4)_tcp(3)pdc(6)_msdcs(11)test(5)intra(0)
6.7.2018 14:48:38 1290 PACKET 00000029EEAFE0F0 UDP Rcv 192.168.150.2 bcd5 Q [0001 D NOERROR] A (5)ping3(10)teamvewer(3)com(0)
8.7.2018 14:54:52 1294 PACKET 00000029ECC531D0 UDP Rcv 202.16.231.61 91f5 R Q [8281 DR SERVFAIL] A (7)qqaqtql(2)cc(0)
8.7.2018 14:54:53 1298 PACKET 00000029F19001E0 UDP Rcv 202.16.231.60 8fd1 R Q [8281 DR SERVFAIL] A (6)test(3)biz(0)

Şekil 2.22 Microsoft Windows DNS Sunucu Debug İz Kayıt Örnekleri

Tablo 2.10 Microsoft Windows DNS Sunucu İz Kayıt Parametreleri

Parametre	**Açıklama**
6.7.2018 14:48:37	İsteğin tarih ve saati
1290	Threat id
00000039D1C131B0	Internal packet identifier
UDP	UDP/TCP protokol göstergesi
192.168.150.2	İstekte bulunan IP adresi
Q	Q : Standard Query N : Notify U : Update ? : Unknown
A	A : Authoritative Answer T : Truncated Response

	D : Recursion Desired R : Recursive Available
(6)shava(4)prot(6)mozaws(3)net(0)	DNS kaydı

2.3.11. WAF (Web Application Firewall) iz kayıtları

WAF, web sayfalarını uygulama seviyesindeki cross-site scripting (XSS), SQL Injection veya file inclusion gibi atak senaryolarına karşı koruyan sistemlerdir. Bu işlemi gerçekleştirmek için WAF sistemi, internet ile web uygulaması arasındaki HTTP trafiğini izleyerek filtrelemeye tabi tutar. Filtreleme işlemi için önceden bilinen saldırı imza tabanını, makine öğrenmesi ile davranış analizini ve uygulama analizi yöntemlerini kullanabilir [46].

Bu çalışmada F5 firmasının WAF çözümü olan BIG-IP Application Security Manager ürününün iz kayıtları incelenmiştir. Aşağıdaki şekillerde bu ürünün oluşturduğu iz kayıtlarından farklı olaylar için örnekler sunulmuştur. Bu iz kayıtları içerisinden elde edilebilecek bilgiler ve bu bilgilerin açıklamaları Tablo 2.11'de gösterilmiştir.

Şekil 2.23'de gösterilen iz kaydı HTTP-GET isteğine aittir. Bu GET isteği *policy_name* parametresinde belirtilen kural dizisinden geçirilerek herhangi bir zararlı içeriğin veya davranışın olup olmadığı incelenmiştir. WAF tarafından belirlenen kurallardan geçirilmiş ve sonuç olarak herhangi bir saldırı tespiti yapılamamıştır. Tarama sonucunda *request_status* parametresinin *passed* değerini aldığı görülmektedir. Bu ilgili isteğin WAF sisteminden başarılı bir şekilde geçtiği ve herhangi bir saldırı ibaresine rastlanmadığını ifade etmektedir. Şekil 2.24'de bulunan HTTP-POST isteği de WAF sisteminden sorunsuz bir şekilde geçmiştir. Şekil 2.25'de gösterilen örnekte web uygulamasına yapılan bir Cross Site Scripting (XSS) Saldırısının tespitine ait iz kaydı görülmektedir. Bu iz kaydı içerisinde *violations* parametresinin aldığı değer tespitin imza tabanlı bir kurala takıldığını ifade etmektedir. *Request_status* parametresinin aldığı *blocked* değeri WAF'ın tespit edilen saldırıya karşı engelleme aksiyonu aldığını göstermektedir. *Request* parametresinde yapılan isteğin bilgileri yer almaktadır. Bu kısım incelendiğinde yapılan XSS isteğinin kanıtlarına rastlanır. Şekil 2.26'da gösterilen iz kaydı SQL Injection Saldırısı sonucu oluşan bir iz kaydını göstermektedir. Bu iz kaydı incelendiğinde saldırının imza tabanlı tespit sistemi tarafından yakalandığını ve aksiyon olarak saldırıya sebep olan isteğin bloklandığı görülmektedir. Yapılan istek incelendiğinde ASCII karakter setine göre encode edilmiş bir SQL cümlesi içerdiği görülebilmektedir. Yapılan istek decode edildiğinde

/page917689.htm?p=1 AND ASCII(SUBSTR((COALESCE(5, NULL)), 1, 1)) > 63 SQL cümlesine ulaşılabilir. Şekil 2.27'de görülen iz kaydı Server Side Code Injection saldırısının tespiti sonucu oluşmuş bir iz kaydını göstermektedir. Bu iz kaydının imza tabanlı güvenlik kuralları tarafından tespit edilip bloklandığı anlaşılmaktadır. Yapılan istek incelendiğinde encode edilmiş şekilde bir unix işletim sistemi komutu içerdiği görülmektedir. İsteği decode edilmiş hali */page846689?filename=sample.sh";&contents=#!/bin/bash id* şeklindedir. Son sırada yer alan iz kaydında yapılan saldırıyı gizlemeye yönelik bir aktivitenin varlığının tespit edildiği ve yapılan isteğin engellendiği görülmektedir. Yapılan istek decode edildiğinde *GET /page798166/iView3/x.jsp -d "c=cmd.exe /c whoami > C:\Users\testuser\Desktop\vulnerable.txt"* şeklinde bir sonuç ortaya çıkmaktadır. Şekil 2.28'de görülen iz kaydında da WAF cihazı tarafından kaçınma saldırısının tespit edildiği ve ilgili trafiğin bloklandığı görülmektedir.

1 - HTTP-GET İsteği

<134>Feb 21 21:02:58 F5-MASTER ASM:unit_hostname="F5-MASTER",management_ip_address="10.10.10.10",management_ip_address_2="N/A",http_class_name="/Common/DISGELEN_WAF_POLICY",web_application_name="/Common/DISGELENWAF_POLICY",policy_name="/Common/DISGELEN_WAF_POLICY",policy_apply_date="2022-02-21 05:21:43",violations="N/A",support_id="7944229503471412663",request_status="passed",response_code="200",ip_client="10.10.10.20",route_domain="0",method="GET",protocol="HTTP",query_string="evrakId=6958428423&dosyaId=555708879&yargiTuru=1",x_forwarded_for_header_value="10.10.10.20",sig_ids="N/A",sig_names="N/A",date_time="2022-02-21 21:02:58",severity="Informational",attack_type="N/A",geo_location="SE",ip_address_intelligence="N/A",username="N/A",session_id="795e6609625f6632",src_port="45041",dest_port="80",dest_ip="10.10.10.250",sub_violations="N/A",virus_name="N/A",violation_rating="0",websocket_direction="N/A",websocket_message_type="N/A",device_id="N/A",staged_sig_ids="N/A",staged_sig_names="N/A",threat_campaign_names="N/A",staged_threat_campaign_names="N/A",blocking_exception_reason="N/A",captcha_result="not_received",microservice="N/A",tap_event_id="N/A",tap_vid="N/A",vs_name="/Common/ PORTAL_DIS_VS_80",sig_cves="N/A",staged_sig_cves="N/A",uri="/main/jsp/market/download_document_brd",fragment="",request="GET /main/jsp/market/download_document_brd?evrakId=6958428423&dosyaId=555708879&yargiTuru=1 HTTP/1.1\r\nHost: market.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36 OPR/83.0.4254.62\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\nCookie: JSESSIONID=0000jX-6k0IdKr0tFsVDlRvbfmh:18irdbbd7; TS018d14cf=010d7db6ddca21618a8d6028acc976fa065a3e5a7817fb5d1586c25e7894ecde40738f2a03dd34d082f1fe793b6b6f9d5a5f79a384b5e16b1761b601b1deb3998a55e4ed5e55c7e8c7bfbfd869fb25ab9b68f6eb7f\r\nReferer: http://market.com/main/jsp/market/

Şekil 2.23 F5 ASM HTTP-GET İsteği

2 - HTTP-POST İsteği

<134>Feb 21 21:02:54 F5-MASTER ASM:unit_hostname="F5-MASTER ",management_ip_address="10.10.10.10",management_ip_address_2="N/A",http_class _name="/Common/PORTAL_DIS_WAF_POLICY",web_application_name="/Commo n/ PORTAL_DIS_WAF_POLICY",policy_name="/Common/ PORTAL_DIS_WAF_POLICY",policy_apply_date="2022-02-21 05:21:43",violations="N/A",support_id="7944229503474589465",request_status="pass ed",response_code="200",ip_client="10.10.10.20",route_domain="0",method="POST", protocol="HTTPS",query_string="",x_forwarded_for_header_value="10.10.10.20",sig_i ds="N/A",sig_names="N/A",date_time="2022-02-21 21:02:54",severity="Informational",attack_type="N/A",geo_location="TR",ip_address_i ntelligence="N/A",username="N/A",session_id="e53bc79e7e3c7c93",src_port="57896" ,dest_port="443",dest_ip="10.10.10.250",sub_violations="N/A",virus_name="N/A",viol ation_rating="0",websocket_direction="N/A",websocket_message_type="N/A",device_ id="N/A",staged_sig_ids="N/A",staged_sig_names="N/A",threat_campaign_names="N /A",staged_threat_campaign_names="N/A",blocking_exception_reason="N/A",captcha _result="not_received",microservice="N/A",tap_event_id="N/A",tap_vid="N/A",vs_na me="/Common/PORTAL_DIS_Pool_443",sig_cves="N/A",staged_sig_cves="N/A",uri ="/main/jsp/market/borclu_bilgileri_goruntule_brd.ajx",fragment="",request="POST /main/jsp/market/borclu_bilgileri_goruntule_mahrumiyet_brd.ajx HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)\r\nAccept: application/xml, text/xml, */*; q=0.01\r\nContent-Type: application/x-www-form-urlencoded; charset=UTF-8\r\nReferer: https://market.com/main/jsp/market/index.jsp\r\nCookie: JSESSIONID=0000bHqXc-oBoI0hfZjGdT-3UCd:19s474fa7\r\nHost: market.uyap.gov.tr\r\nContent-Length: 53\r\nX-Forwarded-For: 212.156.129.142\r\n\r\nplaka=34RGC99&dosyaId=494324040&kisiKurumId=1631985 66",response="Response logging disabled"

Şekil 2.24 F5 ASM HTTP-POST İsteği

3 - Cross Site Scripting (XSS) Saldırısı

<131>Feb 20 21:05:45 F5-MASTER ASM:unit_hostname="F5-MASTER",management_ip_address="10.10.10.10",management_ip_address_2="N/A",http_class_name="/Common/WAF_POLICY",web_application_name="/Common/WAF_POLICY",policy_name="/Common/WAF_POLICY",policy_apply_date="2022-02-14 14:54:42",violations="Attack signature detected",support_id="7944229503281461561",request_status="blocked",response_code="0",ip_client="10.10.10.10",route_domain="0",method="GET",protocol="HTTP",query_string="p=jav%26%23x0D%3Bascript:alert%28%27XSS%27%29",x_forwarded_for_header_value="172.29.0.20",sig_ids="200001174,200000095,200101372",sig_names="HTML entity - &#x... (Parameter),XSS script target (Parameter),javascript: link target (Parameter)",date_time="2022-02-20 21:05:45",severity="Error",attack_type="Cross Site Scripting (XSS)",geo_location="N/A",ip_address_intelligence="N/A",username="N/A",session_id="0",src_port="44511",dest_port="80",dest_ip="10.10.10.254",sub_violations="N/A",virus_name="N/A",violation_rating="3",websocket_direction="N/A",websocket_message_type="N/A",device_id="N/A",staged_sig_ids="N/A",staged_sig_names="N/A",threat_campaign_names="N/A",staged_threat_campaign_names="N/A",blocking_exception_reason="N/A",captcha_result="not_received",microservice="N/A",tap_event_id="N/A",tap_vid="N/A",vs_name="/Common/PICUS_VS_1_80",sig_cves="N/A",staged_sig_cves="N/A",uri="/page980888.htm",fragment="",request="GET /page980888.htm?p=jav%26%23x0D%3Bascript:alert%28%27XSS%27%29 HTTP/1.1\r\nHost: 10.201.156.254:80\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:37.0) Gecko/20100101 Firefox/37.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.5\r\nConnection: Close\r\nX-Session: rDvrDFr_V98aMJpeVwj_NUk_\r\nX-Forwarded-For: 10.10.10.10\r\n\r\n",response="Response logging disabled"

Şekil 2.25 F5 ASM XSS Saldırısı Örneği

4 - SQL Injection Saldırısı

<131>Feb 20 18:29:50 F5-MASTER ASM:unit_hostname="F5-MASTER",management_ip_address="10.10.10.10",management_ip_address_2="N/A",http_class_name="/Common/WAF_POLICY",web_application_name="/Common/WAF_POLICY",policy_name="/Common/WAF_POLICY",policy_apply_date="2022-02-14 14:54:42",violations="Attack signature detected",support_id="7944229503277117507",request_status="blocked",response_code="0",ip_client="10.10.10.20",route_domain="0",method="GET",protocol="HTTPS",query_string="p=1%20AND%20ASCII%28SUBSTR%28%28COALESCE%285%2C%20NULL%29%29%2C%201%2C%201%29%29%20%3E%2063",x_forwarded_for_header_value="10.10.10.20",sig_ids="200002071",sig_names="SQL-INJ substr()",date_time="2022-02-20 18:29:50",severity="Error",attack_type="SQL-Injection",geo_location="N/A",ip_address_intelligence="N/A",username="N/A",session_id="0",src_port="44384",dest_port="443",dest_ip="10.10.10.254",sub_violations="N/A",virus_name="N/A",violation_rating="3",websocket_direction="N/A",websocket_message_type="N/A",device_id="N/A",staged_sig_ids="N/A",staged_sig_names="N/A",threat_campaign_names="N/A",staged_threat_campaign_names="N/A",blocking_exception_reason="N/A",captcha_result="not_received",microservice="N/A",tap_event_id="N/A",tap_vid="N/A",vs_name="/Common/VS_1_443",sig_cves="N/A",staged_sig_cves="N/A",uri="/page917689.htm",fragment="",request="GET /page917689.htm?p=1%20AND%20ASCII%28SUBSTR%28%28COALESCE%285%2C%20NULL%29%29%2C%201%2C%201%29%29%20%3E%2063 HTTP/1.1\r\nHost: 10.201.156.254:443\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:41.0) Gecko/20100101 Firefox/41.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.5\r\nConnection: keep-alive\r\nX-Session: H3FtVMTPb6z7SmtdseNKMPSH\r\nConnection: close\r\nX-Forwarded-For: 10.10.10.20\r\n\r\n",response="Response logging disabled"

Şekil 2.26 F5 ASM SQL Injection Saldırısı Örneği

5 - Server Side Code Injection Saldırısı

<131>Feb 20 10:47:31 F5-MASTER ASM:unit_hostname="F5-MASTER",management_ip_address="10.10.10.10",management_ip_address_2="N/A",http_class_name="/Common/WAF_POLICY",web_application_name="/Common/WAF_POLICY",policy_name="/Common/WAF_POLICY",policy_apply_date="2022-02-14 14:54:42",violations="Attack signature detected",support_id="7944229503259776943",request_status="blocked",response_code="0",ip_client="10.10.10.20",route_domain="0",method="GET",protocol="HTTP",query_string="filename=sample.sh%22%3B&contents=%23!%2Fbin%2Fbash%0Aid",x_forwarded_for_header_value="10.10.10.20",sig_ids="200004182,200101536",sig_names="Unix injection attempt (/bin/bash) (Parameter),Shell command processor (ash/bash) access (Parameter)",date_time="2022-02-20 10:47:31",severity="Error",attack_type="Server Side Code Injection,Command Execution",geo_location="N/A",ip_address_intelligence="N/A",username="N/A",session_id="0",src_port="43909",dest_port="80",dest_ip="10.10.10.254",sub_violations="N/A",virus_name="N/A",violation_rating="2",websocket_direction="N/A",websocket_message_type="N/A",device_id="N/A",staged_sig_ids="N/A",staged_sig_names="N/A",threat_campaign_names="N/A",staged_threat_campaign_names="N/A",blocking_exception_reason="N/A",captcha_result="not_received",microservice="N/A",tap_event_id="N/A",tap_vid="N/A",vs_name="/Common/VS_1_80",sig_cves="N/A",staged_sig_cves="N/A",uri="/page846689",fragment="",request="GET /page846689?filename=sample.sh%22%3B&contents=%23!%2Fbin%2Fbash%0Aid HTTP/1.1\r\nHost: 10.201.156.254:80\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:37.0) Gecko/20100101 Firefox/37.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.5\r\nConnection: Close\r\nX-Session: 7e2XAzWfCIzkpA2tqLq4rtbW\r\nX-Forwarded-For: 10.10.10.20\r\n\r\n",response="Response logging disabled"

Şekil 2.27 F5 ASM Server Side Code Injection Saldırısı Örneği

6 - Evasion technique Saldırısı

<130>Feb 20 05:43:37 F5-MASTER ASM:unit_hostname="F5-MASTER",management_ip_address="10.10.10.10",management_ip_address_2="N/A",http_class_name="/Common/WAF_POLICY",web_application_name="/Common/WAF_POLICY",policy_name="/Common/WAF_POLICY",policy_apply_date="2022-02-14 14:54:42",violations="Evasion technique detected",support_id="7944229503257047141",request_status="blocked",response_code="0",ip_client="10.10.10.20",route_domain="0",method="GET",protocol="HTTP",query_string="",x_forwarded_for_header_value="10.10.10.20",sig_ids="N/A",sig_names="N/A",date_time="2022-02-20 05:43:37",severity="Critical",attack_type="Detection Evasion",geo_location="N/A",ip_address_intelligence="N/A",username="N/A",session_id="0",src_port="43625",dest_port="80",dest_ip="10.10.10.254",sub_violations="Evasion technique detected:IIS backslashes",virus_name="N/A",violation_rating="1",websocket_direction="N/A",websocket_message_type="N/A",device_id="N/A",staged_sig_ids="N/A",staged_sig_names="N/A",threat_campaign_names="N/A",staged_threat_campaign_names="N/A",blocking_exception_reason="N/A",captcha_result="not_received",microservice="N/A",tap_event_id="N/A",tap_vid="N/A",vs_name="/Common/VS_1_80",sig_cves="N/A",staged_sig_cves="N/A",uri="/page798166/iView3/x.jsp -d %22c=cmd.exe /c whoami > C:/Users/testuser/Desktop/vulnerable.txt%22",fragment="",request="GET /page798166/iView3/x.jsp%20-d%20%22c=cmd.exe%20/c%20whoami%20%3E%20C%3A%5CUsers%5Ctestuser%5CDesktop%5Cvulnerable.txt%22 HTTP/1.1\r\nHost: 10.10.10.254:80\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\nConnection: close\r\nContent-Type: application/json\r\nX-Picus-Session: _UI9lRliG-ZxeHBxlokstuVG\r\nAccept-Encoding: gzip\r\nX-Forwarded-For: 10.10.10.20\r\n\r\n",response="Response logging disabled"

Şekil 2.28 Kaçınma Tekniği Saldırı Örneği

Tablo 2.11 F5 ASM İz Kayıt Parametre ve Açıklamaları

Parametre	**Açıklama**
management_ip_address	WAF sisteminin yönetim arayüzünün IP adresidir.
policy_name	Trafiğe uygulanan güvenlik politikasının ismidir.
violations	Saldırı yöntem bilgisini içerir.
request_status	İstemcinin isteğine karşılık alınan aksiyonu gösterir.
Response_code	Uygulama tarafından dönülen HTTP kodu. Bloklanmayan istekler için görünür durumda olur.
İp_client	İstemci kaynak IP adresidir.
method	İstemci tarafından çağrılan HTTP metodudur.
protocol	Protokol adıdır (HTTP/HTTPS)
date_time	YYYY-MM-DD HH:MM:SS formatında tarih ve saat bilgisidir.
severity	Olayın önem derecesidir.
Attack_type	Tespit edilen saldırının tipidir.
Src_port	İstemci kaynak port numarasıdır.
dest_port	İstekte bulunulan servisin dinlediği hedef port numarasıdır.
Dest_ip	İstekte bulunulan servisin dinlediği hedef IP adresidir.
Virus_name	Tespit edilen zararlı yazılım adıdır.
url	İstemci tarafından istenen URI'dir.
request	İstemci tarafından gönderilen istek dizesidir.
response	Sunucu tarafından dönülen HTTP cevabıdır.

2.3.12. NAC (Network Access Control) iz kayıtları

NAC sistemleri kurumsal ağ trafiğinde görünürlüğün artmasını destekleyerek kurumun ağa erişmek isteyen cihazları ve kullanıcıları denetleyecek politikalar üretmesini sağlamaktadır. Kurumların network güvenliği anlamında karşılaştığı büyük sorunlardan birisi personelin kullandığı mobil cihazlardır. Anti-virus güncellemesi almamış veya buna benzer güvenlik önlemlerini karşılamayan cihazlar ağ içerisinde tehdit oluşturmaktadır. NAC çözümleri bu tip cihazları tespit ederek bunları ağdan izole edebilir veya güvenlik sıkılaştırmalarının yapılması için gerekli düzeltmeleri sağlayabilir. Bir diğer sorun ise bilgi işlem personeli

bilgisi haricinde kötü amaçlı kişiler tarafından ağa takılan cihazlardır. NAC sistemleri bu cihazları tespit edebilir ve sadece izin verilen cihazların ağa bağlanmasını sağlayabilir [47].

Bu çalışmada Maysiber firmasının Scopnet isimli NAC ürününün iz kayıtları incelenmiştir. İlgili ürün radius mimarisi kullanarak 802.1x protokolü ile yetkisiz cihazların ağa bağlanmasını engellemektedir. Şekil 2.29'da ürünün örnek iz kayıtları görülmektedir. Bu kayıtların ilkinde ağa erişmeye çalışan bir cihazın başarılı bir şekilde domain üzerinden kullanıcı otantikasyonu ile bağlantıyı gerçekleştirdiği görülmektedir. İkinci sıradaki iz kaydında MAC ve IP adresi verilen bir cihazın otantikasyon aşamasını geçemediği ve erişim isteğinin reddedildiği görülmektedir. Üçüncü sıradaki iz kaydında IP ve MAC bilgileri verilen cihazın ağ bağlantısını kopardığı bilgisi görülmektedir. Bu iz kaydında ayrıca cihazın gerçekleştirdiği ağ bağlantısının süresinin saniye cinsinden değeri de verilmektedir. Son sıradaki iz kaydında cihazın ağa bağlandığı bilgisi bulunmaktadır. Bu kayıt içerisinde cihazın IP ve MAC adresi ve bağlandığı switch'in MAC adres bilgisi bulunmaktadır. Tablo 2.12'da örnek olarak verilen iz kayıtlarında yer alan parametreler ve bu parametrelerin açıklamalarına yer verilmektedir.

1 - Access Accepted
id: "7484936" username: "host/hostname01.deneme.com" pass: "" reply: "Access-Accept" authdate: "2022-02-24 20:32:06.0" user_ip_address: "10.10.10.10" user_mac_address: "AB-CD-EF-12-34-56" nas_ip_address: "10.10.10.20" nas_port: "slot=1;subslot=0;port=7;vlanid=118" ssid: "" uservlan: "" comment: "null" adgroupname: "null"
2 - Access Rejected
id: "7483838" username: "host/ hostname01.deneme.com " pass: "" reply: "Access-Reject" authdate: "2022-02-24 20:03:30.0" user_ip_address: "10.10.10.10" user_mac_address: " AB-CD-EF-12-34-56" nas_ip_address: "10.10.10.20" nas_port: "slot=1;subslot=0;port=9;vlanid=119" ssid: "" uservlan: "" comment: "deneme -Server" adgroupname: "null"
3 - Device Disconnected
<142>Feb 24 20:17:35 SCPNETRAD01 freeradius: Disconnect: [host/ hostname01.deneme.com] (did AB-CD-EF-12-34-56 cli AB-05-AB-74-AB-B2 port 16793803 ip 10.10.10.10) 46372 seconds
4 - Device Connected
<142>Feb 24 20:19:57 SCPNETRAD01 freeradius: Connect: [host/ hostname01.deneme.com] (did AB-CD-EF-12-34-56 cli AB-05-AB-74-AB-B2 port 16806001 ip 10.10.10.10)

Şekil 2.29 Scopnet İz Kayıt Örnekleri

Tablo 2.12 Scopnet İz Kayıt Parametre ve Açıklamaları

Parametre	**Açıklama**
Username	Cihaz için bağlantı isteğinde bulunan kullanıcı adı
Reply	Erişim isteğine karşı sistemin verdiği cevap
Authdate	Erişim isteğini tarih ve saati
User_ip_address	Ağ erişim isteğinde bulunan cihaza atana IP adresi
User_mac_address	Ağ erişim isteğinde bulunan cihazın MAC adresi
Nas_ip_address	Ağ erişim isteğinde bulunan cihazın bağlanmak istediği network cihazının (switch, router vb.) IP adresi

2.3.13. Web proxy iz kayıtları

Ağ adli bilişiminin en önemli kısımlarından birisi delil toplama aşamasıdır. Örneğin bir tehdit aktörü ağa saldırdığında, saldırı trafiği genellikle router üzerinden geçer. Sonuç olarak ağ trafiğinden önemli deliller elde edilebilir. Web Proxy iz kayıtları önemli deliller sağlar. Web Proxy'nin amacı URL isteğini istemciden sunucuya doğru taşımak ve gelen cevabı doğru istemciye ulaştırmaktır. Web Proxy, yerel ağda tarayıcı ve internet arasında bir nevi kapı görevi görür [48].

Bu çalışmada Mcafee firmasının Web Gateway ürününün iz kayıtları incelenecektir. Bu ürün bilinen zararlı URL ve tehditlere karşı koruma sağlarken aynı zamanda makine öğrenme özelliği sayesinde sıfırıncı gün saldırılarına karşı da koruma sağlamaktadır. Üründen elde edilebilecek iz kayıt örnekleri şekil 2.30'de gösterilmektedir. İlk sırada gösterilen iz kaydı izin verilen bir web isteğini göstermektedir. Kayıt incelendiğinde HTTP-200 koduyla isteğin başarılı bir şekilde sunucuya ulaştığı bilgisi, proxy erişimi sırasında kullanıcı doğrulaması yapılan kişinin kullanıcı adı, hedef ve kaynak IP adresleri, erişim isteğinde bulunulan URL bilgisi ve URL sınıflandırma sonuçları görülmektedir. İkinci sırada verilen iz kayıt örneği hedef URL değeri zararlı veri tabanında bulunduğu için erişimin engellendiği bir durumu göstermektedir. Burada isteğin HTTP-403 cevabını aldığı ve *BlockReason* parametresinin *Blocked* değerini aldığı görülmektedir. Son sırada bulunan iz kayıt örneğinde bağlantı için proxy üzerinden otantikasyon sağlayan kişinin ilgili web erişimi için yetkisinin olmaması durumu söz konusudur. Bu durumda ilgili web sayfasına istekte bulunan hesabın yetkisinin olmaması veya kullanılan hesap bilgilerinin yanlış olması durumu söz konusu olabilir. Örneklerde verilen iz kayıtlarından elde edilebilecek parametreler ve bunların açıklamaları tablo 2.13'de verilmiştir.

1 - Allowed
<30>Feb 28 21:07:59 Proxy01 mwg: LEEF:1.0|McAfee|Web Gateway|10.2.6|0|devTime=1646071679000|src=10.10.10.10|usrName=cagri|httpStatus=200|dst=20.20.20.20|urlCategories=Web Ads|blockReason=|url=https://gcdn.deneme.net|Antivirus=|BytesToClient=2644|BytesToServer=1855|urlReputation=Unverified|UserAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36|AuthenticationFailMsg=No failure
2 - Blocked due to an entry in the Filter Database
<30>Feb 28 21:07:56 Proxy01 mwg: LEEF:1.0|McAfee|Web Gateway|10.2.6|10|devTime=1646071676000|src=10.10.10.10|usrName= cagri |httpStatus=403|dst=20.20.20.20|urlCategories=Streaming Media, Social Networking|blockReason=Blocked by URL filtering|url=https://cdn.dimml.io|Antivirus=|BytesToClient=3576|BytesToServer=0|urlReputation=Unverified|UserAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36|AuthenticationFailMsg=No failure
3 - Blocked due to unauthorized access
<30>Feb 28 21:07:20 Proxy01 mwg: LEEF:1.0|McAfee|Web Gateway|10.2.6|81|devTime=1646071640000|src=10.10.10.10|usrName= cagri |httpStatus=403|dst=20.20.20.20|urlCategories=Internet Services|blockReason=|url=https://20.20.20.20|Antivirus=|BytesToClient=2490|BytesToServer=0|urlReputation=Minimal Risk|UserAgent=Mozilla/5.0|AuthenticationFailMsg=No failure

Şekil 2.30 McAfee Web Gateway Örnek İz Kayıtları

Tablo 2.13 McAfee Web Gateway İz Kayıt Parametre ve Açıklamaları

Parametre	**Açıklama**
Src	İstekte bulunan kaynak IP adresi
usrName	Proxy sisteminde otantikasyon sağlayan kullanıcı adı
httpStatus	HTTP cevap kodu
Dst	Hedef IP adresi
urlCategory	URL kategori bilgisi
blockReason	Eğer istek engellendiyse sebebi
url	İstemcinin erişmek isteği URL adresi
BytesToClient	Sunucuya iletilen verinin byte cinsinden değeri
BytesToServer	İstemciye iletilen verinin byte cinsinden değeri
urlReputation	URL sınıflandırma bilgisi. Eğer url sınıflandırmamış ise *Unverified* olarak görünecektir
UserAgent	İstemcinin kullandığı web tarayıcı bilgileri

2.4. İz Kayıt Toplama Yöntemleri

Bilişim sistemleri tasarlandıkları işe uygun olarak birbirinden farklı donanım ve yazılım özelliklerine sahiplerdir. Bu çeşitlilik sebebiyle iz kayıt toplama yöntemlerinde de farklılıklar oluşmaktadır.

2.4.1. Ajan ile iz kayıt toplama

Bilişim sistemlerinden iz kayıtlarını toplama yöntemlerinden birisi sisteme iz kayıtlarını toplama ve SIEM sistemine iletme amacıyla yazılmış ajan programı yüklemektir. Bu çalışmada Windows'dan iz kayıtları toplanması amacıyla IBM tarafından geliştirilmiş Wincollect isimli ajan programı kullanılmıştır.

Wincollect, üzerine kurulduğu sistemden veya uzak bir makineden olay kayıtlarını toplayarak SIEM sistemine syslog protokolü ile gönderen bir yazılımdır. Uygulama bu

toplama işlemini Windows Event Log API yardımıyla gerçekleştirir. Wincollect ile bir sistemden iz kayıtlarını toplamak için iki farklı senaryo mevcuttur. Bunlar Managed Mod ve Stand-Alone Mod'dur [49].

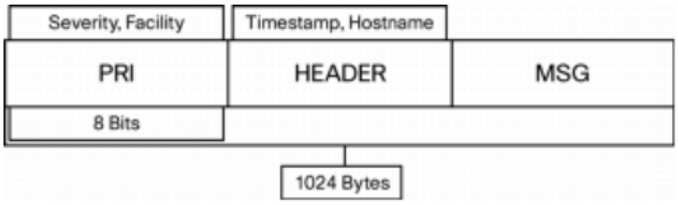
Managed Mod senaryosunda Windows makinelere kurulan ajanlar merkezi SIEM sistemi üzerinden yönetilebilir durumdadır. Bu yönetim kısmında hangi tip iz kayıtlarının toplanmak istendiği (Security, System, Application vb.) veya hangi Event ID değerine sahip kayıtların toplanacağı SIEM sistemi üzerinden belirlenebilir. Bu yöntemde ajanın kurulduğu Windows makineden veya bu makineye ağ bağlantısı bulunan ve gerekli erişim izinlerine sahip uzak makinelerden iz kayıtları toplanarak SIEM sistemine aktarılır. Bu yöntemde Qradar SIEM yönetim sunucusu en fazla 500 uzak makineden iz kayıtlarını çekerek SIEM sistemine aktarılabilir. Eğer 500'ün üzerinde ajan kurulumu gerekiyorsa bu noktada Stand-Alone modu kullanılmalıdır. Bu durumda ajanlar merkezi SIEM sistemi üzerinden yönetilemez ve güncellemeler merkezi olarak yapılamaz. Her iki yöntemde de Windows makinelere kurulan Wincollect ajanına kurulum sırasında SIEM konsol IP adresi ve konsol üzerinde üretilen token bilgisi girilmelidir. Bu token sayesinde SIEM sistemi Wincollect ajanı kurulan makineye güvenebilir. Wincollect ajanı ve SIEM konsol sunucusu arasından yönetim işlemleri 8413 portu üzerinden sağlanırken iz kayıtlarının toplanması aktarımı ve diğer işlemler 514, 445, 137-139, 49152-65535 portlarından sağlanır [49].

2.4.2. Syslog ile iz kayıt toplama

Syslog, UNIX tabanlı işletim sistemlerinde olay kayıtlarının raporlanması için geliştirilmiş bir protokoldür. Sistem kayıtları, işletim sistemi üzerinde çalışan bir servis yardımıyla toplanır ve lokal sistem üzerinde veya uzak bilgisayar üzerinde bir dosyanın içine yazılır. Syslog servisinin konfigürasyonu /etc/syslog.conf dosyasında bulunmaktadır. Syslog protokolü ile farklı sistemlerden elde edilen iz kayıtları merkezi bir sistemde toplanarak sistem yöneticilerinin veya güvenlik analistlerinin incelemelerini kolaylaştırmaktadır. Switchler, routerlar, yazıcılar, güvenlik cihazları gibi birçok farklı ağ ekipmanı syslog protokolünü desteklemektedir. Syslog protokolü varsayılan olarak UDP 514 portunu kullanmaktadır. Syslogd servisi en yetkili kullanıcı olan root yetkileri ile çalıştırılmalıdır. Syslog servisi ile yazılan iz kayıtları okunabilir formatta işletim sisteminin /var/log dosya yolunda bulunan çeşitli isimlerdeki dosyalarda tutulmaktadır [50].

Syslog paketleri 1024 bytes ile sınırlanmıştır ve içerisinde *facility, severity, sunucu adı, zaman damgası ve mesaj* gibi farklı bilgiler yer almaktadır. Şekil 2.31'de [51] bir syslog

paketinin yapısı gösterilmiştir. Bu yapıda PRI olarak adlandırılan kısım *Facility* ve *Severity* bilgilerini içeren 8 bit'den oluşan bir değerdir. Facility değeri mesajı üreten kaynağın ne olduğunu gösterir. Şekil 2.32'de [52] facility değerleri numerik karşılıkları ile birlikte yer almaktadır. Severity değeri mesajın önem derecesini gösteren kısımdır. Şekil 2.33'de [52] numerik karşılıkları ile birlikte verilmiştir [51].



Şekil 2.31: Syslog Paket Yapısı

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Şekil 2.32: Syslog Facility Değerleri

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Şekil 2.33: Syslog Severity Değerleri

2.4.3. JDBC (Java Database Connectivity) protokolü ile iz kayıt toplama

JDBC, Java dilinde yazılmış olan uygulamaların çeşitli veri tabanları ile etkileşimini sağlayan API (Application Programming Interface) arayüzleridir. JDBC API ile herhangi bir ilişkisel veri tabanında tutulan tablosal verilere erişim sağlanabilir. Bu etkileşim sayesinde veri tabanına veri kaydedilebilir, güncellenebilir, çekilebilir veya silinebilir. JDBC API veri tabanlarına bağlantı kurabilmek için JDBC sürücüleri kullanmaktadır. Dört tip JDBC sürücü bulunmaktadır. Bunlar; JDBC-ODBC Bridge sürücü, Thin Sürücü, Native Sürücü ve Network Protocol Sürücüdür [53].

SIEM uygulamalarının JDBC protokolü ile veri tabanlarına bağlanıp gerekli tablo veya view'leri çekebilmesi için veri tabanı üretici firmaların geliştirdiği sürücüler bulunmaktadır. Bu sürücüler SIEM sistemi üzerine yüklenerek ilgili veri tabanına sorunsuz bağlantı kurması sağlanır [54]. Bu yöntemde veri tabanı üzerinde sadece ilgili tablo veya view'i okuma yetkisine sahip bir kullanıcı hesabı oluşturulur. Okunacak olan veri tabanı adı, instance adı, tablo veya view adı, veri tabanı tipi (örneğin MSSQL için MSDE seçilmeli), veri tabanı IP adresi, port bilgisi ve son olarakta tablo içerisinde sonsuza kadar artan bir değeri bulunduran kolon adı bilgilerinin SIEM sistemine tanıtılması gerekmektedir [55].

2.4.4. OPSEC (Open Platform for Security) LEA (Log Export API) ile iz kayıt toplama

OPSEC LEA Check Point marka ürünlerden iz kayıtlarının çekilmesi amacıyla kullanılan bir yöntemdir. Bu yöntem ile iki cihaz arasında güvenilir bir iletişim ortamı kurularak karşılıklı otantikasyon ile veri akışı sağlanır [56].

Bu işlemin gerçekleşmesi için gerekli olan adımlar iz kayıtlarını çekecek uygulamanın özelliklerine göre değişiklik gösterebilir. Aşağıda Qradar ürünü için yapılması gereken işlemlerin genel hatları verilmiştir [57].

- Check Point SmartCenter kullanıcı arayüzüne giriş yapılarak Object sekmesinden New Host seçeneği ile Qradar uygulaması için yeni bir host tanımı yapılır.
- Objects -> More Object Types -> Server -> OPSEC Application -> New Application sekmesinden uygulama objesi oluşturulur ve tek seferlik otantikasyon kullanımı için parola tayin edilir.
- Objects -> Object Explorer sekmesinden Gateways and Servers menüsünden Networks Objects seçilerek gerekli ayarlamalar yapılır.
- Qradar uygulamasına giriş yapılır ve yeni bir kaynak tanımı yapılır. Bu alanda Check Point IP ve port bilgisi, Check Point içerisinde oluşturulan parola bilgisi, Check Point tarafında oluşturulan SIC name, eğer karşılıklı bir sertifika oluşturulmuş ise bu sertifikanın Qradar sunucusu içerisindeki dizin bilgisi gibi bilgiler girilir [57].

2.4.5. MSRPC protokolü ile iz kayıt toplama

Bu Microsoft Security Event Log iz kayıtlarını client tarafında herhangi bir ajan yazılımı yüklemeye gerek kalmayacak şekilde toplamaya yarayan bir yöntemdir. Bu yöntemle şifreli bir şekilde iz kayıtları SIEM sistemine aktarılabilir. Aktarım hızı WMI/DCOM yönteminden daha hızlıdır. MSRPC protokolünün oturum güvenliği için NTLMv2 kullanmaktadır. Kerberos protokol desteği yoktur [58].

Bu yöntem ile olay günlükleri içerisindeki uygulama, sistem, güvenlik, DNS sunucu, dosya çoğaltma, dizin hizmeti günlükleri gibi farklı iz kayıtları SIEM sistemine aktarılabilir. Windows Server 2012 ve üzerindeki sunucu işletim sistemlerinde ve Windows 10 kullanıcı işletim sistemlerinde MSRPC ile iz kayıt toplama işlemi yapılabilmektedir. Bu yöntemde Windows işletim sistemi üzerinde, SIEM sisteminin iz kayıtlarını çekebilmesi için bir kullanıcı hesabı oluşturulur. Bu hesap Event Log Readers grubunun üyesi olmalıdır. MSRPC

protokolü, Remote Procedure Call (RPC) ve RPC Endpoint Mapper Windows servislerini kullanmaktadır. Bu servisler işletim sistemi üzerinde çalışır durumda olmalıdır. MSRPC protokolü ile iz kayıt toplama işleminde TCP 135, TCP 445 ve dinamik olarak değişen TCP 49152 – 65535 arasındaki portları kullanmaktadır [59].

3. MATERYAL VE METOT

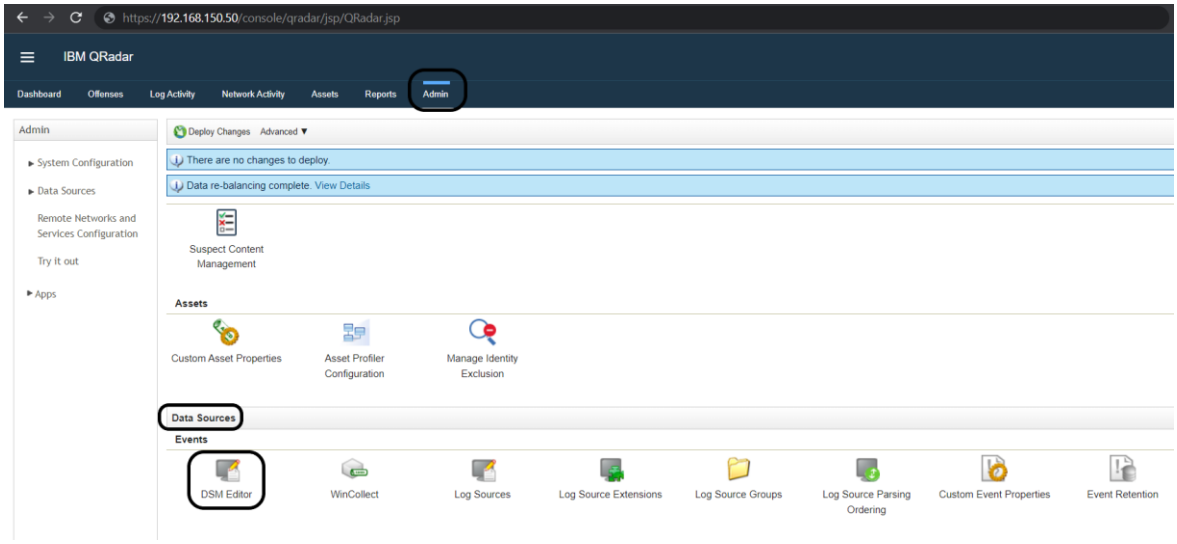
Tez çalışmasının amacı, bilişim sistemlerinde meydana gelen siber saldırıların ve adli soruşturmalarda delil olarak kullanılabilecek verilerin SIEM sistemleri üzerinden nasıl elde edilebileceğini ortaya koymaktır. Bu çalışmada SIEM olarak kullanılan ürün IBM firmasına ait olan Qradar isimli ürünün 7.4.3 versiyonudur. IBM firması bağımsız araştırmacılar ve geliştiriciler için Qradar ürününün deneme sürümünü 30 gün boyunca kullanıma açmıştır. Yapılan çalışmada bu deneme sürümünden faydalanılmıştır.

Önceki bölümlerde adli bilişim olayının tespiti için gerekli iz kayıtlarının neler olduğu ve bu iz kayıtlarından hangi bilgilerin elde edilebileceği anlatılmıştır. Bununla birlikte SIEM sistemine iz kayıtlarının aktarımı için kullanılan yöntemler anlatılmıştır. Tüm bu bilgiler yardımıyla SIEM uygulamasına iz kayıtlarının aktarımı yapılmıştır. SIEM üzerinde tespit için gerekli kuralların yazımı için yapılan tüm adımlar bu bölümde detaylı bir şekilde verilmiştir.

3.1. Qradar SIEM Üzerinde İz Kayıtlarının Anlamlandırılması

Qradar üzerinde global markaların çok bilinen ürünlerinin iz kayıtlarının toplanması ve anlamlandırılması için ön tanımlı eklentiler mevcuttur. Eğer sistemde iz kayıtlarının toplanmasının istenildiği ürün için bir şablon yok ise veya kendi geliştirdiğiniz bir uygulamanın iz kayıtlarını toplayıp bunların anlamlandırıp kullanmak istiyorsanız Qradar üzerinde bu tanımlamaları yapmanız da mümkündür. Tüm bu işlemlerin yapılabilmesi için DSM (Device Support Module) eklentileri geliştirilmiştir.

2.4 maddesinde anlatılan iz kayıt toplama yöntemleriyle Qradar SIEM sunucusuna aktarılan iz kayıtlarının kurallarda ve arama işlemlerinde kullanılabilmesi için bir dizi işlem uygulanmıştır. Ön tanımlı bir kaynak tipi olmadığından yeni kaynak tipi tanımları yapılmıştır. Bu işlem için Qradar uygulamasının Admin sekmesinde Data Source menüsü altındaki *DSM Editor*'e giriş yapılarak *Create New* seçeneği ile yeni kaynak tipi tanımı yapılmıştır. Şekil 3.1'de Qradar arayüzü üzerinde de gösterilmiştir.

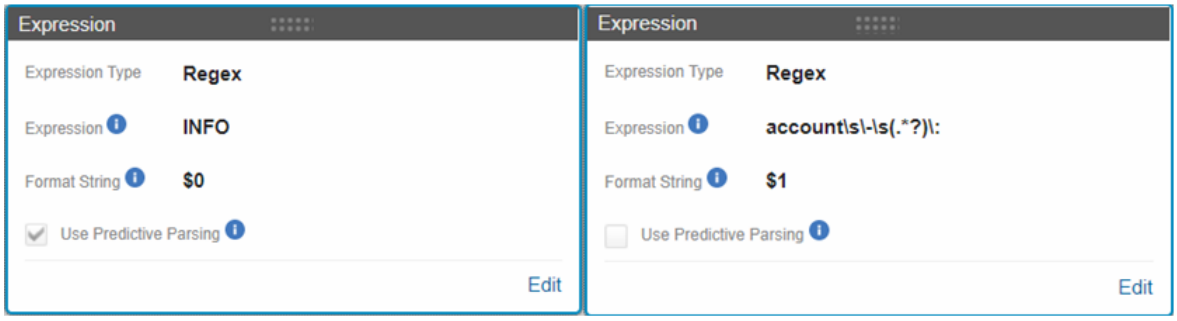


Şekil 3.1: Yeni Kaynak Tipi Oluşturma

Sonraki aşamada oluşturulan kaynak tipi için belirleyici ifadeler seçilip bu alanlar regex kullanılarak ayrıştırma işlemi yapılmıştır. Bu işlemler için Qradar uygulaması içerisindeki *DSM Editor* kullanılmıştır. Qradar SIEM uygulamasına gelen bir iz kaydının doğru kaynak tipi ile etiketlenebilmesi için belirleyici olan iki adet parametre bulunmaktadır. Bunlar *Event ID* ve *Event Category* değerleridir. Örnek olarak Tablo 3.1'de verilen iki iz kaydında tespit edilen *Event Category* ve *Event ID* değerlerinin regex kullanılarak nasıl ayrıştırıldığı Şekil 3.2'de görülmektedir.

Tablo 3.1:Zimbra Mail Uygulası İz Kayıt Örneği

Başarılı Oturum Açma
"<157>Jan 22 15:39:55 zimbra mailbox.log 2022-01-22 15:39:53,326 INFO [Pop3SSLServer-3] [name=cagrifanuscu@test.com;ip=192.168.150.50;oip=192.168.150.10;cid=348902;] account - Authentication successful for user: cagrifanuscu@test.com"
Başarısız Oturum Açma Denemesi
"<157>Jan 22 15:39:55 zimbra mailbox.log 2022-01-22 15:39:53,516 INFO [ImapSSLServer-982] [ip=192.168.150.50;oip=192.168.150.10;via=com.samsung.android.email.provider,192.168.150.50(nginx/1.20.0);ua=Zimbra/8.8.15_GA_4125;cid=348903;] account - Error occurred during authentication: authentication failed for [cagrifanuscu@test.com]. Reason: invalid password."

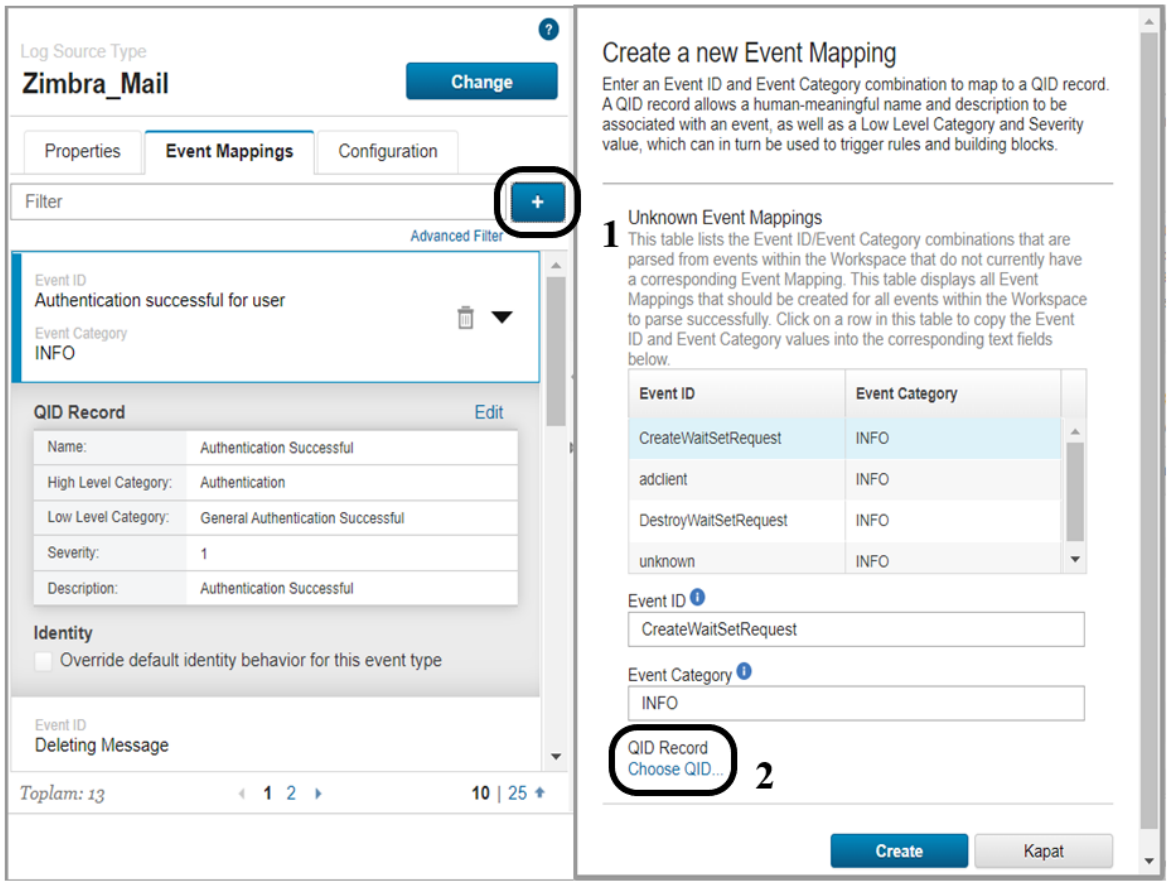


Şekil 3.2: Event ID ve Event Category Parametreleri

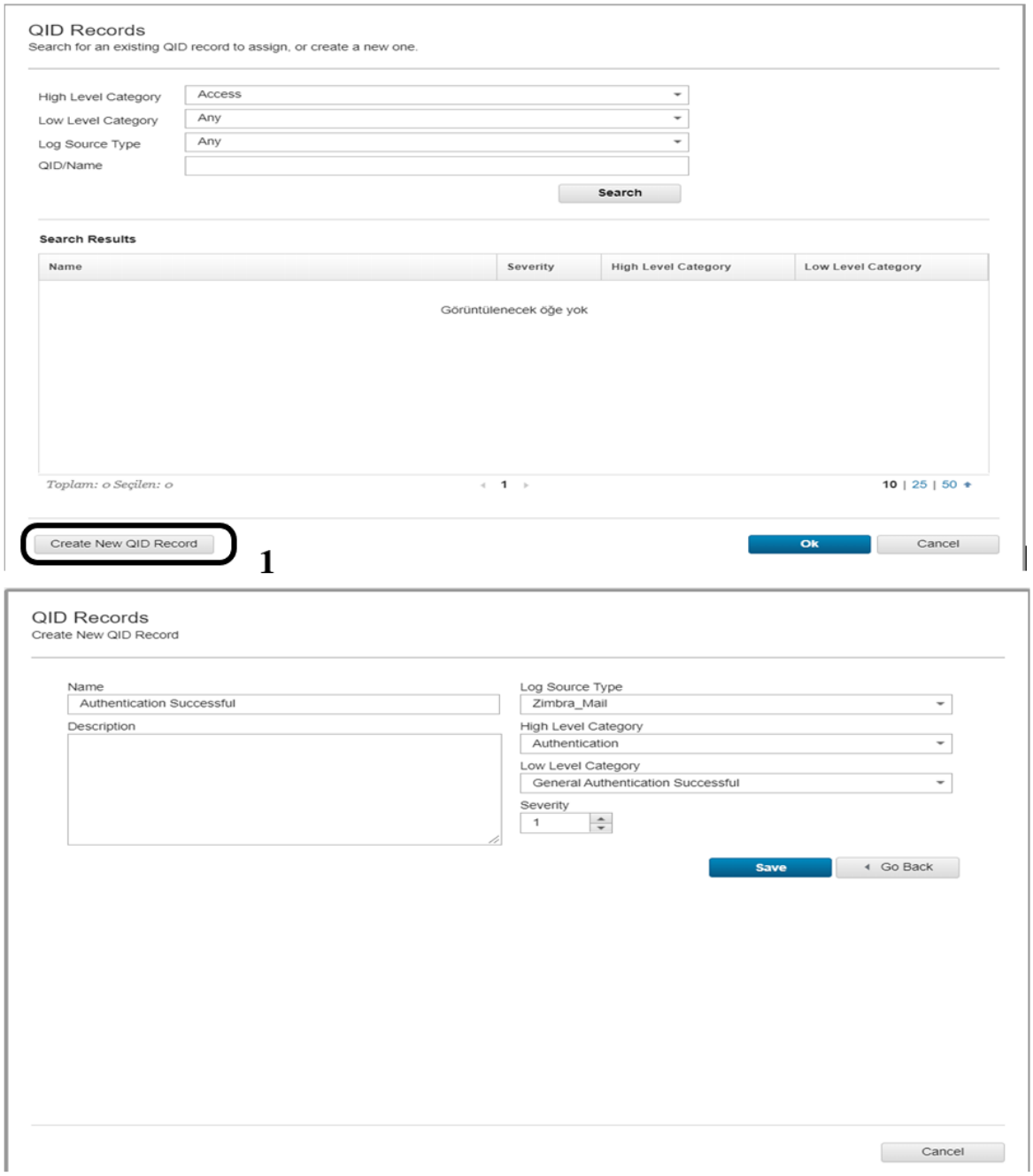
İz kayıtları üzerinde yapılan bir diğer işlem *Event Mapping*'dir. Bu işlemin amacı ham iz kayıtlarının içerisinde olmayan ancak kaydın içeriğini zenginleştirerek kurallarda ve aramalarda analistin işini kolaylaştıran bilgilerin eklenmesidir. Özetle *Event ID* ve *Event Category* değerlerini eşleştirerek benzersiz bir ID değerine atar. Bu esnada oluşan ID değerine öncelik ve önem dereceleri de eklenir. Bu işlem adımları şu şekilde yapılmıştır. *DSM Editor*'e giriş yapıldıktan sonra *Event Mappings* sekmesinde yeni bir Event Mapping oluşturabilmek için Şekil 3.3'de 1 numara ile gösterilen yere tıklanır. Sağ tarafta açılan pencerede seçilen *Event ID* ve *Event Category* değerleri ile eşleştirilecek olan yeni bir *QID* değeri oluşturabilmek için 2 numaralı alana tıklanır. Açılan pencerede mümkünse mevcut bir *QID* değerine eşleştirme yapılır. Bu örnek için yeni bir *QID* değeri oluşturulmuştur. Bunun için Şekil 3.4'de 1 numara ile gösterilen alana tıklanarak açılan penceredeki alanlar doldurulur ve save butonu ile kaydedilir. Bu alanlar;

- Log Source Type: Oluşturulan QID'nin hangi kaynak tipine ait olduğu belirlenir.
- High Level Category ve Low Level Category: Bu alanlar olay kayıtlarının kategorize edilmesinde kullanılır. Arama ve kural oluşturma işlemlerinde aktif olarak kullanılır.
- Severity: Oluşturulacak QID değerinin önem derecesi bu alanda belirtilir.
- Name**:** QID değerinin adıdır.

Tüm bu işlem basamakları sonrasında gelen her bir iz kaydı için bir olay adı tanımı yapılmış olur.

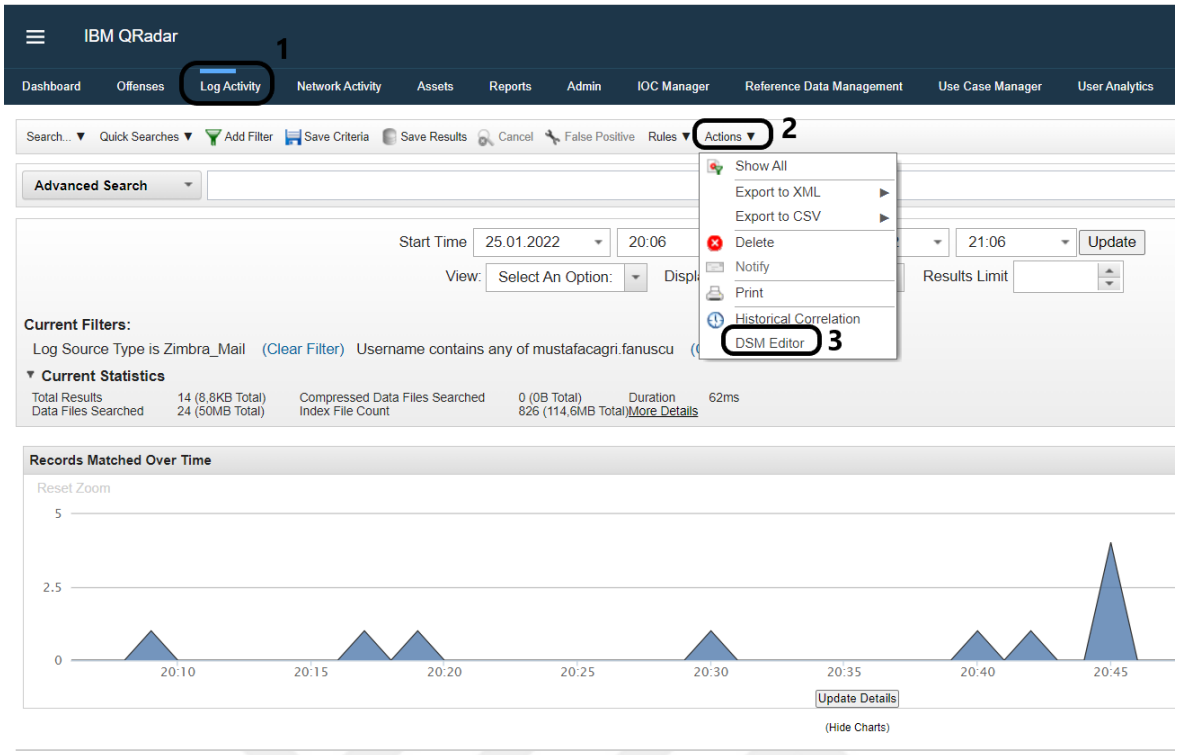


Şekil 3.3: Yeni Bir Event Mapping Oluşturma



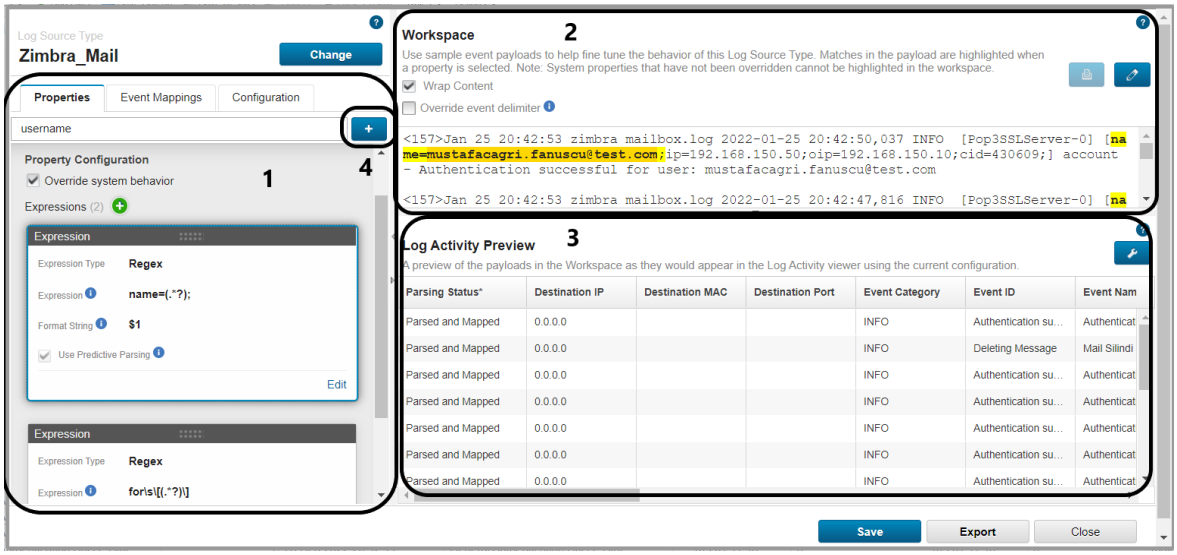
Şekil 3.4: Yeni Bir QID Kaydı Oluşturma

İz kayıtlarının kurallar ve aramalarda efektif bir şekilde kullanılabilmesi için DSM Editör üzerinde Source IP veya Username gibi varsayılan parametreler veya ihtiyaca göre custom olarak oluşturulabilecek parametreler için ayrıştırma işlemi uygulanmalıdır. Bu işlem için Şekil 3.5'da 1 ile gösterilen *Log Activity* sekmesinde istenen kaynak ile ilgili iz kayıtları filtrelenerek fare yardımıyla seçilir. Sonra 2 numara ile gösterilen *Actions* menüsü açılarak 3 numara ile gösterilen *DSM Editor* açılır.

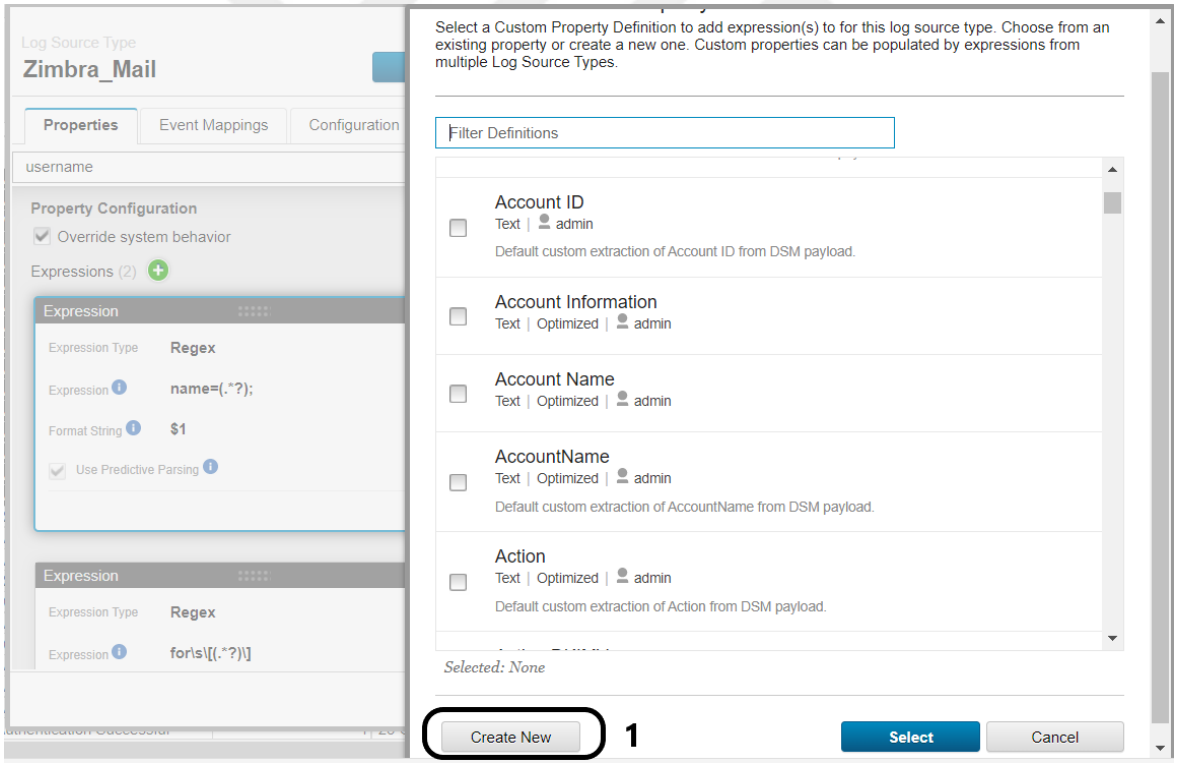


Şekil 3.5: DSM Editor'un Açılması

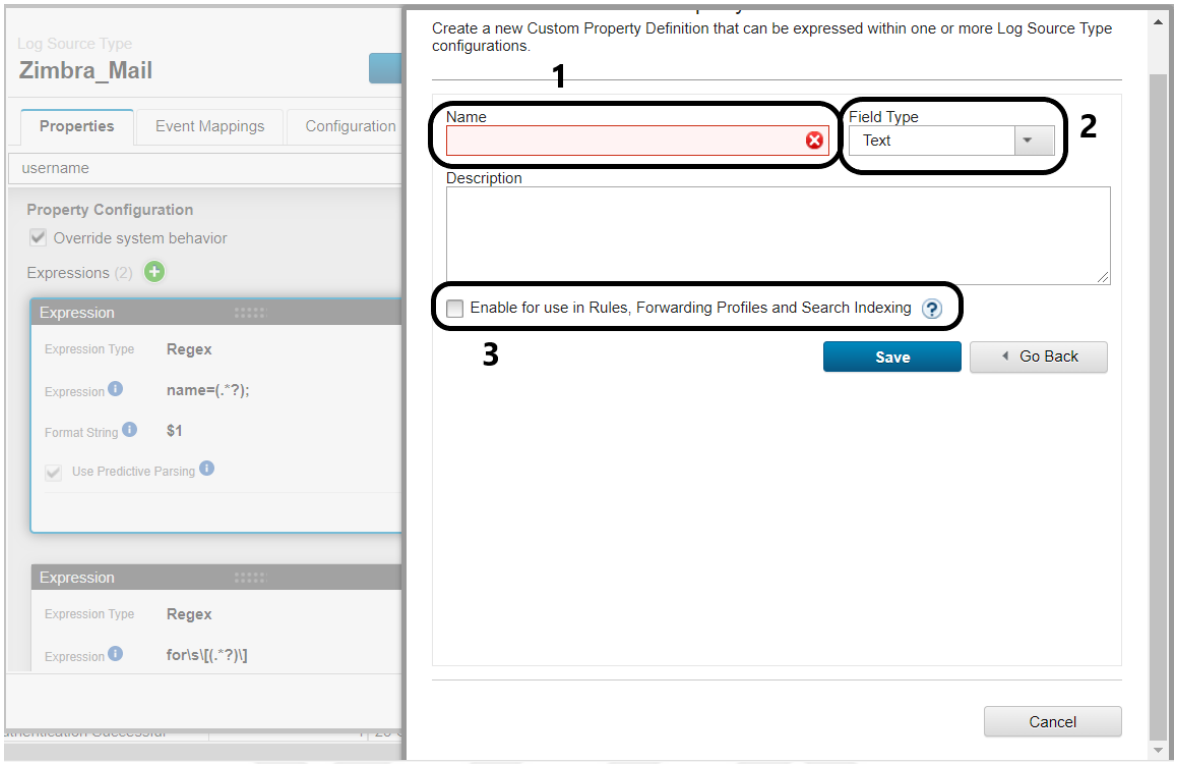
Açılan ekranın bir örneği Şekil 3.6'de yer almaktadır. 1 numaralı kısımda bu DSM için oluşturulmuş varsayılan veya custom olarak eklenmiş parametreler bulunmaktadır. Bu alanda *Expression Type* olarak belirtilen açılır pencere yardımıyla ayrıştırma işlemi için kullanılacak yöntem belirlenir. Bu alanda Regex, JSON, CEF, LEEF, GENERIC LIST, NAME VALUE PAIR, XML seçeneklerinden birisi seçilebilir. Aynı kısımda bulunan *Expression* kutucuğu içerisinde ise belirlenen tip için gerekli tanım yazılır. 2 numaralı alanda bir önceki ekranda seçilen iz kayıtları görüntülenmektedir. 1 numaralı alanda yazılan regex tanımlarına göre bu kısımdaki iz kayıt parçaları boyalı şekilde görülür. 3 numaralı alanda ise oluşturulan parametreler sütunlar halinde görüntülenmektedir. Bu sayfada 4 numaralı alana tıklanarak yeni *Custom Property* ismi verilen parametreler oluşturulabilir. Artı işareti ile açılan ekranın bir örneği Şekil 3.7'de verilmiştir. Bu ekranda mevcutta oluşturulmuş parametrelerden biri seçilebileceği gibi 1 numara ile gösterilen buton yardımıyla yeni parametreler de oluşturulabilir. *Create new* butonuna basıldığında çıkan ekranın bir örneği Şekil 3.8'da gösterilmektedir. Burada 1 numara ile gösterilen alanda parametrenin ismi verilir. 2 numara ile gösterilen alanda parametrenin tipi belirlenir. Bu kısımda text, date, ip, port ve number seçeneklerinden biri seçilebilir. 3 numara ile gösterilen kutucuk seçildiği takdirde ilgili parametre kurallar içerisinde veya indeksli aramalarda kullanılabilir hale gelir.



Şekil 3.6: DSM Editor Ekranları



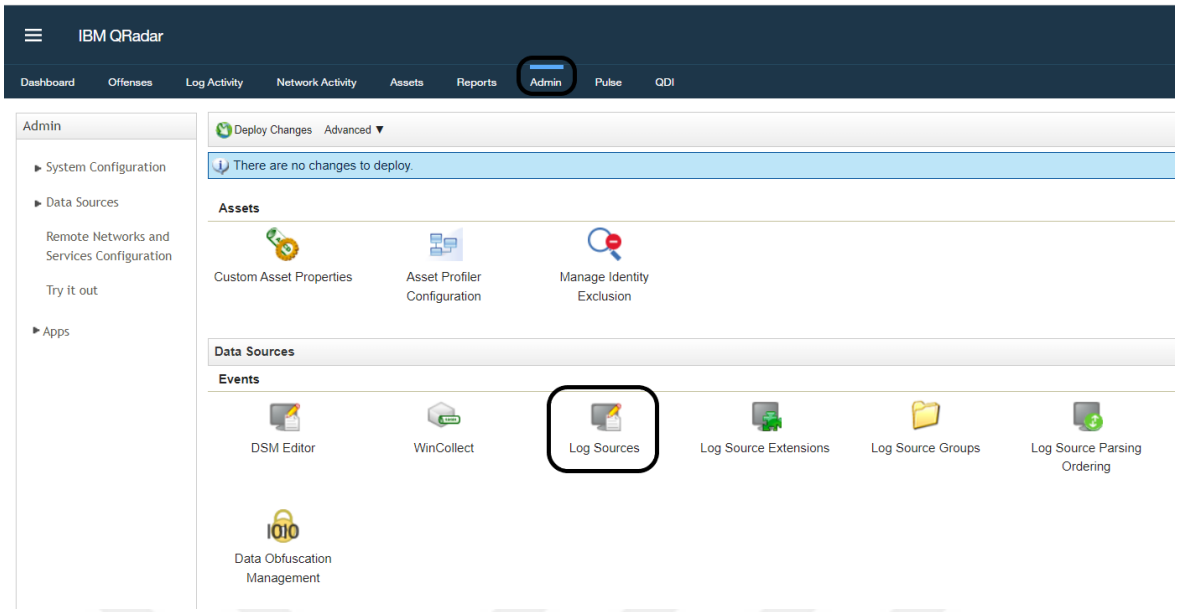
Şekil 3.7: Custom Property seçme ekranı



Şekil 3.8: Yeni Custom Property Oluşturma Ekranı

3.2. Qradar SIEM Üzerinde İz Kayıt Kaynaklarının Oluşturulması

Qradar sistemine gönderilen iz kayıtlarının anlamlandırılabilmesi için uygun şekilde kaynak tanımının yapılması gerekmektedir. Bu sayede SIEM sistemine gönderilen iz kayıtları oluşturulan kaynak altında toplanır. Bu işlem için Şekil 3.9'da görülen Qradar uygulamasının *Admin* sekmesinde *Data Source* menüsü altındaki *Log Sources*'e giriş yapılarak *Create New* seçeneği seçilir. Gelen ekranda ilk önce kaynağın marka ve model bilgisine göre tipi seçilir. Sonraki sayfada kaynaktan hangi iz kayıt toplama yöntemi ile kayıtların alındığı bilgisi seçilmelidir. Sonraki kısımda kaynağın tanımının yapıldığı ekrana geçilir bu alanda kaynak ile ilgili doldurulması gereken bilgiler, bir önceki menüde seçilen kayıt toplama protokolüne göre farklılık göstermektedir. Tablo 3.2'de syslog protokolü için doldurulması gereken parametreler anlamları ile birlikte verilmiştir.



Şekil 3.9: İz Kayıt Kaynağı Oluşturma Ekranına Giriş

Tablo 3.2: Kaynak tanımı için gerekli parametreler

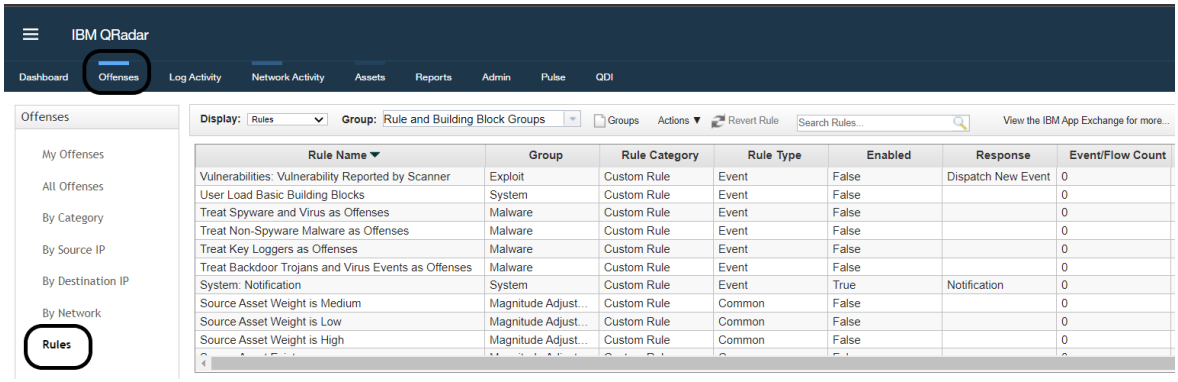
Parametre	**Açıklama**
Name	Kaynağın adı
Description	Açıklaması
Enabled	Kaynağın aktif mi yoksa pasif mi olduğu bilgisi
Groups	Kaynağın grubu(Örneğin Linux sunucular, Mail sunucuları bv.)
Target Event Collector	İz kayıtlarının ulaştığı Qradar Collector sunucusu
Coalescing Events	Ham verisinin tutulma ihtiyacı bulunmayan kaynaklar için performans ve disk alanı iyileştirmesi sağlar. 10 saniye içerisinde aşağıdaki parametreleri aynı olan iz kayıtlarını birleştirir ve tek bir kaynak gibi gösterir. Sadece ilk gelen kaynağın payload bilgisini saklar. ➢ QID ➢ Source IP

	➢ Destination IP ➢ Destination Port ➢ Username
Log Source Identifier	Kaynaktan gelen iz kayıtları içerisinde bulunan tanımlayıcı eşsiz bir değer.(ip adres veya sunucu ismi gibi)
Incoming Payload Encoding	Gelen payload'a hangi tipte encoding uygulanacağını belirten alandır.(Örneğin UTF-8, IBM-500, ISO-8859-15 vb.)

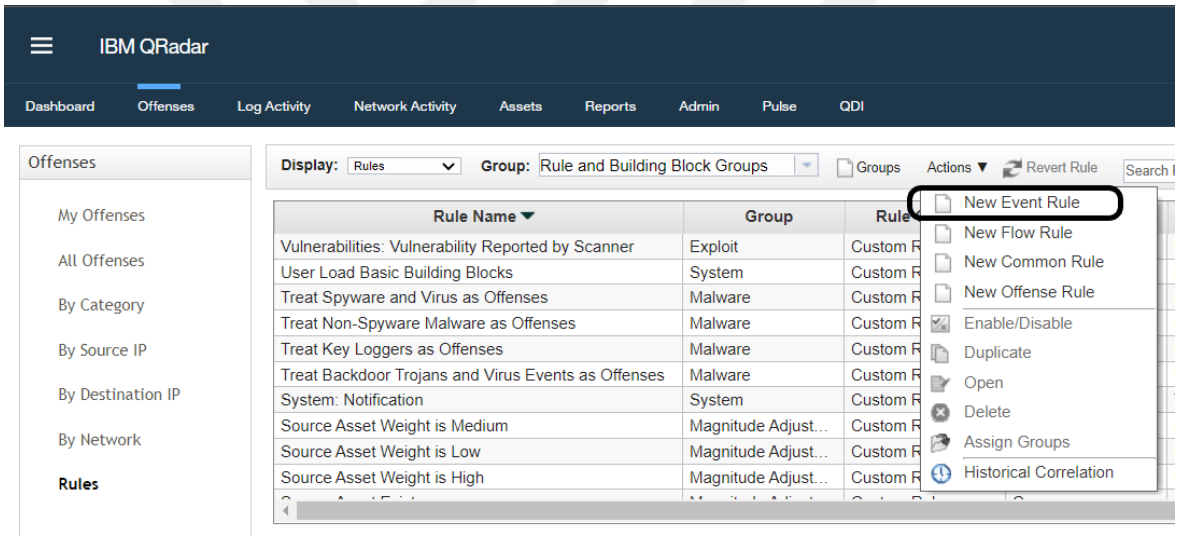
3.3. Qradar SIEM Üzerinde Kural Oluşturma

SIEM sisteminin kurulu olduğu bilgi işlem merkezinde gerçekleşebilecek siber güvenlik olaylarının en hızlı şekilde saptanabilmesi ve hızlı aksiyon alarak gereken önlem adımlarının uygulanabilmesi için kural tanımları yapılır. Bu kuralların tanımlanabilmesi için Şekil 3.10'da görüldüğü gibi Qradar SIEM web arayüzünden *Offenses* sekmesinden *Rules* menüsüne giriş yapılır. Bu ekranda daha önce yazılmış olan veya ürün ile birlikte gelen ön tanımlı kuralların listesi bulunmaktadır. Gelen sayfada Şekil 3.11'de görüldüğü gibi *New Event Rule* seçeneği ile kural oluşturma sihirbazı açılır. Sayfanın görüntüsü Şekil 3.12'de görülmektedir. Sayfanın üst kısmında eklenebilecek ön tanımlı testler yer almaktadır. Yanlarında bulunan "+" simgesi vasıtasıyla istenen test kurala eklenir. Bu testler sayesinde birbirinden farklı filtreler arasında korelasyonlar kurulabilir. Örneğin özellikle belirli bir hedef port numarası üzerine kural yazılması isteniyorsa "*when the destination port one of the following ports"* seçeneği seçilir ve *ports* yazan kısma istenen port numaraları girilir. Ardından ikinci bir test olarak "*when source IP is one of the following IP address"* seçeneği seçilebilir. Eklenen testler birbirlerine AND veya AND NOT kapıları ile bağlanır. Bu sayede her iki teste de uyan iz kayıtları filtrelenmiş olur. En alt kısımda ise oluşturulan kuralın türünün ne olduğu belirlenir. Örneğin zararlı yazılım tespitine yönelik bir kural yazılıyorsa *Malware* seçeneği işaretlenmelidir. *Next* seçeneği ile Şekil 3.13'de görülen sayfaya geçilerek kural tetiklendiğinde yapılması gereken işlemler belirlenir. *Rule Response* menüsü altında kural tetiklendiğinde yeni kural oluşturma, belirli bir adrese e-posta atma, dashboard ekranına alarm oluşturma veya referans setine girdi olarak ekleme gibi aksiyonlar aldırılabilir. Kural tetiklendiğinde oluşan alarmı *Offenses* tabında listeleyip takip edebilmek için Şekil 3.14'de görüldüğü gibi *Dispatch New Event* seçeneği işaretlenerek altında açılan

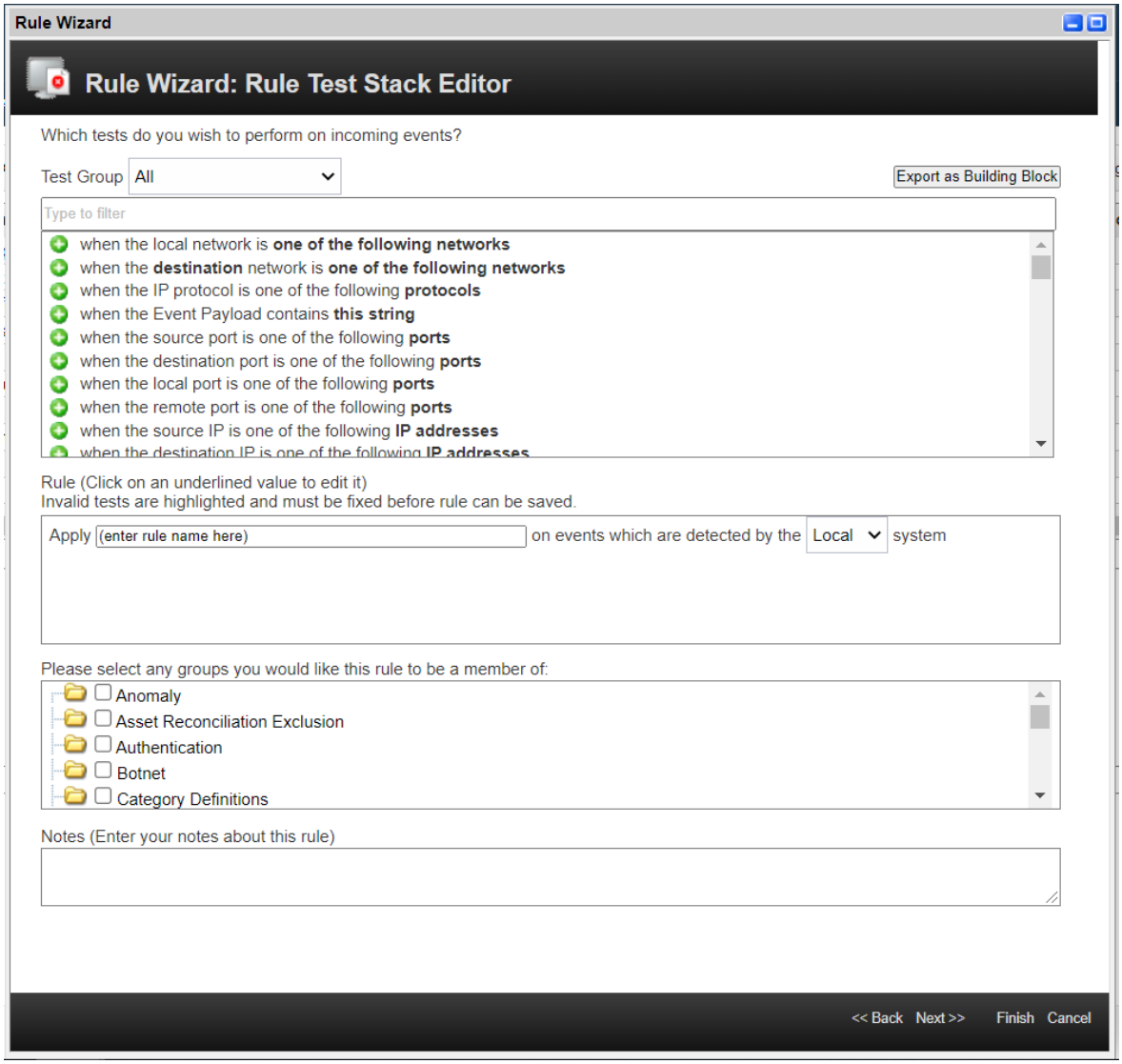
bilgiler doldurulur. Bu kısımda oluşacak alarmın adı, alarmın öncelik ve önem dereceleri ve kategori bilgileri işlenir. *Ensure the dispatched event is part of an offenses* seçeneği ile belirtilen index değerine göre alarmın oluşturulması sağlanır.



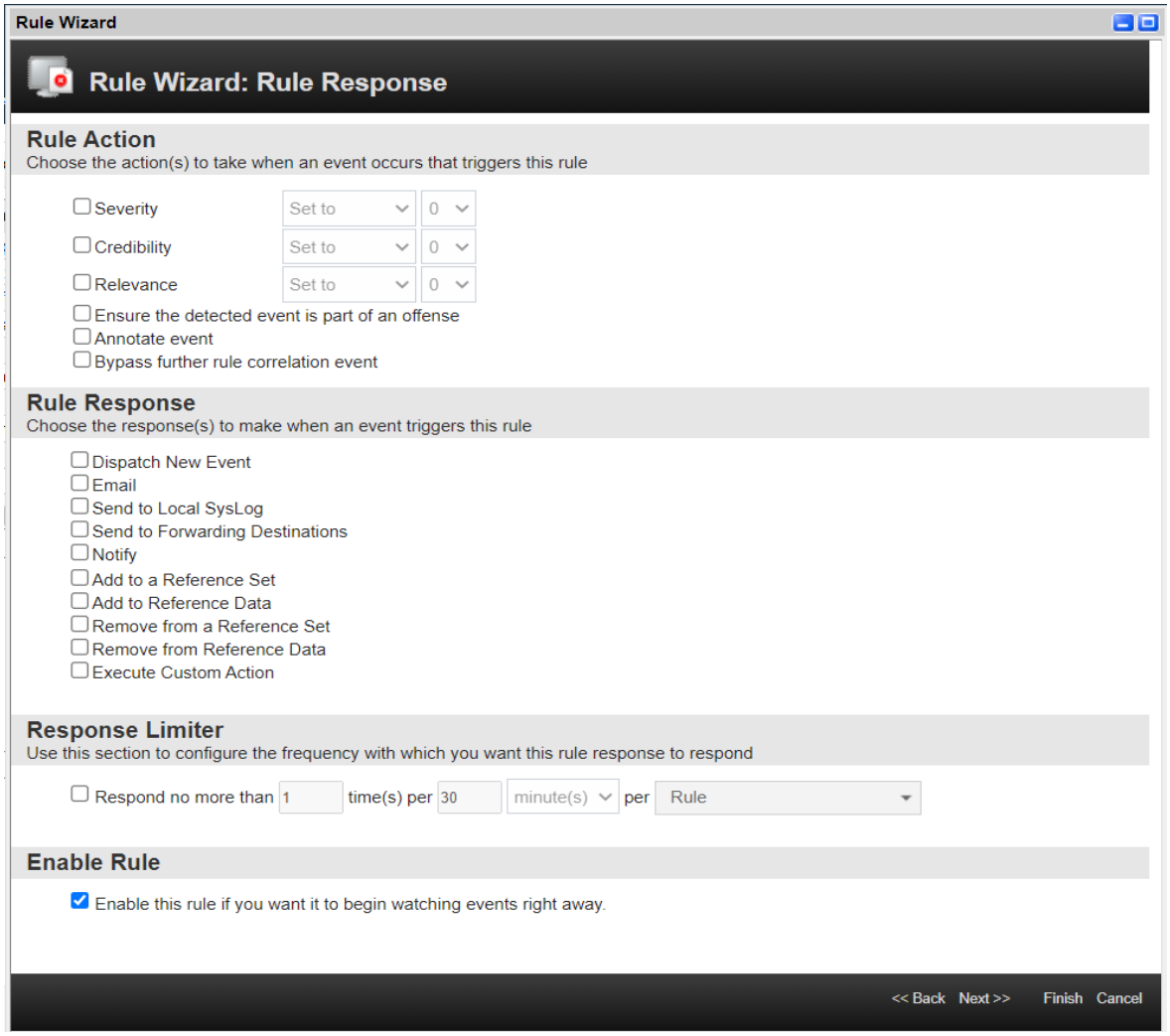
Şekil 3.10: Kural Listesi



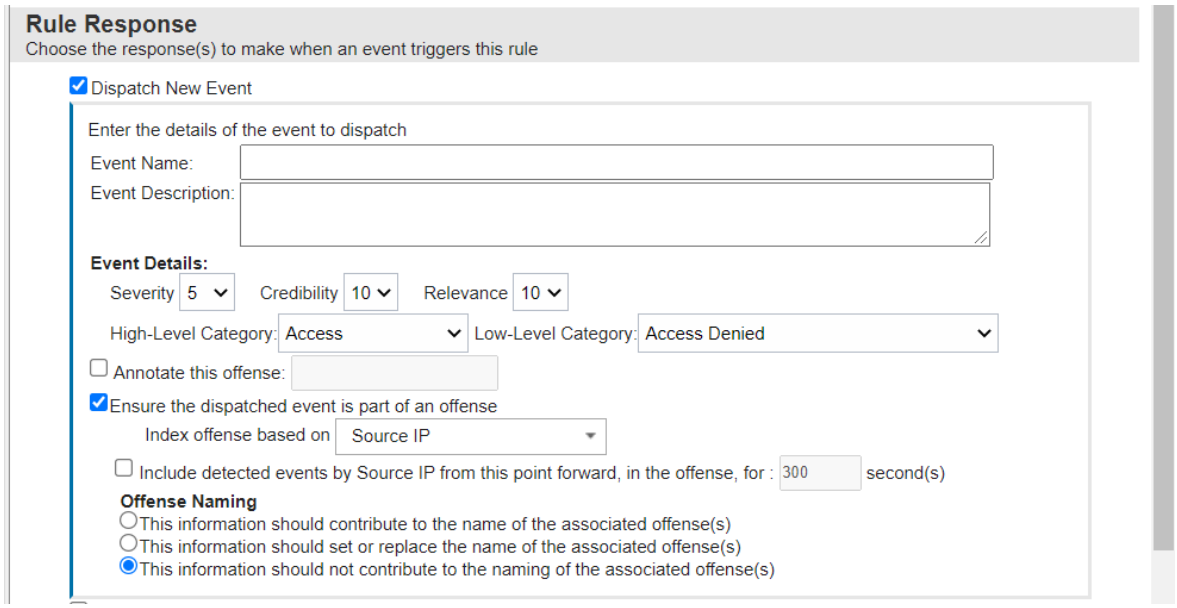
Şekil 3.11: Yeni Kural Oluşturma Ekranına Giriş



Şekil 3.12: Kurala Filtrelerin Eklendiği Bölüm



Şekil 3.13: Kural Tetiklendiğinde Alınacak Aksiyonların Belirlendiği Ekran



Şekil 3.14: Dispatch New Event Aksiyonu

3.4. Kurallar İçin Oluşturulan Use Case Örneği

Bu araştırmada, tespit edilmeye çalışılan siber olaylar için uçtan uça hangi aşamada ne gibi aksiyonların alınması gerektiği ve teknik olarak nelerin yapılması gerektiği bir şablon haline getirilmiştir. Yukarıda açıklanan kural oluşturma adımları izlenerek kurallar yazılmıştır ve bu bilgiler Use Case şablonunda gösterilmiştir. Oluşturulan bu şablon üzerinde gerçekleşen olayın açıklaması, bu olayın tespiti için gereken kural tanımları ve olayın yaşanması durumunda konu hakkında aksiyon alacak gruplar ve yapmaları gereken aksiyonlar belirtilmiştir. Oluşturulan bu şablonun ana hatları ve açıklamaları Tablo 3.3'te yer almaktadır. Yapılan literatür araştırmasında SIEM sistemleri üzerinden olay tepsiti amacıyla yazılmış böyle bir şablona rastlanmamıştır. Şablon özgün olarak oluşturulmuştur.

Tablo 3.3: Use Case şablonu

İsim	Oluşturulan Use Case'i tanımlayacak isim
Amaç/Hedef	Yapılan işin hedefi
Problem Tanımı	Bu use case ile çözülmesi beklenen sorunun tanımı
Gereksinimler	Bu use case'in çalışması için gereklilikler
Tasarım	Yapılan işlem adımlarının teknik anlatımı
Sorumlu Grup	Use case sonucunda tespit edilen olay hakkında sorumlu olan kişi ve ekip
Aksiyon	Sorumlu grubun yapması gereken işlem adımları

4. BULGULAR VE TARTIŞMA

Önceki bölümlerde iz kayıt tipleri, iz kayıt toplama yöntemleri ve uygulama üzerinde bu verilerin nasıl kullanılıp, korelasyona tabi tutulup anlamlı veriler elde edilebileceği anlatılmıştır. Çalışmanın bu bölümünde örnek adli bilişim ve siber güvenlik olayları üzerinden tespit yöntemleri uygulamalı olarak gösterilmiştir.

4.1. Ele Geçirilen Kurumsal E-Posta Hesaplarının Tespiti

Personeller tarafından kullanılan kurumsal e-posta hesaplarının parolaları farklı nedenlerden dolayı ele geçirilebilir. Aşağıda bu senaryolara örnekler verilmiştir.

- Personel, kurumsal e-posta hesabı ve parolası ile kurum dışında internete açık bir web uygulaması üzerinde hesap oluşturabilir. Bu web uygulamasının siber saldırıya uğraması ve parolanın(hash olarak ele geçirilen parolalar da kırılabilir, örneğin "rainbow table" saldırısı) saldırganlar tarafından ele geçirilmesi.
- Personelin, kurumsal e-posta hesabına güvenli olmayan bir bilgisayar üzerinden oturum açması durumunda bilgisayarda bulunabilecek muhtemel zararlı yazılımlar (örneğin "keylogger" zararlı ailesine ait uygulamalar) vasıtasıyla e-posta hesabının parolasının ele geçirilmesi.
- Personelin, phishing saldırısına maruz kalarak e-posta hesap parolasını saldırganların yönettiği sahte bir internet sayfasına girmesi ve parolasının ele geçirilmesi.
- Personel, başka bir e-posta hesabında kullandığı parolayı kurumsal e-posta hesabında da kullanıyor ise bu e-posta hesabının ele geçirilmesi durumunda kurumsal e-posta hesabının da ele geçirilmesi.

Orta ve büyük ölçekli kurumsal yapılarda e-posta hizmetleri genelde kurumlar tarafından on-premise(yerinde) olarak verilmektedir. Mail sunucularının ve uygulamanın yönetimi kurum tarafından yapılır. Bu örnek baz alınarak kurumsal olarak kullanılan açık kaynak kodlu zimbra e-posta uygulamasından alınacak iz kayıtları yardımıyla IBM'in Qradar SIEM ürünü üzerinde yazılacak kurallar ile muhtemel e-posta hesap ele geçirme senaryoları incelenmiştir.

4.1.1. Zimbra iz kayıtlarının SIEM sistemine aktarımı

Yapılan çalışmada Centos işletim sistemi üzerinde çalışan Zimbra uygulamasının iz kayıtları R-syslog uygulaması aracılığı ile SIEM sistemine aktarılmıştır. Öncelikle Centos işletim sistemi üzerinde Rsyslog paketleri kurulmuştur. Sonrasında sunucu içerisinde */etc/rsyslog.conf* dosyası Tablo 4.1'de gösterilen konfigürasyona uygun olarak doldurularak iz kayıtlarının hedef SIEM sunucusuna gönderimi sağlanmıştır.

Bu çalışmada kullanılan örnek konfigürasyon dosyası Tablo 4.1'de gösterilmiştir. Bu konfigürasyon dosyası incelendiğinde FILE0 etiketi ile gösterilen kısımda işletim sisteminin denetim iz kayıtlarının */var/log/audit/audit.log* isimli dosyadan okunduğu görülmektedir. FILE1 etiketi ile gösterilen kısımda Zimbra uygulamasının posta kutusu aktivitelerinin */opt/zimbra/log/mailbox.log* isimli dosyadan okunduğu görülmektedir. Her iki iz kaydının facility değeri local3 olarak belirlenmiştir. Konfigürasyon dosyasının son satırında facility değeri local3 olan tüm iz kayıtlarının 192.168.150.50 IP adresine TCP protokolü üzerinden gönderildiği görülmektedir (tek @ işareti UDP, çift @ işareti TCP olarak gönderildiğini göstermektedir). Bu ip adresi Qradar SIEM sisteminin IP adresidir.

Tablo 4.1: Rsyslog Konfigürasyon Örneği

```
# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
#$OmitLocalLogging on
$ModLoad imfile
$ModLoad imjournal
# File to store the position in the journal
#$IMJournalStateFile imjournal.state

#FILE0
$InputFileName /var/log/audit/audit.log
$InputFileTag audit.log
$InputFileStateFile stat-FILE0
$InputFileSeverity notice
$InputFileFacility local3
```

```
$InputRunFileMonitor

#FILE1
$InputFileName /opt/zimbra/log/mailbox.log
$InputFileTag mailbox.log
$InputFileStateFile stat-FILE1
$InputFileSeverity notice
$InputFileFacility local3
$InputRunFileMonitor

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                 /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
# The authpriv file has restricted access.
authpriv.*                              /var/log/secure
# Log all the mail messages in one place.
mail.*                                  -/var/log/maillog
# Log cron stuff
cron.*                                  /var/log/cron
# Everybody gets emergency messages
*.emerg                                 :omusrmsg:*
# Save news errors of level crit and higher in a special file.
uucp,news.crit                          /var/log/spooler
# Save boot messages also to boot.log
local7.*                                /var/log/boot.log

# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
```

```
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
# ### end of the forwarding rule ###
local3.*    @@192.168.150.50
```

Yukarıda oluşturulan konfigürasyon ile SIEM sistemine gönderilen örnek bir e-posta iz kaydı Tablo 4.2'de gösterilmiştir. Bu örnekteki önemli bazı alanların anlamları aşağıdaki gibidir.

Jan 22 15:39:55: Satırın başında bulunan tarih ve saat rsyslog servisi tarafından basılmıştır.

Zimbra: Bu parametre sunucunun ismini(hostname) ifade etmektedir.

Mailbox.log: Konfigürasyonda ilgili dosyadan okunup gönderilen iz kayıtları için yazılmış etiket değeridir.

2022-01-22 15:39:53,326: İz kaydının oluştuğu tarih ve saat değeridir.

INFO: İz kaydının önem düzeyini ifade eder.

Name: İşlemi yapan e-posta adresi bu alanda görülür.

İp: Mail sunucusunun IP adresidir.

Oip: İşlem yapılan e-posta hesabının bağlantı kurduğu kaynak IP adresidir.

Account: Yapılan işlem ile ilgili bilgilerin bulunduğu alandır.

From: Mail gönderiminin yapan hesap adı.

Status: Mail gönderiminin durumunu gösterir.

Bu rsyslog konfigürasyonu sonucu oluşan ve Qradar sistemine gönderilen örnek iz kayıtlarının iki tanesi Tablo 4.2'de gösterilmiştir. Bu tabloda görülen kuyruğa alındı iz kaydının oluşması e-postanın gerçekten gönderilip gönderilmediği konusunda kesin bir sonuç vermemektedir. E-posta gönderildi örneğinde görülen *status=sent* ibaresini içeren iz kaydının oluşması durumunda e-posta'nın gönderildiği anlaşılabilir. Ancak bu iz kaydı içerisinde de sadece alıcı e-posta adresi bilgisi bulunmaktadır. Gönderici e-posta adresi bilgisi yoktur.

Tablo 4.2: Zimbra Mail Uygulaması İz Kayıt Örneği

Başarılı Oturum Açma
"<157>Jan 22 15:39:55 zimbra mailbox.log 2022-01-22 15:39:53,326 INFO [Pop3SSLServer-3] [name=cagrifanuscu@test.com;ip=192.168.150.50;oip=192.168.150.10;cid=348902;] account - Authentication successful for user: cagrifanuscu@test.com"
Başarısız Oturum Açma Denemesi
"<157>Jan 22 15:39:55 zimbra mailbox.log 2022-01-22 15:39:53,516 INFO [ImapSSLServer-982] [ip=192.168.150.50;oip=192.168.150.10;via=com.samsung.android.email.provider,192.168.150.50(nginx/1.20.0);ua=Zimbra/8.8.15_GA_4125;cid=348903;] account - Error occurred during authentication: authentication failed for [cagrifanuscu@test.com]. Reason: invalid password."
Mail Gönderimi İçin Kuyruğa Alındı
"<157>Jan 29 17:25:52 zimbra zimbra.log 2022-01-29T17:25:45.356099+03:00 zimbra amavis[22616]: (22616-02) KvNzuGkXBG2v FWD from <cagrifanuscu@test.com> -> <cagrifanuscu2@test.com>, BODY=7BIT 250 2.0.0 from MTA(smtp:[127.0.0.1]:10030): 250 2.0.0 Ok: queued as 4C3F4C1D8F44"
Mail Gönderildi
"<157>Jan 29 17:25:52 zimbra zimbra.log 2022-01-29T17:25:45.745751+03:00 zimbra postfix/smtp[9486]: 726A6C1D8F3F: to=<cagrifanuscu2@test.com>,

relay=192.168.150.50[192.168.150.50]:25, delay=0.28, delays=0/0.01/0.01/0.26, dsn=2.0.0, status=sent (250 2.0.0 3dvrhm9c8f-1 Message accepted for delivery)”

4.1.2. Qradar SIEM üzerinde zimbra iz kayıtlarının anlamlandırılması

Rsyslog servisi ile Qradar SIEM sunucusuna aktarılan iz kayıtlarının kurallarda ve arama işlemlerinde kullanılabilmesi için bir dizi işlem uygulanmıştır. Zimbra uygulaması için Qradar üzerinde ön tanımlı bir kaynak tipi tanımı olmadığından manuel olarak “Zimbra_Mail” isimli yeni bir kaynak tipi oluşturulmuştur.

Zimbra e-posta iz kayıtlarının kurallar ve aramalarda efektif bir şekilde kullanılabilmesi için DSM Editör üzerinde parse edilen diğer alanlar ve bu alanların parse edilmesi için gerekli regex tanımları Tablo 4.3’te yer almaktadır.

Tablo 4.3: Zimbra Mail İz Kayıt Parametreleri

Parametre	**Regex İfadesi**	**Format String**
Source IP	oip=(\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})	$1
Username1	name=(.*?);	$1
Username2	for\s\[(.*?)\]	$1
Failure Reason	Reason:\s(.*?)\.	1
Mail_from	from\s\<(.*?)\>\s	1
Mail_to	\-\>\s\<(.*?)\>\,	1
Status	Status=(.*?)\s	1

4.1.3. Qradar SIEM üzerinde mail sunucu kaynağının oluşturulması

Qradar üzerinde kaynakların otomatik olarak keşfedilmesi özelliği aktif ise sunucuya yönlendirilen iz kayıtlarının içeriği ön tanımlı kaynak tanımlarının şablonları ile kıyaslanarak kaynağın tipi ve kaynak tanımlayıcısı (IP adresi veya iz kayıtlarının içerisinde bulunan sunucu adı) otomatik olarak belirlenerek kaynak oluşturulur. Bu çalışma kapsamında kaynak tanımı manuel olarak yapılmıştır. Qradar yönetim arayüzünde *Admin* sekmesinde *Data Sources* menüsü altında *Log Sources* kısmına giriş yapılarak Tablo 4.4’de verilen bilgiler doğrultusunda kaynak tanımı yapılmıştır.

Tablo 4.4: Zimbra Mail Sunucusu Kaynak Tanımı

Parametre	Değer
Name	Zimbra @ 192.168.150.50
Log Source Type	Zimbra_Mail
Protocol Type	Syslog
Target Event Collector	Qradar-console
Coalescing Events	Off
Log Source Identifier	zimbra

4.1.4. Ele geçirilen e-posta hesaplarının tespiti için oluşturulan kurallar

Sadece Türkiye'de personeli bulunan bir kurumun personelinin kurumsal e-posta hesaplarına normal şartlar altında ISP'lerin Türkiye'ye tanımlı IP adreslerinden girmeleri beklenir. Bu ip adresleri RIPE firması tarafından dağıtılır. Bu IP adresleri Qradar ürünü içerisinde ön tanımlı olarak bulunmaktadır. Eğer bir personel yurtdışında bir IP adresinden bağlantı gerçekleştirmiş ise bunun bilinen iki açıklaması olabilir. Birincisi oturum açma işleminin yurtdışından gerçekleşmesi, diğeri ise personelin oturum açtığı bilgisayarında VPN kullanması. Bu bağlamda e-posta hesabına yurt dışından erişim olması şüpheli bir durum olarak değerlendirilip incelenebilir.

4.1.5. Tespit için oluşturulan kural ve use case örneği

Çalışmada bahsedilen Use Case şablonuna uygun olarak ilgili kural için oluşturulmuş use case örneği Tablo 4.5'te yer almaktadır.

Tablo 4.5 Ele Geçirilen Kurumsal Hesapların Tespiti

İsim	Kural-0001 Ele Geçirilen Kurumsal Hesapların Tespiti
Amaç/Hedef	Ele geçirilen kurumsal hesapların en kısa zamanda tespit edilmesi, başka kullanıcılara bu hesap üzerinden phishing veya spam e-posta atılmasının engellenmesi ve e-posta hesabının kurtarılması.
Problem Tanımı	Kurumsal e-posta hesapları saldırı aktörleri tarafından sürekli bir hedef halindedir. Bu e-posta hesapları ele geçirilerek hem posta kutusundaki kurumsal bilgiler alınmaya çalışılır hemde bu e-posta kullanılarak başka hesaplara oltalama veya spam e-postalar atılır. Bu işlemler sonucunda

	kurumsal bilgi ifşasının yanı sıra kurumun itibarinda zedelenmeler ve kanunlar/regülasyonlar karşısında cezalar ile karşılaşılabilir.
Gereksinimler	Bu sorunun çözümü için gerekli bilgiler aşağıdadır: - Kurumsal e-posta uygulamasından kullanıcı otantikasyonu ve e-posta gönderim iz kayıtlarının SIEM sistemine aktarılması. - İz kayıtlarının içerisinde en az kaynak IP adresi, kullanıcı hesap adı, e-posta gönderen hesap adı, e-posta alan hesap adı ve yapılan işlemin çeşidi (başarılı/başarısız oturum açma veya e-posta gönderimi vb) - İz kayıtları içerisinde *username* parametresine e-posta hesap adının, *source IP* parametresine oturum açma isteğinin gönderildiği kaynak IP adresinin, *mail_from* parametresine e-posta gönderen hesap adının ve *mail_to* parametresine e-posta alan hesap adının eşleştirilmesi. - Türkiye'de kullanılan IP adreslerinin tespit edilmesi. - Yurtdışında bulunan personelinin olup olmadığının tespit edilmesi. - VPN kullanımının olup olmadığının tespit edilmesi. - Personellerin saatlik e-posta gönderme sayılarının istatistiğinin çıkarılması.
Tasarım	Öncelikle yurt dışından oturum açan kullanıcı hesaplarının tespiti için gerekli kural yazılır. **Kural Adı:** Yurt Dışından Oturum Açan Kullanıcı Hesaplarının Tespiti **Filtreler;** **AND** Zimbra kaynağından gelen iz kayıtları, **AND** *QID* değeri XXXXX (Başarılı oturum açma event name'ine karşılık gelen ID değeri) olan iz kayıtları, **AND NOT** iz kayıtlarının içerisindeki kaynak IP adresi Türkiye olan kayıtlar, **AND NOT** hesap ismi *Yurt Dışında Çalışan Personeller* referans listesinde olan hesaplar. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *username* parametresinde bulunan hesap adına göre kural tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** - Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.

	- Ortaya çıkan hesap isimlerinin *Yurt Dışından Oturum Açan Hesaplar* referans listesine girdi olarak yazılır. İlk oluşturulan kural güvenlik analistinin incelemelerini yapması için yeterli şüpheyi oluşturur. Ancak aşağıda yazılan ikinci kuralın tetiklenmesi olayın önem seviyesinin daha da yükseltir. Kural açıklamaları aşağıdaki gibidir. **Kural Adı:** Yurt Dışından Oturum Açan ve Spam Mail Atan Hesapların Tespiti **Filtreler;** **AND** Zimbra kaynağından gelen iz kayıtları, **AND** *QID* değeri XXXXXX (Mail Gönderildi event name için ID değeri) olan iz kayıtları, **AND** *mail_from* parametresinin aldığı değer *Yurt Dışından Oturum Açan Hesaplar* referans seti içerisinde geçen iz kayıtları, **AND** 1 saat içerisinde aynı *mail_from* parametre değerine sahip 100'den fazla kayıt göründüğüne, Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *username* parametresinde bulunan hesap adına göre kural tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** - Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. İkinci kural, ilk kuralın ve üzerine başka bir şüpheli davranış oluşması sonucu ortaya çıktığı için ilkine göre daha öncelikli olarak incelenmesi gerekir. İkinci kurulda kullanılan e-posta adedi davranış analizleri sonucu ortaya çıkacak olan değerdir.
Sorumlu Grup	Güvenlik Analisti, E-posta Sistem Yöneticisi, Anti-virus Sistem Yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gerekli aksiyonların alındığından emin olur. E-posta hesabının sahibi olan

	personelle iletişime geçerek parola sızıntısının neden kaynaklanmış olabileceği konusunda araştırmalar yapar. - **E-posta Sistem Yönetici:** Ele geçirildiğinden şüphelenilen E-posta hesaplarını en hızlı şekilde bakım moduna alır. Kullanıcı ile iletişime geçerek e-posta parolasının güvenli bir şekilde yeniden oluşturulmasını sağlar. - **Anti-Virus Sistem Yöneticisi:** Eğer parolanın kullanıcı bilgisayarında bulunan bir zararlı yazılım aracılığı ile sızdığı yönende şüpheler oluşursa, bilgisayar üzerinde kurumsal anti-virus yazılımının olup olmadığını ve güncelliğini teyit eder. Tüm bilgisayarda anti-virus taraması yaparak zararlı yazılımlarını varlığını tespit eder ve temizler.

4.2. Bilgi İşlem Cihazı Üzerinde Zararlı Yazılım Aktivitelerinin Tespiti

Kurum personelinin kullandığı bilgi işlem varlıklarına birçok farklı etken sebebiyle zararlı yazılmların bulaşması mümkündür. Bunlardan bazıları aşağıdaki gibi sıralanabilir.

- Personelin internet sayfalarında gezinirken zararlı yazılımlara maruz kalması olası bir durumdur. Bu durumun önüne geçebilmek için kurumsal proxy sunucuları kurulabilir veya personelin internete bağlanabildiği bilgisayar ile kurum ağına bağlanabildiği bilgisayar birbirinden ayrılabilir. Bu çözümler uygulanmış olsa dahi personelin internetten indirdiği bir dosyadan bilgisayarına zararlı bulaştırması mümkündür.

- Bir diğer olasılık ise personelin taşınabilir bellek kullanırken bilgisayarına zararlı yazılım bulaştırmasıdır. Bu durumda network veya güvenlik cihazlarından trafik geçmeyeceği için tespiti daha zordur.

- Personelin e-posta adresine gönderilen phishing e-postalarının ekinde bulunan veya e-posta içerisinde bulunan zararlı dosya içeren linkler aracılığı ile personel bilgisayarlarına zararlı yazılımların kurulması mümkündür.

Yukarıda bahsedilen durumların gerçekleşmesi ve zararlı yazılımın bilgisayara ulaşması durumunda önündeki bir diğer engel ise antivirüs yazılımlarıdır. Bu yazılımlar sayesinde kurum bilgisayarlarına bulaşan zararlı yazılımlar ilk indirilme aşamasında veya ilk harekete geçme anlarında tespit edilip silinebilir veya karantinaya alınarak alarm oluşturabilir.

4.2.1. Tespit için gerekli iz kayıtlarının toplanması

Bilgi işlem cihazına bulaşan zararlı yazılımın tespiti için ilk bakılması gereken kısım bilgisayar üzerinde antivirüs yazılımının olup olmadığıdır. Antivirüs yazılımlarının oluşturduğu iz kayıtları yaşanan olay ile ilgili zengin bilgiler içerebilir. Tespit için kullanılabilecek bir diğer kayıt çeşidi ise windows işletim sisteminin güvenlik denetim iz kayıtlarıdır. Kurumsal yapılarda domain üzerinden politika ile açılan denetim kayıtları yaşanan siber güvenlik olaylarının tespiti için önemli veriler içerebilir. Bu iz kayıtlarının nasıl toplanabileceği ve içerdikleri verilerin anlamları aşağıda incelenmiştir.

Bu çalışmada iz kayıtları incelenecek olan antivirüs yazılımı Mcafee firmasının ePolicy Orchestrator ürünüdür. Bu ürün merkezi bir yönetim sistemidir ve son kullanıcı bilgisayarlarından toplanan iz kayıtlarını belirli bir formatta tutarak SIEM sistemlerine aktarabilir. Bu çalışmada ePolicy Orchestrator iz kayıtları MsSQL veri tabanı üzerinde ürünün oluşturduğu bir tablodan okunacaktır. SIEM'e aktarılması istenen olay kayıtlarının bulunduğu tablo adı *EPOEvents* olarak belirlenmiştir. Veri tabanı üzerinde bu tabloda okuma yetkisine sahip bir kullanıcı oluşturulmuştur.

Zararlı yazılım tespiti için kullanılacak bir diğer kaynak ise personelin kullandığı bilgisayarların Microsoft Windows Security Event Log'larıdır. Bu çalışmada son kullanıcı bilgisayarına kurulan wincollect ajanı ile iz kayıtları toplanmıştır. Ancak kurumsal altyapılarda Windows Event Forwarding (WEF) yöntemi ile wincollect ajanının birlikte kullanımı daha verimli sonuçlar ortaya koyabilir.

Bazı zararlı yazılımlar ağ üzerinde yatayda veya dikeyde yayılarak daha fazla sisteme bulaşıp daha fazla veriye ulaşmak, daha fazla sistemi şifreleyecek fidye yazılımlarını yaymak veya kuruma daha fazla zarar verebilmek için faaliyetler gerçekleştirebilir. Bu faaliyetlerin tespiti bilgi işlem cihazında faaliyet gösteren zararlı yazılımların tespitini kolaylaştırmaktadır.

4.2.2. Qradar SIEM üzerinde yapılan işlemler

McAfee ePolicy Orchestrator kaynağından iz kayıtlarını SIEM sisteminin çekebilmesi için yapılması gereken kaynak tanımında kullanılan parametreler Tablo 4.6'da yer almaktadır.

Tablo 4.6: McAfee EPO Kaynak Tanımı

Parametre	Değer
Genel Ayarlar	
Name	McAfee-EPO @ 192.168.150.60
Log Source Type	McAfee ePolicy Orchestrator
Protocol Type	JDBC
Target Event Collector	qradar-console
Coalescing Events	No
Protocol Ayarları	
Log Source Identifier	mcafeeepo
Database Type	MSDE
Database Name	ePO_MCAFEEEPO_Events
IP or Hostname	192.168.150.60
Port	1433
Username	qradaruser
Table Name	dbo.EPOEvents
Select List	*
Compare Field	AutoID
Polling Interval	10
Use NTLMv2	Yes

Tanımı yapılan kaynaktan gelen iz kayıtlarının kurallarda ve aramalarda kullanılabilmesi için custom properties'ler tanımlanmıştır. Yapılan bu tanımlardan bazıları tablo 4.7'de gösterilmiştir.

Tablo 4.7: McAfee EPO İz Kayıt Parametreleri

Parametre	**Regex İfadesi**	**Format String**
Action	ThreatActionTaken:\s+"(.*)"\s+ThreatHandled	1
Action Result	ThreatHandled:\s"([^"]+)\"	1
Agent GUID	AgentGUID:\s"([^"]+)\"	1
Analyzer Hostname	AnalyzerHostName:\s"(\S+)"	1
Analyzer IP	AnalyzerIPV4:\s"(\S+)"	1
Analyzer MAC	AnalyzerMAC:\s"(\S+)"	1
Detected UTC	DetectedUTC:\s+"(\d{4}\-(((0)[0-9])|((1)[0-2]))\-([0-2][0-9]|(3)[0-1])\s(?:[01]\d|2[0123]):(?:[012345]\d):(?:[012345]\d.\d+))	1
Filename	TargetName:\s"([^"]+)\"	1
File Path	TargetPath:\s"([^"]+)\"	1
Source Process Name	SourceProcessName:\s+"(.*?)"	1
Threat Name	ThreatName:\s+"(.*?)"	1
Threat Type	ThreatType:\s"(\S+)"	1

Kurum içerisinde kullanılan Windows işletim sistemine sahip bilgi işlem cihazlarının iz kayıtları Wincollect veya MSRCP gibi yöntemler ile SIEM sistemine aktarılmıştır. Aktarılan veriler içerisinde kurallarda ihtiyaç duyulan parametreler regex yöntemi ile ayrıştırılmış ve gerekli event mapping işlemleri yapılmıştır.

Kurum ağında bulunan ve farklı vlanlar arasındaki trafiği denetleyen kurumsal güvenlik duvarı cihazının iz kayıtları SIEM sistemine aktarılmış, gerekli parametreler ayrıştırılmış ve event mapping işlemleri yapılmıştır.

4.2.3. Tespit için oluşturulan kural ve use case örneği

Çalışmada anlatılan Use Case şablonuna uygun olarak ilgili kural için oluşturulmuş use case örnekleri tablo 4.8,4.9,4.10 ve 4.11'da gösterilmiştir.

Tablo 4.8 Bilgi İşlem Cihazı Üzerinde Zararlı Yazılım Aktivitelerinin Tespiti

İsim	Kural-0002 Bilgi İşlem Cihazı Üzerinde Zararlı Yazılım Aktivitelerinin Tespiti
Amaç/Hedef	Kurumsal bilgisayar sistemlerine bulaşan zararlı yazılımların tespit edilmesi ve en kısa sürede bu tehdidin ortadan kaldırılması
Problem Tanımı	Kurum içerisinde personelin çalışması için tahsis edilen bilgisayarlara bulaşan bir zararlı yazılım olup olmadığı tespit edilmelidir. Bu zararlıların kurum içerisinde yayılarak başka bilgisayarlara da bulaşabileceği göz önüne alınarak en kısa sürede müdahale edilmelidir. Bu gibi zararlılar kurumsal bilgisayarlardaki gizli verileri ele geçirerek veya bu verileri şifreleyip fidye isteyerek kuruma zarar verebilirler.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdadır: - Personelin kullandığı tüm bilgisayarlar kurumun kullandığı domaine alınmış olmalıdır. - Personelin kullandığı kurum bilgisayarlarının güvenlik olay kayıtları SIEM sistemine aktarılmalıdır. - Aktarılan iz kayıtları içeirisinde son kullanıcı bilgisayarının IP adresi, bilgisayar adı, EventID değeri, Image, Process Commandline, Message, username gibi parametrelerin tanımlanmış olması gerekmektedir. - Domain Controller üzerinden kurum bilgisayarlarına basılan aşağıdaki aktif dizin grup politikaları aktif hale getirilmelidir. • Group Policy: Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation • Group Policy: Computer Configuration\ Administrative Templates\ System\ Audit Process Creation\ Include Command Line

	• Group Policy: Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell\Turn On Module Logging • Group Policy: Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell\Turn On PowerShell Script Block Logging
Tasarım	Son kullanıcı bilgisayarlarından gelen iz kayıtları içerisinde zararlı yazılım aktivitelerinin tespiti yapılmalıdır. Bu tespitler için bir dizi kural yazılabilir. Bunlardan birkaç örnek aşağıdaki gibidir. **Kural Adı:** BadRabbit Fidye Yazılımının Tespiti **Filtreler;** **AND** *Log Source Type* değeri *Microsoft Windows Security Event Log* olan iz kayıtları, **AND** *EventID* parametresi 4688 değerini alan iz kayıtları, **AND** *Image* parametresi içerisinde *\schtasks.exe* değerini barındıran iz kayıtları, **AND** *Process CommandLine* parametresi ((*C:\WINDOWS\system32* **AND** *viserion* **AND** */Create*) **OR** (*C:\WINDOWS\system32* **AND** *drogon* **AND** */Create*) **OR** (*C:\WINDOWS\system32* **AND** *rhaegal* **AND** */Create*)) değerlerini içeren iz kayıtları. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *hostname* parametresinde bulunan bilgisayar adlarına göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** - Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** Mimikatz Aracı ile Kullanıcı Otantikasyon Bilgilerinin Elde Edilmesine Yönelik Faaliyetlerin Tespiti **Filtreler;** **AND** *Log Source Type* değeri *Microsoft Windows Security Event Log* olan iz kayıtları,

	AND *EventID* parametresi 4688 değerini alan iz kayıtları, **AND** *Image* parametresi içerisinde (*\schtasks.exe* **OR** *\powershell.exe*) değerini barındıran iz kayıtları, **AND** *Process CommandLine* parametresi (*schtasks* **AND** sekurlsa::LogonPasswords) değerlerini içeren iz kayıtları. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *hostname* parametresinde bulunan bilgisayar adlarına göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** Windows Hash Veritabanını Ele Geçirmeye Yönelik Faaliyetlerin Tespiti **Filtreler;** **AND** *Log Source Type* değeri *Microsoft Windows Security Event Log* olan iz kayıtları, **AND** *EventID* parametresi 4104 değerini alan iz kayıtları, **AND** *Message* parametresi içerisinde (*windows\system32\config\SAM* **OR** *windows\system32\config\SYSTEM* **OR** *ntds.dit* **OR** *win32_shadowcopy*) değerini barındıran iz kayıtları, Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *hostname* parametresinde bulunan bilgisayar adlarına göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** Invoke-TheHash Aracı Kullanılarak Yapılan Pass the Hash Saldırı Tespiti **Filtreler;** **AND** *Log Source Type* değeri *Microsoft Windows Security Event Log* olan iz kayıtları,

	AND *EventID* parametresi 4688 değerini alan iz kayıtları, **AND** *Image* parametresi içerisinde ((*Invoke-SMBEnum.ps1* **AND** *hash*) **OR** (*Invoke-SMBExec.ps1* **AND** *hash*) **OR** (*Invoke-SMBClient.ps1* **AND** *hash*) **OR** (*Invoke-WMIExec.ps1* **AND** *hash*)) değerini barındıran iz kayıtları, Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *hostname* parametresinde bulunan bilgisayar adlarına göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik Analisti, Aktif Dizin Yöneticisi, Antivirüs Sistem Yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Tespit edilen cihazın sahibi ile iletişim kurar ve konu hakkında bilgilendirir. - **Anti-Virus Sistem Yöneticisi:** Tüm bilgisayarda antivirüs taraması yaparak zararlı yazılımların varlığını tespit eder ve temizler. Anti-virus yazılımının güncellenmiş olduğundan emin olur. - **Aktif Dizin Yöneticisi**: Gerekli güvenlik testlerinin ve yasal zorunlulukların tamamlanması sonrasında ilgili bilgisayara format atar. Gerekli işletim sistemi güvenlik güncellemelerini yapar.

Tablo 4.9 Bilgi İşlem Cihazı Üzerinde Silinemeyen Zararlı Yazılım Tespiti

İsim	Kural-0003 Bilgi İşlem Cihazı Üzerinde Silinemeyen Zararlı Yazılım Tespiti
Amaç/Hedef	Kurumsal bilgisayar sistemlerine bulaşan zararlı yazılımların tespit edilmesi ancak antivirus yazılımı tarafından bu zararlının etkisiz hale getirilememesi durumlarını tespit etmek amaçlanmıştır.
Problem Tanımı	Kurum içerisinde personelin çalışması için tahsis edilen bilgisayarlara bulaşan bir zararlı yazılım olup olmadığı tespit edilmelidir. Bu

	zararlıların kurum içerisinde yayılarak başka bilgisayarlara da bulaşabileceği göz önüne alınarak en kısa sürede müdahale edilmelidir. Bu gibi zararlılar kurumsal bilgisayarlardaki gizli verileri ele geçirerek veya bu verileri şifreleyip fidye isteyerek kuruma zarar verebilirler.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdaki gibidir. - Personelin kullandığı tüm bilgisayarlarda kurumsal antivirus yazılımı kurulu olmalı ve düzenli olarak güncellemeleri yapılmalıdır. - Kurumsal antivirus yazılımının son kullanıcılardan topladığı veriler SIEM sistemine aktarılmalıdır. - Aktarılan iz kayıtları içerisinde son kullanıcı bilgisayarının IP adresi, bilgisayar adı, tespit edilen zararlı yazılımın türü, zararlı olarak tespit edilen dosya adı ve bulunduğu dizin bilgisi, antivirus yazılımının aldığı aksiyon ve aksiyonun sonucu, olayın tespit ve kayıt tarihleri bulunmalıdır.
Tasarım	Son kullanıcı bilgisayarlarında zararlı yazılımın tespit edildiği ancak antivirus ajanının bu zararlı yazılımı silemediği durumlar tespit edilir. Bu durum yüksek önceliğe sahip bir durumdur. **Kural Adı:** Bilgi İşlem Cihazı Üzerinde Silinemeyen Zararlı Yazılım Tespiti **Filtreler;** **AND** McAfee E-policy Orchestrator kaynağından gelen iz kayıtları, **AND** *Low Level Category* parametresi *Virus Detected* değerlerini alan iz kayıtları, **AND** *Threat Handled* parametresi *false* değerini alan iz kayıtları. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *Analyzer Hostname* parametresinde bulunan hesap adlarına göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** - Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik Analisti, Anti-virus Sistem Yöneticisi

Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Tespit edilen cihazın sahibi ile iletişim kurar ve konu hakkında bilgilendirir. - **Antivirüs Sistem Yöneticisi:** İlgili bilgisayar üzerinde bulunan antivirus ajanının zararlı yazılımı neden silemediği ile ilgili teknik incelemelerde bulunur. Sorunun çözülmesi sonrasında ilgili bilgisayar üzerinde geniş çaplı tarama ve temizlik işlemlerini gerçekleştirir.

Tablo 4.10 Komuta ve Kontrol Merkezleri İle Haberleşen Bilgi İşlem Cihazlarının Tespiti

İsim	Kural-0004 Komuta ve Kontrol Merkezleri İle Haberleşen Bilgi İşlem Cihazlarının Tespiti
Amaç/Hedef	Kurumsal bilgi işlem cihazlarından komuta ve kontrol merkezleriyle haberleşenlerinin tespit edilmesi ve gereken güvenlik önlemlerinin alınması.
Problem Tanımı	Kurum içerisinde personelin çalışması için tahsis edilen bilgisayarlardan zararlı olduğu bilinen veya bir saldırı grubunun komuta ve kontrol merkezi olduğu bilinen IP adresleri veya domain adreslerine doğru yapılan trafik o cihaza bulaşan bir zararlı yazılımın varlığını işaret edebilir. Bu aktivitenin bir zararlı yazılım kaynaklı olup olmadığı tespit edilmelidir.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdadır: - Kurum ağından internete doğru yapılan trafikte güvenlik duvarı konumlandırılmalıdır. İlgili güvenlik duvarı üzerinden geçen trafik kayıt altına alınmalı ve SIEM sistemine aktarılmalıdır. - Personelin kurumsal bilgisayarları ile internete çıkmak için kullandıkları proxy sunucular var ise bu sistemlerin iz kayıtları SIEM sistemine aktarılmalıdır. - SIEM sistemine aktarılan iz kayıtlarında en az kaynak IP adresi, hedef IP adresi, hedef port numarası, istekte bulunan kullanıcı adı, istekte bulunulan URL bilgisi bulunmalıdır. - Bilinen komuta ve kontrol merkezi ip adresi ve domain adları siber istihbarat servislerinden düzenli olarak çekilmelidir. Elde edilen bu

	bilgileri SIEM sisteminin referans setlerine eklenerek sürekli güncel tutulmalıdır.
Tasarım	**Kural Adı:** Komuta ve Kontrol Merkezleri İle Haberleşen Bilgi İşlem Cihazlarının Tespiti **Filtreler;** **AND** *McAfee Proxy Server* kaynağından gelen iz kayıtları, **AND** *URL* parametresi içerisinde *Zararlı URL Listesi* referans setinde bulunan değerler ile eşleşen iz kayıtları. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *source IP* parametresinde bulunan IP adreslerine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik analisti, anti-virus sistem yöneticisi, güvenlik duvarı/proxy sistem yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Saptanan IP adresine göre istekte bulunan personelin bilgilerine erişir. Tespit edilen cihazın sahibi ile iletişim kurar ve konu hakkında bilgilendirir. - **Güvenlik Duvarı/proxy Sistem Yöneticisi:** Güvenlik analistinden gelen bildirime istinaden ilgili zararlı IP/domain adresinden gelen ve bu adrese giden trafiği engeller. - **Anti-Virus Sistem Yöneticisi:** İlgili bilgisayar üzerinde bulunan antivirus ajanı ile geniş çaplı tarama ve temizlik işlemlerini gerçekleştirir.

Tablo 4.11 Kurum Ağında Port Taraması Yapan Lokal IP Adreslerinin Tespiti

İsim	Kural-0005 Kurum Ağında Port Taraması Yapan Lokal IP Adreslerinin Tespiti
Amaç/Hedef	Kurum ağı içerisinde port taraması yapılması durumunda tarama faaliyetini gerçekleştiren lokal IP adresinin tespit edilmesi

Problem Tanımı	Kurum ağı içerisinde bulunan bilgi işlem cihazına herhangi bir sebepten dolayı zararlı yazılım bulaşması durumunda, zararlı yazılım kurum içerisinde yayılımını arttırmak için aynı ağ içerisinde yeni kurban makineler arayacaktır. Bu arama faaliyetinde birçok farklı makinenin belirli miktarda veya tüm portlarına istekte bulunarak zafiyetini sömürebileceği açık portlar arayacaktır. Bu gibi faaliyetler tespit edilmeli güvenlik incelemesinden geçirilmelidir.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdadır: - Kurum ağı içerisinde farklı vlanlar arasında yapılan intranet trafiğini denetlemek amacıyla güvenlik duvarı konumlandırılmalıdır. İlgili güvenlik duvarı üzerinden geçen trafik kayıt altına alınmalı ve SIEM sistemine aktarılmalıdır. - SIEM sistemine aktarılan iz kayıtlarında en az kaynak IP adresi, hedef IP adresi, hedef port numarası, kaynak port numarası bilgisi bulunmalıdır.
Tasarım	**Kural Adı:** SMB Port Taraması Yapan Bilgi İşlem Cihazlarının Tespiti **Filtreler;** **AND** *Güvenlik Duvarı* kaynağından gelen iz kayıtları, **AND** QID değeri *XXXXXX* olan iz kayıtları,(Session Allowed) **AND** *Destination Port* değeri *445* olan iz kayıtları, **AND** Aynı *Source IP* adresinden farklı *Destination IP* adreslerine *2 dakika* içerisinde en az *50* iz kaydının oluşması. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *source IP* parametresinde bulunan IP adreslerine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik analisti, anti-virus sistem yöneticisi, güvenlik duvarı/proxy sistem yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Saptanan IP adresine göre istekte bulunan personelin bilgilerine erişir. Tespit edilen cihazın sahibi ile iletişim kurar ve konu hakkında bilgilendirir.

	- **Güvenlik Duvarı/proxy Sistem Yöneticisi:** Güvenlik analistinden gelen bildirime istinaden ilgili zararlı IP/domain adresinden gelen ve bu adrese giden trafiği engeller. - **Anti-Virus Sistem Yöneticisi:** İlgili bilgisayar üzerinde bulunan antivirus ajanı ile geniş çaplı tarama ve temizlik işlemlerini gerçekleştirir.

4.3. Karşı Adli Bilişim Faaliyetlerinin Tespiti

Kötücül kullanıcılar ya da saldırganlar yaptıkları işlemlerin takibini zorlaştırmak veya izlerini kaybettirmek için çeşitli aksiyonlar alabilirler. Uygulanabilecek bazı karşı adli bilişim uygulamaları aşağıdadır:

- İşletim sistemi üzerindeki iz kayıtlarının silinmesi,
- İşletim sisteminin iz kayıtlarını toplayan sevislerinin veya uygulamalarının devre dışı bırakılması,
- İşletim sistemi üzerinde bulunan disklerin wipe işlemine tabi tutulması [60].

4.3.1. Tespit için gerekli iz kayıtlarının toplanması

Yukarıda bahsedilen tespitlerin yapılabilmesi amacıyla gerekli iz kayıtları SIEM sisteminde toplanmıştır. Windows tabanlı işletim sistemlerinde Microsoft Windows Security Event Logs iz kayıtlarının SIEM sistemine aktarılması gerekmektedir. Bu amaçla Windows sunucu üzerine Wincollect ajanı kurulmuştur. UNIX tabanlı işletim sistemlerinde auditd servisi çalışır duruma getirilmiştir. İz kayıtları rsyslog servisi ile SIEM sistemine aktarılmıştır. Bu çalışmada Linux işletim sistemi çekirdeğinin RedHat dağıtımı kullanılmıştır. Tespit için kullanılabilecek iz kayıt örnekleri Tablo 4.12'de görülmektedir.

Redhat versiyon 8.x işletim sistemine sahip işletim sistemlerinde auditd servisi çalışır hale getirilmiştir. Çalıştırılan her komutun auditd servisi tarafından kayıt altına alınabilmesi için root yetkisi ile aşağı gösterilen komut çalıştırılmıştır.

```
auditctl -a exit,always -S execve
```

Tablo 4.12: Anti-Forensics faaliyetlerinin tespiti için gerekli iz kayıt örnekleri

Windows İşletim Sistemi İz Kayıtlarının Silinmesi
Mar 25 10:58:03 hostname1.deneme.com AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.0.41 Source=Microsoft-Windows-Eventlog Computer=hostname1.deneme.com OriginatingComputer=10.10.20.20 User= Domain= EventID=1102 EventIDCode=1102 EventType=4 EventCategory=104 RecordNumber=11240 TimeGenerated=1648195002 TimeWritten=1648195002 Level=Informational Keywords=AuditSuccess Task=el:LogClear Opcode=Info Message=The audit log was cleared. Subject: Security ID: deneme\cagri Account Name: cagri Domain Name: deneme Logon ID: 0x702FC5
Linux İşletim Sistemi İz Kayıtlarının Silinmesi
type=PROCTITLE msg=audit(1529121745.550:323): proctitle=726D002D69002F7661722F746D702F746573745F66696C65 type=PATH msg=audit(1529121745.550:323): item=1 name="/var/tmp/test_file" inode=16934921 dev=ca:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1529121745.550:323): item=0 name="/var/tmp/" inode=16819564 dev=ca:01 mode=041777 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:tmp_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1529121745.550:323): cwd="/root" type=SYSCALL msg=audit(1529121745.550:323): arch=c000003e syscall=263 success=yes exit=0 a0=ffffffffffffff9c a1=9930c0 a2=0 a3=7ffe9f8f2b20 items=2 ppid=2358 pid=2606 auid=1001 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=2 comm="rm" exe="/usr/bin/rm" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="delete_var" type=EXECVE msg=audit(1543671660.203:64): argc=2 a0="tail" a1="/var/log/audit/audit.log"
Windows İşletim Sistemi Denetim İz Kayıtlarını Toplayan Servisin Kapatılması
Mar 26 16:13:57 hostname1.deneme.com AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.0.41 Source=Microsoft-

Windows-Eventlog Computer=hostname1.deneme.com OriginatingComputer=10.10.20.20 User= Domain= EventID=1100 EventIDCode=1100 EventType=4 EventCategory=103 RecordNumber=1197794 TimeGenerated=1648300276 TimeWritten=1648300276 Level=Informational Keywords=AuditSuccess Task=el:Shutdown Opcode=Info Message=The event logging service has shut down.
Linux İşletim Sistemi Denetim İz Kayıtlarını Toplayan Servisin Kapatılması
type=EXECVE msg=audit(1543671660.203:64): argc=4 a0="/bin/bash" a1="/usr/sbin/service" a2="auditd" a3="stop"
Windows İşletim Sistemi Üzerinde Yeni İşlem Oluşturulması
Jan 09 20:28:37 hostname01.deneme.com AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.0.41 Source=Microsoft-Windows-Security-Auditing Computer=hostname01.deneme.com OriginatingComputer=10.10.10.10 User= Domain= EventID=4688 EventIDCode=4688 EventType=8 EventCategory=13312 RecordNumber=143924768 TimeGenerated=1641749227 TimeWritten=1641749227 Level=Log Always Keywords=Audit Success Task=SE_ADT_DETAILEDTRACKING_PROCESSCREATION Opcode=Info Message=A new process has been created. Creator Subject: Security ID: deneme\user01 Account Name: user01 Account Domain: deneme Logon ID: 0x1AFBF1 Target Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Process Information: New Process ID: 0x3c58 New Process Name: C:\Program Files\Eraser\Eraser.exe Token Elevation Type: %%1936 Mandatory Label: Mandatory Label\Medium Mandatory Level Creator Process ID: 0xf9ec Creator Process Name: C:\Windows\System32\cmd.exe Process Command Line: \??\C:\Program Files\Eraser\Eraser.exe 0xffffffff -ForceV1

SIEM sistemi üzerinde yönlendirilen iz kayıtlarının anlamlandırılması ve güvenlik olay kurallarında kullanılabilmesi için ayrıştırma işlemi yapılmıştır. Bu işlem için regex (Regular Expression) dil kuralları kullanılmıştır. Tablo 4.13'de yazılan regex kuralları ve sonucunda elde edilen parametrelerin örnekleri verilmiştir.

Tablo 4.13 Olay ID 1102 İz Kayıt Örneği için Regex Örnekleri

Parametre Adı	Regex	Açıklama
Kullanıcı Adı(Username)	Account\sName\:\s(.*?)\s	İşlemi gerçekleştiren hesap adı.
Bilgisayar Adı (Computer Name)	Computer=(.*?)\s	İşlemin uygulandığı bilgisayar adı.
Olay ID (Event ID)	EventID=(\d+)	Olay ID değeri
Log Source Time	TimeGenerated=(\d+)	Olayın gerçekleşme zamanının epoch tipinde değeri.
Kaynak IP (Source IP)	OriginatingComputer=(\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})	İşlemin yapıldığı bilgisayarın IP adresi

4.3.2. Tespit için oluşturulan kural ve use case örneği

Çalışmada anlatılan Use Case şablonuna uygun olarak ilgili kural için oluşturulmuş use case örnekleri Tablo 4.14, 4.15 ve 4.16'da gösterilmiştir.

Tablo 4.14 İşletim Sistemi Üzerindeki İz Kayıtlarının Silinmesi

İsim	Kural-0006 İşletim Sistemi Üzerindeki İz Kayıtlarının Silinmesi
Amaç/Hedef	İşletim sistemi üzerinde güvenlik olay kayıtlarının silinmesi durumlarının tespit edilmesi.
Problem Tanımı	Rutin ve günlük kullanımda bir işletim sisteminin güvenlik olay kayıtlarının silinmesi normal bir durum olarak değerlendirilmez. İstisnai durumlarda bir takım teknik sorunların çözümü için bu eyleme ihtiyaç duyulabilir. Aksi takdirde bu eylem karşı adli bilişim uygulaması olarak değerlendirilir ve detaylı incelenmesi gereken bir durumdur.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdadır:

	- Kurum ağında bulunan sunucu ve bilgisayarlar merkezi SIEM sistemine güvenlik olay kayıtlarını göndermelidir. - Windows işletim sistemi iz kayıtları içerisinde Event ID değeri, username değeri ve Computer Name değerleri bulunmalıdır. - Linux işletim sisteminde çalıştırılan komut, username, Computer Name değerleri bulunmalıdır.
Tasarım	**Kural Adı:** Windows İşletim Sistemi Üzerindeki İz Kayıtlarının Silinmesi **Filtreler;** **AND** İz kayıt tipi *Microsoft Windows Security Event Log* olan iz kayıtları, **AND** *Event ID* değeri (*1102* **OR** *1104*) olan iz kayıtları, Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *Computer Name* parametresinde bulunan bilgisayar adına göre kurallar tetiklenir. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** Linux İşletim Sistemi Üzerindeki İz Kayıtlarının Silinmesi **Filtreler;** **AND** İz kayıt tipi *Linux OS* olan iz kayıtları, **AND** *type* değeri *EXECVE* olan iz kayıtları, **AND** iz kayıt gövdesi içerisinde (*rm* **AND** *audit*) değerleri bulunan iz kayıtları. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *Computer Name* parametresinde bulunan bilgisayar adına göre kurallar tetiklenir. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik analisti, Aktif Dizin Sistem Yöneticisi, Unix Sistem Yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Saptanan IP adresine göre istekte bulunan personelin bilgilerine erişir.

	- **Aktif Dizin Sistem Yöneticisi:** İlgili bilgisayarı muhafaza altına alarak yapılan işlemin doğruluğunu teyit eder. Bilgisayarın imajını olarak güvenli bir şekilde saklanmasını sağlar. - **Unix Sistem Yöneticisi:** İlgili bilgisayarı muhafaza altına alarak yapılan işlemin doğruluğunu teyit eder. Bilgisayarın imajını olarak güvenli bir şekilde saklanmasını sağlar.

Tablo 4.15 İşletim Sistemi Üzerindeki İz Kayıt Servislerinin Kapatılması

İsim	Kural-0007 İşletim Sistemi Üzerindeki İz Kayıt Servislerinin Kapatılması
Amaç/Hedef	İşletim sistemi üzerinde güvenlik olay kayıtlarının oluşmasını sağlayan servislerin kapatılması durumlarının tespit edilmesi.
Problem Tanımı	Rutin ve günlük kullanım sırasında bir işletim sisteminin güvenlik olay kayıtlarının oluşturulmasından sorumlu olan servisin manuel olarak kapatılması normal bir durum olarak değerlendirilmez. İstisnai durumlarda bir takım teknik problemlerin çözümü için bu eyleme ihtiyaç duyulabilir. Aksi takdirde bu eylem karşı adli bilişim uygulaması olarak değerlendirilir ve detaylı incelenmesi gereken bir durumdur.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdadır: - Kurum ağında bulunan sunucu ve bilgisayarlar merkezi SIEM sistemine güvenlik olay kayıtlarını göndermelidir. - Windows işletim sistemi iz kayıtları içerisinde Event ID değeri, username değeri ve Computer Name değerleri bulunmalıdır. - Linux işletim sisteminde çalıştırılan komut, username, Computer Name değerleri bulunmalıdır.
Tasarım	**Kural Adı:** Windows İşletim Sistemi İz Kayıt Servisinin Kapatılması **Filtreler;** **AND** İz kayıt tipi *Microsoft Windows Security Event Log* olan iz kayıtları, **AND** *Event ID* değeri *1100* olan iz kayıtları. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *Computer Name* parametresinde bulunan bilgisayar adına göre kurallar tetiklenir. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;**

	Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** Linux İşletim Sistemi Üzerindeki Auditd Servisinin Silinmesi **Filtreler;** **AND** İz kayıt tipi *Linux OS* olan iz kayıtları, **AND** *type* değeri *EXECVE* olan iz kayıtları, **AND** iz kayıt gövdesi içerisinde (*auditd* **AND** *stop*) değerleri bulunan iz kayıtları. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *Computer Name* parametresinde bulunan bilgisayar adına göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik analisti, Aktif Dizin Sistem Yöneticisi, Unix Sistem Yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Saptanan IP adresine göre istekte bulunan personelin bilgilerine erişir. Tespit edilen bilgisayarın sahibi ile iletişim kurar ve konu hakkında bilgilendirir. - **Aktif Dizin Sistem Yöneticisi:** İlgili bilgisayarı muhafaza altına alarak yapılan işlemin doğruluğunu teyit eder. Bilgisayarın imajını olarak güvenli bir şekilde saklanmasını sağlar. - **Unix Sistem Yöneticisi:** İlgili bilgisayarı muhafaza altına alarak yapılan işlemin doğruluğunu teyit eder. Bilgisayarın imajını olarak güvenli bir şekilde saklanmasını sağlar.

Tablo 4.16 İşletim sistemi üzerinde disk wipe işlemi için kullanılan işlemlerin çalıştırılması

İsim	Kural-0008 İşletim sistemi üzerinde disk wipe işlemi için kullanılan işlemlerin çalıştırılması

Amaç/Hedef	İşletim sistemi üzerinde yeni bir process (işlem) başlatıldığında bu işlemin disk wipe işlemi için kullanılıp kullanılmadığının tespit edilmesi.
Problem Tanımı	İşletim sistemi üzerinde gizlediği dosyaları ya da yaptığı işlemlerin kalıntılarını saklamaya çalışan bir kişi bilgisayar üzerinde yer alan disklere wipe işlemi uygulayabilir. Bu işlem, bilgisayara uygulanan adli bilişim işlemlerini zorlaştırmak ve delil elde etme süreçlerine zarar vermek amacıyla yapılmaktadır.
Gereksinim	Bu sorunun çözümü için gereken bilgiler aşağıdadır: - Kurum ağında bulunan sunucu ve bilgisayarlar merkezi SIEM sistemine güvenlik olay kayıtlarını göndermelidir. - Windows işletim sistemi iz kayıtları içerisinde Event ID değeri, username, Computer Name ve New Process Name değerleri bulunmalıdır.
Tasarım	**Kural Adı:** İşletim sistemi üzerinde disk wipe işlemi için kullanılan işlemlerin çalıştırılması **Filtreler;** **AND** İz kayıt tipi *Microsoft Windows Security Event Log* olan iz kayıtları, **AND** *Event ID* değeri *4688* olan iz kayıtları. **AND** *New Process Name* parametresi içerisinde *Eraser.exe* bulunan kayıtlar. Eraser.exe bu kuralda örnek olarak verilmiştir. Bilinen tüm wipe uygulamalarının işlem isimleri saptanarak kurala eklenebilir. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *Username* parametresinde yer alan hesap adına göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik analisti, Aktif Dizin Sistem Yöneticisi.
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Saptanan bilgisayara el konulur ve

	IP adresine göre istekte bulunan personelin bilgilerine erişir. Tespit edilen cihazın sahibi ile iletişim kurar ve konu hakkında bilgilendirir. - **Aktif Dizin Sistem Yöneticisi:** İlgili bilgisayarı muhafaza altına alarak yapılan işlemin doğruluğunu teyit eder. Bilgisayarın imajını olarak güvenli bir şekilde saklanmasını sağlar.

4.4. Kurum Dışına Doğru Yapılan Yüksek Boyutlu Veri Çıkışının Tespiti

Kurum içerisinde çalışan personelin günlük faaliyetleri sırasında internet ile olan veri trafikleri büyük oranda download (veri indirme) trafiğidir. Özel şartlar veya işi gereği kullanım zorunluluğu olan personeller haricinde yüksek boyutlu upload (veri yükleme) trafiğine rastlanması durumunda bu trafik incelenmelidir. Kurum dışındaki bir ortama yüksek boyutlu verinin çıkarılması şüpheli bir durumdur. Personel kurumsal ve gizli verileri kurum dışına çıkarıp bu verileri satıyor veya kurumun itibarını zedeleyebilecek faaliyetlerde bulunuyor olabilir. Kurumun gizli ve hizmete özel verilerini kurum ağından dışarıya bir kaç farklı yöntem ile çıkarılabilir. Bu yöntemlerden bazıları aşağıda sıralanmıştır.

- Kurum personeli kurumsal e-posta servisini veya harici bir e-posta servisini kullanarak kurum ağının dışına veri çıkarabilir.
- USB veya benzeri depolama birimlerini kullanarak kurum bilgisayarlarından veri çıkarılabilir.
- Bulut depolama servisleri (one drive, googler drive, wetransfer vb.) kullanarak kurum bilgisayarlarından elde edilen veri internete yüklenebilir.
- Fotoğraf veya video kayıt özelliği bulunan herhangi bir cihaz ile bilgisayarı ekran görüntüsü kaydedilerek kurum dışına çıkarılabilir.

Tablo 4.17'de verilen kural örneğinde kurum dışına doğru yapılan yüksek boyutlu veri trafiğinin tespiti sağlanarak güvenlik analistlerinin incelemesi için alarm oluşturmaktadır.

Tablo 4.17 Kurum Dışına Doğru Yüksek Boyutlu Veri Transferinin Tespiti

İsim	Kural-0009 Kurum Dışına Doğru Yüksek Boyutlu Veri Transferinin Tespiti

Amaç/Hedef	Kurum dışına doğru çıkan verinin takibini yapmak, yüksek boyutlu veri trafiklerini tespit etmek ve güvenlik analisti tarafından incelenmesini sağlamak.
Problem Tanımı	Kurumsal altyapılarda gizli veya hizmete özel etiketli verilerin kurum dışına çıkarılıp çıkarılmadığının takibi oldukça zor bir iştir. Bu gibi trafiklerin tespitinin yapılması ve gereken müdahale prosedürlerinin uygulanması için SIEM sistemleri üzerinde kurallar yazılabilir. Tek başına yeterli olmamakla birlikte birçok farklı senaryoda veri sızıntılarının tespiti yapılabilecektir.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdadır: - Kurumum internete çıkan ağında konumlanan güvenlik duvarı cihazının trafik iz kayıtları SIEM sistemine aktarılmalıdır. İz kayıtlarının içerisinde yapılan trafiğinin upload ve download yönlerindeki veri boyutlarının bytes cinsinden değerleri bulunmalıdır. SIEM sistemlerinde bu alanlar parse edilerek kurallarda kullanılabilecek duruma getirilmelidir. - Kurum ağında var ise web gateway (internet proxy) sunucularının iz kayıtları SIEM sistemine aktarılmalıdır. Bu iz kayıtları içerisinde upload ve download yönlerindeki veri boyutlarının bytes cinsinden değerleri bulunmalıdır. SIEM sisteminde bu alanlar parse edilerek kurallarda kullanılabilecek duruma getirilmelidir. - Her iki güvenlik cihazında da iz kayıtlarında bulunan, gönderilen veri boyutu değeri *Bytes_Sent* isimli parametre ile ayrıştırılmıştır.
Tasarım	**Kural Adı:** Tek Bir Oturumda Yüksek Boyutlu Veri Transferinin Tespiti **Filtreler;** **AND** (*Güvenlik Duvarı* **OR** *Web Proxy*) cihazlarından gelen iz kayıtları, **AND** İç ağdan internete doğru olan iz kayıtları, **AND** *Bytes_sent* değeri 1,073,741,824 değerine eşit veya büyük olan iz kayıtları. **AND** Aynı *kaynak IP* adresinden aynı *hedef IP* adresine 1 gün içerisinde en az 1 iz kaydı bulunması.

	Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *Kaynak IP* parametresinde bulunan IP adresine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** Çok sayıda Oturum İle Yüksek Boyutlu Veri Tranferinin Tespiti **Filtreler;** **AND** (*Güvenlik Duvarı* **OR** *Web Proxy*) cihazlarından gelen iz kayıtları, **AND** İç ağdan internete doğru olan iz kayıtları, **AND** *Bytes_sent* değeri 10,485,760 değerine eşit veya büyük ise olan iz kayıtları. **AND** Aynı *kaynak IP* adresinden aynı *hedef IP* adresine 1 gün içerisinde en az 100 iz kaydı bulunması. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde *Kaynak IP* parametresinde bulunan IP adresine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik analisti, Anti-Virus Sistem Yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Saptanan IP adresine göre istekte bulunan personelin bilgilerine erişir. Personelin ve kullanılan bilgisayarın diğer iz kayıtlarını da inceleyerek anomalileri tespit etmeye çalışır. - **Anit-Virus Sistem Yöneticisi:** İlgili bilgisayar üzerinde detaylı anti-virus taramalarını gerçekleştirerek zararlı yazılımların varlığını tespit etmeye çalışır. Testpini durumunda etkisiz hale getirilmesi için gereken işlemleri uygular.

4.5. Kurum Ağında Veri tabanı Taraması Yapan Lokal IP Adresi Tespiti

Güvenlik sıkılaştırmaları yapılmış bir kurumsal ağ içerisinde veri tabanlarının yönetim arayüzlerine yapılan erişimler güvenlik cihazları tarafından sınırlandırılmıştır. Veri tabanı yöneticileri haricinde erişimler engellenmiş olmalıdır. Kötücül kullanıcılar kurumsal ağ içerisinde bulunan veri tabanlarını tespit edebilmek amacıyla tüm ağ içerisinde port taramaları yaparak erişim denetiminin düzgün yapılmadığı durumlarda veri tabanı IP adreslerini ele geçirebilir, gözetleme ve zafiyet tarama faaliyetleri yaparak veri tabanına yetkisiz erişimleri deneyebilirler. Birçok zararlı yazılım da bulaştığı cihazın bulunduğu ağ içerisinde bu taramayı yaparak bilgi toplamaya çalışmaktadır. Bu gibi durumların tespiti için SIEM yazılımları üzerinde Tablo 4.18'de gösterilen kural yazılmıştır.

Tablo 4.18 Kurum Ağında Veri tabanı Taraması Yapan Lokal IP Adresi Tespiti

İsim	Kural-0010 Kurum Ağında Veri tabanı Taraması Yapan Lokal IP Adresi Tespiti
Amaç/Hedef	Kurumsal ağda veri tabanlarını tespit etmeye yönelik yapılan aktivitelerin tespit edilmesi
Problem Tanımı	Kurumsal ağ içerisinde port taraması yaparak veri tabanlarını tespit etmeye yönelik yapılan bir faaliyetin legal ve zararsız olma ihtimali düşüktür. Bu gibi durumlar bir an önce tespit edilmeli ve aktiviteyi gerçekleştiren cihaz üzerinde gereken incelemeler yapılmalıdır.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdadır: - Kurum iç ağında konumlanan güvenlik duvarı iz kayıtları SIEM sistemine yönlendirilmelidir. - Güvenlik duvarı iz kayıtları içerisinde, kaynak IP, hedef IP, hedef port bilgisi bulunmalı ve bu alanlar parse işleminden geçirilerek kurallarda kullanılmaya uygun durumda olmalıdır. - Kurum ağında kullanılan veya kullanılmasa bile global olarak kabul görmüş veri tabanlarının default port bilgileri bulunmalıdır.
Tasarım	**Kural Adı:** Kurum Ağında Veri tabanı Taraması Yapan Lokal IP Adresi Tespiti **Filtreler;** **AND** *Güvenlik Duvarı* kaynağından gelen iz kayıtları, **AND** hedef port'u (*1433* **OR** *1434* **OR** *1521* **OR** *5432*) olan iz kayıtları,

	AND Kaynak IP adresi (*172.16.0.0/12* **OR** *10.0.0.0/8* **OR** *192.168.0.0/16*) olan iz kayıtları, **AND** İki dakika içerisinde aynı kaynak IP adresinden farklı hedef IP adreslerine doğru 10'den fazla kayıt tespit edildiğinde. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde bulunan kaynak Ip adresine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik analisti, güvenlik duvarı sistem yönetici, anti-virus sistem yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. Saptanan IP adresine göre istekte bulunan personelin bilgilerine erişir. Tespitte bulunulan cihazın sahibi ile iletişim kurar ve konu hakkında bilgilendirir. - **Güvenlik Duvarı Sistem Yöneticisi:** İlgili kaynak IP adresinden yapılan tüm trafikleri engeller. - **Antivirüs Sistem Yöneticisi:** İstekte bulunan IP adresine sahip bilgisayarı herhangi bir zararlı bulaşmış olma ihtimaline karşı gereken tarama faaliyetlerini gerçekleştirir.

4.6. Web Sayfalarına Yapılan Saldırıların Tespiti

İnternete açık bulunan web sayfaları global tehdit aktörleri tarafından sürekli olarak zafiyet taramalarından ve sızma testlerinden geçirilir. Herhangi bir kurumsal altyapıda internete bakan güvenlik duvarından alınan iz kayıtları incelenirse birçok yurtdışı IP adresinden port tarama faaliyetinin yapıldığının tespit edilmesi muhtemeldir. Bununla birlikte web sayfalarının erişim iz kayıtları da incelenirse birçok anormal isteğin yapıldığı görülebilir. Bu gibi durumların tespiti ve tehdit aktörlerinin hedef ve faaliyetlerinin erken anlaşılabilmesi için bu zararlı aktivitelerin SIEM sistemleri tarafından tespiti ve güvenlik analistinin kontrolünden geçirilmesi kritik öneme sahiptir. Bu tip saldırıların tespiti için gerekli kurallar bu başlık altında incelenmiştir.

Tablo 4.19'da http 200 cevabı almış bir web erişim iz kaydı örneği görünmektedir. Burada kalın olarak yazılan kısım http-uri parametresi olarak parse edilip kurallarda kullanılmıştır. Tablo 4.20'de web sayfalarına yapılan saldırılan tespitine yönelik yazılan use case örneği gösterilmiştir.

Tablo 4.19 HTTP 200 Web Erişim İz Kayıt Örneği

10.10.10.10 [20/Jan/2022:20:04:51 +0300] deneme.test.com.tr "POST **/main/jsp/esatis/getTekliflerim_brd.ajx** HTTP/1.1" 200 35 9733 + deneme.test:9123 10.10.10.20 0000tD19s474fa7

Tablo 4.20 Web Sayfalarına Yapılan Saldırıların Tespiti

İsim	Kural-0011 Web Sayfalarına Yapılan Saldırıların Tespiti
Amaç/Hedef	Web sayfalarına yapılan zafiyet tarama ve sızma denemelerinin tespit edilerek tehdit aktörlerinin engellenmesinin sağlanması.
Problem Tanımı	İnternete açık bulunan web sayfaları dış dünyadan gelebilecek her türlü saldırıya karşı açık bulunmaktadır. Her ne kadar güvenlik duvarı, web uygulama güvenlik duvarı, IPS/IDS gibi güvenlik sistemleri altyapıda konumlanmış olsa bile yapılan saldırıların sunuculara kadar ulaşması muhtemeldir. Güvenlik sistemlerinden geçen bu gibi saldırıların tespitinin yapılması ve gerekli önlemlerin en kısa sürede alınması gerekmektedir.
Gereksinimler	Bu sorunun çözümü için gereken bilgiler aşağıdadır: - Web sayfalarının erişim iz kayıtlarının SIEM sistemlerine anlık olarak gönderiliyor olması gerekmektedir. - Web sayfası erişim iz kayıtları içerisinde bulunan http-uri değeri parse edilerek kurallarda kullanılabilecek duruma getirilmelidir. - Legal bir web erişim isteğinde kullanılan web servisinin http-uri parametresinin alabileceği değerler belirlenmelidir. - Web sayfalarına yapılan zafiyet tarama ve sızma aktiviteleri sırasında http uri parametresine girilen zararlı içerikler tespit edilmelidir.
Tasarım	**Kural Adı:** Directory Traversal Saldırılarının Tespiti **Filtreler;**

	AND *Web Server* kaynağından gelen iz kayıtları, **AND** *http-uri* parametresi (*../* **OR** *..* **OR** *%2e%2e%2f* **OR** *%252e%252e%252f* **OR** *%c0%af*) değerlerini içeren iz kayıtları tespit edildiğinde. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde bulunan kayna Ip adresine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** SQL Injection Saldırılarının Tespiti **Filtreler;** **AND** *Web Sunucu* kaynağından gelen iz kayıtları, **AND** *http-uri* parametresi (*select+* **OR** *order+* **OR** *union+* **OR** *waitfor* **OR** *+and%* **OR** *select%* **OR** *union%* **OR** *+or%* **OR** *group+by* **OR** *insert%* **OR** *'INJ'||'ECT'||'X*) değerlerini içeren iz kayıtları tespit edildiğinde. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde bulunan kayna Ip adresine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** XSS Saldırılarının Tespiti **Filtreler;** **AND** *Web Sunucu* kaynağından gelen iz kayıtları, **AND** *http-uri* parametresi (*<script>* **OR** *py-script* **OR** *<SCRIPT/XSS* **OR** *</x:script>* **OR** *</script>* **OR** *"ale"+"rt(1)"*) değerlerini içeren iz kayıtları tespit edildiğinde. Yukarıda yer alan filtreden sonra kalan iz kayıtları içerisinde bulunan kayna Ip adresine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;**

	Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur. **Kural Adı:** SSRF Saldırılarının Tespiti **Filtreler;** **AND** *Web Sunucu* kaynağından gelen iz kayıtları, **AND** *http-uri* parametresi (*http:* **OR** *127.0.* **OR** *pas$(te)swd?* **OR** *:$(br)* **OR** *0x7f.0x00.0x00.0x01* **OR** *[0:0:*) değerlerini içeren iz kayıtları tespit edildiğinde. Yukarıda yer alan filtreden sonra kalan iz kayıtları içinde bulunan kaynak IP adresine göre kurallar tetiklenmiş olur. **Kural Tetiklenmesi Durumunda Alınacak aksiyonlar;** Güvenlik analistinin takip edebilmesi için izleme ekranına alarm oluşturulur.
Sorumlu Grup	Güvenlik analisti, güvenlik duvarı sistem yönetici, anti-virus sistem yöneticisi
Aksiyon	- **Güvenlik Analisti:** Meydana gelen alarmın incelenmesi ve doğrulanması üzerine ilgili diğer personelleri uyararak gereken aksiyonların alındığından emin olur. - **Güvenlik Duvarı Sistem Yöneticisi:** İlgili kaynak IP adresinden yapılan tüm trafikleri engeller. Sistemde WAF ürünü var ise ilgili saldırının neden tespit edilip engellenmediği konusunda incelemelerde bulunur.

5. SONUÇLAR VE ÖNERİLER

Son yıllarda siber saldırı çeşitleri ve saldırı yoğunluğu artmıştır ve bu nedenle alanda çalışan kişilerin ve teknoloji kaynaklarının en verimli şekilde kullanılması oldukça önemlidir. Buna ek olarak saldırılara karşı verilecek tepki süresinin kısaltılması, saldırının oluşturabileceği hasarın en aza indirilmesini ve delillerin yok edilmesi riskini azaltacağı düşünülmektedir.

Yapılan ilk uygulama çalışmasında kurumsal e-posta uygulamasından alınan iz kayıtlarının SIEM sistemine aktarılarak anlamlandırılması ve korelasyon kurallarına tabi tutulması sonucunda ele geçirilen personel e-posta hesaplarının tespit edilebileceği görülmüştür. Tespitin başarısında saldırganın davranışlarının belirleyici rol oynadığı görülmüştür. Örneğin ilgili kuralda 1 saat içinde 100 farklı kişiye e-posta atılması şeklinde yazılan eşik değer direkt olarak saldırgan davranışını tahmin etmeye yöneliktir. Aynı şekilde saldırganın Türkiye'den bir IP adresi kullanması durumunda da ilgili kuralı atlatabileceği görülmektedir.

Bilgi işlem cihazları üzerinde bulunan zararlı yazılımların tespitine yönelik yapılan çalışmada bilgisayar üzerinde kurulu olması muhtemel zararlı yazılımın işletim sistemi iz kayıtları üzerinden yazılan korelasyon kuralları ile tespit edilebileceği görülmüştür. Bilgisayardan internete doğru yapılan erişim istekleri incelenerek zararlı yazılım komuta ve kontrol merkezlerine yapılan erişimlerin tespiti ile de bilgisayar üzerinde zararlı yazılım olabileceği yönünde bilgilerin edinilebileceği görülmüştür. Benzer şekilde antivirüs yazılımlarından alınan iz kayıtlarında ilgili bilgisayar üzerinde zararlı yazılım tespitinin yapıldığı ancak antivirüs yazılımı tarafından silinemediği şeklinde gelen iz kayıtlarının da ilgili bilgisayar üzerinde tehlike arz eden bir yazılımın bulunduğu yönünde bilgi verdiği görülmüştür.

Yapılan bir diğer uygulama çalışmasında iz kayıtlarının toplanmasının engellenmesi ve wipe işlemi uygulanarak verinin silinmesi şeklinde gerçekleştirilen karşı adli bilişim faaliyetlerinin tespitine yönelik kurallar yazılmıştır. Bu kurallar sayesinde yaşanan karşı adli bilişim olaylarının tespit edilebildiği görülmüştür. Yapılan bu tespit neticesinde izleri yok etmeye yönelik yapılan faaliyetlerin henüz ortaya çıkmamış bir adli bilişim vakasının tespiti için ip ucu niteliğinde değerlendirilebileceği düşünülmektedir.

Kurum dışına yapılan yüksek boyutta veri çıkışının tespitine yönelik yazılan kurallar kurum içerisinde veri sızıntısını tespite yöneliktir. Yazılan kural sonucunda oluşan alarmın tek başına bir veri sızıntısını işaret etmesinin zor olduğu, güvenlik analistinin inceleme süresini

düşürmeye yönelik yeterli katkıyı sunmadığı ve çok sayıda yanlış alarm ürettiği görülmüştür. Aynı zamanda 10 MB altında çok sayıda veri paketi ile işlem yapılması durumlarında veri sızıntısı tespitin yapılamadığı görülmüştür.

Saldırganların veri tabanlarını tespit etmek amacıyla yaptıkları faaliyetlerin yakalanmasına yönelik yazılan SIEM kuralının beklendiği gibi çalıştığı görülmüştür. Ancak verilen eşik değerlerinin kurumun altyapısına uygun olarak ayarlanması gerektiği aksi halde çok sayıda hatalı alarm üreterek güvenlik analistinin iş yükünü arttıracağı değerlendirilmiştir.

Web sayfalarına yapılan saldırılarının tespitine yönelik yazılan kuralların doğru şekilde çalıştığı görülmüştür. Ancak pratikte web sayfalarına yapılabilecek saldırı senaryolarının ve bu senaryoları gerçekleştirirken URI kısmında görülen saldırı desenlerinin çok sayıda olması yapılan her saldırının tespitini zorlaştırmaktadır. Bununla birlikte yapılan çalışmada sadece HTTP URI değeri incelenmiş olmasına rağmen web sayfalarının birçok farklı bileşeni üzerinden saldırılar gelebileceği ve bu saldırıların çalışma kapsamında yazılan kurallar ile tespit edilemediği görülmüştür. Bu duruma örnek olarak user-agent alanı üzerinden yapılan saldırılar gösterilebilir.

Yapılan araştırma çalışmaları ve uygulamalar göstermektedir ki, sunucuların, son kullanıcı cihazlarının ve ağ cihazlarının oluşturduğu iz kayıtları merkezi bir SIEM sisteminde toplanması ve bu iz kayıtlarının sistem üzerinde işlenmesi, güvenlik kuralları oluşturularak kurumsal ağlarda gerçekleşen adli bilişim olaylarının tespit edilmesi mümkündür. İlerleyen çalışmalarda yazılan kuralların çeşitlendirilerek mümkün olan tüm saldırı senaryolarının tespitinde kullanılabileceği, güvenlik cihazlarının yakalayamadığı durumlarda uç sistemlere kadar ulaşan zararlıların tespit edilerek, zararlının verebileceği zararın azaltılarak personelin saldırıya tepki sürelerinin azaltılabileceği görülmüştür.

Gerçekleşen saldırılar SIEM sistemlerinde delil olarak tutulabilmektedir ve adli vakalarda hızla bu deliller yetkililer ile paylaşılabilmektedir. Buradan yola çıkarak SIEM sistemleri sayesinde bir saldırı durumunda adli mercilerin olaya ayıracağı araştırma süresinin kısalacağını düşünmekteyiz.

Bu çalışmada yer alan örnekler, zaman ve kaynak yetersizliğinden dolayı sınırlı tutulmuştur. Bu örnekler arttırılabilir ve yeni geliştirilen saldırı tipleri için şu an bilmediğimiz yeni tespit kuralları yazılabilir. Ayrıca güvenlik analistinin ve bilgi işlem personelinin alması gereken aksiyonlara yüzeysel olarak değinilmiştir. Bu gibi olaylarda personelin alması gereken

aksiyonlar detaylandırılabilir.

Bu çalışma kapsamında yapılan araştırma ve uygulama çalışmalarında tespit edilen adli bilişim olaylarının hukuki boyutu değerlendirilmemiştir.

KAYNAKLAR

1. Check Point Cyber Security Report 2021. (2021).
2. González-Granadillo, G., S. González-Zarzosa, and R. Diaz. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), 4759.
3. Vielberth, M. and G. Pernul. *A security information and event management pattern.* (2018).
4. Žgela, M. and I. Penga. (2019). *Security Information and Event Management–Capabilities, Challenges and Event Analysis in the Complex IT System*. Central European Conference on Information and Intelligent Systems. Faculty of Organization and Informatics Varazdin.
5. Dubuc, C., *A.* (2021). *Real-time Log Correlation System for Security Information and Event Management*.
6. Gökçeoğlu, D. (2021). *Güvenlik Bilgileri ve Olay Yönetimi(SIEM)/Log Korelasyon Kurallarının Yazılması*. Firat Üniversitesi.
7. Irfan, M. (2016). *A framework for cloud forensics evidence collection and analysis using security information and event management.* Security and Communication Networks, 9(16), pp.3790-3807.
8. Kent, K.A. and M. Souppaya. (2006). Guide to Computer Security Log Management.
9. Di Mauro, M. and C. Di Sarno. (2018). Improving SIEM capabilities through an enhanced probe for encrypted Skype traffic detection. *Journal Of Information Security And Applications*, 38, 85-95.
10. Raja, M.S.N. and A. Vasudevan. (2017). Rule generation for TCP SYN flood attack in SIEM Environment. *Procedia computer science,* 115, 580-587.
11. Zeinali, S.M. (2016). *Analysis of security information and event management (SIEM) evasion and detection methods*. Master Thesis, Tallinn University of Technology.
12. Nicolett, M. and K.M. Kavanagh. (May 2009). *Magic quadrant for security information and event management.* Gartner RAS Core Reasearch Note.
13. Kişisel Verilerin Korunmasi Kanunu. 2016 [cited 2022; Available from: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5.
14. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. 2013 [cited 2022; Available from: https://www.iso.org/standard/54534.html.
15. Butts, J.W., R.F. Mills, and R.O. Baldwin. (2005). Developing an insider threat model using functional decomposition. *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer.
16. Insider Threats Rise by 47% in Two Years: Report. 2020 [cited 2022; Available from: https://cisomag.eccouncil.org/insider-threats-rise-by-47-in-two-years-report/.
17. Dorigo, S. (2012). *Security information and event management.* Radboud University, Nijmegen.
18. What is SIEM? [cited 2022; Available from: https://www.exabeam.com/siem-guide/what-is-siem/.
19. Data aggregation. [cited 2022; Available from: https://www.ibm.com/docs/en/tnpm/1.4.2?topic=data-aggregation.
20. Baker, K. WHAT IS CYBER THREAT INTELLIGENCE? 2021 [cited 2022; Available from: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/.

21. Karlzén, H. (2009). An Analysis of Security Information and Event Management Systems-The Use or SIEMs for Log Collection, *Management and Analysis*.
22. Wang, K., et al. (2016). Attack detection and distributed forensics in machine-to-machine networks. *IEEE Network,* 30(6), 49-55.
23. Mavroeidis, V. and A. Jøsang. (2018). *Data-driven threat hunting using sysmon*. Proceedings of the 2nd International Conference on Cryptography, Security and Privacy.
24. Al Sabbagh, B. (2019). *Cybersecurity Incident Response: A Socio-Technical Approach*. Department of Computer and Systems Sciences, Stockholm University.
25. Perera, A., et al. (2021). *The Next Gen Security Operation Center*. 2021 6th International Conference for Convergence in Technology (I2CT). 2021. IEEE.
26. Security auditing. 2021 [cited 2022; Available from: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview.
27. Appendix L: Events to Monitor. 2021 [cited 2022; Available from: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor.
28. 4625(F): An account failed to log on. [cited 2022; Available from: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625.
29. Introduction to IIS Architectures. [cited 2022; Available from: https://docs.microsoft.com/en-us/iis/get-started/introduction-to-iis/introduction-to-iis-architecture.
30. Log Data Fields. [cited 2022; Available from: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-wmlog/2c5d9a4c-58ef-4718-a2bd-bd45a853b3bd.
31. What is Linux? [cited 2022; Available from: https://www.redhat.com/en/topics/linux/what-is-linux.
32. CHAPTER 7. SYSTEM AUDITING. [cited 2022; Available from: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing.
33. What is AIX? [cited 2022; Available from: https://www.precisely.com/glossary/aix.
34. AIX AUDIT: The Audit Subsystem in AIX. [cited 2022; Available from: https://www.ibm.com/support/pages/aix-audit-audit-subsystem-aix.
35. Apache Http Server Project. [cited 2022; Available from: https://httpd.apache.org/.
36. Apache Temel Özellikleri. [cited 2022; Available from: https://httpd.apache.org/docs/2.4/tr/mod/core.html#errorlog.
37. HTTP. [cited 2022; Available from: https://developer.mozilla.org/en-US/docs/Web/HTTP.
38. What Is a Firewall? [cited 2022; Available from: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.
39. Güvenlik duvarı nedir? [cited 2022; Available from: https://www.forcepoint.com/tr/cyber-edu/firewall.
40. Intrusion Prevention System – IPS. [cited 2022; Available from: https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/.
41. Antivirus nedir? [cited 2022; Available from: https://www.eset.com/tr/antivirus-software/.
42. ePolicy Orchestrator Management Information Base Overview. [cited 2022; Available from: https://kc.mcafee.com/corporate/index?page=content&id=KB89607.

43. Cheung, K.H. and J. Mišić. (2002). On virtual private networks security design issues. *Computer Networks*, 38(2), 165-179.
44. Vixie, P. (2007). *DNS Complexity: Although it contains just a few simple rules, DNS has grown into an enormously complex system.* Queue, 5(3), 24-29.
45. DNS Logging and Diagnostics. 2016 [cited 2022; Available from: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn800669(v=ws.11).
46. Clincy, V. and H. Shahriar. (2018). *Web application firewall: Network security models and configuration*. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE.
47. Inamdar, M.S. and A. Tekeoglu. (2018). *Security analysis of open source network access control in virtual networks*. 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE.
48. Fei, B., et al. (2006). *Analysis of web proxy logs*. IFIP International Conference on Digital Forensics. Springer.
49. WinCollect overview. [cited 2022; Available from: https://www.ibm.com/docs/en/qradar-on-cloud?topic=7-wincollect-overview.
50. Nawyn, K.E. (2003). *A security analysis of system event logging with syslog.* SANS Institute, no. As part of the Information Security Reading Room, 2003.
51. Messina, A., I. Fontana, and G. Giacalone. (2015). *Log monitoring and analysis with rsyslog and Splunk.* Institute of Calculation and Networks.
52. Gerhards, R., *The syslog protocol*. 2009, RFC 5424, March.
53. Bierhoff, K., N.E. Beckman, and J. Aldrich. (2009). *Practical API protocol checking with access permissions*. European Conference on Object-Oriented Programming. Springer.
54. Barker, R.. (2020). *The uses and benefits of Splunk in continuous integration.*
55. JDBC protocol configuration options. [cited 2022; Available from: https://www.ibm.com/docs/en/dsm?topic=one-jdbc-protocol-configuration-options.
56. A Quick Guide to Check Points OPSEC LEA. [cited 2022; Available from: https://www.fir3net.com/Firewalls/Check-Point/a-quick-guide-to-checkpoints-opsec-lea.html.
57. Integrate Check Point by using OPSEC. [cited 2022; Available from: https://www.ibm.com/docs/en/dsm?topic=point-integrate-check-by-using-opsec.
58. QRadar: Agentless Windows Events Collection using the MSRPC Protocol (MSRPC FAQ). [cited 2022; Available from: https://www.ibm.com/support/pages/qradar-agentless-windows-events-collection-using-msrpc-protocol-msrpc-faq.
59. Microsoft Security Event Log over MSRPC Protocol. [cited 2022; Available from: https://www.ibm.com/docs/zh/dsm?topic=options-microsoft-security-event-log-over-msrpc-protocol.
60. Pujari, R.S.A.K., Information Systems Security. 2008.

GAZİLİ OLMAK AYRICALIKTIR.