SOC ANALİSTLERİNİN MAKİNE ÖĞRENMESİ ALGORİTMALARI İLE VERİMİNİN ANALİZ EDİLMESİ

Mehmet YILDIRIM

2022
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

Tez Danışmanları
Dr. Öğr. Üyesi İsa AVCI
Dr. Öğr. Üyesi Cihat ŞEKER

SOC ANALİSTLERİNİN MAKİNE ÖĞRENMESİ ALGORİTMALARI İLE VERİMİNİN ANALİZ EDİLMESİ

Mehmet YILDIRIM

T.C.
Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalında
Yüksek Lisans Tezi
Olarak Hazırlanmıştır

Tez Danışmanları
Dr. Öğr. Üyesi İsa AVCI
Dr. Öğr. Üyesi Cihat ŞEKER

KARABÜK
Ağustos 2022

Mehmet YILDIRIM tarafından hazırlanan "SOC ANALİSTLERİNİN MAKİNE ÖĞRENMESİ ALGORİTMALARI İLE VERİMİNİN ANALİZ EDİLMESİ" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Dr. Öğr. Üyesi İsa AVCI .....
Tez Danışmanı, Bilgisayar Mühendisliği Anabilim Dalı
Dr. Öğr. Üyesi Cihat ŞEKER .....
Tez İkinci Danışmanı, Elektrik-Elektronik Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından Oy Birliği ile Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 10/08/2022

Ünvanı, Adı SOYADI (Kurumu)	İmzası
Başkan : Doç. Dr. Muhammed Ali AYDIN (İÜC)	.....
Üye : Dr. Öğr. Üyesi İsa AVCI (KBÜ)	.....
Üye : Dr. Öğr. Üyesi Sait DEMİR (KBÜ)	.....

KBÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulu, bu tez ile, Yüksek Lisans derecesini onamıştır.

Prof. Dr. Hasan SOLMAZ .....
Lisansüstü Eğitim Enstitüsü Müdürü

"Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim."

Mehmet YILDIRIM

ÖZET

Yüksek Lisans Tezi

SOC ANALİSTLERİNİN MAKİNE ÖĞRENMESİ ALGORİTMALARI İLE VERİMİNİN ANALİZ EDİLMESİ

Mehmet YILDIRIM

Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanları:
Dr. Öğr. Üyesi İsa AVCI
Dr. Öğr. Üyesi Cihat ŞEKER

Ağustos 2022, 107 sayfa

Siber güvenlik günümüzde artık ulusal güvenlik stratejilerinden birisi haline gelmiştir. Teknolojinin her geçen gün gelişmesiyle beraber, siber güvenlik hususunda meydana gelen gelişmeler, alınan önlemler ve yasal düzenlemeler yetersiz kalmaktadır. Olası ihtiyacın ve tehditlerin doğrultusunda alınan kararlar ileriye dönük olarak yeterli güveni sağlamamaktadır. İleriye dönük ve güven ortamının oluşması içinse, günümüzde SOC merkezleri kurulmaya başlanmıştır. SOC merkezi bir kurum ya da kuruluşun güvenliğini devamlı olarak izler ve bu merkez güvenlik olaylarında oluşan logların analizinden sorumludur. Bu merkezde çalışan kişilere ise SOC analistleri denilmektedir. Bu analistler siber saldırılara karşı teknolojik çözümler kullanarak, iyi bir süreç yönetimi yapmaktadır ve siber güvenlik olaylarının tespit edilmesini sağlayarak yapılan analizi sunmaktadır. Siber saldırılara karşılık aksiyon almaktadır. Bu araştırma da SOC analistlerinin veriminin analiz edilmesi amacı ile araştırma

çalışması yapılmıştır. Bu çalışmadan elde veriler ile makine öğrenmesi algoritmaları kullanılarak SOC analistlerinin performans verimliliği değerlendirilmiştir. Kullanılan algoritmalarda başarım olarak XGBoost Algoritması en iyi performans göstererek 0.90 Precision, 0.92 Recall, 0.99 Accuracy ve 0.98 F1-Score sonuçları elde edilmiştir.

Anahtar Sözcükler **:** Güvenlik Operasyon Merkezi (SOC), Siber Güvenlik, Dijital Güvenlik

Bilim Kodu **:** 92403

ABSTRACT

Master Thesis

ANALYZING SOC ANALYST'S EFFICIENCY WITH MACHINE LEARNING ALGORITHMS

Mehmet YILDIRIM

Karabuk University
Institute of Graduate Programs
Department of Computer Engineering

Thesis advisor:
Assist. Prof. Dr. İsa AVCI
Assist. Prof. Dr. Cihat ŞEKER

August 2022, 107 pages

Cyber security has now become one of the national security strategies. With the development of technology day by day, developments in cyber security, measures taken and legal regulations remain insufficient. Decisions taken in line with possible needs and threats do not provide sufficient confidence for the future. Today, SOC centers have started to be established in order to create an environment of forward-looking and trust. SOC constantly monitors the security of a central institution or organization and this center is responsible for the analysis of the logs of security events. The people working in this center are called SOC analysts. These analysts use technological solutions against cyber attacks, make good process management and provide analysis by detecting cyber security events. It takes action against cyber attacks. In this research, a research study was conducted with the aim of analyzing the

efficiency of SOC analysts. The performance efficiency of SOC analysts was evaluated using the data obtained from this study and machine learning algorithms. In the algorithms used, the XGBoost Algorithm showed the best performance and 0.90 Precision, 0.92 Recall, 0.99 Accuracy and 0.98 F1-Score results were obtained.

Keywords : Security Operations Center (SOC), Cyber Security, Digital Security
Science Code : 92403

TEŞEKKÜR

Bu tez çalışmasının planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren sayın hocam Dr. Öğr. Üyesi İsa AVCI'ya, çalışma arkadaşım Evren PAZOĞLU'ya, işyerimde bana destek olan yöneticilerime ve ekip arkadaşlarıma sonsuz teşekkürlerimi sunarım.

Hiçbir yardımını esirgemeden yanımda olan sevgili eşim Elif YILDIRIM'a tüm kalbimle teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

BÖLÜM 1

GİRİŞ

Geçmişten günümüze kadar insanlık tarihine baktığımızda, toplumsal gelişim ve değişimin farklı etkenler ile, çeşitli dönemlerde çeşitli özellikler ile birlikte hızla gerçekleşmiş olduğu görülmüştür. İlkel çağdan günümüze kadar teknoloji ve bilgi, toplumsal gelişimin ana itici gücünü oluşturmaktadır. Daha fazla ilgi çekici olanıysa, 1950'li yıllardan sonra, teknolojik gelişmelerin tümü insanlık tarihindeki teknoloji olanakların hemen tümünden daha çok ve hızlıdır. İnsanlık tarihinde insan, ateşin buluşundan, pişirilen tuğlaya yaklaşık bin senede geçebilmiştir. Pişirilen tuğladan ilk buhar makinelerine geçişse, on bin yılda gerçekleştiği bilinmektedir. Daha sonra elektriğin icadı ile birçok teknoloji de beraberinde gelişmeye başlamıştır. Atom enerjisi, uzay teknolojileri, internet, bilgisayar, nano-teknoloji vb. gelişmelerinde ise ne on bin sene ne de onlarca sene beklenilmesi gerekmektedir. Teknoloji de baş döndüren bu hızlı gelişme insanlığı şaşkına çevirmiştir.

Günümüzde kurumsal ve bireysel anlamda vazgeçilmeyen bir unsur haline gelmiş bilgisayar, öncelikle haberleşme, şifreleme ve şifre çözme amaçlı olarak gelişmiştir ve ilerleyen dönemlerde kullanımı da giderek artış göstermiştir. İnternet ise 1960 yıllarında ABD savunma bakanlığı tarafından olası bir savaş halinde iletişimin zarar görmemesi maksadıyla, kullanıma devam edebilmesi için bilgisayardaki verilerin başka bilgisayara aktarılması amacı ile kurulan "ARPANET" ile ortaya çıkmıştır. İnternet, milyonlarca cihazın ve ağın birbirleri ile iletişimi sağlayan teknoloji olarak bilinmektedir. Belli protokoller kapsamında bilgi alışverişinin yapılmasına imkân sağlamıştır. İnternet, haberleşme, bilgi alışverişi ve aynı zamanda bilgisayar-kullanıcı arasındaki bağlantıyı sağlayabilmesi sebebiyle, bütün dünyada kullanılmış olan hızlı yaygınlaşmanın adıdır. Bilişim teknolojileri, hızlı gelişme sayesinde artış gösteren

internet kullanımı ile, “özel sektörde, kamuda ve kişisel” ölçekte hayatın vazgeçilmeyen bir unsuru haline gelmiştir. İnternet ve bilişimin dünyada bir anda yaygınlaşması ile kullanıcılara sınırsız özgürlük tanımaktadır. Diğer taraftan internet ve bilişimin yaygınlaşması ile birlikte oluşan güvenlik açıklıkları ve bilişim sisteminin kötüye kullanılması, bu kapsamda bir suç işleme mekanizmasına dönüşmektedir. Bunun önlenebilmesi için de “SOC (Security Operation Center)” merkezleri, yani güvenlik operasyon merkezleri kurulmuştur. Güvenlik operasyon merkezlerinde izleme, tespit etme vb. siber güvenlik işlemlerinin yapıldığı bir merkezdir. SOC denildiğinde özetle; bir kuruma gelen “ihlal, saldırı, tehdit, analiz, soruşturma, müdahale ve önleme” aşamalarının planlanmış olduğu bu süreçlerin aşama aşama, kısım kısım takip edildiği yer olarak açıklayabiliriz. SOC merkezi, web sitelerin, veri tabanları, sunucular, ağlar ve kritik altyapılar gibi sistemlerin güvenliğinin tek bir merkezden yönetilmesine olanak sağlamaktadır. Bu araştırmada SOC analistlerinin veriminin analiz edilmesi amaç edinilmiştir.

BÖLÜM 2

GENEL KAVRAMLAR VE TANIMLAR

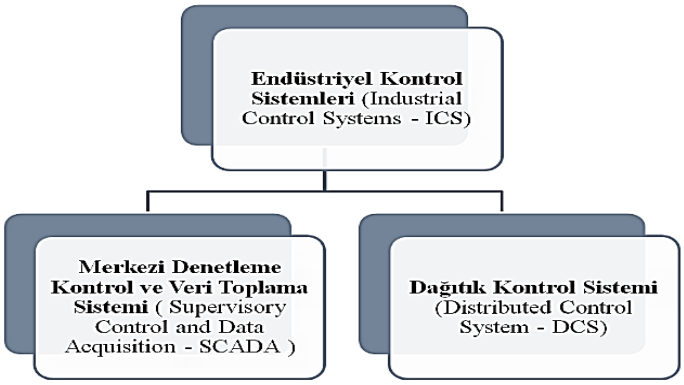
2.1. SİBER GÜVENLİK

Bilginin insan hayatında vazgeçilmez bir yeri vardır. İçerisinde yaşamış olduğumuz bu bilgi çağında ve teknolojinin de hızla gelişmesiyle birlikte, hayatımıza getirmiş olduğu yenilikler ve kolaylıkların etkisinin de görülmesi kısa zamanda görülmektedir. İnsanların teknolojiye olan bağımlığı artış gösterdikçe teknolojinin dezavantajları da artış göstermiştir. İletişim ve bilgi teknolojilerinin hızlı bir şekilde her geçen gün gelişmesi, sistem ve teknolojilerin sunmuş olduğu hizmetin yaygınlaşması ile, iletişim ve bilgi teknolojilerinin özellikle de "sosyal, siyasi, finansal ve askeri" anlamdaki etkisi de artış göstermiştir. Bütün bu gelişmelerin ışığında birden fazla kuruluş, kurum ve kişi, bilgi iletişim teknolojilerini en üst seviyede kullanmaya başlamışlardır. Bilgi teknolojileri bütün bu faaliyetlerin ayrılmayan birer parçası haline gelmiştir. Netice olarak bilgi teknolojileri, devletlerin kritik altyapı sektörleri için, yaşamsal derecede önem taşıyan hale gelmiştir. Son zamanlarda organize terör ve suç örgütlerinde eğitim, planlama, propaganda ve bilgi teknolojileri kullanılmaktadır. Siber tehdit ve saldırılar ile beraber, siber güvenlik savunma etkinlikleri de devletler, kuruluşlar ve kurumların nazarında büyük bir hale gelmiştir [1].

Siber saldırılar ve tehditler, hasar gördüğünde ve/veya yok edildiğinde vatandaşların güvenliğini, sağlığını ve ekonomik refahını veya kamu hizmetlerinin sağlanmasını olumsuz yönde etkileyen hayati tesisleri, ağları, hizmetleri ve varlıkları hedef almaktadır. Tüm bunlar devletlerin ülkeden ülkeye değişimi ile, "enerji, finans, ulaşım, sağlık, temel kamu ve akıllı şebekeler" hizmetlerinin alt yapısını oluşturmaktadır ve tüm bunların hepsi kritik alt yapılar olarak tanımlanmıştır [1].

Kritik bütün alt yapı sektörlerinin dağılımlarını ve karmaşıklığını çözebilmek için, tüm

bu sektörlerin operatörleri tarafından uzaktan gözlemlenmiş olması, komuta edilmesi ve kontrol edilmesi gereklidir. Günümüzdeki ağ sistemlerinden, operatörlerinden ya da yetkililerin kritik altyapı alanlarını uzaktan kontrol etmesi, yönetmesi ve izlenebilmesini sağlamaktadır. Günümüzdeki teknolojide bu sistemler Merkezi İzleme ve Veri Toplama Sistemi (SCADA - Supervisory Control and Data Acquisition) ve Distributed Control System – DCS şeklinde 2 gruba ayrılmaktadır. Adı geçen bu sistemler genel olarak elektriğin dağıtımı ve üretimi hususunda "sulama sistemleri, barajlar, doğalgaz sistemleri, fabrikalar, petrol rafinerisi" vb. endüstriyel tesis bazlı ve altyapı süreçlerini izleyen ve kontrol edebilen "Endüstriyel Kontrol Sistemlerini (EKS)" ifade etmektedir. "SCADA" sistemleri ile "DCS" arasındaki ana fark, "SCADA" sistemlerinin çok geniş alana dağıtılmış olması yatmaktadır [2].



Şekil 1.1 Endüstriyel kontrol sistemleri [2].

EKS, kritik altyapı alanlarının "cep telefonu, tablet ya da bilgisayar" aracılığı ile tek bir cihaz ve merkezden izlenilmesine olanak tanımaktadır. Bu işlevi ile sistemlerin kontrol, denetim ve yönetimini kolaylaştırsa da ciddi güvenlik sorunları da ortaya çıkarmıştır. Bunun nedeni ise, mevcut bulunmuş olduğu ağda "EKS" üstünden gerçekleştirilebilir saldırıların "donanım, yazılım ya da insan kaynaklı" hatalar bütün ağın sistemine etki etmektedir. Kritik altyapı sektörlerinin karşılaşmış olduğu siber tehditler, büyük bir özen ve dikkatle tasarlanmaktadır. Bu nedenle savunma stratejilerinin geliştirilmesi ve dikkate alınması gerekmektedir [3].

Son dönemlerde tüm dünya genelindeki kurum ve kuruluşlar, alt yapı sektörlerini

“EKS” sistemlerini tehditlerden koruyabilmek için, savunma ve siber güvenlik faaliyetine hız vermişlerdir. Siber güvenlik ve savunmanın sağlanabilmesi için “yasal, idari ve teknik” kapasitenin geliştirilebilmesi, milli donanım ve yazılımların üretimi, kritik alt yapı sektöründe mümkün olduğu sürece milli güvenlik sistemlerinin kullanımı büyük bir önem kazanabilmiştir. Saldırıların siber uzaya etkilerini en aza indirebilmek için, kritik alt alanlarının belirlenmesi gerekmektedir. Güvenliğin sağlanabilmesi ve alınan yasal/teknik tedbirlerin geliştirilmiş olması gerekmektedir. Tüm bunların önemi gün geçtikçe artış gösterdikten sonra siber güvenliğin kuramı, geleceğin en popüler hususlarından birisidir [3].

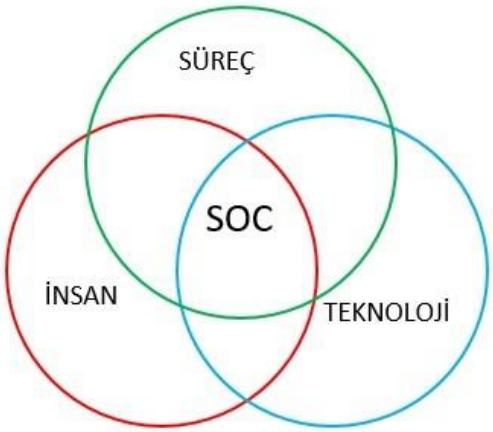
2.2. SOC (SECURİTY OPERATİON CENTER)

Güvenlik Operasyonları Merkezi, bir organizasyonun siber güvenlik sorunlarıyla ilgilenen merkezi bir birimdir. SOC, tanımlanmış süreçlere sahip, yetenekli bir grup insan olarak çalışır ve entegre güvenlik istihbarat teknolojileri tarafından desteklenir. ICT (Bilgi ve İletişim Teknolojisi) sistemlerini izleyen ağ güvenliği analistleri için bir merkezdir. SOC, tutarlı stratejik desteğe sahip genel güvenlik operasyonları ortamının bir parçası olarak özellikle siber tehdit gözetimi, adli soruşturma ve olay müdahalesi ve raporlamaya odaklanır. Sonuç olarak, bir Güvenlik Operasyon Merkezinin birincil amacı, bir kuruluşun güvenliğini ICT gözetimi yoluyla geliştirmektir. Başka bir deyişle, bir SOC, sistem analistlerini ve mühendislerini içeren bir ekip olarak tanımlanabilir. Bu son derece yetenekli ekip, ağı günde 24 saat, yılda 365 gün izler. SOC, kurumu siber tehditlere karşı korur ve müdahale eder. SOC özellikle siber tehditler, gözetim, adli soruşturma ve olay yönetimi ve raporlamaya odaklanmaktadır [4].

Bir SOC aşağıdaki gibi adlandırılabilir [4];

1. “*Bilgisayar Güvenliği Olay Müdahale Ekibi (CSIRT)*
2. *Bilgisayar Olayı Müdahale Ekibi (CIRT)*
3. *Bilgisayar Olayı Müdahale Merkezi (CIRC)*
4. *Bilgisayar Güvenliği Olay Müdahale Merkezi (CSIRC)”*

SOC kendisini insanlar, süreçler ve teknoloji olarak tanımlar. Şekil 2.2, bir SOC'un üçlülerini göstermektedir. Özetle, SOC'un üç yönü vardır: insanlar, süreçler ve teknoloji.



Şekil 2.2. SOC'un 3 önemli bileşeni [60].

SOC iyi planlanmış olmalıdır çünkü bir SOC planlama kadar iyidir. Bu ekip bilgisayar ağlarında yasaklanmış olanlara karşı savunma yapar. SOC personeli, sistem ağı savunması (CND), işletim sistemleri (OS), ağ güvenlik duvarı donanımları, yönlendirici sistemleri, "switchler, güvenlik duvarları, programlama, veri tabanları, adli analiz, İzinsiz Giriş Tespit Sistemleri (IDS) ve İzinsiz Giriş Önleme Sistemleri (IPS)" verileriyle ustalıkla analiz yapar. SOC organizasyonunda aranan nitelikler dört evreden oluşur"[4]. Bunlar;

1. Tier 1 (Seviye 1) Güvenlik Analisti
2. Tier 2 (Seviye 2) Güvenlik Analisti veya Olay Müdahale (Incident Response) Görevlisi
3. Tier 3 (Seviye 3) Güvenlik Analisti (Threat Hunter)
4. SOC Yöneticisi

Yapılan başka bir çalışmada araç olarak anket formları kullanılmıştır. Anketin içeriği, kavramsal modele dayanıyordu. Amacı, SOC'un başarılı bir şekilde geliştirilmesi ve uygulanması için bir model geliştirmektir. Bunlar; insan, süreç ve teknoloji olarak 3

unsuru kapsamaktadır. Anket formları iki kategoriye ayrılmıştır. İlk yöntem, verilen ifadelere doğru veya neredeyse doğru cevabı kabul ettiği şeklinde uygulamıştır. Bu yöntemin seçilmesi, analizin verimli, doğru ve doğrudan anket formuna dayalı olarak gerçekleştirilmesine olanak tanır. İkinci yöntem, bir (1) ila beş (5) arasında ölçmek için bir Likert ölçeği kullanılmıştır. Likert ölçeği, görüşleri, algıları ve davranışları ölçmek için güvenilir bir yol sağlayabileceğinden anketin yaygın bir biçimidir. Ayrıca, katılımcıların herhangi bir ifadeye katılıp katılmadıklarını da gösterir [64]. Çalışmamızda araştırma sorularının hazırlanması ve fikir oluşturması açısından bu makaleden yararlanılmıştır.

2.2.1. Tier 1 (Seviye 1) Güvenlik Analisti

Bu personel, güvenlik sensörlerinin ağı ve sağlığını sürekli olarak izlemeli ve uç noktalar güvenlik uyarılarına öncelik vermelidir. Seviye 2 (Level 2) analiste aktarılmak üzere hassas verileri toplar. Bunlar, Seviye 1 (Level 1) analistin görevlerindendir. Öte yandan, izinsiz giriş tespiti, ağ güvenliği, TCP/IP Protokolleri, SQL, ana bilgisayar tabanlı sorgulayıcı eğitim, güvenlik bilgileri ve olay yönetimi (SIEM) ve araç tabanlı eğitimlerin Seviye 1 SOC analistin gereksinimleridir [4].

2.2.2. Tier 2 (Seviye 2) Güvenlik Analisti veya Olay Müdahale (Incident Response) Görevlisi

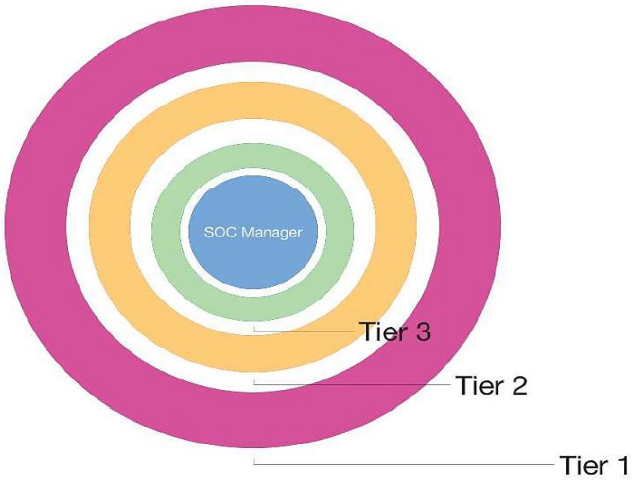
SOC Seviye 2 veya olay müdahale görevlilerinin, çeşitli kaynaklardan veri toplayıp ilişkilendirerek ve sistemlere zararlı olup olmadıklarını kontrol ederek olayların derinlemesine analizini yapmaları gerekmektedir. Kritik sistemler veya veriler zarar gördüğünde, yeni analiz yöntemleri arayıp ve bunları tespit edilen tehditlere uygularlar. Seviye 1 analist ile karşılaştırıldığında, Seviye 2 güvenlik analisti ağ, adli tıp, ana bilgisayar tabanlı adli tıp, olay müdahale teknikleri, günlük (log) kaydı, temel kötü amaçlı yazılım algılama ve tehdit istihbaratı hakkında daha ileri düzeyde bilgiye sahip olmalıdır [4].

2.2.3. Tier 3 (Seviye 3) Güvenlik Analisti (Threat Hunter)

SOC Seviye 3 analistler tehdit avcısı (threat hunter) olarak da görev alırlar. Seviye 3 uzmanlar, ağ, uç noktalar, tehdit istihbaratı, adli tıp ve kötü amaçlı yazılım analizi hakkında derinlemesine bilgi sahibidir. Ayrıca, SOC Seviye 3 uzmanları, BT altyapısı, anomali tespiti ve tehdit istihbaratı konusunda da derin bir bilgiye sahiptir [4].

2.2.4. SOC Yöneticisi

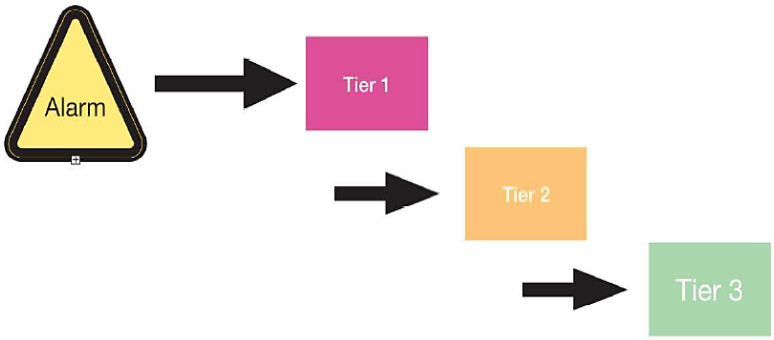
SOC yöneticisi, personel, bütçe, vardiya planlaması ve teknoloji stratejisiyle ilgilenir. Önemli iş etkinlikleri için kurumsal uç nokta görevi görür ve SOC üzerinde genel kontrole sahiptir. SOC Yöneticisi, işi etkileyebilecek olayları tespit etmek, araştırmak ve azaltmak için kaynakları hesaplamak ve düzenlemekten sorumludur. SOC yöneticisi bir süreç modeli oluşturur ve olay işleme süreci için önceliklendirme ve yanıt günlükleri aracılığıyla analistlere rehberlik etmek için yapılandırılmış çalışma talimatları sağlar. Proje yönetimi, olay müdahale yönetimi ve insan yönetimi, SOC yöneticisi için talep edilen becerilerdir [4].



Şekil 2.3. SOC organizasyonu [4].

2.2.5. Süreç

SOC disk görüntülerinin veya nesnelerinin gelişmiş adli analizlerini yapabilmektedir. Bir olaydaki saldırının niteliğini belirlemek için tam oturumda paket yakalama veya toplanan kötü amaçlı yazılım örneklerinin tersine mühendisliğini yapabilmektedir. Bazen adli kanıtları yasal olarak güvenli bir şekilde toplamak ve analiz etmek önemlidir. SOC, bu tür durumlarda prosedürlerindeki gibi katı ve tekrarlanabilir olmalıdır. SOC iş akışı modeli aşağıdaki Şekil 2.4'te gösterilmektedir [4].



Şekil 2.4. SOC iş akış modeli [5].

SOC analistleri, olayların tekrarlanabilir bir triyajını ve inceleme prosedürlerini tanımlarlar. Tekrarlanabilir bir kriz müdahale süreci tasarlayarak, ekip üyelerinin rolleri ve faaliyetleri, bir uyarı oluşturulmasından ve ilk Seviye 1 değerlendirmesinden, personelin Seviye 2 veya Seviye 3'e yükseltilmesine kadar haritalandırılır. Kaynaklar, SOC iş akışına göre verimli bir şekilde tahsis edilebilir. En popüler olay müdahale süreci modeli DOE/CIAC'dır. NIST 800 serisinde (Dempsey ve diğerleri), bu model altı aşamadan oluşur: hazırlık, tanımlama, sınırlama, imha, kurtarma ve alınan derslerdir.

2.2.6. Teknoloji

Şirketin güvenlik duruşu doğrultusunda doğru çevre bilincini sağlayan bir dizi teknoloji ürünü ile bir SOC kurulmalıdır. SOC, iş için tam olarak hangi kaynakların doğru olduğunu belirlemek için doğru teknolojileri seçerken profesyonel güvenlik

detayı vermelidir [2]. Gerekli araçlardan bazıları, izinsiz giriş algılama ve önleme teknolojisini içerebilir; SIEM sistemleri, tehditleri ve güvenlik açıklarını ele almak için yazılım, filtre teknolojileri, veri kaybı önleme araçları, trafik / paket denetim çözümleri, veri analizi için çerçeveler ve gözetim teknolojileridir [2].

Teknolojik çözümler gerekli olmakla birlikte, teknolojinin geliştirilmesini sağlamak yüksek maliyet gerektirebilir. SOC uygulama girişimleri, önce SOC gereksinimlerini karşılamak için kuruluş içinde nelerin mevcut olduğunu değerlendirmelidir. SOC'a daha sonra yeni araçlar ve teknolojiler ekleyerek mevcut yetenekleri geliştirebilir ve genişletebilir. Teknolojiler dört kategoriye ayrılır [4]:

1. Günlük Kaydetme (Logging)
2. Veri Yönetimi (Data Management)
3. Analiz (Analysis)
4. İş Akışı (Workflow)

2.2.6.1. Günlük Kaydetme (Logging)

Günlüğe kaydetmenin amacı, SOC analizini gerçekleştirmek için gereken temel kapsamı dahil etmektir. İdeal olarak, bir SOC, bir hizmet içindeki olayları kapsamak için gereken sınırlı bilgileri toplar, ancak ek veri kaynakları kullanılabilir hale geldikçe, bunları sorunsuz bir şekilde sağlayabilir. Günlüğe kaydetme uygulamalarının doğası ve yeteneklerinin kapsamı değişebilir [6].

2.2.6.2. Veri Yönetimi (Data Management)

Veri yönetim sisteminde iki ana rol vardır: birincisi, verilerin protokol katmanından dağıtılması ve ikincisi, verilerin verimli depolanması. Her iki prosedür de güvenli bir şekilde gerçekleştirilmelidir. SOC'un gerçek zamanlı işlevselliğe sahip olup olmamasına ya da birleşik veya hiyerarşik bir modelin kullanılmasına bağlı olarak, farklı veri işleme sistemleri kullanılabilir. Bazı hususların da ele alınması gerekir: Örnek olarak; kararlı yarı iletken, veri normalizasyonu ve ölçeklenebilir seçimi

kolaylaştırmak için ağ bağlantıları arasında veri tekrarını en aza indirmek gerekir. Bu noktada, verileri daha fazla filtrelemek ve yalnızca ilgili bilgileri toplamak mümkündür [6]. Veriler toplanırken, belirli güvenlik duruşunu belirlemek için analitik katmanı tarafından analiz edilir. Bazı SIEM sistemleri, aşağıdaki bilgi işlem etkinliklerinden bir veya daha fazlasına dayanır:

1. Veri normalleştirme - ağ, ana bilgisayar ve cihaz veri toplama için standart bir çerçeve sağlar ve daha fazla metin çalışmasına olanak tanır.
2. Veri sınıflandırması - çeşitli olayların terminolojilerine göre bir tanımını sağlar.
3. Veri korelasyonu - BT ile ilgili olayların biçimleri açısından sınırlı esneklikle başlayan araçlar sağlar. Korelasyonlar ayrıca fiziksel ve kavramsal konum bilgilerini de dikkate alabilir. Teknolojiler, çok aşamalı saldırıları belirlemek için daha gelişmiş yetenekler eklenebilir.
4. İstatistiksel analiz - daha ilgili olayları algılamak için zaman ve mekân (birden çok cihaz) üzerinde çalışarak üç seviyeli olayların daha istatistiksel analiziyle ilişki kurma yeteneğini genişletir.

2.2.6.3. İş Akışı (Workflow)

Siber olaylarda aksiyon önceliklidir. Siber olaylara genellikle işle alaka düzeyine göre öncelik verilir. Bunlar ayrıca gerekli teknik becerilere bağlı olarak derecelendirilebilir. SOC'u destekleyen teknolojiler, iş biletlerinin gönderilmesini de sağlamalıdır. Ortak bilet sistemleri, belirli prosedürlere uyarlanabilen bireysel yapılandırma seçenekleri sunar. Çoğu kurumsal koruma yönetimi paketi, siber olaylara müdahalenin izlenmesine olanak tanıyan iş akışı araçlarını da içerir [6].

2.3. SIEM (SECURITY INFORMATION EVENT MANAGEMENT)

Güvenlik Bilgileri ve Olay Yönetimi (SIEM) sistemleri; yazılımları, servisleri, Güvenli Bilgi Yönetimi (SIM) ve Güvenli Olay Yönetim (SEM) özelliklerini bir arada kullanırlar. Güvenlik Olay Yönetiminin (SEM), gerçek zamanlı izleme, olayların korelasyonu, ikazlar ve konsol görüntüsü gibi özellikleri varken; Güvenlik Bilgi Yönetiminin (SIM) log analizi ve raporlama gibi özellikleri vardır. Bu iki işlevi bir

araya getiren SIEM sistemleri, kuruluşların güvenlik ihtiyaçlarını tek bir merkezden hızlı ve kolay bir şekilde karşılamak için kullanılır. Bunu yaparken tek bir platform üzerinde birçok aracı kullanabilir. Günümüzde SIEM sistemleri şirketler tarafından yaygın olarak kullanılmaktadır. Hewlett Packard tarafından yapılan bir araştırmada şirketlere "SIEM sistemlerini kullanıyor musunuz veya kullanmayı planlıyor musunuz?" diye sorulduğunda, %42'si kullandığını, %10'u hiç ilgilenmediğini, %48'inin ise kullanabileceğini belirtmektedirler [7].

SIEM sistemleri aşağıdaki görevleri yerine getiren unsurlardan oluşmaktadır. Bu görevler [8];

1. *"Log toplama ve yüksek depolama kabiliyeti*
2. *Filtreleme*
3. *Ön Hazırlık*
4. *Normalizasyon*
5. *Kural oluşturma*
6. *Veri zenginleştirme ve bağlam yapma*
7. *Korelasyon*
8. *Olay gruplandırma*
9. *Gerçek zamanlı analiz, alarm üretme ve raporlama."*

Log yönetimi ve SIEM birbirine bağlı sistemlerdir. Özellikle aktif log yönetimi korelasyon tekniklerini kullanır ve SIEM kavramına girer. Ağlarda günlük oluşturmak için birçok araç vardır. Özellikle sistemlerin kritikliğine veya boyutuna bağlı olarak bağlantı kurmak ve tüm kayıtları hemen veya sonrasında kontrol etmek zorlaşmaktadır. Bu sorunu çözmek için tasarlanmış SIEM sistemleri; Farklı kaynaklardan gelen log kayıtlarının ilişkilendirilip analiz edilmesini ve yöneticiye uyarı gönderilmesini sağlayan sistemlerdir. SIEM ürünlerinde, logları analiz etmek için bir veya iki günlük sunucusu ve günlükleri depolamak için bir veya daha fazla veri tabanı sunucusu bulunur. SIEM ürünleri günlükleri iki şekilde toplar. Ajansız ve Ajan tabanlı olmak üzere iki türü vardır [9].

Ajansız: SIEM sunucusu, herhangi bir yazılım gerektirmeden sunuculardan günlükleri

toplar. SIEM sunucusu, olay filtreleme, olay birleştirme, günlük normalleştirme ve toplanan günlüklerin analizini gerçekleştirir. Bu yöntemin avantajı, günlük toplama sistemlerine herhangi bir aracı programın yüklenmesine gerek olmaması ve çok büyük sistemler için kullanılabilmesidir. Dezavantajı, log toplama sistemlerinde filtreleme ve sadeleştirme olmadığı için merkezde toplanan kayıtlar büyük ve karmaşıktır. Bu nedenle, onları filtrelemek ve analiz etmek çok zaman alır. Diğer bir dezavantaj ise, SIEM sunucusunun günlükleri toplarken tüm sistemlerden kimlik doğrulaması gerektirebilmesidir. Bu, bazı durumlarda zaman alıcı olabilir [10].

Ajan tabanlı: Ajan programı, günlük oluşturma sistemlerine kurulur; bu program, günlükleri filtreler ve normalleştirir ve genellikle gerçek zamanlı veya neredeyse gerçek zamanlı olarak analiz için SIEM sunucusuna iletir. Bazı SIEM ürünleri, yöneticilere farklı günlük biçimlerini kullanmak için özel olarak hazırlanmış aracı programları sunar. Bu yöntemin avantajı, SIEM sunucusu kapatılsa dahi veri kaybı olmaması ve log toplama zamanlarının yönetici tarafından ayarlanabilmesidir. Dezavantajı ise; saldırganların müdahale ederek kullanılan ajan programlarını özelleştirebilme, bu programların log göndermesini engelleme ve veri kaybı gibi işlemleri gerçekleştirebilmeleridir [10].

Ajan tabanlı veya ajansız olsun, SIEM sunucusu, çeşitli kaynaklardan gelen günlük kaynaklarını analiz eder ve ilişkilendirir, önemli olayları tanımlar ve istenirse olaylara göre hareket eder. SIEM ürünleri için belirlenmiş bir standart yoktur. Bu nedenle SIEM ürünleri verileri farklı formatlarda saklayabilir ve aktarabilir. Ayrıca SIEM ürünleri, günlük kayıtları için erişilebilirlik, bütünlük ve gizlilik ilkeleri sağlar. Bu nedenlerle SIEM ürünleri günümüzde birçok kurumda yaygın olarak kullanılmaktadır [11].

2.4. GÜVENLİK OPERASYONLARI MERKEZİ (SOC) NESİLLERİ

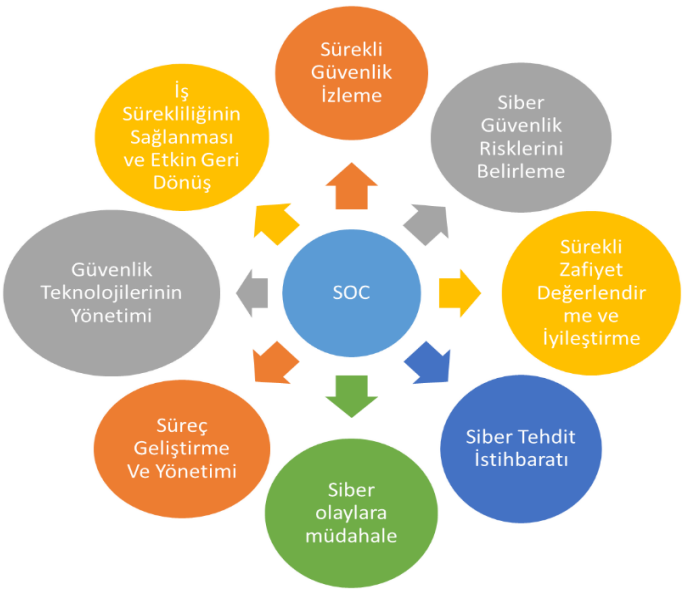
Güvenlik Operasyon Merkezi, tüm sistemi uçtan uca izleyerek kurum içinden yapılabilecek olası siber saldırılar veya insan yaralanmalarına karşı izleme ve önlem alma merkezidir. Güvenlik operasyonları merkezleri, güvenlik açıklarını, virüsleri ve kötü amaçlı kodları yönetme, güvenlik olaylarını yönetme, kuruluşun bilgi güvenliğine

yönelik tehditleri analiz etme, yönetme ve günlüğe kaydetme gibi görevleri yerine getirmektedir [11].

2.5. GÜVENLİK OPERASYONLARI MERKEZİ (SOC) MODELLERİ

SOC kavramını bilmeyen ama merak edenler için görselleştirmek adına bu anlamlı cümle ile yazıma başlamak istedim. Çünkü burada başkalarını tanıma ve "tehlikede olmama" noktası aslında bu merkezi kapsamaktadır. Saldırganlar, bilgisayar korsanları ve hatta bot denilen sanal makinelerdir [14].

Güvenlik Operasyonları Merkezi (SOC), Siber güvenlik ile ilgili tüm olaylarını tespit ettiğinde, analiz ederken ve önlerken, herhangi bir kuruluşun güvenlik duruşunu devamlı olarak izlemek ve iyileştirebilmek için insanları, teknolojileri ve süreçleri kullanmakta olan, büyük öneme sahip bir olgudur. SOC merkezinde genel olarak güvenlik operasyonları ve güvenlik analistlerini denetleyebilen, yöneticiler ve mühendisler yer almaktadır [12].



Şekil 2.5. Güvenlik operasyonları merkezi (SOC) [14].

2.5.1. Güvenlik Operasyonları Merkezinde Yapılan Eylemler

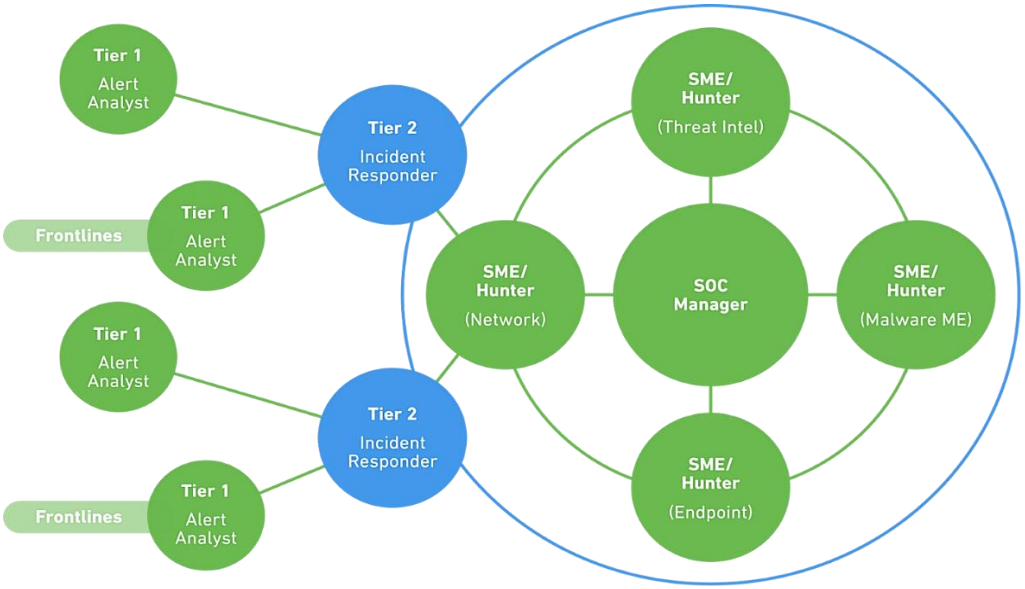
Bir SOC merkezinin stratejisinde, bütün organizasyonları daha verimli ve daha güvenli hale getirebilmek için, verilerin toplanılmasını ve bütün verileri şüpheli etkinlikler için analiz edebilmek için, tehdit yönetiminin etrafında dönmektedir. SOC merkezi ekiplerinin etrafında izlenen ham verilerin hepsi güvenlik ile ilişkilidir. Güvenlik duvarlarında, "tehdit istihbaratı (threat intelligence), izinsiz giriş önleme ve tespit sistemleri (IPS/IDS'ler)", güvenlik soruşturma, güvenlik bilgi ve olay yönetimi (SIEM)" sistemleri tarafından toplanmaktadır. Verilerin anormal olduğu ya da tehlike göstergeleri olan "IOC'ler" olduğu zaman ekip üyeleri tarafından iletişime geçebilmek için uyarılar oluşturulabilmektedir [13].

SOC'un Amacı

Teknolojinin çözümlenmesi ve güçlü bir dizi sürecin kombinasyonu kullanılarak, siber güvenlik olaylarını tespit ederek, bunlara yanıt vermektedir [13].

SOC'un İçeriği

Tipik bir SOC altyapısı "Firewall (Güvenlik Duvarı), IPS / IDS (Intrusion Prevention/Detection System), DLP (Data Loss Protection), Endpoint Security ve SIEM (Security Information and Event Management)" sistemi içerir [13].



Şekil 2.6. SOC rolleri [13].

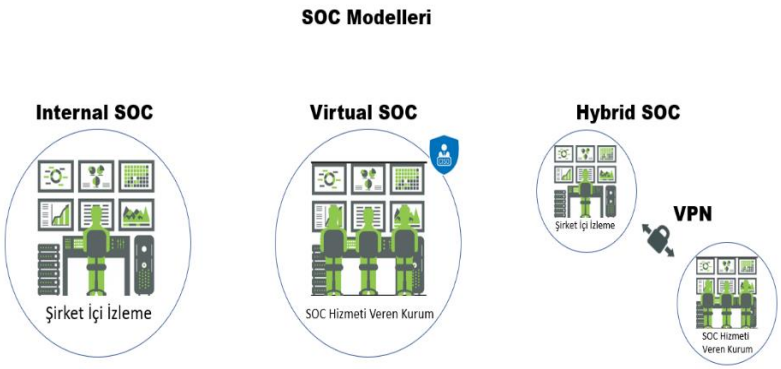
Güvenlik operasyonu kapsamında hem kullanılan güvenlik araçlarından hem de SOC ekiplerinde oluşturulan bireylerden meydana gelmektedir [14].

Level 1 Analisti (Analyst) (Tier 1): Analistler, gelen tüm uyarıları izlemektedir ve gerçek bir olayın meydana getirmiş olduğu doğruladıktan sonra, gerekirse Seviye 2 analiste eskale etmekten sorumlu olmaktadır [14].

Olay Yanıtlayıcısı (Incident Responder) (Tier 2): Olayların derinlemesine olan çalışmalarından ve ortadan kaldırılmış olmasında ya da alınması gereken tüm önlemlerden sorumlu olmaktadır [14].

Tehdit Avcısı (Threat Hunter) (Tier 3): Ağ oluşturma, uç noktalar, tehdit istihbaratı ve kötü amaçlı yazılım, tersine mühendislik konularında uzmanlığa sahiptir. Sistem üzerindeki etkilerini ve bunların nasıl yok edileceğini belirlemek için kötü amaçlı yazılım sürecini izleme hususunda uzmanlaşmıştırlar. Aynı zamanda, potansiyel tehdidi algılamak ve algıladıktan sonra tehdit araçlarını uygulama ile yakından ilgilenmektedirler. Tehdit avcıları da ağda bulunan fakat henüz tespit edilmeyen siber tehditleri aramaktadır [14].

SOC Yöneticisi (SOC Manager): Ekibin bütün kaynaklarını yönetmektedir ve daha büyük organizasyonlar ya da müşteriler için iletişim noktası olmaktadır [14].



Şekil 2.7. SOC modelleri [14].

Takımlara hangi iş rollerine dahil edileceğine karar verilmesinin yanında, belli bir organizasyonun uygulanabileceğine yönelik birkaç SOC modeli bulunmaktadır. Bu modeller şu şekildedir [14];

Özel veya Kendi Kendini Yöneten (Dahili) SOC (Dedicated or Self-Managed (Internal) SOC) : Bu modelin kendine özgü ekibi ve özellikleri bulunmaktadır [14].

Virtual SOC (Sanal SOC): İlgili bu modelin bir özel dahili kurulumu bulunmamaktadır. Sanal bir SOC için, kurum ve kuruluşlar tarafından çalıştırabilmektedir ya da tamamı ile yönetilebilmektedir. Kurumsal bir SOC için, tipik bir yerel personel ya da yerel isteklere bağlı, bulut sisteme konumlandırılmış personeli bulunmaktadır. Literatürde "SOC veya Hizmet olarak SOC (SOCaaS)" olarak da bilinmekte olan tam anlamı ile yönetilebilen, bir sanal SOC'un dahili personeli bulunmamaktadır [15].

Dağıtılmış (Hibrit) SOC (Distributed (Hybrid) SOC): Ortak bir şekilde yönetim sistemidir. Bu modelde 3'üncü tarafta yönetilen güvenlik hizmeti sağlayıcıları "(MSSP)" ile çalışılması üstüne, dahili bir şekilde işe alınmış olan, kısmi ve özel olarak ayrılan tam zamanlı ya da yarı zamanlı ekip üyeleri bulunmaktadır [16].

Yönetilen SOC (Managed SOC): İlgili bu modelde, "MSSP"ler belli bur kurum ve kuruluş için bütün SOC hizmetini sağlamaktadır. "Yönetilen Algılama ve Yanıt (MDR)" iş ortağı, yönetilmiş olan SOC'un başka birer biçimidir [15].

Komut SOC (Command SOC): Bu model ise, tipik bir şekilde tahsis edilmiş olan SOC merkezinde tehdit istihbaratlarına karşı iç görüleriyle güvenlik uzmanlığı sağlamaktadır. Belli bir komut olarak SOC, gerçek güvenlik operasyonunda ya da sürecinde yer almamaktadır. Sadece istihbarat tarafında yer almaktadır [16].

Füzyon Merkezi (Fusion Center): Bu modelde, diğer SOC türleriyle ya da BT departmanları dahil edilmesi üstüne, güvenlik odaklı herhangi bir girişimi ya da tesisi denetlemektedir. Füzyon merkezi, gelişmiş SOC olarak da kabul edilmektedir ve BT operasyonlarında DevOps ve ürün geliştirme vb. iş ekipleri ile beraber çalışmaktadır.
Çok işlevli SOC (Multifunction SOC): Bir kurum ya da özel bir tesisi bulunmaktadır. Fakat sorumlulukları ve rolleri, BT yönetiminin diğer kritik alanlarını da (NOC gibi) kapsamaktadır [16].

SOCaaS: Yazılım ve abone tabanlı bu modeller de SOC süreçlerinin belli bir kısmı ya da tamamı bir bulut sağlayıcısı tarafından kaynağı sağlanmaktadır [16].

2.5.2. SOC'un Faydaları

Bir güvenlik operasyon merkezinin ana faydası, veri etkinliğinin sürekli izlenmesi ve analizi yoluyla güvenlik olaylarının daha iyi tespit edilmesidir. SOC ekipleri, bir kuruluşun ağlarını, uç noktalarını, sunucularını ve veri tabanlarındaki bu etkinlikleri 7/24 analiz ederek güvenlik olaylarını zamanında tespit etmek ve bunlara yanıt vermek için kritik öneme sahiptir. Bir SOC tarafından 7/24 gözetim, kuruluşlara, kaynak, günün saati veya saldırı türü ne olursa olsun, olaylara ve davetsiz misafirlere karşı kendilerini savunma avantajı sağlar. Saldırganların bir sistemin güvenliğini aşması için geçen süre ile kuruluşların sistemi algılaması için geçen süre arasındaki farkın küçük olması ve bir güvenlik operasyon merkezinin kuruluşların bu boşluklarını doldurmasına ve ortamlarının karşılaştığı tehditlerin üstesinden gelmesine yardımcı olması önemlidir.

2.6. SİBER SAVUNMA MERKEZİ (CYBER DEFENSE CENTER)

Günümüzde işletmeler, sistemlerine çoktan girildiğini varsaymalıdır; aksi takdirde, bir saldırının bir sonraki kurbanı olacaklardır. Bu söz, güvenlik izleme dediğimiz şeyin aslında ne kadar önemli olması gerektiğini düşündürüyor. Bu yüzden; Güvenlik Operasyon Merkezi'ne (SOC) ek olarak, hızlı bir şekilde yanıt uygulamak ve güvenlik altyapısını uygun şekilde optimize etmek için bir Siber Savunma Merkezi'ne (CDC) ihtiyaç vardır. CDC ekibi; Tespit, müdahale, tehdit avcılığı, tehdit istihbaratı ve veri bilimi gibi kavramlar üzerinde çalışan daha uzmanlaşmış bir savunma ekibi olarak görülebilir. SOC ve CDC, bir organizasyonun ağlarına ve sistemlerine ilişkin görünürlüğünü, tehditlere karşı duruşunu ve bunları yönetmek ve azaltmak için uygun bir sürecin geliştirilmesini artırmak için kritik olan olay müdahale zincirinde birbirine sıkı sıkıya bağlı birimlerdir [14].

2.7. SİBER GÜVENLİK ANALİSTİ

Siber güvenlik, temelde siber saldırılara karşı alınan önlemlerin bütününe verilen isimdir. Siber güvenlik unsuru “kuruluş, kurum ve kullanıcıların” bilgi varlığını kullandıkları araçları, yazılı belgeleri, elektronik ortamda tuttukları belgeleri ve bilişim alanında kullanılan güvenlik teknolojilerini korumak ve korumak için tasarlanmış politika ve uygulamalarını içerir. Siber tehditlere ve saldırılara maruz kalan bir ülke veya şirket, bu tehdit ve saldırıları ortadan kaldırmak için siber savunma faaliyetinde bulunur [17].

Ülkeler, siber saldırı sonucu zarar gören kritik altyapıları ile toplumsal düzenin ve kamu hizmetlerinin devamlılığını engelleyen hasar veya yıkıma uğrayan sistem ve uygulamaları korumak için siber savunma yöntemlerini kullanmaktadır. Kritik altyapılar, erişim veya hizmet engellendiğinde yapısal, ekonomik ve sosyal sıkıntıya neden olan hizmet ve hizmetlerdir. Bir siber güvenlik analisti, ağlar, donanım ve yazılım dahil olmak üzere BT altyapısını tehditlerden korur. Bu kapsamda Siber Güvenlik Analistinin görevleri arasında ağların ve sistemlerin izlenmesi, güvenlik tehditlerinin tespit edilmesi ve değerlendirilmesi ve gerekirse güvenlik sorunlarının çözülmesi yer almaktadır [18].

Siber güvenlik analistlerinde izleme sırasında körlüğe neden olan false-positive (yanlış alarm) alarmlardır. Alarmların sınıflandırılması karışıklık matrisi ile belirlenmektedir. Örnek olarak, bir e-mail “spam değil” olarak sınıflandırıldığında tahminler 4 şekilde değerlendirilir [65]:

1. Doğru Pozitif (True Positive): Gerçekte doğru olan ve doğru olarak tahmin edilenlerdir.
Örnek: Spam olarak tahmin edilen ve gerçekten spam olan e-maillerdir.

2. Yanlış Pozitif (False Positive): Gerçekte yanlış olan ancak doğru olarak tahmin edilenlerdir.
Örnek: Spam olarak tahmin edilen ancak normal olan e-maillerdir.

3. Doğru Negatif (True Negative): Gerçekte yanlış olan ve yanlış olarak tahmin edilenlerdir.
Örnek: Normal olarak tahmin edilen ve gerçekten normal olan e-maillerdir.

4. Yanlış Negatif (False Negative): Gerçekte doğru olan ancak yanlış olarak tahmin edilenlerdir.
Örnek: Normal olarak tahmin edilen ancak spam olan e-maillerdir.

BÖLÜM 3

KAVRAMLAR VE PRENSİPLER

3.1. TEMEL GÜVENLİK PRENSİPLERİ

Bilgi güvenliği, bilginin yetkisiz veya yetkisiz erişiminin, kullanımının, değiştirilmesinin, ifşa edilmesinin, imha edilmesinin ve yok edilmesinin önlenmesidir. Gizlilik, bütünlük ve erişilebilirlik olarak adlandırılan üç temel unsurdan oluşur. Bu üç temel güvenlik unsurundan herhangi biri bozulursa, bir güvenlik ihlali meydana gelir.

1. Gizlilik: Bilginin yetkisiz erişime karşı korunmasıdır.
2. Bütünlük: Bilgilerin yetkisiz kişiler tarafından değiştirilememesidir.
3. Erişilebilirlik: Bilginin yetkili kişiler tarafından ihtiyaç duyulduğunda erişilebilir ve kullanılabilir olmasıdır.

3.1.1. Bilgisayara Giriş Güvenliği Aşamaları

Bilgisayarlara erişim güvenliği, ayrıca bilgisayarda saklamış olduğu bilginin güvenliği anlamına gelmektedir. Bu sebeple, bilgisayara erişim güvenliği aşamaları oldukça önemlidir. Bilgisayara giriş güvenliği aşamalarında ilk adım fiziki güvenliktir. Öncelikli olarak bilgisayarın bulunmuş olduğu yerin güvenliğini garanti etmektedir. Unutulmaması gerekir ki, en yaygın problemlerden biri de diz üstü bilgisayar hırsızlığıdır. Bilgisayar açıldığında kullanıcı adı ve şifre istemeden, bilgisayardan fiziki erişimi olan herkes tarafından açılıp bireysel bilgilere erişebilmektedir. Fiziki güvenliğin sağlanmasının ardından “kullanıcı adı" ve "parola” ile bilgisayarın açılıyor olması gerekmektedir. Bunu 2 türlü gerçekleştirebiliriz [14]:

1. Bilgisayar her açıldığı zaman (BIOS) parolanın sorulması gerekmektedir.
2. Başlangıçta bilgisayarda kurulu olan işletim sisteminden bir parola istenilerek yapılması gerekmektedir.

3.1.2. Parola Güvenliği Aşamaları

Kişisel bilgilerin en önemli parçalarından biri olan parolaya, birçok farklı yöntemle el konulabilir ve aleyhimize kullanılabilir. Bu nedenle parola güvenliği son derece önemlidir. Bu sebeple [19];

1. *"Kolay tahmin edilemeyen (güçlü) parolalar kullanılmalı, parolalar uzun olmalı (en az 8 karakter), büyük – küçük harf, özel karakterler ve rakamlar kullanılmalıdır.*
2. *Kullanılan parolalar korunmalı ve paylaşılmamalı,*
3. *Belirli sürelerle değiştirilmeli,*
4. *Herhangi bir yerde yazılı bulundurulmamalı*
5. *Anti-virüs programı güncel tutulmalıdır."*

Parolamız başka biri tarafından ele geçirilirse veya bundan şüphelenirsek [19];

1. Yapmamız gereken ilk şey parolamızı değiştirmek ve daha sonra başka sistemlerde aynı veya çok benzer parolalar kullanılıyorsa bunları da değiştirmektir.
2. Bu durumdan etkilenebilecek diğer kişilere haber verilmesi daha fazla sorun yaşanmasını önlememize yardımcı olacaktır.
3. Benzer problemlerin tekrar yaşanmaması için oluşturacağınız parolalar güçlü, tahmin edilmesi zor parolalar olmalıdır.

3.1.3. E posta Güvenliği Aşamaları

Gündelik yaşamımızda dosya aktarımı ve iletişim için yaygın olarak kullanmış olduğumuz "e-postalar", dikkatle kullanmadığımız sürece bireylere zarar verebilmek,

bireyleri aldatabilmek ve dolayısı ile finansal fayda sağlayabilmek için kolaylık ile kullanılabilmektedir. Bu nedenle [20];

1. *"E-posta adresleri herkese açık web sitelerinde paylaşılmamalı*
2. *Tanımadığınız kişilerden gelen her türlü e-postaya cevap verilmemeli*
3. *Kişisel ve mali bilgiler e-posta üzerinden hiç kimseyle paylaşılmamalı*
4. *E-posta içinde bulunabilecek bağlantılara tıklanılmamalı*
5. *İçeriği ne olursa olsun, başkalarına gönderilmeyi isteyen e-postalar kimseye gönderilmemeli"*
6. *Güncel anti-virüs ve güvenlik duvarı yazılımları kullanılmalıdır."*

3.1.4. İnternet Erişimi Güvenliği Aşamaları

İnternet birçok yönden hayatımızı kolaylaştırsa da dikkatsizce kullanıldığında sorunlara neden olabilir. İnternette var olan tuzakların farkında olmak, hangi web sitesine güvenileceğini ve nasıl güvende kalınacağını bilmek önemlidir. Ayrıca [21];

1. *"Özellikle internet ortamında, hassas bilgilerin paylaşımı güvenli iletişim yolları ile gerçekleştirilmelidir.*
2. *Tuzak web sitelerine dikkat etmek ve güvenilmeyen web sitelerini ziyaret etmemek.*
3. *E-posta mesajları ile gönderilen bağlantılara dikkat etmek*
4. *Web sitelerinde gezerken yayılabilen zararlı programlardan korunmak için açılır pencere engelleyicisi kullanmak gereklidir.*
5. *Bunların yanı sıra çocukların güvenliğini sağlamak anne babanın görevidir ve bu konuda alınabilecek tedbirler konusunda aileler hem kendilerini hem de çocuklarının bilinçli birer kullanıcı olmaları için özen göstermelidir."*

3.1.5. Sosyal Medya Güvenliği Aşamaları

Kişilerin web aracılığı ile BT kullanılarak, birbirleri ile etkileşimini sağlayabilen sanal hizmet uygulamalarına "Sosyal Medya" denilmektedir. Sosyal medya güvenliğinde dikkat edilmesi gerekenler şunlardır [21]:

1. Sosyal ağ siteleri ne olursa olsun, resmi olmayan sayfalar ile ve profillere itibar edilmemesi gerekmektedir.
2. Bireysel bilgiler herkes tarafından açık bir şekilde görünmemesi gerekmektedir.
3. Paylarının ne olduğu ve suç unsurlarını içerdiğine dikkat edilmesi gerektiği esastır.

Aynı tarzda paydaşların suç unsurlarını, hakaret, taciz, küfür, ya da aşağılayıcı sözleri içermemelerine özen göstermesi gerekmektedir. Bu durumda size yöneltilmiş olan davranış ve sözler için suç duyurusunda bulunulması hakkı yer almaktadır. Bunlar [21]:

1. Özel bilgileriniz hiçbir yerde paylaşılmamalı ve tanımadığınız kişilerin listenizde olmasına izin vermemelisiniz.
2. Fotoğraf veya video paylaşmadan önce fotoğrafta görünen kişilerden izin alınmalıdır.
3. Konum bildirirken adres ve bulunulan konumun da bildirilmiş olduğu unutulmamalıdır.
4. Ekranlarda görüntülenen tüm bilgilerin doğruluğu sorgulanmalı ve buna göre hareket edilmelidir.
5. Twitter, facebook, instagram gibi sosyal ağlarda gezinirken kaynağı belirtilmeyen yanıltıcı linklere tıklanmamalıdır.
6. Sosyal ağ sitesinde etiketlenmesi vb. durumların yaşanılmaması için bireysel profil bilgileri için onay alınması gibi özelliklerin aktif edilmesi gerekmektedir.

3.1.6. Sosyal Mühendislikten Korunma Yöntemleri

Sosyal mühendislik, web ortamında bireylerin zaafından yararlanılarak farklı aldatma ve ikna yöntemleri kullanılarak, istenilen bilgileri elde etmeye çalışmaktadır. Bireylerin karar verme süreçlerindeki değişime yönelik teknikleri içermektedir. Sosyal mühendislik yöntemleri büyük bir çeşitlilik gösterse de en yaygın biçimde kullanılanları aşağıdaki gibidir [21]:

a) **Telefonda:** Bu, en etkili sosyal mühendislik saldırılarından biridir. Hedef kişi bir dolandırıcı tarafından aranır ve arayan kişi yetkiliymiş gibi davranır, yavaş yavaş kişisel bilgilere erişir veya istediği eylemi yapmasına neden olur.

b) **Dumpster Diving:** Önemli ve kötü niyetli kişilerden kurum veya şirket çöplüğünden faydalı bilgilerin toplanmasıdır.

c) **İkna:** Taklit etmeye, kendini sevdirmeye, itaat etmeye, sorumluluğu yaymaya ve basit bir arkadaş gibi davranmaya çalışmaktır.

d) **Çevrimiçi Sosyal Mühendislik Sosyal ağlar (Twitter, Instagram, Facebook vb.):** Çok etkili bir şekilde kullanarak sizi ve arkadaşlarınızı tanıyabilirler. Facebook üzerinden anne kızlık soyadınızı öğrenmek dakikalar alabilir ve bu basit bilgi ile birçok işlem yapılabilir.

Sosyal Mühendislikten korunmak için aşağıdakilere dikkat etmek gerekmektedir:

1. Tüm kullanıcıların eğitilmesi gerekmektedir.
2. Telefonla arayan kimseyle parolalar ve önemli bilgiler paylaşılmamalıdır.
3. Büyük şirketlerin veya kurumların "yardım masaları" adı verilen departmanları vardır. Bu bölümleri aramanız ve kendinizin tamamen doğrulaması gerekir.
4. Kurumsal bilgiler uygunsuz yöntem ve kanallarla paylaşılmamalıdır.
5. Kuruluş genelinde parola gizliliği ilkesi uygulanmalıdır.
6. Gerekirse “sizi şirket yönetiminden arayacağım” denilmelidir.
7. Şirket sırrı niteliğindeki belgeler uygun yöntemlerle imha edilmelidir.

e) **Shoulder Surfing:** Omuz sörfü, hedefin omzunun üzerinden bakarak kişisel kimlik bilgilerini, şifrelerini ve diğer gizli verileri elde etmek için kullanılan sosyal mühendislik tekniklerinden biridir.

3.1.7. Dosya Erişim ve Paylaşım Güvenliği Aşamaları

Bilgisayarda bilgi depolayan birimlere dosyalar denir. Dosyadaki bilgiler; görüntü, metin, çizim, ses gibi herhangi bir şey olabilir. Dosya paylaşım yazılımı kullanarak veya paylaşım yoluyla başkalarının erişmesine izin verdiğinizde bilgisayarınızı korumak için güvenlik önlemleri almalısınız. Öyle ise [22];

1. Paylaştığınız dosya veya klasörler, kimin hangi haklara sahip olması gerektiği dikkate alınarak yapılandırılabilir.
2. Kişisel veya önemli bilgiler içeren dosyalar şifrelenebilir ve kaydedilebilir.
3. Zaman zaman paylaştığınız dosya veya klasörleri kontrol etmeniz ve daha önce verilen hakları güncellemeniz gerekmektedir.
4. Dosya paylaşım yazılımı kullanırken telif hakkını dikkate almak gerekir.

3.1.8. Zararlı Yazılımlardan Korunma Aşamaları

Kötü amaçlı yazılımlar, diğer bireylerin bilgisayarlarının kontrol edilmesinde ele geçirmek için izin vermektedir. Böylece programlar bozulur ve artık istenildiği gibi çalışamamaktadır. Zararlı yazılımlardan korunulmazsa, özel bilgiler başka kişilerin eline geçebilir. Bu sebeple [22];

1. Antivirüs ve casus yazılım önleme programlarının kullanılması gerekmektedir.
2. “Anti-virüs ve anti-spyware” programlarının güncel tutulması gerekmektedir.
3. İşletim sistemlerinin güncel tutulması gerekmektedir
4. Güvenlik duvarının kullanılması gerekmektedir.
5. İnternette ziyaret etmiş olduğumuz web sitelerinde ve indirmiş olduğumuz dosyalara dikkat edilmesi gerekmektedir.
6. Ücretli lisans programlarının kullanılması gerekmektedir.

3.1.9. Mobil Cihaz Güvenlik Aşamaları

İletişim bankacılığından, alışverişten e-cüzdana kadar gündelik yaşamda bütün türler iş için kullanmış olduğumuz mobil iletişim araçları ile cep telefonlar, hemen hemen

herkesin cebinde en önemli araç olarak yerini almaktadır. Bu yüzden mobil cihazlardaki güvenlik aşamalarını önem sırasına göre, şu şekilde sıralayabiliriz [22];

1. Kaynağı belli olmayan ve şüphe uyandıran e-postaların açılmaması gerekmektedir.
2. Kaynakları belli olmayan şüpheli e-postaların ekine tıklanmadan ya da bu eklerin cihaza indirilmemesi gerekmektedir.
3. Cihaza, kaynağının bilinmediği ya da işlevinin bilinmediği herhangi bir yazılımın yüklenmemesi gerekmektedir.
4. Uygulamayı mağazamızdan indirmiş olduğumuz uygulama yazılımı, özellikle de ücretsiz olanının mümkün olduğu kadar dikkatli seçilmesi gerekmektedir.
5. Cihazda saklanılan kritik belge ve parolaların özel bir şekilde şifrelenmesi gerekmektedir.
6. Cihaz kurulduktan sonra, dışardan gelebilecek ya da giden verilerin onayının istenmesi gerekmektedir.
7. Tanımadığınız bireylere cihazın verilmemesi gerekmektedir.
8. Üretici firmanın resmi bakım ve onarım merkezi dışında cihazının tamir edilmemesi gerekmektedir.
9. Şüpheli kaynaklardan hediye telefonun kabul edilmemesi gerekmektedir.
10. Cihazda antivirüs programının olduğundan emin olunması gerekmektedir.

3.2. UZLAŞMA GÖSTERGELERİ (INDICATOR OF COMPROMİSE-IOC)

Uzlaşma göstergeleri (IOC'ler), bir ana bilgisayar sistemi veya ağ üzerindeki olası izinsiz girişlerin adli kanıtı olarak hizmet eder. Bu yapılar, bilgi güvenliği (InfoSec) uzmanlarının ve sistem yöneticilerinin izinsiz giriş girişimlerini veya diğer kötü amaçlı etkinlikleri algılamasını sağlamaktadır. Güvenlik araştırmacıları, belli bir kötü amaçlı yazılımı tekniğini ve davranışını daha iyi analiz edebilmek için "IOC"ları kullanmaktadır. Aynı zamanda kuruluşun olaylarının iyileştirilmesi ve müdahale edilme stratejilerini daha iyi bir şekilde iyileştirebilmek için, topluluğun içerisinde paylaşılan eylemlere geçirilebilmektedir. InfoSec uzmanları ve BT/sistem yöneticileri, saldırı ve ihlaller önlenmese de azaltmaya yardımcı olabilmek için "IOC"ları izleyen

farklı araçlar kullanılmaktadır. BT güvenliği uzmanlarından ve sistem yöneticisinin dikkat etmesi gereken bazı tehlike göstergeleri şu şekildedir [23];

1. Ağa giren ve çıkan olağandışı trafik
2. Kaba kuvvet saldırılarını gösteren şüpheli oturum açmalar, erişim ve diğer ağ etkinlikleri
3. Şirket dosyalarında anormal talep artışları ve okuma hacmi
4. Alışılmadık şekilde kullanılan bağlantı noktalarından geçen ağ trafiği
5. Kurcalanmış dosya, Etki Alanı Adı Sunucuları (DNS) ve kayıt defteri yapılandırmalarının yanı sıra mobil cihazlardakiler de dahil olmak üzere sistem ayarlarındaki değişiklikler
6. Büyük miktarda sıkıştırılmış dosya ve veri, açıklanamayacak şekilde bulunmamaları gereken yerlerde bulunması şeklinde açıklanabilir.

3.3. ATAK MODELLERİ

Siber güvenlik analistlerinin Cyber Kill Chain metodolojisine ve MITRE ATT&CK frameworküne hâkim olması saldırıları analiz etme bakımından önem arz etmektedir. Bunlara aşağıda detaylıca yer verilmiş ve bilinen örnek saldırılar hakkında bilgiler aktarılmıştır.

3.3.1. Cyber Kill Chain

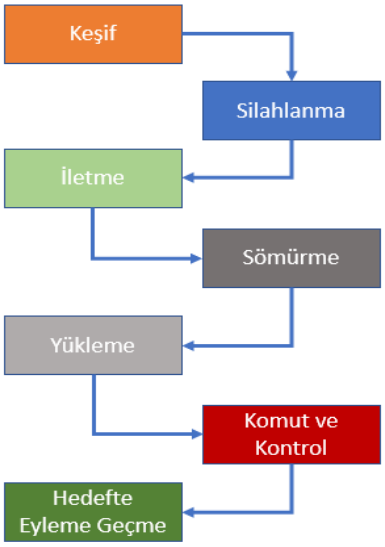
Mitnick et al. (2003)'ün de belirtmiş olduğu gibi birden fazla yazılım ve donanım çözümlerinin geliştirilmiş olmasına karşılık, bilgi sistemlerine yönelik güvenlik saldırısı da her geçen gün artış göstermektedir. Bilginin gizlice olması, bütünlüğünden ve erişilebilirliğine yönelik saldırıların, onarılmaz ve ciddi zararlara sebep olmaktadır. Tüm bu kayıplar ise, tamamı ile ortadan kaldırılmamaktadır. Fakat, güvenlik önleminin zamanında ya da önceden alınması ile, kayıpların en aza indirilmesi mümkün olabilmektedir [24].

Geleneksel güvenlik sisteminden gelişen siber saldırıların karşısında, yetersiz kalınmasının ardından sonra geliştirilen yavaşlatma, aldatma ve karşı saldırıların vb.

dinamik çözümlerin ya da yaklaşımların, aktif siber savunma tekniğini ya da aktif siber savunma yaklaşımları olarak literatürde yerini almıştır [25]. ABD ordusu aktif savunma, belli bir düşmandan sınırlı saldırı eylemi ve karşı saldırıların yolu ile avantajları bir konum elde edebilmesini engelleyebilme olarak tanımlamıştır [26]. Aktif siber savunma sistemleri, belli bir siber saldırının öncesinde ve sonrasında saldırganları engellemeye yönelik amaçların bir proaktif önlemidir. Aktif siber savunmaların, karmaşık bir siber saldırı için, tespit etme, önleme ve tüm bunlara yanıt verme çabasını arttırmaktadır [27]. Diğer bir yaklaşımda aktif siber savunmalar, kötü niyetli yazılımlar ve diğer saldırılara yönelik, aktif önlemlerin yanı sıra tehdit ajanlarını etkisiz hale getirebilmek için, agresif dış teknikleri içeren bir siber güvenlik yaklaşımıdır [28].

Güvenlik duvarları ve saldırı önleme sistemleri/saldırı tespit sistemleri (IPS/IDS) gibi güvenlik çözümleri ileri düzey siber saldırılara karşı koyamadığı için aktif siber savunma teknikleri ile saldırıları önlemeye veya yavaşlatmaya yönelik girişimlerde bulunulmaktadır. Saldırganları karşı saldırılarla durdurma girişimi de aktif siber savunma kavramının bir parçasıdır. Kötü amaçlı yazılımlar geleneksel güvenlik önlemleriyle tespit edilmemiş olsa bile, halihazırda güvenliği ihlal edilmiş sistemlerdeki tüm tehditlerin engellenemeyeceğini varsayarak; Olayların tanınma ve yanıtlanma hızı çok önemlidir [29].

Gelişmiş siber saldırılarda önemli faktörlerden biri, kurbanların askeri, siyasi ve ticari öneme sahip gizli ve kritik bilgilerinin çalınması olduğundan, saldırganın yanlış bilgi almamasını sağlamak da aktif bir siber savunma yaklaşımının bir parçasıdır. Bu nedenle, saldırgan ve ne tür bilgilere erişmeye çalıştığı hakkında bilgi toplamak önemlidir. Çok gelişmiş olan siber saldırıların doğası gereğince, karmaşık olması sebebiyle, bu saldırılar ile mücadele edebilmek için ve tüm bunlara karşılık savunma yapılması oldukça güçtür. Aldatma, yavaşlatmak ve karşı saldırılar gibi, savunması yaklaşımın uygulanması için, siber saldırıları iyi analiz edebilmeleri gerekmektedir. Bu sebeple, Hutchins ve ark. As (2011) saldırılara yönelik karşı çözümlerin, gelişmiş olan siber saldırılar araştırılarak ve doğru zamanda doğru savunma yaklaşımları kullanılarak oluşturulmaktadır [30]. Cyber Kill Chain 7 aşamadan oluşmaktadır [61].



Şekil 3.1. Cyber kill chain aşamaları [61].

1. Keşif (Reconnaissance) Aşaması: Araştırma ve planlama aşaması olan keşif aşaması, saldırganın hedef üzerinde bilgi toplama aşamasıdır. Saldırganlar genellikle keşif faaliyetlerine, gerçek saldırıdan daha fazla zaman harcamaktadır. Bu aşamada hedef seçimi, organizasyonun ayrıntılı araştırılması, hedefin teknoloji seçimleri, sosyal ağ etkinlikleri hakkında bilgiler toplanmakta ve bu aşamada saldırganlar, hedeflerine karşı hangi saldırı yöntemlerinin en etkili olacağını bulmaya çalışmaktadır [61].

2. Silahlanma (Weaponization)Aşaması: Silahlanma aşaması, saldırı öncesi hazırlık aşamasıdır. Saldırgan, sistem hakkında gereken bilgileri keşif aşamasında topladıktan sonra bu aşamaya geldiği için, bu veriler saldırgana giriş noktaları belirlemesi açısından yardımcı olmaktadır. Saldırgan, keşif sonucu elde ettiği veriler ile bir arka kapı (backdoor) ve bir sızma planı tasarlama ile ilgilenmektedir [61].

3. İletme (Delivery): İletme veya iletim aşaması, siber saldırı kısmının girişim (attempt) aşaması olarak geçmektedir. Bu aşama savunucuların, saldırıları azaltmak için teknolojiyi kullanabilecekleri ilk fırsatı sağlamaktadır. Keşif ve silahlanma aşamalarında savunmacılar, saldırıya herhangi bir müdahalede bulunamamaktadırlar. Savunma tarafı, saldırıya müdahale etme fırsatının ilk adımını bu aşamada yapabilmektedir [61].

4. Sömürme (Exploitation): Sömürme aşaması da iletme (delivery) aşaması gibi girişim (attempt) aşamasında bulunmaktadır. Teslim edilen saldırı araçlarının tetiklendiği kısımdır. Saldırgan bu aşamada, silahlanma aşamasında oluşturduğu silah ile hedef sistemin güvenlik zafiyetini sömürmektedir. Sömürme aşaması genellikle kullanıcı sistemlerdeki zafiyetin sömürüldüğü aşamadır [61].

5. Yükleme (Installation): Hedefin sömürülmesinin ardından, kalıcı bir tehdit haline gelmek, güvenlik sisteminin ötesinde, sistemin başarılı bir şekilde kontrol edilebilmesi için hedefe asıl zararlı yazılımın indirilmesini, zararlı yazılımın sistemde kalacağı süreyi mümkün olduğunca uzun süre tutmayı hedefleyen aşamadır [61].

6. Komut ve Kontrol (Command and Control) Aşaması: Yönetim ve etkinleştirme aşaması olarak, komuta ve kontrol (command and control veya C&C) aşaması C2 olarak da bilinmektedir. Uzaktan yürütülen siber saldırının önemli bir parçasıdır. Burada saldırgan, hedef ağa yönetim ve iletişim kodunu kurmuştur. Saldırgan artık kötü amaçlı kodu tamamen yönetebilir, ağda daha da ilerleyebilir, veriler sızdırabilir ve imha veya hizmet reddi operasyonları gerçekleştirebilmektedir [61].

7. Hedefte Eyleme Geçme (Actions on Objectives) Aşaması: Siber ölüm zinciri modelinin son aşaması olan eylem aşamasında hedef sistem ele geçirildikten sonra, saldırgan amacına ulaşmak için çeşitli eylemleri gerçekleştirebilecektir. Bu aşamadaki genel amaç, olabildiğince fazla sisteme yayılıp saldırganlar için değerli olan bilgileri ele geçirmektir. Saldırganlar bu aşamada, izlerini kaybettirmek için de hazırlık yapmaktadırlar. Bunun örneklerinden biri de ele geçirilen sistemlerin bilinçli olarak bozulması veya hizmet kesintisi yaşatacak saldırılarla hedef şaşırtılmasıdır [61].

3.3.2. MITRE ATT&CK

"MITRE ATT&CK Matrix", reel dünya gözlemine dayandırılan, siber saldırı teknikleri ve taktikleri ile ilgili global erişilebilen bir bilgi tabanı olarak belirtilmiştir. ATT&CK deposu, siber güvenlik hizmetleri ve ürünler için özel sektörde, devletteki belli tehdit modelleri ve metodolojileri geliştirebilmek için, belli bir temel olarak

kullanılmaktadır. Bu özgür ve açık yapı devamlı olarak gelişime açık olmaktadır. Mavi ve kırmızı ekipleri için farklı testleri sistemsel olarak yürütmek, büyük katkı sağlamaktadır. “MITRE ATT&CK” prosedürleri ve teknikleri, ağdaki veya uç sistemden toplanılan bilgilerin analiz edilmesiyle saldırıları tespit edebilmek için, davranışsal olarak gözlemlenebilirlik sağlamaktadır [31].

“MITRE ATT&CK ICS Matrix” EKS teknoloji alanlarında siber negatif davranışlar ile organize olan bilgi tabanıdır. Belli bir saldırganın saldırıları, hayat döngüsünün farklı aşamasına ve hedeflenmiş olduğu bilinen varlığına ve sistemini yansıtmaktadır. Endüstriyel kontrol sisteminde varlığın farklılığını göz önünde bulundurabilmek, doğru birer sınıflandırma yapabilmek için “Purdue” mimarisinde işlevsel düzeyine ve varlık sınıflarına odaklanılan “ICS ATT&CK” matris oluşturulmaktadır. Mevcut sistemde ise “11 taktik ve 81” teknik yer almaktadır. Bu sayıların geliştirebilen saldırı yöntemlerine yönelik güncellenebilmektedir. Teknik ve taktik arasındaki ilişkide “ATT&CK” matrisi görselleştirilmektedir. “MITRE ICS” matrisi Çizelge 3.1'de yer almaktadır. Matriste her birer başlık belli bir taktik ismini tanımlar ve her bir başlığın altında ise ilgili taktiklerin amaçlarına uygun olarak kullanılacak teknikler tanımlanmaktadır. Belli bir teknik, kullanım amaçlarına göre birden çok taktiğin altında sınıflandırılabilmektedir. “ICS” matrisindeki taktikler, somutlaştırılarak, tekniklerin sebebini temsil etmektedir. Saldırganın eylemlerinin gerçekleşmesine izin vermenin sebebi, taktik ve tekniklerinin belirlenmesidir. Taktikler, saldırganın hedefe ulaşabilmesi için, nasıl bir yol izlediğini göstermektedir. Teknikler ise, saldırganın hedefe ulaşabilmesi için, kullandığı yöntemlerdir [32].

Çizelge 3.1. MITRE ICS matrisi [32].

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation For Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Model Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man it the Middle	System Firmware	Rootkit	Network Sniffling	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss Of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Modul Firmware	Loss Of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operation Mode	Serial Connection		Monitor Process State		Denial of Service	Program Download	Loss Of Safety

Siber dünyada savunma alanı olan kritik altyapılar, siber dünyada devletler arasında oldukça önemli görülmektedir. Geçmişten günümüze kadar kritik alt yapılar ile yapılan saldırıların vermiş olduğu zararlar göz önünde bulundurulduğunda, bu durum çok kritik bir konu halini almıştır. Diğer saldırganlarda olduğu gibi, "APT" gruplarından da veri çalmak, operasyonun kesintiye uğratılmasına ya da alt yapıları yok etmek için çalışan süreçler geliştirilmektedir. Birçok siber saldırganın aksine "APT" grupları yıllar ve aylar boyunca hedefini takip etmektedir. Siber savunmalara uyum sağlamaktadırlar ve tekrar aynı hedefi nişan almaktadırlar. Güvenlik ekiplerince, en verimli APT gruplarından haberinin olması ve önceki APT saldırı ile ilgili kötü amaçlı yazılımların tespit edilmesi ekstra önlemleri almaları gerekmektedir. Aşağıdaki bazı APT gruplarının saldırıları ve "MITRE ICS ATT&CK" matrisi hakkındaki sınıflandırmalara yönelik bilgiler sunulacaktır [33].

3.3.2.1. Stuxnet

Stuxnet, İran'ın nükleer araştırmalarını bozabilmek için, kullanılmış olan bir solucan yazılım olarak belirtilmektedir. 2010 yılında ortaya çıkmış olan bu yazılım, "İran'ın Buşehr ve Natanz"daki nükleer santrallerini etkilemiştir. Stuxnet kötü amaçlı yazılımların, özellikle de endüstriyel kontrol sistemini hedef almakta olan, halka açık bir şekilde ilk kötü amaçlı birer yazılım olduğu belirtilmektedir. Stuxnet, birçok güvenlik açıkları, gelişmiş olan "Windows rootkit ve ağ bulaşma teknikleri" dahil olunması üstüne birden fazla karmaşık taktik kullanılan büyük ve karmaşık bir kötü amaçlı yazılım olarak belirtilmektedir. Yazılımın içeriği "kod nesne" yönelimlidir ve "Windows işletim sistemi, Microsoft SQL Server, Siemens yazılımı ve Siemens PLC"ler ile birlikte üstüne birçok alanda ileri seviye bilgi gerektirebilen, birden fazla programlama tekniği kullanılmaktadır [35]. "ICS-CERT, USB" sürücülerinde birincil bulaşma yöntemleri gibi gözükse de "Stuxnet"in ağ paylaşımı ve "SQL" veri tabanı ayrıcalığı ile de sistemlere bulaşacağı belirlenmiştir. Belli bir sisteme bulaşmasının ardından, kötü amaçlı bu yazılım "MS SQL" sunucusundan, "Windows kayıt defteri"nden ve uygulama yazılımlarından çok geniş kapsamlı bir veri toplamaktadır. Çizelge 3.2, "MITRE ICS ATT&CK" matrisi "Stuxnet" kötü amaçlı bir yazılım tarafında kullanılan teknik ve taktik bir gösterim sağlamaktadır [34].

Çizelge 3.2. Stuxnet zararlı yazılımı MITRE ICS ATT&CK teknikleri.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation For Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Model Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man it the Middle	System Firmware	Rootkit	Network Sniffling	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss Of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Modul Firmware	Loss Of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operation Mode	Serial Connection		Monitor Process State		Denial of Service	Program Download	Loss Of Safety
Spearphishing Attachment	Scripting					Point & Tag		Modify Alarm Settings		Manipulation of Control
						Program Upload		Modify Control Logic	Unauthorized Command Message	Manipulation of View
								Program Download		
								Root		

3.3.2.2. Black Energy

2015 yılında Ukrayna devletine bir siber saldırı gerçekleştirilmiştir ve bu saldırı da uzun bir süre elektrik kesintisine sebep olmuştur. Bu saldırı, belli bir elektrik şebekesine yapılan, bilinen ilk başarılı siber saldırıdır. Siber saldırıyı gerçekleştirenler 30 trafo merkezinde elektriği keserek 230 bin kişiyi altı saat kadar elektriksiz bırakmıştır. SCADA ekipmanı çalışamaz bir hale getirilmiştir. Çalışmacılar, saldırganlar "Microsoft Excel" belgesinde makrolardan yararlanabilmek için "Black Energy" kötü amaçlı yazılım kullanarak, kesintinin kolayca gerçekleştiğini keşfetmişlerdir [36].

Blackenergy kötü amaçlı yazılımların bir türüdür. BlackEnergy hem siber saldırganları hem de APT grupları tarafından kullanılmış olan kötü amaçlı birer yazılım türüdür. KillDisk'in bir türünün de dahil olması suretiyle farklı eklentileri de desteklemektedir. Ukrayna elektrik şebekelerine karşı kullanılmış olduğu belirtilmektedir. BlackEnergy, kötü amaçlı yazılımları şimdiye kadar Ukrayna endüstrilerine yönelik, hedefli saldırılarda kullanılmıştır. Popüler "Microsoft Windows platformları"nı ve sunucular hedeflemektedirler [38]. Blackenergy zararlı yazılımının "MITRE ICS ATT&CK" matrisinde kullandığı taktik ve tekniklerin haritalandırılması Çizelge 3.3.'de verilmiştir.

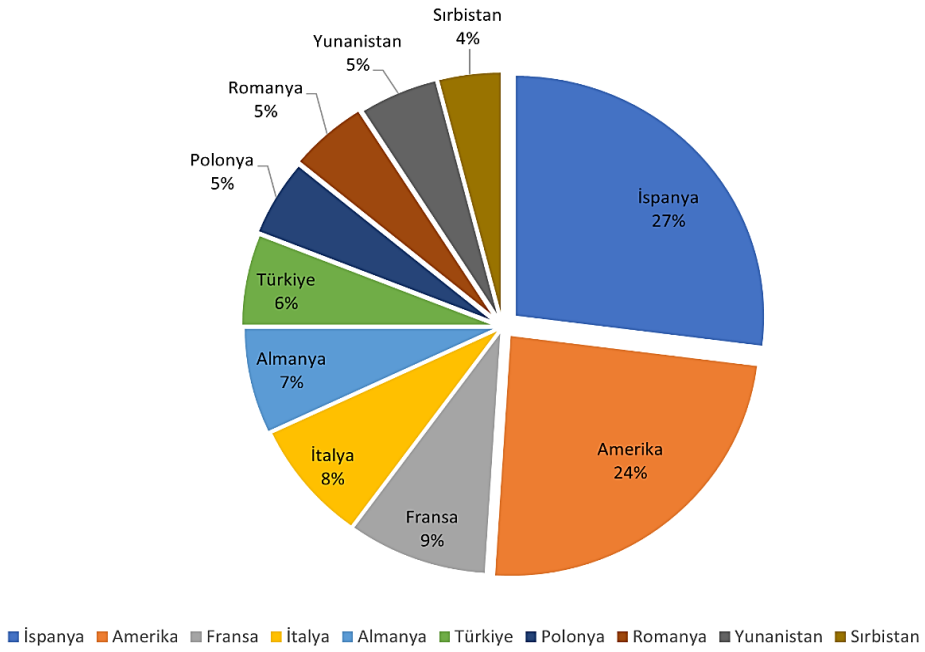
Çizelge 3.3. Blackenergy 3 zararlı yazılımı MITRE ICS ATT&CK teknikleri.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation For Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Model Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man it the Middle	System Firmware	Rootkit	Network Sniffling	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss Of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Modul Firmware	Loss Of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operation Mode	Serial Connection		Monitor Process State		Denial of Service	Program Download	Loss Of Safety
Spearphishing Attachment	Scripting									

3.3.2.3. Havex

Havex/Dragonfly kötü amaçlı yazılımda kullanılan “APT” saldırıları 2010 yılının sonların da başlamıştır. Fakat, 2013 yılına kadar keşfedilmemiştir. “Dragonfly” kötü amaçlı yazılımların ilk hedefi Kanada ve ABD’deki savunma/havacı endüstrileri olmuştur. Fakat, 2013 yılının başında enerji endüstrisi yayılmıştır [37]. “F-Secure ve Symantec”teki siber güvenlik çalışmacıları tarafından keşfedilmiştir. 2014 senesinde bu 2 şirketten alınan bilgiler kullanılarak “ICS-CERT” tarafından rapor edilmiştir. Sisteme izinsiz girebilmek için, hedefli kimlik avı yöntemi de kullanılmıştır. PHP programlama dilinde yazılmış olan bir “RAT ve bir C&C” sunucusuyla ilgili iletişim kurabilen diğer birer modül olmak üstüne 2 ana yapıdan oluşan bir kötü amaçlı yazılım olarak bilinmektedir. Aynı zamanda, ağda endüstriyel cihazları arayabilmek için kullanılan bir “OPC” tarama modülünü içermektedir. “OPC” tarama modülü “44818, 105 ve 502” bağlantı noktasında çalışabilen ve “TCP” protokolüne sahip cihazları tarayabilmek için tasarlanmış bir modüldür [40].

Havex kötü amaçlı yazılımı, endüstriyel ve enerji şirketlerini hedef alarak dünya çapında çeşitli ölçeklerde dağıtıldı. Bu 2014 Symantec orantılı güvenlik raporuna göre, en çok etkilenen 10 ülke Şekil 2.8'de gösterilmiştir [38].



Şekil 3.2. Havex zararlı yazılımından en çok etkilenen 10 ülke [38].

Çizelge 3.4'te MITRE ICS ATT&CK matrisinde Havex kötü amaçlı yazılımı tarafından kullanılan taktik ve tekniklerin bir haritasını göstermektedir.

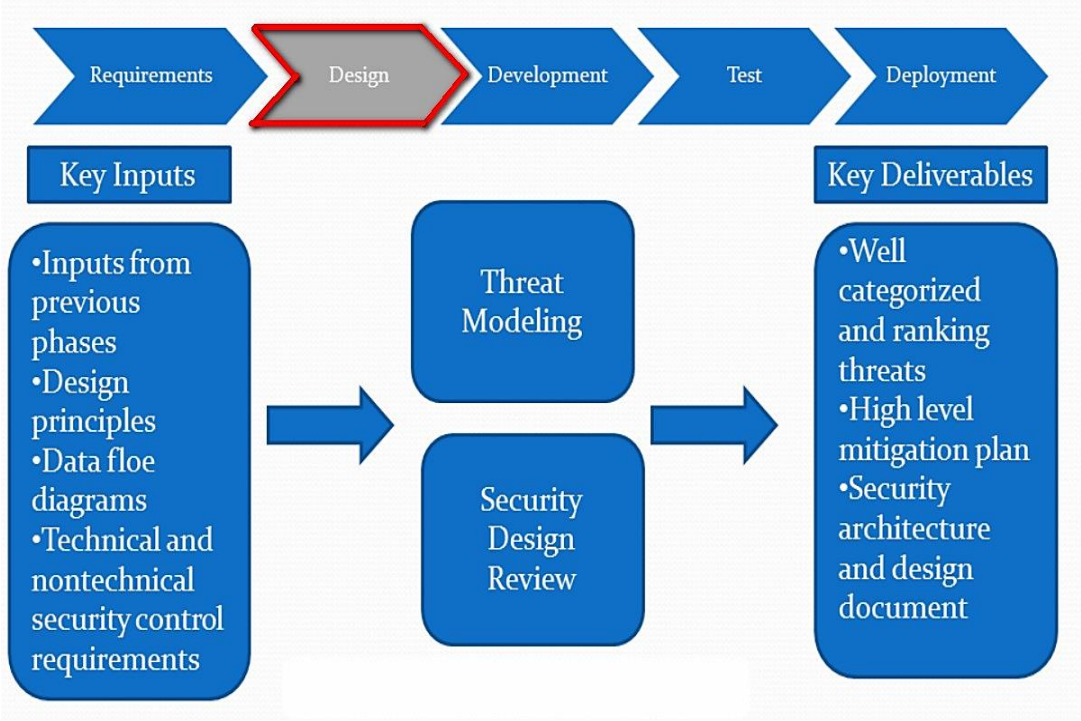
Çizelge 3.4. Havex zararlı yazılımı MITRE ICS ATT&CK teknikleri [38].

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation For Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Model Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loos of Availability
External Remote Services	Man it the Middle	System Firmware	Rootkit	Network Sniffling	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss Of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Modul Firmware	Loss Of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operation Mode	Serial Connection		Monitor Process State		Denial of Service	Program Download	Loss Of Safety
Spearphishing Attachment	Scripting									
Supply Chain Compromise	User Execution									

3.4. TEHDİT MODELLEME (THREAT MODELLİNG)

3.4.1. Kullanım Amacı

Tehdit modelleme, tasarlanmış olan bir sistemin uygulanmasında, güvenlik riski ile ilgili bilinçli karar vermeyi sağlamaktadır. Belli bir model oluşturabilmeye ek olarak, tipik bir tehdit modelleme çabalarıyla, gereksinimler, konsept, uygulama ya da tasarım yönünden öncelikli bir güvenlik iyileştirme listesi de oluşturabilmektedir. "Yazılım Geliştirme Yaşam Döngüsünün (SDLC)" tasarım yönünden bir parça olarak tehdit modellemesiyle, yazılım mimarının potansiyel güvenlik problemlerini erken ve kolay bir biçimde belirlenmesini, azaltmasını sağlamaktadır. Böylelikle, genel geliştirme maliyetlerinin azalmasına da yardımcı olabilmektedir [39].



Şekil 3.3 Tehdit modelleme (threat modelling) [39].

Tehdit modelleme, güvenlik açıklarını ve hedefleri belirledikten sonra, sisteme yönelik tehdidi önleyebilmek ya da azaltabilmek için, karşı önlemleri tanımlayarak "ağ/uygulama/internet güvenliği" optimize edilmesine yönelik bir tekniktir. Tehdit, kötü niyetli olan "(örneğin bir DoS saldırısı) veya kazara (bir depolama cihazının

arızalanması)" oluşabilecek gerçek ve potansiyel istenmeyen bir olaydır. Tehdit modelleme, uygulama tehditlerini ve güvenlik açıklarını belirlemek ve değerlendirebilmek için, planlanmış olan bir etkinliktir [39].

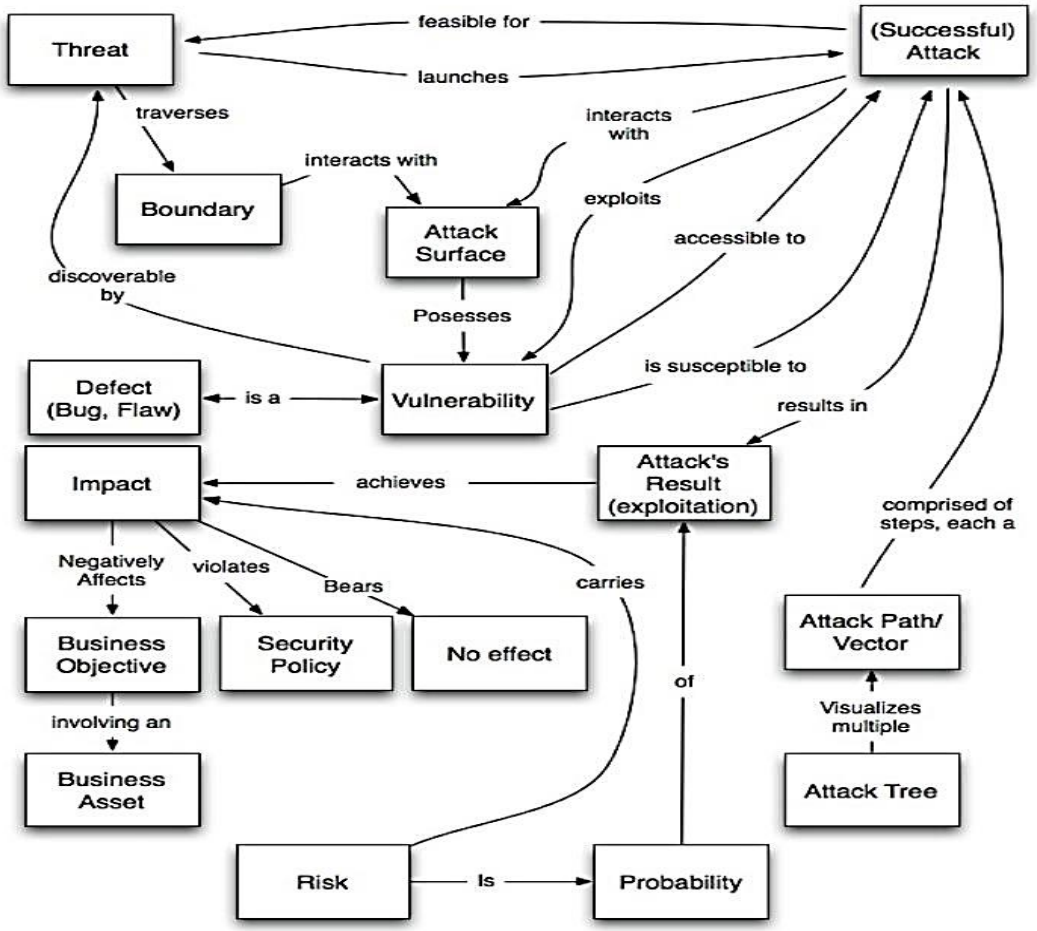
3.4.1.1. Tehdit Modelleme Süreci

Bu modelleme sürece aşağıda yer alan adımlardan oluşmaktadır. Arama alanını keşfetme sürecinde yinelenmesi gerekmektedir ve günümüze kadar yaptıklarına bağlı olarak devamlı olarak iyileştirilmektedir. Örneğin, çoğu tehdit aracılarının saldırılarına karşı savunmasız olmadığından, bir güvenlik önlemiyle korunduğundan veya sonuçları olmadığından, olası tüm güvenlik açıklarıyla başlamak genellikle anlamsızdır. Tehdit modelleme süreci aşamaları aşağıdaki gibidir [39]:

1. **Değerlendirmenin kapsamını belirleyin:** BT ya da hassas dosyalar vb. maddi varlıkları belirleyebilmek genel olarak kolay olmaktadır. Uygulamanın sağlamış olduğu "kapasite ve yetenek" anlayabilmek çok daha güçtür.
2. **Mevcut karşı önlemleri anlayın:** Model, kuruluşun içerisinde hali hazırda konumlandırılmış olan, bütün mevcut karşı önlemi içermektedir.
3. **Öncelikli Belirlenmiş Riskler:** Öncelikli belirlenmiş olan yani kısaca önceliklendirme, tehdit modellemelerinde her şeydir. Çünkü, her zaman fark edilmeyen çok fazla riski bulunmaktadır. Her tehdit için, genel bir risk bulunmaktadır ya da önem seviyesini belirleyebilmek için, bir dizi etki ve olasılık faktörünün tahmini bulunmaktadır.
4. **Sömürülebilir güvenlik açıklarını belirleyin:** Uygulamada güvenlik alındıktan sonra, yeni güvenlik açıkları analiz edilebilir. Odak nokta, tanımlamış olduğumuz olası tanımladığımız negatif sonuçların arasında ilişki kurabilen güvenlik açıkları olmaktadır.
5. **Tehdit aracılarını ve olası saldırıları belirleyin:** Herhangi bir uygulamaya saldıracak çeşitli insan gruplarının karakterize edilmesidir. Bu gruplar hem kasıtsız hem de kötü niyetli saldırılar yapan içinden ve dışından bireyleri içermektedir.

6. **Tehdit azaltma eylemlerini belirleyin:** Son adım ise, kuruluşun riskine dayalı olarak, riski kabul edebilen bir seviyeye indirebilmek için, karşı önlemleri belirlemektedir.
7. **Yöntemi/Süreci Anlamak:** Güvenlik mimarı/uzmanları, güvenlik ve risk açıklığı faaliyetlerinin belirlenmesinin ardından, bu adımları takip etmelerini sağlayabilmek için, tehdit modellemenin ana kavramları anladığından emin olması gerekmektedir.

Tehdit modellemeye yönelik genel kuramlar ile ilgili, detaylı bilgi için **Synopsys** bağlantısı incelenebilir;



Şekil 3.4. Synopsys bağlantısı [39].

3.4.1.2. Kişisel Tedbirler

Bireylerin mağdur olmamak ve güvenlik riskini azaltabilmek için, alınacak bazı adımları şu şekilde sıralanabilmektedir [39]:

1. Çalışandan ya da diğer yönden bilgi isteyenler herhangi birinden gelen istenmeyen telefon aramasından, ziyaretinden ya da e-postasından şüphelenilmesi gerekmektedir. Bilinmeyen bir birey saygın bir kuruluşta olduğunu iddia ederse, kimliğini doğrudan firma ile doğrulamak gerekir.
2. Bir bireyin bu bilgileri bilme hakkı olmasından dolayı, emin olmadığınız müddetçe, kuruluşun yapısından ya da ağları dahil edebilmek üzere, kuruluşun hakkında herhangi bir şey ile ilgili bilgiler verilmemesi gerekmektedir.
3. Bireysel ve finansal bilgilerin e-posta ile paylaşılmaması gerekmektedir.
4. Bir sitenin güvenliğini doğrulayabilen bilgilerin clear text olarak web üstünden gönderilmemesi.
5. İstenilmeyen trafiği azaltabilmek için, güvenlik duvarı ve virüs koruma yazılımları gerekir.

3.1.4.3. Kurumsal Tedbirler

1. Gizli bilgileri işlemek için güvenlik protokollerinin, politikalarının ve prosedürlerinin oluşturulması.
2. Çalışanların pozisyonlarıyla ilgili güvenlik protokolleri konusunda eğitilmesi.
3. Güvenlik çerçevesinin habersiz, periyodik olarak test edilmesi.
4. Yukarıdaki adımların düzenli olarak gözden geçirilmesi; Hiçbir bilgi bütünlüğü çözümü mükemmel değildir.
5. Kilitli kapıların ve anahtarların olması.

3.1.4.4. Tehdit Modelleme Yöntemleri

Teknoloji ile gelişmiş olduğu günden bugüne, birden fazla “tehdit modelleme” yöntemi geliştirilmiştir. Bu yöntemlerin hepsi insan merkezli ve soyuttur. Bazı yöntemler özellikle de mahremiyet ya da risk endişelerine odaklanmaktadır.

Potansiyel tehditlere yönelik daha kapsamlı ve sağlam bir görüntü oluşturabilmek için birleştirilebilmektedirler [40].

Tehdit modellemesi, daha maliyetli bir düzeltmeden kaçınarak potansiyel sorunların erken belirlenip düzeltilebileceği geliştirme döngüsünün başlarında yapılmalıdır. Güvenlik gereksinimi ile ilgili düşünebilmek için tehdit modellerinin kullanılması gerekmektedir. Herhangi bir tehdit modelleme yöntemi benimsendiğinde hedef, süreç ve yaklaşım farklılıklarını anlayabilmek de son derece büyük bir önem arz etmektedir. Siber tehdit ve güvenlik istihbarat uygulamasını geliştirebilmek için, kullanılmakta olan birkaç tane siber tehdit modelleme yöntemi bulunmaktadır. Tehdit istihbaratının eyleme geçirilir olmasını sağlayabilmek için, bilgi güvenlik uzmanları hangi yöntemin belli iş hedefleri ile uyumlu olduğunu belirlemiştirler. Başlıca tehdit modelleme yöntemleri şu şekilde sıralanabilir [40].

Çizelge 3.5. Başlıca tehdit modelleme yöntemleri [40].

	OCTAVE	Trike	P.A.S.T.A	Microsoft	VAST
Tasarım sırasında uygulama güvenliğini uygulama	X	X	X	X	X
İlgili hafifletici kontrolleri tanımlama	X	X	X	X	X
Risk yönetimine doğrudan katkıda bulunma	X	X	X		X
Tehdit azaltma çabalarına öncelik verme	X	X	X		X
Tüm paydaşlar arasında iş birliğini teşvik etme	X	X			X
Kuruluş genelinde paydaşlar için çıktılar üretme	X				X
Tutarlı tekrarlanabilirlik		X			X
Tehdit modelleme sürecinin otomasyonu		X			X
Çevik DevOps Ortamına entegre olma					X
Binlerce tehdit modelinde ölçeklendirme yeteneği					X

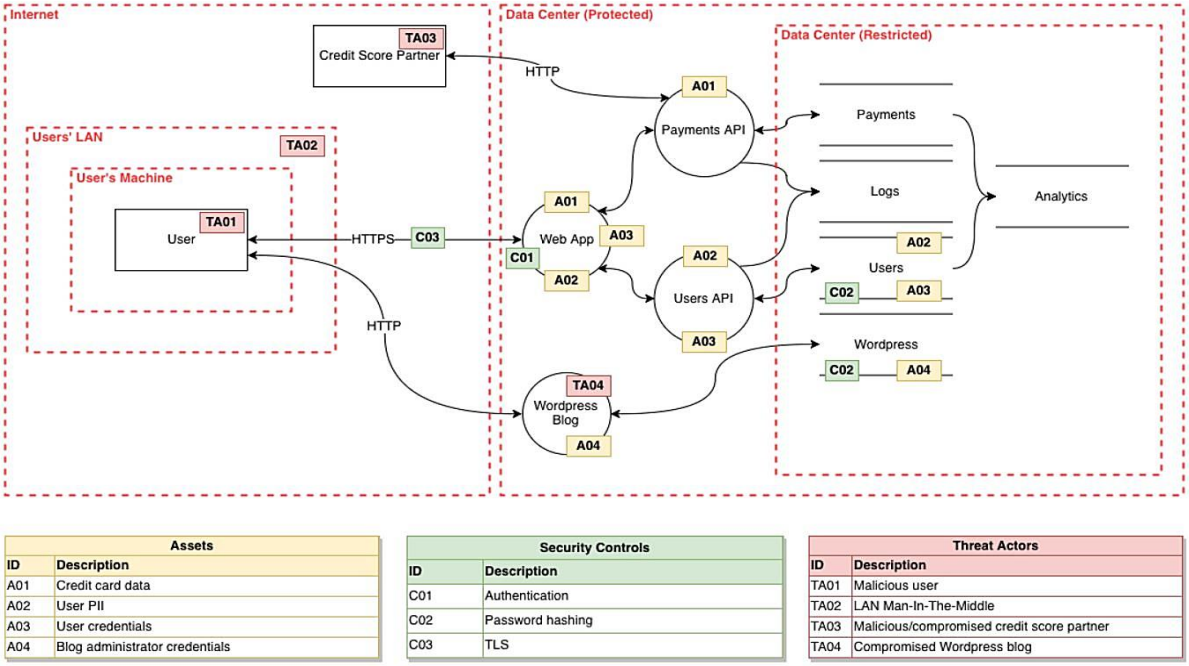
3.1.4.5. Stride

1999 yılında yapılmış olan ve 2002 yılında "Microsoft" tarafından tanıtımı yapılan "STRIDE" şu anda en olgun tehdit modelleme yöntemi olarak bulunmaktadır. STRIDE, aşağıda yer alan tabloda gösterilmiş olduğu gibi, herkes tarafından da bilinen isimleriyle bazı tehditler uygulamaktadır. Bunlar [40]:

Çizelge 3.6. STRIDE [40].

Threat (Tehdit)	Property (Özellik)	Mitigation Approach (Azaltma Yaklaşımı)
Spoofing (Sahtecilik)	Authentication (Kimlik Doğrulama)	● Parolalar, çok faktörlü kimlik doğrulama ● Dijital imzalar
Tampering (Kurcalamak)	Integrity (Bütünlük)	● İzinler/ACL'ler ● Dijital imzalar
Repudiation (İnkâr Etme)	Non-Repudiation (İnkâr Edememe)	● Güvenli log kaydı ve denetim ● Dijital imzalar
Information Disclosure (Bilgi açıklaması)	Confidentiality (Gizlilik)	● Şifreleme ● İzinler/ACL'ler
Denial of Service (Hizmet Reddi)	Availability (Kullanılabilirlik)	● İzinler/ACL'ler ● DAaAS filtreleme ● Kota
Elevation of Privilege (Ayrıcalık Yükseltme)	Authorization (Yetki)	● İzinler/ACL'ler ● Giriş doğrulama

STRIDE, sistem detay tasarımlarını değerlendiren sistem yerinde, modelleri bulunmaktadır. Veri akış diyagramları "(Data Flow Diagram- DFD)" oluşturularak sistemin sistemsel örneklerini, sınırlarını ve olaylarını açıklayabilmek için kullanılmaktadır.



Assets	
ID	Description
A01	Credit card data
A02	User PII
A03	User credentials
A04	Blog administrator credentials

Security Controls	
ID	Description
C01	Authentication
C02	Password hashing
C03	TLS

Threat Actors	
ID	Description
TA01	Malicious user
TA02	LAN Man-In-The-Middle
TA03	Malicious/compromised credit score partner
TA04	Compromised Wordpress blog

Şekil 3.5. Veri akış diyagramları [40].

3.1.4.6. Pasta

"Saldırı Simülasyonu ve Tehdit Analizi Süreci (PASTA)", 2012 yılında geliştirilmiş olan risk merkezli bir modelleme kapsamındadır. Bu yöntem 7 adımdan oluşmaktadır ve iş hedefleri teknik gereksinimleri ile bir araya getirmeyi amaç edinmiştir [40]. Saldırı Simülasyonu ve Tehdit Analizi Süreci (PASTA)" Adımları [40].

Çizelge 3.7. Saldırı simülasyonu ve tehdit analizi süreci (PASTA) [40].

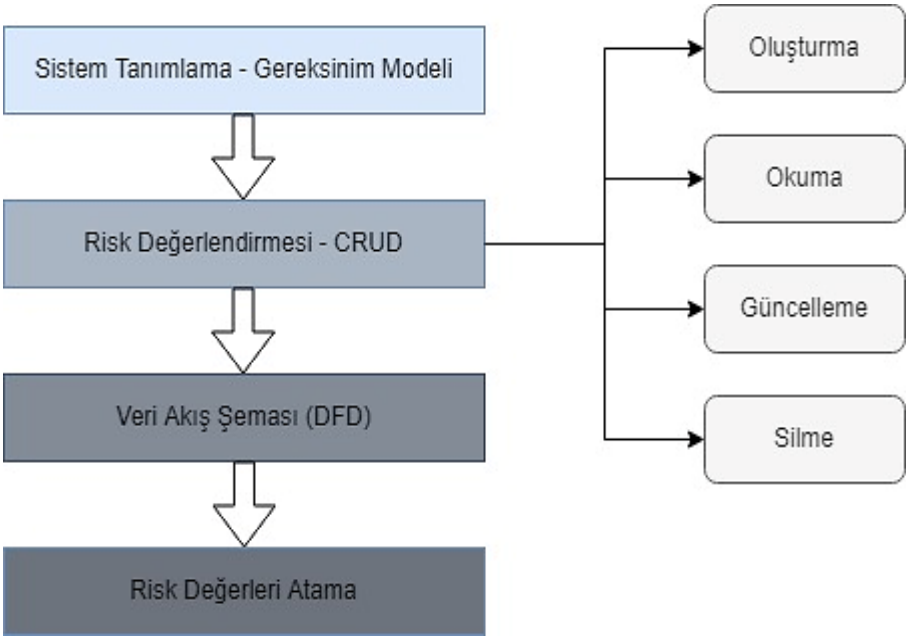
1. Hedefleri Tanımlama	• İş Hedeflerini Belirleme • Güvenlik ve Uyumluluk Gereksinimlerini Belirleme • İş Etki Analizi
2. Teknik Kapsamı Tanımlama	• Teknik Ortamın Sınırlarını Yakalama • Yakalama Altyapısı - Uygulama - Yazılım Bağımlılıkları

3. Uygulama Ayrıştırma	• Kullanım Durumlarını Tanımlama - Uygulamayı Tanımlama - Giriş Noktaları ve Güven Düzeyleri • Aktörleri Belirleme - Varlıklar - Hizmetler - Roller - Veri kaynakları • Veri Akış Şeması (DFD'ler) - Güven Sınırları
4. Tehdit Analizi	• Olasılıksal Saldırı Senaryoları Analizi • Güvenlik Olaylarına İlişkin Regresyon Analizi • Tehdit İstihbaratı Korelasyonu ve Analitiği
5. Güvenlik Açığı ve Zayıf Yönler Analizi	• Mevcut Güvenlik Açığı Raporlarının Sorguları ve Sorunların Takibi • Tehdit Ağaçlarını Kullanarak Mevcut Güvenlik Açığı Eşleme Tehdidi • Kullanım ve Kötüye Kullanım Durumlarını Kullanarak Tasarım Kusur Analizi • Puanlar (CVSS/CWSS) - Numaralandırmalar (CWE/CVE)
6. Saldırı Modelleme	• Saldırı Yüzeyi Analizi • Saldırı Ağacı Geliştirme - Saldırı Kitaplığı Yönetimi • Güvenlik Açığına Saldırı ve Saldırı Ağaçlarını Kullanarak Analizden Yararlanma
7. Risk ve Etki Analizi	• Niteliklendirme ve İş Etkisini Ölçme • Karşı Tedbir Tanımlama ve Artık Risk Analizi • Kimlik Riski Azaltma Stratejileri

Çeşitli aşamada farklı analiz araçları kullanılmaktadır. Bu yöntemde, kilit karar verenler dahil edilerek ve operasyonların, mimari, yönetim ve geliştirilmesinden güvenlik iç görüleri gerektirilerek tehdit modelleme sürecini stratejik bir düzeye yükseltmektedir. Yaygın olarak risk merkezinden belli bir kapsamı olarak kabul edilen "PASTA" tehdit sayımları ve değerlendirmeleri biçiminde varlık merkezli çıktılar üretebilmek için, saldırgan merkezli bir bakış açısı kullanmaktadırlar.

3.1.4.7. Trike

Risk yönetimi amacı ile güvenlik denetiminin yapılmasında kullanılan açık kaynaklı bir tehdit modelleme yöntemidir.



Şekil 3.6. TRIKE tehdit modellemesi [39].

TRIKE tehdit modellemesi, gereksinim modeli ve uygulama modeli olmak suretiyle 2 modelin birleşimidir. Gereksinim modelinde, bir BT sistemi güvenlik özelliklerinin tanımlanmasında ve her bir varlığın kabul edilebilir risk seviyesini atayan "TRIKE" modellemesinin ana temelidir. İlgili bu model ile, ayrıca çeşitli güvenlik ekipleri ve paydaşların arasında koordinasyonu sağlayabilen kuramsal bir çerçeve sağlamaktadır. Bundan sonra da uygulama modeli gelmektedir. Bu modelde, bir sistemin içinde veri akışını kullanıcı eylemlerini temsil edebilmek için, "veri akış diyagramı (DFD)" oluşturulmaktadır. Bu model, tehditlerin belli bir risk puanını belirleyebilmek ve atayabilmek için analiz ekmektedir. Tüm bunlara dayanarak, atanmış ve öncelikli tehditlere dayalı olarak, karşı güvenlik kontrolleri ya da önleyici tedbirlerin tanımlanması gerekmektedir [39].

3.1.4.8. Vast

VAST "Görsel, Çevik ve Basit Tehdit" modelinde, otomatik bir tehdidin modelle platformu olan "ThreatModeler"ı temel almaktadır [39].

Çizelge 3.8. VAST (görsel, çevik ve basit tehdit) [39].

Automation (Otomasyon)	• Tehdit Modellemede Tekrarlamayı Ortadan Kaldırır • Devam Eden Tehdit Modelleme • Tüm Kuruluşu Kapsayacak Şekilde Ölçeklendirilmiştir
Integration (Entegrasyon)	• SDLC Boyunca Araçlarla Entegrasyon • Çevik DevOps'u destekler
Collaboration (İş birliği)	• Kilit Paydaşlarla İş Birliği Uygulama Geliştiricileri • Sistem mimarları, Güvenlik Ekibi ve Kıdemli Yöneticiler

Kullanılabilir ve ölçeklenebilir olması sebebiyle, farklı paydaşlar için de uygulanabilmektedir ve güvenilir sonuçlar elde edebilmek için, bütün alt yapının genelinde büyük kurum ve kuruluşlar ile de kullanılabilmektedir. VAST, alt yapı ve geliştirme ekipleri arasında operasyonel çeşitlilikleri ve endişeleri tanımaktadır. Bu iki modelin oluşturulmuş olması gerekmektedir. "Uygulama tehdit modelleri ve operasyonel tehdit modeli" mimari yönden temsil edebilen sürecin akış diyagramlarını kullanmaktadır. Operasyonel tehdit modelleri, "DFD"lere dayalı olarak belli bir saldırganın bakış yönünden oluşturulmaktadır. Bu yaklaşımda "VAST"ın kurulumun geliştirilmesinde ve "DevOps" hayat döngüsünde entegrasyonunu sağlamaktadır [39].

3.1.4.9. Dread

DREAD metodolojisi, tehditleri derecelendiren risk olasılıklarını değerlendirebilmek, analiz edebilmek ve bulmak için kullanılmaktadır [39].

Çizelge 3.9. DREAD metodolojisi [39].

Damage (Zarar)	Saldırının Etkisi
Reproducibility (Yeniden Üretilebilirlik)	Saldırı Ne Kadar Kolayca Yeniden Üretilebilir?
Exploitability (Kullanılabilirlik)	Saldırıyı Başlatmak Ne Kadar Kolay?
Affected users (Etkilenen Kullanıcılar)	Kaç Kullanıcı Etkilenecek?

Discoverability (Keşfedilebilirlik)	Güvenlik açığı ne kadar kolay bulunabilir?

3.1.4.10. Diğerleri

Tehdit modelleme, sistemin daha güvenilir olmasına yardımcı olmaktadır. Modellerin bazılarında tipik bir şekilde tek başlarına kullanılmaktadır. Bazıları genel olarak diğerleri ile beraber kullanılmaktadır. Herhangi bir proje için en iyi yöntemleri seçebilmek, hedeflemek istemiş olduğu belli alanları "(risk, güvenlik, gizlilik)" tehdit modellemesinin ardından ne kadar süreceğine yönelik, tehdit modelleme deneyimlerinin düzeyini ve çaba seviyesini dikkate alması gerekmektedir. Bu yöntemlerin hepsi, süre aciliyeti ve modellemenin ne sıklık ile tekrarlanmış olduğuna bağlı olarak çevik bir ortamda kullanılabilmektedir [39].

3.1.4.11. Tehdit Modelleme Araçları

Tehdit modelleme için birçok araç bulunmaktadır. Bu araçlardan bazıları aşağıdaki gibi sıralanabilir.

1. Microsoft Threat Modelling Tool [https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool]
2. ThreatModeler [https://threatmodeler.com/]
3. securiCAD Professional [https://iriusrisk.com/threat-modeling-tool/]
4. IriusRisk [https://iriusrisk.com/threat-modeling-tool/]
5. SD Elements [https://www.securitycompass.com/sdelements/]
6. Tutamen [https://www.tutamantic.com/]
7. OWASP Threat Dragon [https://owasp.org/www-project-threat-dragon/]

3.5. MAKİNE ÖĞRENMESİ, YAPAY ZEKÂ VE DERİN ÖĞRENME

Makine öğrenmesi yapısal ve işlevsel olarak öğrenmeye açık, yorumlama yeteneğine sahip, verileri anlayarak sonuçlar ya da çıktılar ortaya koyan bir sistemdir. Kendilerine bir model oluşturarak çalışmaktadır. Belli bir algoritmaya göre giriş verilerini verip, çıkış parametresiyle istatistiksel tahminler de bulunarak doğru tahmin etmeye çalışan

bir öğrenimdir [62].

Makine öğrenimi ve derin öğrenme ile ilgili yapay zekâ karşılaştırmalarını anlayabilmek için, aşağıdaki tanımlar göz önünde bulundurulması gerekmektedir. Derin öğrenme, yapay sinir ağlarına dayalı makine öğrenimlerinin bir alt kümesi olarak tanımlanmaktadır. Yapay sinir ağlarının yapısı çoklu girdilerden ve gizli katmanlardan oluştuğu için öğrenme süreci de çok derindir. Her katman, girdi verilerinin bir sonraki katmanın belli bir tahmin görevi için kullanılacakları bilgilere dönüştüren varlıkları içermektedir. Bu yapı sayesinde, herhangi bir makine kendi verisini işleyerek öğrenebilmektedir. Makine öğrenimi, makinelerin görevlerini iyileştirebilmek için, deneyimlerin kullanılmasına izin veren tekniklerin "derin öğrenme gibi" kullanılmış olan bir yapay zekâ alt kümesidir. Öğrenme süreçlerinde aşağıdaki adımlar uygulanmaktadır [41]:

1. Verileri bir algoritmayla besleme. (Bu adımda, örneğin özellik ayıklama gerçekleştirerek modele ek bilgi sağlayabilirsiniz.)
2. Modeli eğitmek için bu verileri kullanın.
3. Modeli test edin ve dağıtın.
4. Otomatik tahmine dayalı bir görev yapmak için dağıtılan modeli kullanın. (Başka bir deyişle, model tarafından döndürülen tahminleri almak için dağıtılan modeli çağırın ve kullanın.)

Makine öğrenim tekniklerini kullanılarak, yaygın olarak insan zekâsı ile ilişkili görevler gerçekleştirebilen, bilgisayar sistemli uygulamalar oluşturulabilir. Bu görevlerin görüntüleri tanıma, dil çevirisi ve ses tanıma gibi işlevleri bulunmaktadır [41].

3.5.1.Öğrenme Aktarımı Nedir?

Derin öğrenme modelleri genel olarak "yüksek düzeyde bilgi işlem kaynakları (GPU, TPU) ve eğitim verisi" kullanmaktadır. Yapılan çalışmada öğrenme transferi adı verilen bir teknik kullanılarak, eğitim süreci kısaltılabilir. Böylece, öğrenme aktarımı da kısa sürmüş olur. Sinir ağlarının doğası gereğinde, 1'inci katman seti genel olarak

daha düşük seviyede özellikler içermektedir. Son katman setinde ise, mevzu bahis alana daha yakın olabilen daha yüksek seviyede özelliği içermektedir. Yeni bir etki alanından ya da sorunlarından kullanım için, son birkaç katman yeniden kullanılarak, yeni modelleri eğitebilmek için gereken süre, hesaplama ve verilerin kaynakları önemli ölçüde azaltılabilir [41]. Azure Machine Learning: Öğrenme aktarımı kullanıldıktan sonra, derin öğrenme "PyTorch" modelinin eğitilmesi bölümünde açık kaynak kapsamında kullanılmaktadır [42].

Adlandırılmış varlıkların tanınması: Metinleri girdi olarak alan ve belli bir sınıfa dönüştüren bir derin öğrenme yöntemidir. Bu yeni bilgiler "ürün kimliği, tarih ve posta kodu" olabilmektedir. Bilgiler daha sonrasında, yapılandırılan bir şemada ya da kimlik doğrulama motoru için, belli bir kıyaslama noktası olarak oluşturulmuştur ya da kullanılan bir adres listesinde saklanılabilmektedir [43].

Nesne algılama: Nesne algılama 2 bölümden oluşmaktadır. Bunlar; "görüntü lokalizasyonu ve görüntü sınıflandırmadır." Görüntü sınıflandırmasında, görüntüdeki arabalar ve insanlar gibi nesneleri tanımlamaktadır. Görüntü yerleştirme de, bu nesnelerin belli konumları sağlanmaktadır. "Perakende, oyun, turizm, nesne tanıma ve kendi kendini süren arabalar" vb. sektörlerde hali hazırda kullanılabilmektedir. Görüntü tanımada görüldüğü gibi, belli bir görüntüde başlamış olduğu sistemin görüntüsü içeriğini açıklayabilen, belli bir başlık oluşturmaktadır. Fotoğraftaki nesnede tanımlanmış olan ve etiketlemenin bir diğer adımında, bu etiketler açıklayıcı cümlelere dönüştürülmektedir. Görüntü açıklama uygulamasında, belli bir görüntüdeki nesneleri tanımlayabilmek için, genel olarak karmaşık bir sinir ağı kullanılmaktadır ve hemen ardından etiketini tutarlı bir biçimde cümleye dönüştürebilmek için, yinelemeli bir sinir ağı kullanmaktadır [44].

Makine Çevirisi: Makine çevirisi, herhangi bir dilden sözcükleri ya da tümceleri almaktadır. Bunları otomatik bir şekilde, herhangi bir dile çevirebilmektedir. Makine çevirisi uzun bir süre kullanılmaktadır. Fakat derin öğrenme 2 alanı da etkileyen sonuçlar üretmektedir: Makine çevirisi, daha büyük ses dosyasındaki parçacıkları tanımlayabilmek ve konuşulan kelimeleri ya da görüntüleri metin olarak yazmak için kullanılmaktadır [45].

Metin Analizi: Derin öğrenme yöntemlerinden birisi olan metin analizi, büyük ölçekli ve sayıdaki metin verisini "(örneğin tıbbi belgeler veya gider makbuzları)" analiz edebilmek, kalıplar tanımak ve tüm bunlardan yapılandırılmış olan, net bilgiler oluşturmak ile ilişkilidir. Firmalar, dosyaların içinden öğrenmiş oldukları bilgileri ticarette ve devlette uyumluluğunu tespit edebilmek ve metin analizi yapabilmek için, derin öğrenme kullanılmaktadır [46].

BÖLÜM 4

ORGANİZASYON VE TEKNOLOJİ

4.1. OLGUNLUK SEVİYELERİNE GÖRE SOC ORGANİZASYON MODELLERİ

SOC organizasyonları olgunluk seviyelerine göre 4'e ayrılır. Bunlar aşağıda detaylı olarak açıklanmaktadır.

4.1.4. Olgunluk Seviyesi 1: Başlangıç Seviyesi

Giriş düzeyinde, süreç uygulamaları ve sonuçları tutarlı değildir. İşlemler nadiren tanımlanır veya belgelenir ve tanımlanmış süreçler nadiren takip edilir. Kuruluş genelinde süreç uygulaması için istikrarlı bir ortam sağlamaz. Aşırı iş yükü, giriş seviyesi kuruluşlar için tipiktir. Bireyler görevlerini yerine getirseler de bunu yaparken kişisel yöntemler kullanırlar. Bu organizasyonlarda başarı, kanıtlanmış süreçlerin uygulanmasına değil, organizasyon içindeki kişilerin yetkinlik ve becerilerine bağlıdır. Süreç yeteneği, organizasyonun değil, bireylerin bir özelliğidir. Bu tutarsız ortama rağmen, birinci düzey kuruluşlar genellikle işe yarayan ürünler ve hizmetler üretebilir, ancak bunlar genellikle aşırı finanse edilir, programları kaçırılır ve üretkenlik düşer. Bu kuruluşlar, iş ortamındaki değişikliklere uyum sağlamaya çalışırken büyük zorluklarla karşı karşıyadır. Model açısından bakıldığında, birinci olgunluk düzeyindeki bir kuruluş, ikinci düzey için tanımlanan süreç alanlarıyla ilişkili hedeflere henüz ulaşmamıştır [47].

4.1.2. Olgunluk Seviyesi 2: Yönetilebilir Seviye

İkinci olgunluk düzeyinde, her iş birimi ve her proje; Temel planlama ve yönetim süreçlerini oluşturmuştur ve ürünlerini/hizmetlerini geliştirmek, hazırlamak,

dağıtmak, işletmek ve desteklemek için gerekli tüm faaliyetleri gerçekleştirir. Üst ve orta yönetim, süreç iyileştirmeyi destekler ve koordine eder, iş birimi ve proje sorumluluklarını tanımlar ve iş akışını kontrol eder. Önceki çalışmalar, iş alanı ihtiyaçları ve geçmiş deneyimler kullanılarak belirlenen sorumluluklar gerçekçidir. Yöneticiler, sorumlulukların yerine getirilmesinde maliyetleri, çizelgeleri, çıktıları, gereksinimleri ve sorunları analiz eder. Üst yönetimin bu seviyede öncelikli olarak ilgilendiği değişkenler maliyet, çizelgeleme ve çıktıdır. Kalite bilinci artırılmış olsa da kalite hedefleri üst yönetimin birincil yönetim kaygısı değildir [48].

Bu düzeyde, süreçler iş birimleri arasında farklılık gösterebilir. Şirket süreç yönetimi politikalarının oluşturulmasında ve geliştirilmesinde üst yönetimin desteklenmesi, bu seviyeye ulaşmanın en önemli şartıdır [48]. Ayrıca, iş birimlerinin süreçleri tutarlı bir şekilde yürütebilmesi için organizasyon ortamının dengelenmesi gerekir. Kuruluşların ikinci olgunluk düzeyinde elde ettikleri bu disiplin, stres zamanlarında mevcut uygulamaların korunmasını sağlar. İş birimleri, belgelenmiş planlara, süreçlere ve prosedürlere göre çalışır ve yönetilir. Ürünler/hizmetler genellikle planlanan program ve bütçe dahilinde teslim edilir [49].

4.1.3. Olgunluk Seviyesi 3: Standartlaştırılmış Seviye

Üçüncü olgunluk düzeyinde, ürün veya hizmetlerin geliştirilmesi, hazırlanması, satışı, yönetimi ve desteklenmesi için gerekli standart süreçler oluşturulur ve kuruluş genelinde kullanılmak üzere belgelenir. Kurumun standart süreçleri iş süreçleri; destek süreçleri ve yönetim süreçleri olarak ikiye ayrılmaktadır. Bu süreçler, organizasyon genelinde faaliyetlerin tutarlı bir şekilde yürütülmesini sağlayan süreç tanımlarını içerir. Ayrıca organizasyonun süreç faaliyetlerini koordine etmekten sorumlu bir birim de vardır. Örgütsel öğrenmeyi desteklemek için bir örgütsel altyapı oluşturulmuştur. Kuruluşun standart süreçlerini iyileştirmek için kullanılan teknikler vardır. Kuruluş genelinde öğrenilen dersler toplanır, düzenlenir ve birimlerin kullanımına sunulur. Kuruluşun ve süreçlerinin performansını ve diğer özelliklerini anlamak ve iyileştirme faaliyetlerini belirlemek için veriler toplanır ve analiz edilir. Çalışanların bilgi ve becerilerini geliştirmek için kuruluş çapında bir program oluşturulur [49].

Tanımlanmış süreçler, kuruluşun standart süreçlerinin uyarlanmasıyla oluşturulur. Özelleştirme, her çabanın özel ihtiyaçlarına yöneliktir (örneğin, farklı ürünler geliştirmek, farklı hizmet türleri sunmak). Herhangi bir tanımlanmış süreç; Girdi kriterleri, girdiler, standartlar ve prosedürler, faaliyetler, doğrulama mekanizmaları, çıktılar ve çıkış kriterleri gibi belirli bilgileri içerir. Süreç iyi tanımlandığından, yönetim iş ilerlemesi ve iş faaliyetleri arasındaki ilişkiyi kolayca takip edebilir. Her iş birimi için ayrı bir süreç tanımlanır (örneğin süreç ve ürün güvence grubu, konfigürasyon yönetimi grubu, süreç mühendisliği grubu, eğitim grubu vb.). Tanımlanan her süreç, tutarlı ve bütünleşik alt süreçler içerir. Belirli bir faaliyette yer alan farklı disiplinlerin süreçleri arasındaki ilişkiler iyi tanımlanmış, belgelenmiş ve istikrarlı olduğu kanıtlanmıştır [49].

4.1.4. Olgunluk Seviyesi 4: Öngörülebilir Seviye

Üçüncü olgunluk seviyesindeki bir organizasyonda, performans ve kalite için ulaşılabilir nicel hedefler oluşturulmuş ve son kullanıcının ve organizasyonun ihtiyaçlarına göre uyarlanmıştır. Hedeflerin ulaşılabilirliği, tanımlanan süreçlerin ve planların nicel olarak analiz edilmesi ve bu hedeflere ulaşma yeteneğinin elde edilmesi anlamına gelir. Varyasyonların nicel olarak anlaşılması, azaltılması ve kontrolü; ulaşılacak performans ve kalite sorunlarının istatistiksel değerlendirmesi; Performans ve kalite hedeflerine ulaşmak için süreç düzeltici aksiyonların alınması dördüncü olgunluk seviyesinin temel kaygılarıdır. Nicel tahminler, nicel performans ve kalite hedefleriyle doğrudan ilişkilidir. Performansa ve kaliteye önemli ölçüde katkıda bulunması beklenen çalışmalar istatistik ve diğer nicel teknikler kullanılarak kontrol edilir. Bu düzeydeki öncelikli faaliyetler aşağıdaki gibi özetlenebilir [50]:

1. Kuruluşun süreç varlıklarının oluşturulması ve yönetimi
2. Ürünlerin/hizmetlerin geliştirilmesi, hazırlanması, satışı, işletilmesi ve desteklenmesi ile ilgili çeşitli süreçlerin entegrasyonu
3. Önceden tanımlanmış ve üzerinde anlaşmaya varılmış performans ve kalite hedeflerine ulaşabilen tanımlanmış süreçler ve planlar oluşturmak
4. Faaliyetlerin nicel yönetimini desteklemek için kuruluş genelinde verileri toplamak ve analiz etmek

5. Performansı yönetmek ve faaliyetleri değiştirmek
6. Nicel performans ve kalite hedeflerine ulaşılmasını kontrol etmek

Dördüncü düzeyde, farklı etkinlikler için farklı yöntemlerin kullanılması normaldir. Bazı durumlarda kontrol grafikleri kullanılabilirken, diğer durumlarda regresyon analizi, histogramlar, çizgi grafikler veya diğer yöntemler kullanılabilir. Bu düzeydeki kuruluşlar, niceliksel sınırlar içinde çalıştıkları için kontrol edilebilir, ölçülebilir ve öngörülebilir olarak nitelendirilebilir. Bu sayede ürün/hizmetlerin performansı ve kalitesi tahmin edilebilir, istisnai sapmalar tespit edilebilir ve düzeltici aksiyonlar alınabilir [50].

4.2. ROLLER VE SORUMLULUKLAR

4.2.1. Siber Güvenlik Analisti

Siber güvenlik analistleri, siber tehditleri önleyebilmek, tespit edebilmek ve yönetebilmek için, farklı teknolojilerin süreçleri kullanılarak, belli bir kuruluşun korunmasına yardımcı olmaktadır. Bu bilgisayarın, verilerin, ağların ve programların korunmasını içerebilmektedir. Siber güvenlik analistleri genel olarak, aşağıda yer alan alanların birinde çalışmaktadır [50]:

1. Çalışmış oldukları kurumun siber güvenliğini korumak için çalışmaktadır.
2. Bilginin güvenlik analisti, güvenlik analistleri, bilgi güvenlik danışmanlık, güvenlik operasyon merkezinde siber istihbarat analistidir.

Sorumlulukları ve görevleri nelerdir:

1. Son teknoloji ve güvenlik gelişiminden haberdar olmak
2. Ortaya çıkan siber güvenlik tehdidini ve bunları ele almak
3. Bir güvenlik ihlali söz konusu olduğunda, olağanüstü durum kurtarma planını yapmak
4. Olağandışı, izinsiz ve yetkisi faaliyetleri izlemek
5. Güvenlik ürünlerinin test edilmesini ve değerlendirilmesini yapmak

6. “Dolandırıcılık” ve “Kimlik avı” etkinliklerini yanıtlamak ve izlemek
7. İstenmeyen kötü yazılımlara veya kötü niyetli e-postalara tavsiyede bulunabilmek ve öncülük etmek.

Yapılan başka bir çalışmada, SOC zorluklarının nicel ve nitel analizinden elde edilen sonuca dayanarak, en çok karşılaşılan zorlukların, otomasyon eksikliği, BT güvenliğine ilişkin görünürlük eksikliği, yanlış alarmlar, süreç veya playbook eksikliği, SOC eğitimi ve saldırı simülasyonlarının eksikliği, pratik eksikliği, SOC analistinin değerlendirmesi için yeterli metrik eksikliği olduğu gözlemlenmiştir [63].

4.2.2. Siber Tehdit Avcısı

Geleneksel siber güvenlik çözümleri, siber güvenlik alarm değerlendirme sistemleri, sorgu tabanlı günlük (log) yönetim sistemleri, ağ güvenliği için IDS/IPS (Saldırı Tespit Sistemi/Saldırı Önleme Sistemi) sistemleri, merkezi günlük toplama ve korelasyon yöntemleri için SIEM (Güvenlik Bilgileri ve Olay Yönetimi) kullanan bir kurumsal ağda, çözümler ve çeşitli yazılımların yanı sıra kullanılan teknikler. Bu çözümler sistem güvenliğini artırmak için kullanılsa da siber saldırılar her geçen gün artıyor. Bu saldırıların çoğu otomatik ve düşük riskli olsa da kuruluşların hassas verileri için büyük bir tehdit oluşturuyor ve risk düzeyini artırıyor. Tüm bu çözümler ve teknikler, siber tehditleri aramak için basit teknikler kullanır. Ancak gelişmiş saldırıları tespit etmek için bu tekniklerden çok daha sofistike ve güçlü av yaklaşımları gereklidir [51].

4.3. GÜVENLİK BİLGİLERİ VE OLAY YÖNETİMİ (SIEM)

SIEM sistemleri, tehdit saldırılarına karşılık savunma yapan kurum ve kuruluşlar için kritik bir önemi bulunmaktadır. Ortalama bir kuruluşun “Güvenlik Operasyonları Merkezi (SOC)” günde on bin den daha çok uyarı almaktadır. En büyük kuruluşlar 150 binden fazla uyarı almaktadır. Fakat, giderek karmaşıklaşan ve artan siber tehditlerin oluşturduğu risklerin uyarılarını görmezden gelmek son derece tehlikeli bir hal almaktadır. Tek bir uyarı da büyük bir olayı tespit etmek ve önleyebilmek ya da onu tamamı ile ortadan kaldırmak arasında fark vardır. SIEM güvenlik uyarıları oluşturabilmek ve araştırabilmek için, daha verimli bir yol sağlamaktadır. SIEM

teknolojisi ile ekipler, güvenlik verilerinin sınırını izleyebilmektedir [52].

“Güvenlik Bilgileri ve Olay Yönetimi (SIEM)” çözümleri, tehdit algılanmasını hızlandırabilmek ve güvenlik olay yönetimini yasal uyumluluğunu destekleyebilmek için, günlükleri toplamaktadır. Güvenlik olaylarını diğer veriler ile birlikte analiz etmesi gerekmektedir. Belli bir SIEM teknoloji sisteminde, birden fazla kaynaktan veri toplanılarak daha hızlı tehdit yanıtı sağlamaktadır. Belli bir anormallik algılanmasının ardından daha çok bilgi toplayabilmektedir. Belli bir uyarı tetikleyebilir ya da bir öğeyi karantina altına alabilmektedir. SIEM teknolojisi, geleneksel olarak uyumluluk gösterebilmek isteyen kurum ve kamu şirketleri tarafından kullanılsa da güvenlik istihbaratı ve olay yönetiminin daha da güçlü olduğunu göstermiştir. SIEM teknolojisi olduğu günden beri her büyüklükte bir kuruluş için vazgeçilmez bir tehdit algılama aracı haline girmiştir. Günümüzdeki tehditlerin karmaşıklığından ve siber güvenlik becerilerinin eksikliği göz önüne alındığında ise, diğer güvenlik endişelerinin otomatik ve hızlı olarak tanımlayabilen güvenlik olayları yönetimine sahip olması büyük bir öneme sahiptir. SIEM yetenekleri aynı zamanda orta ve küçük ölçekli işletmeler ile güvenlik ve olay yönetiminin çözümü için kullanmaya teşvik etmektedir [52].

4.4. KULLANICI VE VARLIK DAVRANIŞ ANALİZİ (USER AND ENTİTY BEHAVİOR ANALYTİCS)

Kullanıcı davranışı analizi (UBA) olarak da bilinen kullanıcı ve varlık davranışı analizi(UEBA), kullanıcıların her gün oluşturduğu ağ olaylarına ilişkin iç görü toplama sürecidir. Toplanıp analiz edildikten sonra, güvenliği ihlal edilmiş kimlik bilgilerinin, yanal hareketin ve diğer kötü niyetli davranışların kullanımını tespit etmek için kullanılabilir. Gartner Pazar Rehberi (Market Guide), yalnızca bireysel kullanıcılardan ziyade dış kuvvetlerden gelen ve artan tehditler nedeniyle Kullanıcı Davranışı Analizine 'Varlık'ı ekledi. Bu dış kuvvetler, yönlendiriciler, sunucular, uygulamalar ve muhtemelen tehlikeye girebilecek diğer ağ cihazlarını da içerir, ancak bunlarla sınırlı değildir. Özetle, bu diğer davranış analiz türleri, sistemlerin davranışına ve bunlar üzerindeki kullanıcı hesaplarına odaklanmak için geleneksel kullanıcı davranış analitiğinden sapar [53].

UEBA çözümleri, sunucular, yönlendiriciler ve veri havuzları gibi bir BT ortamındaki kullanıcılar ve varlıklar için standart davranışı modelleyen profiller oluşturur. Bu, temel oluşturma olarak bilinir. UEBA teknolojisi, çeşitli analiz teknikleri kullanarak, yerleşik temellere kıyasla anormal olan faaliyetleri belirleyebilir, tehditleri keşfedebilir ve güvenlik olaylarını tespit edebilir. Gartner, UEBA çözümlerini üç kısımda tanımlar [54]:

1. **Kullanım senaryoları:** UEBA çözümleri, kurumsal ağdaki kullanıcıların ve diğer varlıkların davranışları hakkında bilgi sağlar. Anormalliklerin izlenmesini, tespit edilmesini ve uyarılmasını sağlamalıdırlar. Ayrıca, çalışan izleme, güvenilir ana bilgisayar izleme, dolandırıcılık vb. için özel araçlardan farklı olarak, birden fazla kullanım durumu için geçerli olmalıdırlar.
2. **Veri kaynakları:** UEBA çözümleri, veri gölü veya veri ambarı gibi genel bir veri havuzundan veya bir SIEM aracılığıyla verileri alabilir. Verileri toplamak için aracıları doğrudan BT ortamına yerleştirmemelidirler.
3. **Analiz:** UEBA çözümleri, istatistiksel modeller, makine öğrenimi, kurallar, tehdit imzaları ve daha fazlası gibi çeşitli analitik yaklaşımları kullanarak anormallikleri tespit eder.

4.4.1. UEBA ve SIEM'in Yakınsaması

UEBA ve SIEM teknolojileri arasında yakın bir ilişki vardır, çünkü UEBA, analizlerini gerçekleştirmek için kuruluşlar arası güvenlik verilerine dayanır ve bu veriler tipik olarak bir SIEM tarafından toplanır ve saklanır. Gartner, UEBA'yı bir SIEM'e dahil edilmiş bir özellik olarak görüyor. Davranış analizi, Gartner'ın Güvenlik Bilgileri ve Olay Yönetimi için Magic Quadrant'ta satıcıları değerlendirdiği yeteneklerden biridir. Gartner, bir SIEM için aşağıdaki yetenekleri özetlemektedir [54]:

1. Güvenlik cihazları, ağ altyapısı, sistemler ve uygulamalar tarafından üretilen toplu olay verileri
2. Puanlama, önceliklendirme ve araştırmaları hızlandırma amacıyla olay verilerini kullanıcılar, varlıklar, tehditler ve güvenlik açıkları hakkında bağlamsal bilgilerle birleştirme

3. Daha verimli analiz etmek için verileri normalleştirme
4. Güvenlik izleme, kullanıcı ve varlık davranışlarının gelişmiş analizi, analitik sorgulama, olay araştırmasını ve yönetimini destekleme ve raporlama için olayların gerçek zamanlı analizini sunmak
5. UEBA kullanım örnekleri.

Üç tür içeriden tehdit vardır:

İhmalci: Uygun BT prosedürlerini izlemedikleri için istemeden kuruluşlarını riske atan BT sistemlerine ayrıcalıklı erişime sahip bir çalışan veya yüklenicidir. Örneğin, oturumunu kapatmadan bilgisayarından ayrılan biri veya varsayılan parolayı değiştirmeyen veya bir güvenlik düzeltme eki uygulayamayan bir yönetici. Bir kullanıcı için normal ve anormal aktiviteyi belirlemek, ihmal nedeniyle güvenliği ihlal edilmiş bir kullanıcıyı tespit etmenin anahtarıdır.

Kötü niyetli içeriden bilgi: Kötü niyetli içeriden bilgi, kuruluşa karşı bir siber saldırı gerçekleştirmeyi amaçlayan BT sistemlerine ayrıcalıklı erişime sahip bir çalışan veya yüklenicidir. Kötü niyetli niyeti ölçmek, günlük dosyaları veya normal güvenlik olayları aracılığıyla keşfetmek zordur. UEBA çözümleri, bir kullanıcının tipik davranışı için bir temel oluşturarak ve anormal aktiviteyi tespit ederek yardımcı olmaktadır [55].

Gizliliği ihlal edilmiş içeriden bilgi: Saldırganların bir kuruluşa sızması ve ağdaki ayrıcalıklı bir kullanıcı hesabını veya güvenilen ana bilgisayarı tehlikeye atması ve saldırıya oradan devam etmesi yaygındır. UEBA çözümleri, saldırganın ele geçirilen hesap aracılığıyla gerçekleştirdiği kötü amaçlı etkinliği hızla tespit etmeye ve analiz etmeye yardımcı olabilir. Geleneksel güvenlik araçları, saldırı modeli veya öldürme zinciri, şu anda bilinmeyen (sıfır gün saldırısında olduğu gibi) veya kimlik bilgilerini, IP adreslerini veya makineleri değiştirerek, bir kuruluşta yanal hareket eden güvenliği ihlal etmiş içeriden kişiyi tespit etmeyi zor hale getirmektedir. Ancak UEBA teknolojisi bu tür saldırıları tespit edebilir, çünkü bunlar neredeyse her zaman varlıkları yerleşik taban çizgilerinden farklı davranmaya zorlar.

4.3. SOAR (SECURITY ORCHESTRATION AUTOMATION AND RESPONSE)

SOAR, güvenlik orkestrasyonu, otomasyonu ve müdahalesi olarak bilinmektedir. Güvenlik ekiplerinin çeşitli kaynaklardan bilgi toplamasına ve önceden tanımlanmış süreç ve prosedürlerle tutarlı iş akışları yürütmesine olanak tanır.

4.3.1. Güvenlik Düzenlemesi

Güvenlik düzenlemesi, özel ya da yerleşik entegrasyonların, uygulama programlama arabirimleri (API'ler) aracılığı ile çeşitli harici ve dahili araçları birbirine bağlamaktadır. Bağlantılı sistemler, güvenlik açığı tarayıcıları, uç nokta koruma ürünleri, son kullanıcı davranışları analitiği, güvenlik duvarı, izinsiz giriş algılama sistemleri ve izinsiz giriş önleme sistemleri "(IDS'ler / IPS'ler) ve güvenlik bilgileri ve olay yönetimi (SIEM)" platformlarının yanında harici tehdit istihbarat beslenmesini içermektedir [56].

Toplanan tüm veriler, daha kapsamlı bağlam ve gelişmiş iş birliği ile birlikte tehditleri tespit etmede daha iyi bir şans sağlar. Bununla birlikte, yedek almak ve analiz etmek için daha fazla uyarı ve daha fazla veridir. Güvenlik düzenlemesinin, yanıt işlevlerini başlatmak için verileri birleştirdiği durumlarda, güvenlik otomasyonu harekete geçer [56].

4.3.2. Güvenlik Otomasyonu

Güvenlik düzenlemesinden toplanan veriler ve uyarılarla beslenen güvenlik otomasyonu, verileri alır, analiz eder ve manuel süreçlerin yerini almak için tekrarlanan, otomatikleştirilmiş süreçler oluşturur. Güvenlik açığı taraması, günlük analizi, bilet (ticket) kontrolü ve denetim yetenekleri gibi daha önce analistler tarafından gerçekleştirilen görevler, SOAR platformları tarafından standartlaştırılabilir ve otomatik olarak yürütülebilir. Analistlerin iç görülerini deşifre etmek ve uyarlamak için yapay zekâ (AI) ve makine öğrenimini kullanan SOAR otomasyonu, önerilerde bulunabilir ve gelecekteki yanıtları otomatikleştirebilir.

Alternatif olarak, insan müdahalesi gerekiyorsa otomasyon tedbirleri artırılabilir.

4.3.3. Güvenlik Yanıtı

Güvenlik yanıtı, bir tehdit algılandığında gerçekleştirilen eylemlerin planlanması, yönetilmesi, izlenmesi ve raporlanması konusunda analistler için tek bir görünüm sunar. Ayrıca vaka yönetimi, raporlama ve tehdit istihbaratı paylaşımı gibi olay sonrası müdahale faaliyetlerini de içerir. Bunlar [55]:

1. SOAR'ın Elemanları
2. SOAR'ın Faydaları
3. SOAR platformları, kurumsal güvenlik operasyonları (SecOps) ekipleri için aşağıdakiler dahil birçok avantaj sunmaktadır.

Daha hızlı olay algılama ve tepki süreleri: Güvenlik tehditlerinin ve olaylarının hacmi ve hızı sürekli artmaktadır. SOAR'ın geliştirilmiş veri bağlamı, otomasyonla birleştiğinde, daha düşük ortalama algılama süresi (MTTD) ve ortalama yanıt verme süresi (MTTR) getirilebilir. Tehditlere daha hızlı tespit edip yanıt vererek etkileri azaltılabilir.
Daha iyi tehdit bağlamı: SOAR platformları, daha geniş bir araç ve sistem dizisinden daha fazla veriyi entegre ederek daha fazla bağlam, daha iyi analiz ve güncel tehdit bilgileri sunabilir.

Basitleştirilmiş yönetim: SOAR platformları, çeşitli güvenlik sistemlerinin panolarını tek bir arayüzde birleştirir. Bu, bilgi ve veri işlemeyi merkezileştirerek, yönetimi basitleştirerek ve zamandan tasarruf ederek SecOps'a ve diğer ekiplere yardımcı olur [56].

Ölçeklenebilirlik: Zaman alıcı manuel süreçleri ölçeklendirmek, çalışanlar için bir yük olabilir ve hatta güvenlik olayı hacmi arttıkça yetişmek imkânsız olabilir. SOAR'ın düzenleme, otomasyon ve iş akışları, ölçeklenebilirlik taleplerini daha kolay karşılayabilir. Alt düzey tehditleri otomatikleştirmek, SecOps ve güvenlik operasyonları merkezi (SOC) ekiplerinin sorumluluklarını arttırarak, görevleri daha

etkin bir şekilde önceliklendirmelerine ve insan müdahalesi gerektiren tehditlere daha hızlı yanıt vermelerine olanak tanır [55].

İşlemleri kolaylaştırma: Alt düzey görevleri otomatikleştiren standartlaştırılmış prosedürler ve çalışma kitapları (playbooklar) SecOps ekiplerinin aynı zaman diliminde daha fazla tehdide yanıt vermesini sağlar. Bu otomatikleştirilmiş iş akışları, aynı standartlaştırılmış iyileştirme çabalarının kuruluşun tüm sistemlerinde uygulanmasını da sağlar.

Raporlama ve iş birliği: SOAR platformlarının raporlaması ve analizi, bilgileri hızlı bir şekilde birleştirir, daha iyi veri yönetimi süreçleri ve daha etkili güvenlik için mevcut güvenlik politikalarını ve programlarını güncellemek için daha iyi yanıt çabalarını mümkün kılar. Bir SOAR platformunun merkezileştirilmiş kontrol paneli, farklı kurumsal ekipler arasında bilgi paylaşımını da geliştirerek iletişimi ve iş birliğini geliştirebilir.

Düşük maliyetler: Birçok durumda, güvenlik analistlerini SOAR araçlarıyla artırmak, tüm tehdit analizi, algılama ve müdahale çabalarını manuel olarak gerçekleştirmenin aksine maliyetleri azaltabilir [56].

4.3.4. SOAR Zorlukları

SOAR ne gümüş bir kurşun teknolojisidir ne de bağımsız bir sistemdir. SOAR platformları, özellikle tehditleri başarılı bir şekilde tespit etmek için diğer güvenlik sistemlerinin girdisini gerektirdiğinden, derinlemesine savunma güvenlik stratejisinin bir parçası olması gerekmektedir. SOAR, diğer güvenlik araçlarının yerine geçmez, tamamlayıcı bir teknolojidir. SOAR platformları ayrıca insan analistlerin yerini almaz, bunun yerine daha etkili olay tespiti ve müdahalesi için becerilerini ve iş akışlarını arttırmaktadır. SOAR'ın diğer bazı potansiyel dezavantajları şunları içerir [56]:

1. Daha geniş bir güvenlik stratejisini iyileştirmede başarısızlık;
2. Birleştirilmiş beklentiler;
3. Dağıtım ve yönetim karmaşıklığı, metriklerin olmaması veya sınırlı olması.

4. SOAR'ın faydalarını ve dezavantajlarını gösteren grafik
5. SOAR platformlarının faydalarının ve sınırlamalarının karşılaştırılması.

4.3.5. SOAR ve SIEM

SOAR ve SIEM platformlarının her ikisi de birden fazla kaynaktan veri toplarken, terimler birbirinin yerine kullanılamaz. SIEM sistemleri veri toplar, sapmaları belirler, tehditleri sıralar ve uyarılar oluşturur. SOAR sistemleri de bu görevleri yerine getirir, ancak ek yetenekleri vardır. İlk olarak, SOAR platformları hem güvenlik hem de güvenlik dışı olmak üzere daha geniş bir iç ve dış uygulama yelpazesiyle bütünleşir. İkincisi, SIEM sistemleri yalnızca güvenlik analistlerini potansiyel bir olay hakkında uyarırken, SOAR platformları bu tehditlere daha fazla bağlam ve otomatik yanıtlar sağlamak için otomasyon, yapay zekâ ve makine öğrenimi kullanır. Birçok şirket, şirket içi SIEM yazılımını artırmak için SOAR hizmetlerini kullanır. Gelecekte, SIEM satıcılarının hizmetlerine SOAR yetenekleri eklemeleri bekleniyor, bu da bu iki ürün hattının pazarının birleşeceği anlamına geliyor. Birçok SIEM satıcısı, SIEM ürünlerinde SOAR yetenekleri sunar. E-posta güvenlik ağ geçitleri, uç nokta algılama ve yanıt (EDR), ağ algılama ve yanıt (NDR) ve genişletilmiş algılama ve yanıt (XDR) gibi diğer ürünler de SOAR özelliklerini benimsemektedir [56].

4.4. UÇ NOKTA ALGILAMA VE YANIT

Uç nokta tehdit algılama ve yanıt ya da (ETDR) olarak da bilinen uç nokta algılama ve yanıt (End Point Detection and Response (EDR)), gerçek zamanlı sürekli izleme ve uç nokta verilerinin toplanmasını kurallara dayalı otomatik yanıt ve analiz yetenekleriyle birleştiren entegre bir uç nokta güvenlik çözümüdür. Terim, Gartner'dan Anton Chuvakin tarafından, güvenlik ekiplerinin tehditleri hızlı bir şekilde belirlemesini ve yanıt vermesini sağlamak için yüksek derecede otomasyon kullanarak, ana bilgisayarlar ve uç noktalardaki şüpheli etkinlikleri tespit eden ve araştıran yeni güvenlik sistemlerini tanımlamak için önerilmiştir. Bir EDR güvenlik sisteminin temel işlevleri şunlardır [57]:

1. Bir tehdidi gösterebilecek uç noktalardan etkinlik verilerini izler ve toplar

2. Tehdit kalıplarını belirlemek için bu verileri analiz eder
3. Tanımlanan tehditlere, bunları kaldırmak veya kontrol altına almak için otomatik olarak yanıt verir ve güvenlik personelini bilgilendirir
4. Tanımlanan tehditleri araştırmak ve şüpheli faaliyetleri aramak için adli bilişim ve analiz araçlarını kullanır.

4.5. AKTİF SAVUNMA ÇÖZÜMLERİ

4.5.1. Bal Küpü (Honeypot)

Siber saldırıları çekmek için kendini bir yem olarak feda eden bir bilgisayar sistemidir. Bilgisayar korsanları için sahte bir hedef oluşturmak ve siber suçluların nasıl çalıştıkları hakkında daha fazla bilgi edinmek veya onları diğer hedeflerden uzak tutmak için savunma girişimleri kullanılmaktadır [58].

4.5.2. Bal Küpleri Nasıl Çalışır?

Görünüşte siber suçluları kandırmak için meşru bir hedef olan bal küpü, uygulamalar ve verilerle gerçek bir bilgisayar sistemini andırmaktadır. Örneğin, kredi kartı numaralarını arayan suçlular, ortak hedef olan bir şirketin müşteri faturalandırma sistemini taklit edebilir. Hacklendikten sonra, bilgisayar korsanları izlenebilir ve gerçek ağın nasıl daha güvenli hale getirileceğine dair ipuçları için saldırganın davranışları değerlendirilebilir. Honeypot'lar, özellikle güvenlik açıkları oluşturarak saldırganlar için çekici hale getirilir. Örneğin, bir bal küpü, bağlantı noktası taramalarına veya zayıf parolalara yanıt veren bağlantı noktalarına sahip olabilir. Saldırganları daha güvenli canlı ağ yerine bir bal küpü ortamına çekmek için savunmasız bağlantı noktaları açık bırakılabilir. Bal küpleri, belirli bir sorunu çözmek için ayarlanmamıştır. Örneğin; bir güvenlik duvarı veya bir antivirüs programı gibi. Bunun yerine, kuruluşa yönelik mevcut tehditleri anlamaya ve ortaya çıktıklarında yeni tehditleri belirlemeye yardımcı olabilecek bilgilendirici bir araçtır. Bir bal küpünden alınan bilgilerle güvenliği sağlama çabalarına öncelik verilebilir ve odaklanılabilir [58].

4.5.3. Farklı Bal Küpü Türleri ve Bunların Çalışma Şekilleri

Farklı türdeki tehditleri tespit etmek için farklı türde bal küpleri kullanılabilir. Honeypot açıklamaları, hedefledikleri tehdit türlerine dayalıdır. Hepsinin kapsamlı ve etkili bir siber güvenlik stratejisinde yeri vardır.

E-posta tuzakları veya spam tuzakları, yalnızca otomatik adres toplayıcının bulabileceği gizli bir konuma sahte bir e-posta adresi yerleştirir. Bu adres spam tuzağı dışında herhangi bir amaçla kullanılmadığından, kendisine ulaşan her e-postanın spam olduğundan %100 emin olabilirsiniz. Spam tuzağına gönderilenlerle aynı içeriğe sahip tüm mesajlar otomatik olarak engellenebilir ve gönderenlerin kaynak IP'leri kara listeye alınabilir. Yazılım güvenlik açıklarını ve güvenli olmayan sistem mimarisinden yararlanan saldırıları veya SQL enjeksiyonu, SQL hizmetlerinden yararlanma veya ayrıcalıklardan yararlanma gibi saldırıları izlemek için sahte bir veri tabanı oluşturulabilir. Kötü amaçlı yazılım bal küpü, kötü amaçlı yazılım saldırılarını davet etmek için yazılım uygulamalarını ve API'leri taklit eder. Kötü amaçlı yazılımın özellikleri daha sonra kötü amaçlı yazılımdan koruma geliştirmek veya API'deki güvenlik açıklarını yamalamak için analiz edilebilir [58].

Spider Honeypot, yalnızca gezginlerin erişebildiği web sayfaları ve bağlantılar oluşturarak web tarayıcılarını (örümcekler) yakalamak için tasarlanmıştır. Tarayıcıları tespit ederek, reklam ağı tarayıcılarını ve kötü niyetli botları engellemeyi öğrenebilirsiniz. Bal küpü sistemine gelen trafiği izleyerek şunları değerlendirebilirsiniz [58]:

1. Siber suçluların nereden geldiğini
2. Tehdidin düzeyini
3. Hangi yöntemi kullandıklarını
4. Hangi veri ve uygulamalarla ilgilendiklerini
5. Güvenlik önlemlerinizin siber saldırıları durdurmak için ne kadar iyi çalıştığını.

Honeypot'un başka bir tanımı, yüksek veya düşük katılımlı bir bal küpü olmasına bağlıdır. Düşük etkileşimli bal küpleri daha az kaynak kullanır; seviye, tür ve tehdidin

nereden geldiği hakkında temel bilgileri toplar. Tipik olarak bazı simüle edilmiş temel TCP/IP protokolleri ve ağ hizmetleri ile kurulumu kolay ve hızlıdır. Ancak bal küpü saldırganı uzun süre meşgul edemez, bu nedenle alışkanlıkları veya karmaşık tehditleri hakkında derin bilgi edinemezsiniz. Yüksek etkileşimli bal küpleri ise hackerların bal küpünde olabildiğince fazla zaman geçirmelerini sağlayarak hackerların niyetleri ve hedefleri, açıkları ve yararlandıkları yöntemler hakkında çok fazla bilgi sağlamayı amaçlar. Veri tabanlarını, sistemleri ve süreçleri içeren bir bal küpü, başka bir deyişle saldırganı daha uzun süre meşgul edebilecek "yapıştırıcı" olarak düşünün. Bu, araştırmacıların, hassas bilgileri bulmak için saldırganların sistemde nereye gittiklerini, ayrıcalıkları yükseltmek için hangi araçları kullandıklarını veya sistem gizliliğini ihlal etmek için hangi güvenlik açıklarından yararlandıklarını izlemelerine olanak tanır [58].

4.5.4. Siber Güvenlikte Bal Küpleri Neden Kullanılır?

Yüksek etkileşimli bal küplerinin kurulumu ve takibi daha zor ve zaman alıcıdır. Ayrıca risk oluşturabilir; Bir "bal küpü güvenlik duvarı" ile güvence altına alınmadığı sürece, kararlı ve kurnaz bir bilgisayar korsanı, yüksek etkileşimli bal küpünü diğer internet sunucularına saldırmak veya güvenliği ihlal edilmiş bir bilgisayardan istenmeyen posta göndermek için kullanabilir [58].

Her iki bal küpünün de siber güvenlikte yeri vardır. Her ikisinin bir karışımını kullanabilir ve düşük etkileşimli bal küplerinden gelen tehdit türleriyle ilgili temel bilgileri daraltmak için yüksek etkileşimli bal küpünden amaç, iletişim ve açıklardan yararlanma hakkında bilgi ekleyebilirsiniz [58].

Bir kuruluş, bir tehdit istihbarat çerçevesi oluşturmak için siber bal küplerini kullanarak, siber güvenlik harcamalarını doğru yerlerde hizaladığından ve güvenlik açıklarının nerede olduğunu belirlediğinden emin olabilir [58].

4.5.5. Bal Küplerini Kullanmanın Avantajları

Honeypot'lar, büyük sistemlerdeki güvenlik açıklarını ortaya çıkarmanın iyi bir yolu olabilir. Örneğin, bir bal küpü, IoT cihazlarına yönelik yüksek bir saldırı tehdidini gösterebilir. Ayrıca güvenliğin nasıl iyileştirileceği konusunda tavsiyelerde bulunabilir. Bir bal küpü kullanmak, gerçek sistem izinsiz girişlerini tespit etme konusunda birçok avantaj sunar. Örneğin, doğası gereği, bir bal küpü meşru trafik almamalıdır, bu nedenle kaydedilen herhangi bir faaliyet büyük olasılıkla araştırma veya bilgisayar korsanlığı girişimleridir. Bu, bir ağ taraması gerçekleştirmek için kullanılan benzer IP adresleri (veya bir ülkeden IP adresleri) gibi kalıpları tespit etmeyi çok daha kolaylaştırır. Buna karşılık, çekirdek ağınızda yüksek düzeyde yasal trafiğe bakarsanız, bu tür saldırılara ilişkin herhangi bir işaret fark etmeyebilirsiniz. Honeypot güvenliğini kullanmanın en büyük yararı, yalnızca gördüğünüz adreslerin bu kötü amaçlı adresler olabilmesi ve saldırının tespit edilmesini çok daha kolay hale getirmesidir. Honeypot'lar, çok sınırlı trafikle başa çıktıkları için kaynak tüketimi açısından da düşüktür. Donanımdan büyük taleplerde bulunmazlar; Artık kullanmadığınız eski bilgisayarlarla bal küpü kurmanız mümkün.

Yazılıma gelince, çevrimiçi depolardan bir dizi hazır bal küpü mevcut olup, bir bal küpü çalıştırmanın dahili ek yükünü azaltır. Yüksek düzeyde yanlış alarm üretebilen geleneksel izinsiz giriş tespit sistemlerinin (IDS) aksine honeypot'ların yanlış pozitif üretme oranı düşüktür. Ayrıca, çabalara öncelik verilmesine ve bir bal küpünün kaynak gereksinimlerini düşük tutmaya yardımcı olur. Aslında, bal küpleri tarafından toplanan ve diğer sistem ve güvenlik duvarı günlükleriyle ilişkilendirilen verileri kullanarak, IDS, daha az yanlış pozitif oluşturmak için daha alakalı uyarılarla yapılandırılabilir. Bu şekilde, bal küpleri diğer siber güvenlik sistemlerinin geliştirilmesine ve iyileştirilmesine katkıda bulunabilir [58].

4.6. BULUT ERİŞİM GÜVENLİK ARACISI

Bulut erişim güvenlik aracısı veya cloud access security broker (CASB), kullanıcılar ve bulut hizmeti sağlayıcıları arasında aracı görevi gören bulutta barındırılan yazılım, şirket içi yazılım veya donanımdır. Bir CASB'ın güvenlikteki boşlukları ele alma

yeteneği, hizmet olarak yazılım (SaaS), hizmet olarak platform (PaaS) ve hizmet olarak altyapı (IaaS) ortamlarını kapsar. Bir CASB, görünürlük sağlamanın yanı sıra, kuruluşların güvenlik politikalarının erişimini mevcut şirket içi altyapılarından buluta genişletmesine ve buluta özel bağlam için yeni politikalar oluşturmasına da olanak tanır. CASB'ler, kurumsal güvenliğin hayati bir parçası haline gelmiştir ve işletmelerin hassas kurumsal verilerini korurken bulutu güvenli bir şekilde kullanmalarını da sağlamıştır. CASB, yönetilmeyen akıllı telefonlar, IoT cihazları veya kişisel dizüstü bilgisayarlar dahil olmak üzere, ne tür bir cihazın erişmeye çalıştığından bağımsız olarak, birden çok türde güvenlik politikası uygulamasını birleştirerek ve bunları işletmenizin bulutta kullandığı her şeye uygulayarak bir ilke uygulama merkezi olarak hizmet etmektedir [59].

BÖLÜM 5

YÖNTEM VE BULGULAR

5.1. YÖNTEM

Anket için nitel verilerden yararlanılmıştır ve makine öğrenmesi algoritmaları ile verim analizi yapılmıştır.

5.2. EVREN VE ÖRNEKLEM

Araştırmanın evreni olarak Türkiye seçilmiştir. Araştırma örneklemi Türkiye'de bulunan SOC analistlerinden oluşmaktadır. Likert ölçeği baz alınarak 1 – 10 puan aralığında değerlendirme yapılmıştır. Majid ve arkadaşlarının yaptığı siber güvenlik operasyon merkezinin başarılı bir şekilde geliştirilmesi ve uygulanması için model adlı çalışmada ve Chamkar ve arkadaşlarının yaptığı güvenlik operasyon merkezinde insan faktörü yetenekleri adlı çalışmada anket çalışması kullanılmıştır [63, 64]. Araştırmaya, 100 L1 analist, 50 L2 analist, 40 L3 analist olmak üzere toplam da 190 siber güvenlik analistinin bilgisine başvurulmuştur ve ölçeklere vermiş oldukları cevaplardan, veri datası oluşturulmuştur.

5.3. ARAŞTIRMA MODELİ VE HİPOTEZLERİ

İlgili alan yazın incelemesi sonucunda aşağıdaki hipotezler test edilmek üzere geliştirilmiştir.

H 1: Siber güvenlik analistlerinin (L1) verim arttırıcı yöntemlerinin belirlenmesinde, manuel olarak yapılan işlemlerin otomatize olarak yapılması anlamlı yönde etkilemektedir.

H 2: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, maaşın düşük olması olumsuz yönde etkilemektedir.

H 3: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, iş yükünün artması olumsuz yönde etkilemektedir.

H 4: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, belirlenen aksiyon alma süreleri (SLA süreleri) yeterlidir.

H 5: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, takım içerisindeki uyumsuzluk olumsuz yönde etkilemekte midir?

H 6: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, donanımın kaliteli olması ile verimlilik arasında anlamlı bir ilişki bulunmaktadır.

H 7: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, lisanslı threat intelligence (tehdit istihbaratı) ürünlerinin işveren kurum/kuruluş tarafından satın alınıp kullanılması olumlu yönde etkilemektedir.

H 8: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, takım liderleri veya yöneticilerle iletişim içerisinde olmak olumlu yönde etkilemekte midir?

H 9: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, sektörel eğitimlerin verilmesi olumlu yönde etkilemekte midir?

H 10: Siber güvenlik analistlerinin (L1) verim arttırıcı yöntemlerinin belirlenmesinde, False-Positive alarmlar (Yanlış alarm) izleme sürecini olumsuz yönde etkilemektedir.

H 11: Siber güvenlik analistlerinin (L1, L2, L3) verim arttırıcı yöntemlerinin belirlenmesinde, yöneticilerin, analistlerin isteklerini/fikirlerini dikkate almaları olumlu yönde etkilemektedir.

H 12: Siber güvenlik analistlerinin (L1) verim arttırıcı yöntemlerinin belirlenmesinde, SOAR ile izleme (monitoring) yapmak, SIEM ile izleme yapmaya göre olumlu yönde etkilemekte midir?

5.4. MAKİNE ÖĞRENMESİ İLE SOC ANALİSTLERİNİN VERİM ARTTIRICI YÖNTEMLERİNİN BELİRLENMESİ

5.4.1. Problem

Yapılan araştırmalara göre SOC analistlerinin stres ve iş yükü sebebiyle yaklaşık %70'inin tükenmişlik sendromu yaşadığı bilinmektedir. Bu da analistlerinin verimini önemli ölçüde düşürmektedir. Yapılan bu tez çalışmasında SOC analistlerinin verimini arttıran yöntemlerin belirlenmesi amaç edinilmiştir. Bu doğrultuda anket çalışmasından elde edilen sonuçlar veri setine özellik sütunu ile eklenerek eksik olan veriler sentetik veri ile çoğaltılarak makine öğrenmesi yöntemlerinden faydalanılmıştır.

5.4.2. Veri Kümesi Analizi

Bu tez çalışmasında, SOC alanında çalışan siber güvenlik uzmanlarının çeşitli özelliklerini içeren veri seti oluşturulmuştur. Oluşturulan veri seti bu çalışmaya özgün olarak hazırlanmıştır. Verinin elde edilmesinde, bu çalışma için hazırlanan anket sonuçlarına bakılarak özellik sütunları oluşturulmuştur. Bu veri seti ile, SOC analisti olarak çalışanların "verim" kaybının ana etkenlerini makine öğrenmesi algoritmaları kullanılarak tahminleme yapılmıştır. Veri seti özellikleri Şekil 5.1'de verilmiştir.

```
1  df.info()
```

```
0   Cinsiyet                                          1470 non-null   int64
1   Yaş                                               1470 non-null   int64
2   Eğitim Durumu                                     1470 non-null   int64
3   Tecrübe Yılı                                      1470 non-null   int64
4   Raporların Otomatize Yapılması                    1470 non-null   int64
5   Threat Intelligence Lisanslı Ürünlerinin Kullanımı 1470 non-null   int64
6   Maaş                                              1470 non-null   int64
7   İş Yükü                                           1470 non-null   int64
8   SLA Süresi                                        1470 non-null   int64
9   Ekip İçi Uyumluluk                                1470 non-null   int64
10  Donanım Kalitesi                                  1470 non-null   int64
11  Yöneticiler İle İlişki                            1470 non-null   int64
12  Kurum/Kuruluş İçi Eğitimler                       1470 non-null   int64
13  False-Positive Alarmlar                           1470 non-null   int64
14  Çalışma Şekli                                     1470 non-null   int64
15  Medeni Hali                                       1470 non-null   int64
16  Fazla Mesai                                       1470 non-null   int64
17  İşini Sevmesi                                     1470 non-null   int64
18  Verim                                             1470 non-null   int64
```

Şekil 5.1. Veri seti bilgisi.

Kullanılan veri seti cinsiyet, yaş, eğitim durumu, tecrübe yılı, raporların otomatize yapılması, threat intelligence lisanslı ürünlerin kullanımı, maaş, iş yükü, SLA süresi, ekip içi uyumluluk, donanım kalitesi, yöneticiler ile ilişki, kurum/kuruluş içi eğitimler, false-positive alarmlar, çalışma şekli, medeni hali, işini sevmesi ve verim şeklinde özellik sütunları bulunmaktadır. Oluşturulan veri seti nümerik (sayısal) değerler ile dağılımı yapılmıştır.

Veri kümesinde herhangi bir eksik veya hatalı veri değeri bulunmamaktadır ve tüm özellikler doğru veri türündedir. Burada olan "verim" sütunu output (çıktı) olarak verilerek Denetimli Makine Öğrenme Yöntemlerinden Random Forest, Lojistik regresyon, Karar Ağaçları, Destek Vektör Makineleri, En yakın Komşu (K-NN) ve XGBOOST algoritmaları kullanılarak başarım hesaplanması yapılmıştır. Elde edilen sonuçlar performans ölçüm metrikleri olan Recall (Kesinlik), Precision (Duyarlılık), Accuracy (Doğruluk) ve F1-score metrikleri ile sonuçlar üretilmiştir.

5.4.3. Verileri Eğitim ve Test Setlerine Bölme

Veri seti eğitim ve test setleri olarak parçalanmıştır. %80 eğitim işlemi için %20 test seti için ayrılmıştır. Yapılan işleme ilave olarak cross validation (çapraz doğrulama) ile veriyi verilen parametre sayısına göre parçalara bölerek, bir parçası test için, diğer kalan parçalar ise eğitim için ayrılmıştır. Bu işlemi cv değerine kadar tekrar ederek, verinin tamamı hem test hem de eğitim için kullanılmıştır.

5.4.4. Makine Öğrenmesi ile Model Oluşturma

Bu çalışmada kullanılan makine öğrenmesi algoritmaları aşağıda detaylı olarak verilmiştir.

5.4.4.1. Lojistik Regresyon

Lojistik regresyon, denetimli makine öğrenmesi algoritması çeşididir. İkili sınıflandırma şeklinde bir sorunu çözmek için kullanılmaktadır. Lojistik regresyon, matematiksel bir modeldir, matematiksel işlemler sayesinde çıktı vermektedir. İkili

sınıflandırmayı modelleme işlevi ve lojistik regresyon için fonksiyonlar kullanılmaktadır. Belirli bir verinin, bir sınıfa ait olma olasılığı regresyon modeli oluşturularak genellikle sigmoid fonksiyonu tercih edilir.

Lojistik regresyon birçok önemli noktaya sahiptir, Bunlar: uygulama kolaylığı, hesaplama verimliliği, eğitime dayalı verimlilik, düzenleme kolaylığı gibi. Giriş işlevleri, ölçeklendirme gerekmez. Bununla birlikte, çözme yeteneği doğrusal olmayan bir problemdir ve fazla uydurmaya (overfit) eğilimlidir [67].

5.4.4.2. Random Forest (Rasgele Orman)

Random forest, aynı zamanda olabilecek bir topluluk modelidir. En yakın komşu algoritmasının tahmin edicisinin bir başka formu olarak ortaya çıkmıştır. Ana fikir, topluluk yaklaşımlarıdır. Modeli güçlü bir model haline getirmeye çalışır. Random forest algoritmasına, üstte bir girdi girilir ve veriler paketlenerek ağaçtan geçerken daha küçük kümelere dönüşür. Random forest bunları birleştirerek, bu kavramı bir sonraki seviyeye getirir. Topluluk kavramına sahip ağaçlar buradan meydana gelmektedir. Random forest sınıflandırıcısının avantajı, alışma zamanlarından kıt, dengesiz ve eksik verilerle başa çıkabilmesidir [75, 76]. Random forest'ta, yeni veri seti veya test verileri, oluşturulan tüm alt ağaçlara dağıtılır. Ormandaki her karar alt ağacı, veri kümesinin sınıfına karar verebilir. Daha sonra model, çoğunluk oyu ile en uygun sınıfı seçer.

5.4.4.3. Destek Vektör Makineleri

Destek vektör makinesi (SVM) 1990'ların ortalarında ortaya çıkmıştır [66]. Makine öğreniminde, bir destek vektör makinesi (SVM, bir vektör ağını destekler), sınıflandırma ve regresyon analizi için kullanılan veri analizi ile ilgili öğrenme algoritmalarına sahip denetimli bir öğrenme modelidir. Her biri bir veya iki kategoriye ait olarak işaretlenmiş bir dizi eğitim örneği verildiğinde, SVM öğrenme algoritması, kategorilere göre yeni örnekler atayan bir model oluşturur [74]. Destek vektörü tarafından oluşturulan sınıflandırıcı makineler metodolojisi, giriş alanını normal nesnelerin bulunduğu ve tamamının bulunduğu sonlu bölge uzayının geri kalan

kısmında, anomalileri içerdiğini varsayarak işlem yapar [68].

5.4.4.4. Decision Tree (Karar Ağacı)

Decision tree algoritması hedefin değerini tahmin etmek için bir sınıflandırıcı oluşturarak, veriyi eğitim seti ve test verisi olarak ayırıp bilinen örnekler ile işlem yapmaktadır. Karar ağacının (DT) görevi sorular üzerinden ilerlemektir, verilen cevaba göre ağaç şekillenmektedir. Sorular aracılığıyla kararlar dizisi, görünmeyen bir test örneği karar ağacı tarafından sınıflandırılır [69]. Karar ağacı basitliği sebebiyle tek bir sınıflandırıcı olarak oldukça kullanılan ve daha kolay uygulaması yapılabilen algoritma olduğu için tercih edilmektedir [72].

5.4.4.5. En Yakın Komşu Algoritması (KNN)

K-nearest komşuda çeşitli mesafe ölçüm teknikleri kullanılmaktadır. K-en yakın komşu k parametresi bulunmaktadır. Bu parametre ile test örneğine en yakın olan eğitim verilerindeki örnekler ve daha sonra aralarında en sık görülen sınıf etiketine bakarak atama işlemi yapar. Sınıflandırmak için örneklerde, K-en yakın komşu bir yaklaşım olarak bilinir. Kolay ve parametrik olmayan [67], K-en yakın komşu algoritması tümevarımcı değil, örneğe dayalı öğrenen olarak bilinmektedir [73].

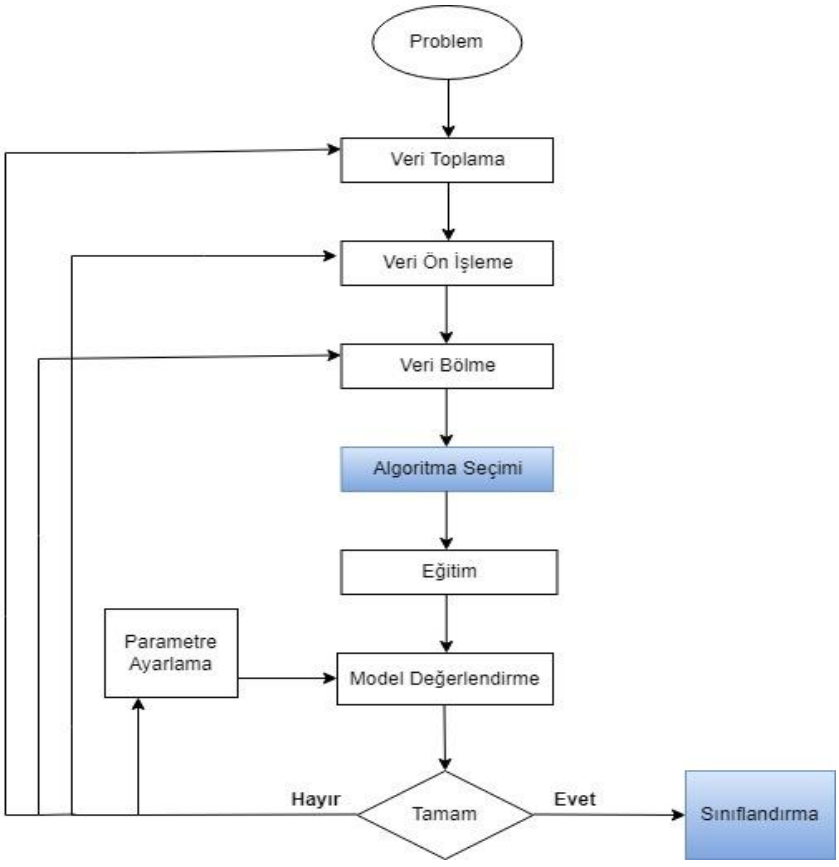
5.4.4.6. XGBOOST Algoritması

Chen ve Guestrin tarafından geliştirilen ölçeklenebilir bir ağaç güçlendirme sistemi olarak performanslı, gradyan karar ağaçlarına dayalı hızlı ve güçlü bir algoritmadır. XGBoost algoritmasında işlemler oldukça hızlı yapılır. Bunun sebebi olarak, karar ağaçları oluştururken paralel yürütme gerçekleştirmektedir. Algoritma çalışırken önce ağacın derinliğini max_depth parametresi ile belirler [70]. Ağaç aşağı akışta çok derinse geriye doğru temizleyerek işlemlerine devam eder. XGBoost algoritmasındaki max_depth, min_child_weight ve gama hiper parametrelerini optimize etmek karmaşıklığı azaltır. sub_sample ve comsample_bytree hiper parametrelerini optimize ederek oluşturulan modelin rastgeleliğini artırır. Bu sayede modelin verileri hatırlamasını engeller ve aşırı öğrenme sorununa çözüm bulur. Anahtar özelliklerinden

biri, verileri ağaçlara ayırırken doğru noktayı ayırmak için veri kümesindeki gözlem noktalarını, ağırlıklarına göre kullanmasıdır [71]. Veri setine göre tahminler yaparak genel minimum gereksinimlerle başarılı sonuçlar üretir.

5.4.5. Çalışmanın Akışı

Denetimli Makine Öğrenmesinin model akış şeması Şekil 5.2'de verilmiştir. Bu adımlar izlenerek çalışma tamamlanmıştır. Anketten elde edilen verilerin sonuçları göz önünde bulundurularak özgün veri seti elde edilmiştir. Anketle elde edilen sonuçlar göz önünde bulundurularak özgün bir veri seti oluşturulmuştur. Veri ön işleme yapılarak, verinin daha kullanılabilir, doğru ve mantıklı hale getirilmesi sağlanmıştır. Veri bölme işlemi yapılarak test ve eğitim verileri ayrılmıştır. Kullanılacak algoritmalar hakkında bilgi toplanarak model oluşturulmuştur. Oluşturulan modellerin performansları değerlendirilerek işleme alınmıştır. Performansı düşük olan modellerde parametre ayarları değiştirilerek yüksek başarım elde edilmiştir.



Şekil 5.2. Denetimli makine öğrenmesinin süreçleri.

5.5. BULGULAR

Demografik bulgular, hipotez bulguları ve ML algoritmaları ve elde edilen sonuçlar yer almaktadır.

5.5.1. Demografik Bulgular

Çizelge 5.1'de araştırmamıza katılım sağlayan kişilerin, betimsel istatiksel dağılımları verilmiştir. Araştırma kapsamında örneklemin 157'si erkek, 33'ü kadın katılımcılardan oluştuğu tespit edilmiştir. Araştırmamıza katılım sağlayan katılımcıların unvanına göre dağılımlarına baktığımızda; L1 analisti 100 kişi, L2 analist 50 kişi ve L3 analist 40 kişi olduğu görülmektedir. Araştırmamıza katılım sağlayan İlköğretim öğrenci sayısı 3 kişi, Lise 8, Ön lisans 17, Lisans 144, Yüksek Lisans 14 ve Doktora 4 kişidir. İş tecrübesine göre araştırmaya katılım sağlayanların dağılımına baktığımızda 0-2 yıl 37, 3-5 yıl 134, 5-7 yıl 12, 7-10 yıl 5 ve 10 yıl üzeri 2 kişi katılım sağlamıştır. Yaşa göre 18-25 arası 67 kişi, 26-32 arası 76 kişi, 33-42 44 kişi ve 43 ve üzeri 3 kişi olduğu görülmektedir.

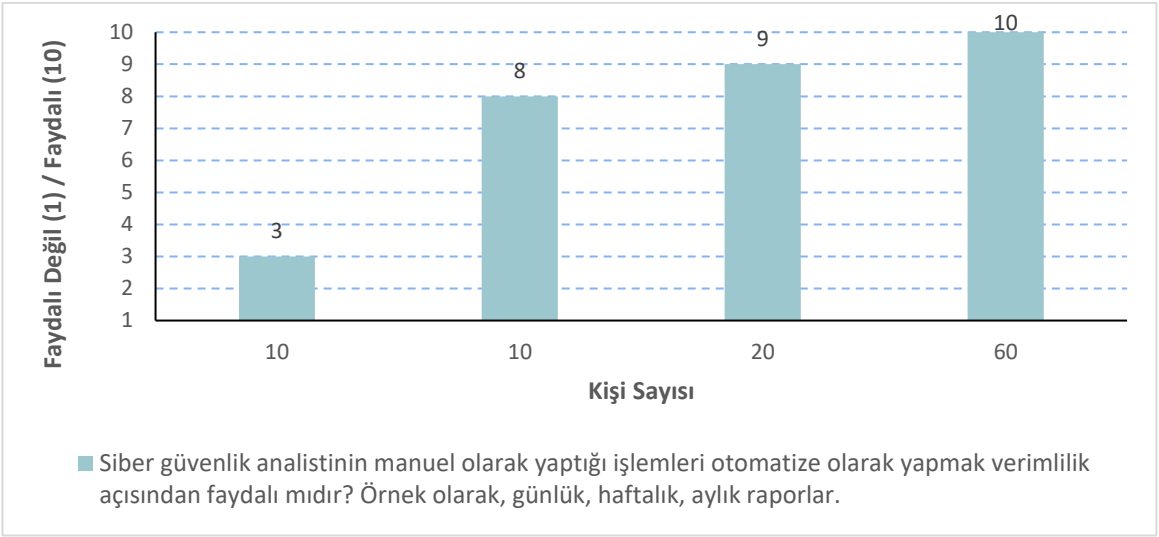
Çizelge 5.1. Demografik bulgular tablosu.

Özellikler		**Sayı**
Cinsiyet	Erkek	157
	Kadın	33
	Toplam	190
Unvanınız	L 1 Analist	100
	L 2 Analist	50
	L 3 Analist	40
	Toplam	190
Eğitim Durumu	İlköğretim	3
	Lise	8

	Ön lisans	17
	Lisans	144
	Yüksek Lisans	14
	Doktora	4
	Toplam	190
İş Tecrübesi	0-2 Yıl	37
	3-5 Yıl	134
	5-7 Yıl	12
	7-10 Yıl	5
	10 Yıl ve Üzeri	2
	Toplam	190
Yaş	18-25	67
	26-32	76
	33-42	44
	43 ve Üzeri	3
	Toplam	190

5.5.2 . Hipotez Bulguları

Hipotez bulguları aşağıda detaylı olarak verilmiştir.



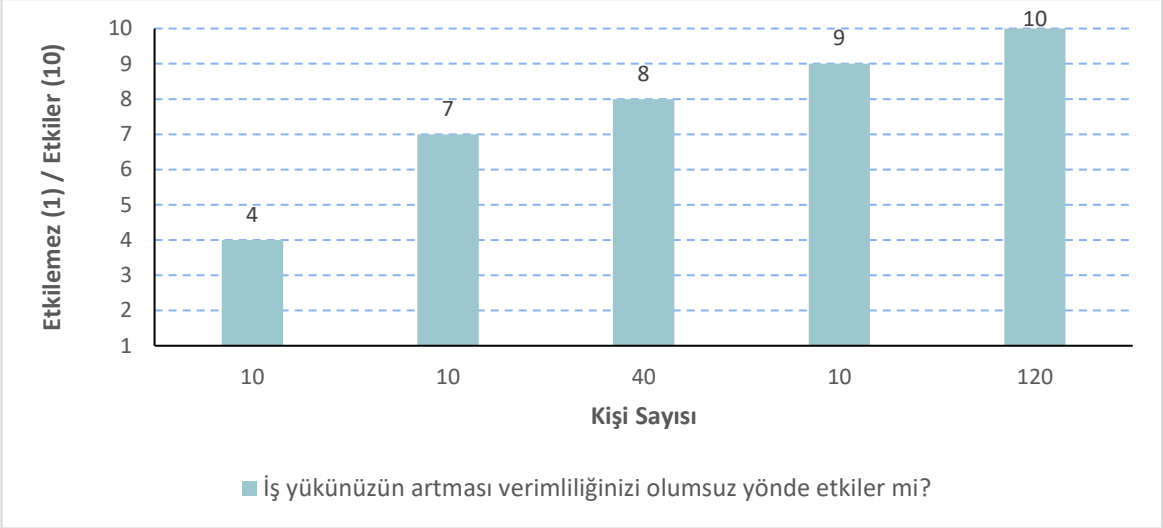
Şekil 5.3. Hipotez 1 grafiği.

100 L1 siber güvenlik analistinin katıldığı bu ankette, 10 kişinin 3/10 seviyesinde, 10 kişinin 8/10 seviyesinde, 20 kişinin 9/10 seviyesinde, 60 kişinin 10/10 seviyesinde cevapları Şekil 5.3'te verilmiştir. Ortalama olarak 8.9/10 oranında faydalı olarak tespit edilmiştir. Bu sonuçlara göre manuel olarak yapılan işlemlerin otomatize olarak yapılması verimlilik açısından %89 oranında anlamlı yönde etkilemektedir.

Şekil 5.4. Hipotez 2 grafiği.

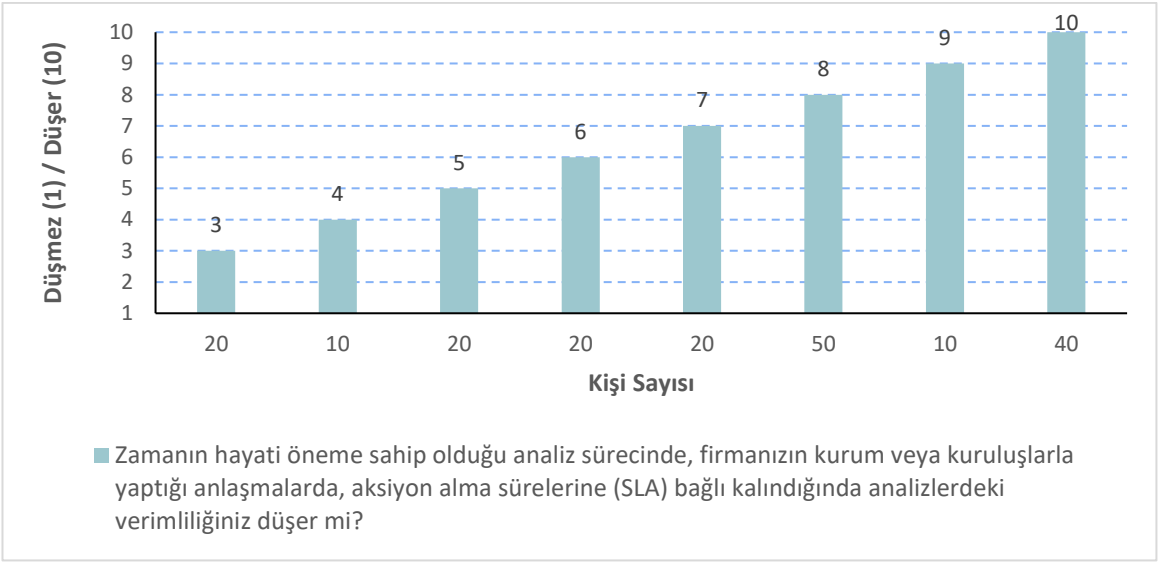
100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber

güvenlik analistinin katıldığı bu ankette, 10 kişinin 7/10 seviyesinde, 20 kişinin 9/10 seviyesinde, 160 kişinin 10/10 seviyesinde cevapları Şekil 5.4'te verilmiştir. Ortalama olarak 9.7/10 oranında etkilediği tespit edilmiştir. Bu sonuçlara göre maaş skalasının piyasanın altında olması verimlilik açısından %97 oranında olumsuz yönde etkilemektedir.



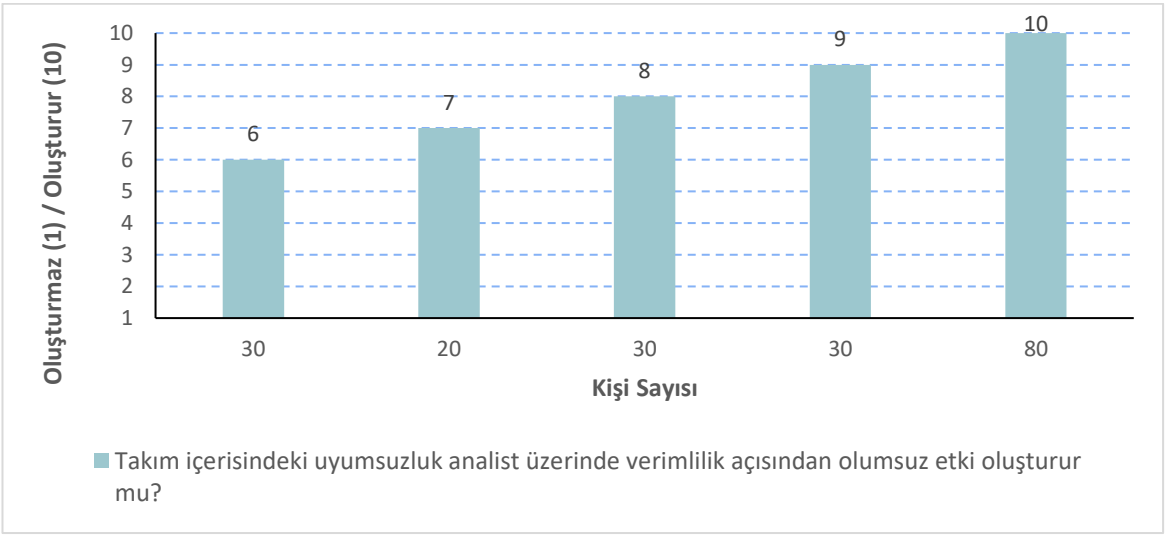
Şekil 5.5. Hipotez 3 grafiği.

100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber güvenlik analistinin katıldığı bu ankette, 10 kişinin 4/10 seviyesinde, 10 kişinin 7/10 seviyesinde, 40 kişinin 8/10 seviyesinde, 10 kişinin 9/10 seviyesinde, 120 kişinin 10/10 seviyesinde cevapları Şekil 5.5'te verilmiştir. Ortalama olarak 9.1/10 oranında etkilediği tespit edilmiştir. Bu sonuçlara göre iş yükünün artması verimlilik açısından %91 oranında olumsuz yönde etkilemektedir.



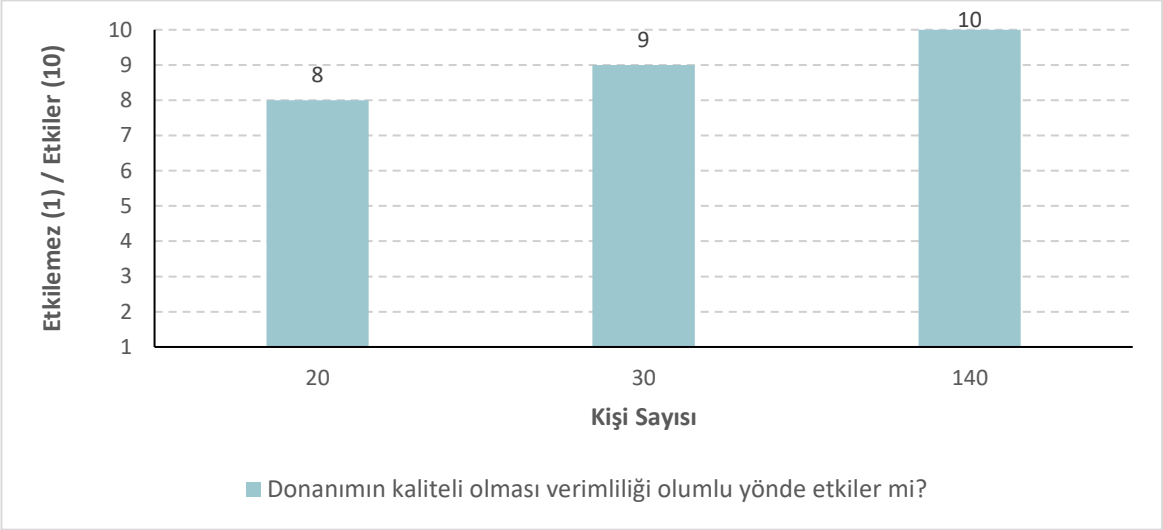
Şekil 5.6. Hipotez 4 grafiği.

100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber güvenlik analistinin katıldığı bu ankette, 20 kişinin 3/10 seviyesinde, 10 kişinin 4/10 seviyesinde, 20 kişinin 5/10 seviyesinde, 20 kişinin 6/10 seviyesinde, 20 kişinin 7/10 seviyesinde, 50 kişinin 8/10 seviyesinde, 10 kişinin 9/10 seviyesinde, 40 kişinin 10/10 seviyesinde cevapları Şekil 5.6'da verilmiştir. Ortalama olarak 7.1/10 oranında düşürdüğü tespit edilmiştir. Bu sonuçlara göre aksiyon alma sürelerine (SLA) bağlı kalınması, verimlilik açısından %71 oranında olumsuz yönde etkilemektedir.



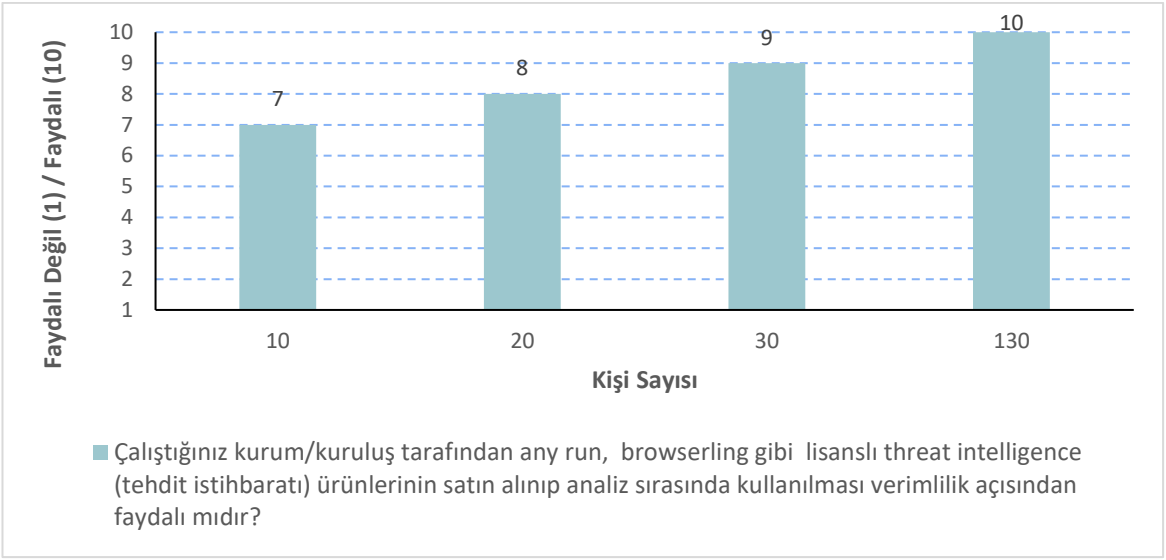
Şekil 5.7. Hipotez 5 grafiği.

100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber güvenlik analistinin katıldığı bu ankette, 30 kişinin 6/10 seviyesinde, 20 kişinin 7/10 seviyesinde, 30 kişinin 8/10 seviyesinde, 30 kişinin 9/10 seviyesinde, 80 kişinin 10/10 seviyesinde cevapları Şekil 5.7'de verilmiştir. Ortalama olarak 8.6/10 oranında etki oluşturduğu tespit edilmiştir. Bu sonuçlara göre takım içerisindeki uyumsuzluk, verimlilik açısından %86 oranında olumsuz yönde etkilemektedir.



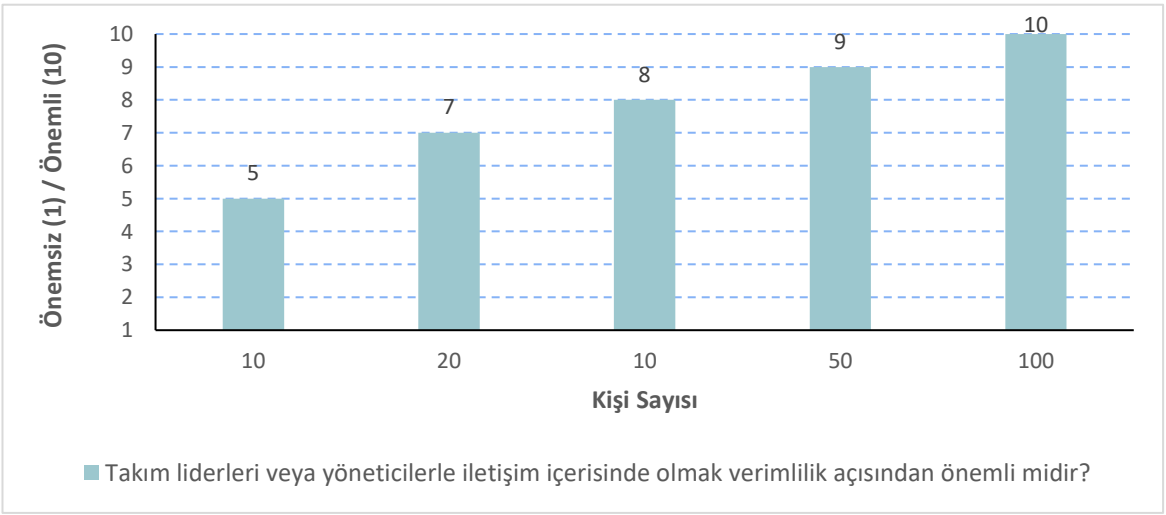
Şekil 5.8. Hipotez 6 grafiği.

100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber güvenlik analistinin katıldığı bu ankette, 20 kişinin 8/10 seviyesinde, 30 kişinin 9/10 seviyesinde, 140 kişinin 10/10 seviyesinde cevapları Şekil 5.8'de verilmiştir. Ortalama olarak 9.6/10 oranında etkilediği tespit edilmiştir. %96 olarak çıkan bu sonuca göre, donanımın kaliteli olması ile verimlilik arasında anlamlı bir ilişki bulunmaktadır.



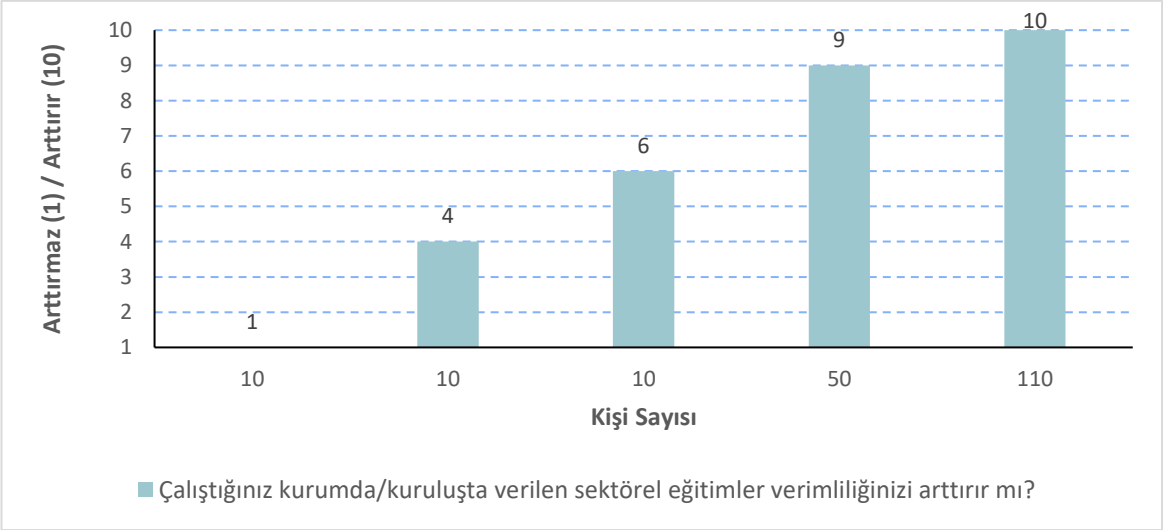
Şekil 5.9. Hipotez 7 grafiği.

100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber güvenlik analistinin katıldığı bu ankette, 10 kişinin 7/10 seviyesinde, 20 kişinin 8/10 seviyesinde, 30 kişinin 9/10 seviyesinde, 130 kişinin 10/10 seviyesinde cevapları Şekil 5.9'da verilmiştir. Ortalama olarak 9.5/10 oranında faydalı olduğu tespit edilmiştir. Bu sonuçlara göre lisanslı threat intelligence (tehdit istihbaratı) ürünlerinin işveren kurum/kuruluş tarafından satın alınıp kullanılması verimlilik açısından %95 oranında olumlu yönde etkilemektedir. Bu doğrultuda H 7 hipotezinin doğru olduğu sonucuna varılmıştır.



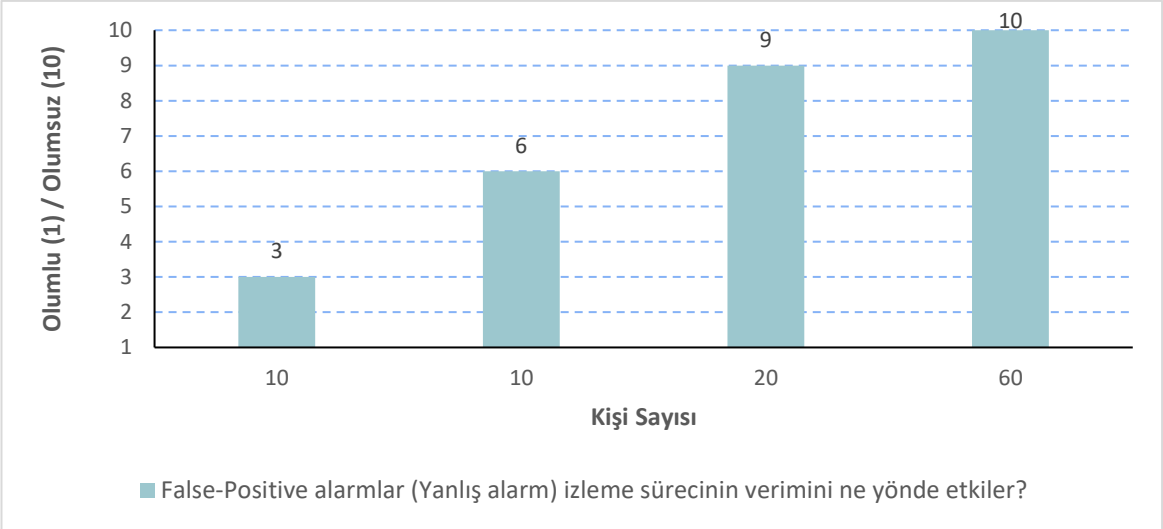
Şekil 5.10. Hipotez 8 grafiği.

100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber güvenlik analistinin katıldığı bu ankette, 10 kişinin 5/10 seviyesinde, 20 kişinin 7/10 seviyesinde, 10 kişinin 8/10 seviyesinde, 50 kişinin 9/10 seviyesinde, 100 kişinin 10/10 seviyesinde cevapları Şekil 5.10'da verilmiştir. Ortalama olarak 9.1/10 oranında önemli olduğu tespit edilmiştir. Bu sonuçlara göre takım liderleri veya yöneticilerle iletişim içerisinde olmak verimlilik açısından %91 oranında olumlu yönde etkilemektedir.



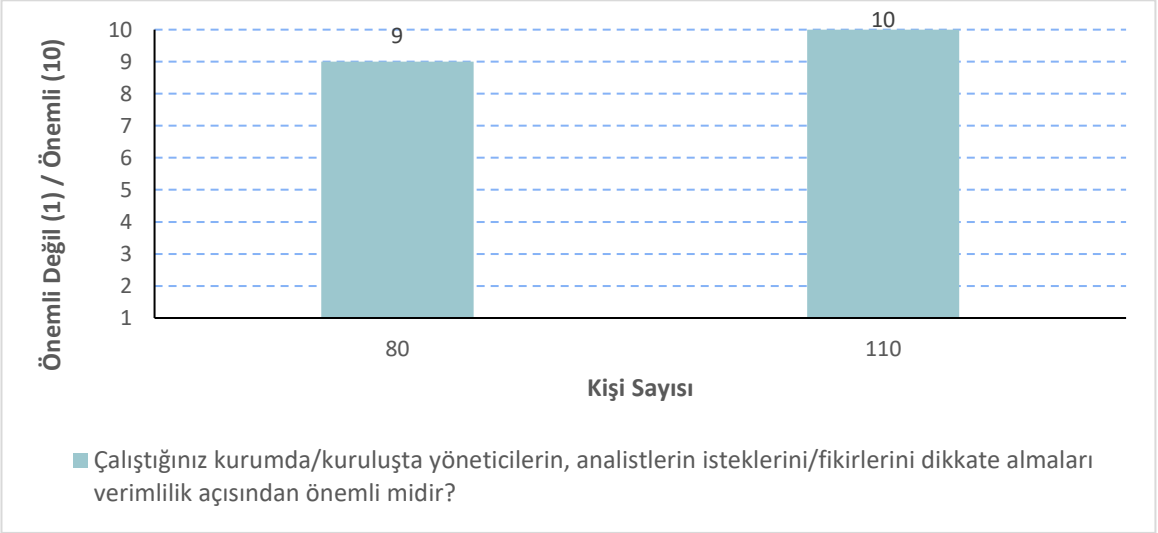
Şekil 5.11. Hipotez 9 grafiği.

100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber güvenlik analistinin katıldığı bu ankette, 10 kişinin 1/10 seviyesinde, 10 kişinin 4/10 seviyesinde, 10 kişinin 6/10 seviyesinde, 50 kişinin 9/10 seviyesinde, 110 kişinin 10/10 seviyesinde cevapları Şekil 5.11'de verilmiştir. Ortalama olarak 8.7/10 oranında önemli olduğu tespit edilmiştir. Bu sonuçlara göre takım liderleri veya yöneticilerle iletişim içerisinde olmak verimlilik açısından %87 oranında olumlu yönde etkilemektedir.



Şekil 5.12. Hipotez 10 grafiği.

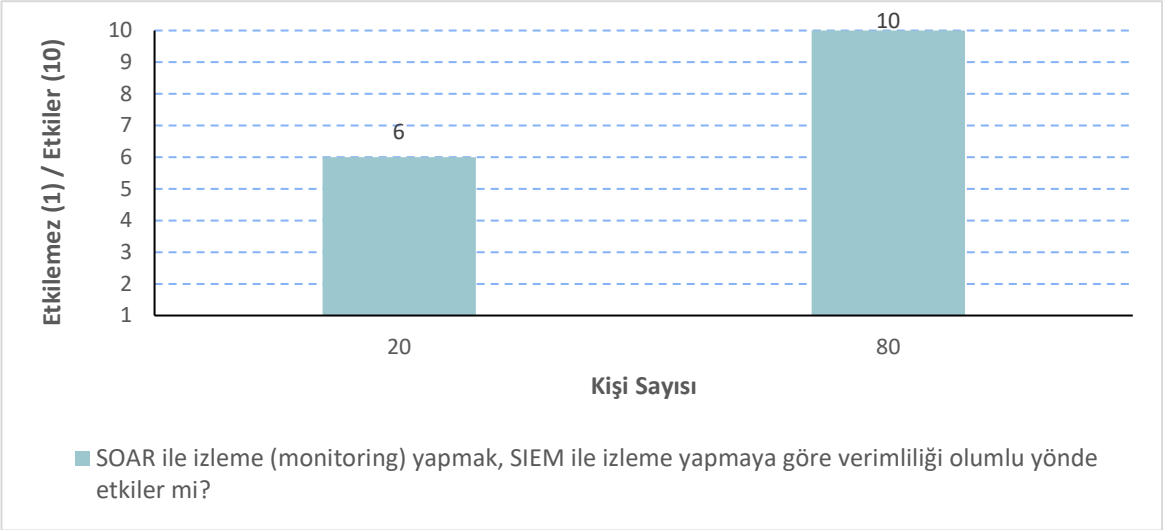
100 L1 siber güvenlik analistinin katıldığı bu ankette, 10 kişinin 3/10 seviyesinde, 10 kişinin 6/10 seviyesinde, 20 kişinin 9/10 seviyesinde, 60 kişinin 10/10 seviyesinde cevapları Şekil 5.12'de verilmiştir. Ortalama olarak 8.7/10 oranında olumsuz olarak tespit edilmiştir. Bu sonuçlara göre False-Positive alarmlar (Yanlış alarm) verimlilik açısından %87 oranında olumsuz yönde etkilemektedir.



Şekil 5.13. Hipotez 11 grafiği.

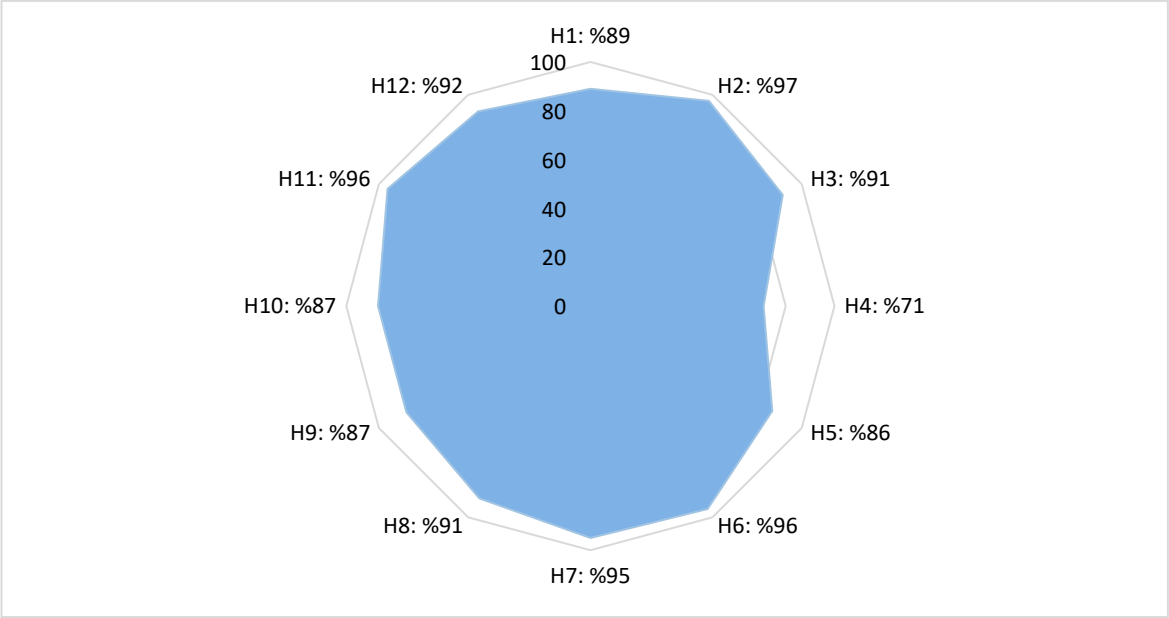
100 L1 siber güvenlik analistinin, 50 L2 siber güvenlik analistinin, 40 L3 siber

güvenlik analistinin katıldığı bu ankette, 80 kişinin 9/10 seviyesinde, 110 kişinin 10/10 seviyesinde cevapları Şekil 5.13'te verilmiştir. Ortalama olarak 9.6/10 oranında önemli olduğu tespit edilmiştir. Bu sonuçlara göre yöneticilerin, analistlerin isteklerini/fikirlerini dikkate almaları verimlilik açısından %96 oranında olumlu yönde etkilemektedir.



Şekil 5.14. Hipotez 12 grafiği.

100 L1 siber güvenlik analistinin katıldığı bu ankette, 10 kişinin 6/10 seviyesinde, 90 kişinin 10/10 seviyesinde cevapları Şekil 5.14'te verilmiştir. Ortalama olarak 9.2/10 oranında etkilediği tespit edilmiştir. Bu sonuçlara göre SOAR ile izleme (monitoring) yapmak, SIEM ile izleme yapmaya göre verimlilik açısından %92 oranında olumlu yönde etkilemektedir. Şekil 5.15'te de ankette belirtilen hipotezlerin yüzdesel oranları radar grafiği ile verilmiştir.



Şekil 5.15. SOC analistleri için oluşturulan hipotezlerin yüzdesel oranları.

5.5.3. Makine Öğrenmesi Algoritmaları ve Elde Edilen Sonuçlar

Bu bölümde ele alınan algoritmalar şunlardır: XGBOOST(eXtreme Gradient Boosting), Decision Tree, SVM(Support Vector Machine), Random Forest ve Logistic Regression.

Çizelge 5.2. Kullanılan ML algoritmaları ve elde edilen sonuçlar.

Algoritma	**Precision(Kesinlik)**	**Recall(Duyarlılık)**	**Accuracy(Doğruluk)**	**F1-Score**
XGBOOST	**0.90**	**0.92**	**0.99**	**0.98**
Decision Tree	0.87	0.98	0.95	0.92
KNN	0.89	0.86	0.92	0.90
SVM	0.75	0.90	0.87	0.82
Random Forest	0.68	0.78	0.71	0.81
Logistic Regression	0.68	0.75	0.70	0.81

BÖLÜM 6

SONUÇLAR

SOC merkezleri, siber güvenlik olaylarının tespit edilmesi, analiz edilmesi için ve bu olaylara (saldırılara) karşılık aksiyon verebilmek için kurulmuştur. İnternet korsanlarının her gün artış göstermesi ve daha bilgili hale gelmesiyle beraber, şirketlerin güvenlik açıklarını yakalamaları ve hemen hemen her firmanın bu tip tehditlerin altında kalması, kaçınılmaz bir hal almıştır. Siber saldırılar ile beraber hem maddi kayıplar hem de bilgi kayıpları yaşanmaktadır.

Siber güvenlik, dünya genelinde can, mal ve milyar dolarlık maddi krizlere sebep olmuş bir sektördür. Bu da aslında saldırganların bu konuda ne kadar kararlı olduklarının bir göstergesidir. Bu sebeple Siber Güvenlik Operasyonları Merkezi'nin (SOC) geliştirilmesi ve uygulanması zorunlu hale gelmiştir. SOC, bir kurum, kuruluş veya siber uzayda korunmaya ihtiyacı olan her şey için, yapılacak olan kötü niyetli aktiviteleri izlemek, tespit etmek, analiz etmek ve bu kötü niyetli saldırılara karşı koruma görevini yerine getiren merkezi bir yönetim birimidir.

Siber saldırıların önceden analiz edilmesiyle birlikte, bunlara karşı koyabilmek için, önlemlerin alınmasına yönelik araştırma yapan ekipler SOC merkezlerinde çalışmaktadırlar.

Yapılan araştırmalara bakıldığında SOC' un başarılı bir şekilde geliştirilmesine ve yönetilmesine yön verecek uluslararası bir kılavuz veya standart bulunmamaktadır. Bu sebepten dolayı, bu çalışma da SOC' un başarılı bir şekilde yürütülmesini sağlayacak üç önemli faktör olan teknoloji, süreç ve insan yer almaktadır. Bu çalışmada insan faktörü olan siber güvenlik analistlerin performans göstergeleri verimlilik açısından ele alınacaktır. Bu analistler yoğun bir çalışma temposuna sahiptirler. SOC’ ta L1 (Level 1), L2 (Level 2) ve L3 (Level 3) olmak üzere üç seviye siber güvenlik analisti

bulunmaktadır. L1 güvenlik analistleri izlemeden sorumludur, 7x24 çalışma düzenine göre çalışmaktadırlar. Herhangi bir tehdidi insan faktörü açısından ilk gören kişidir. Olayı analiz eder, olayın kritik olduğuna karar verirse ve detaylı incelenmesi gerektiğini düşünürse, L2 analiste eskale eder. L2 analist ise, olayı biraz daha derinlemesine inceleyip kök nedeni tespit edemezse ya da kök nedeni tespit edip müdahale ihtiyacı duyarsa olayı L3 analiste eskale edecektir. L2 analist tarafından kök neden tespit edilemediği durumda L3 analiste eskale edilen olay, L3 analist tarafından bir analist gözüyle derinlemesine incelenerek kök neden tespiti yapılır. L3 analist, L2 analist tarafından kök neden tespiti yapılmış ve müdahale gerektiren bir olayda, olay müdahale sürecini başlatır.

Bu araştırmada SOC analistlerinin veriminin ölçülmesi ve verim arttırıcı yöntemlerin belirlenmesi amaç edinilmiştir ve bu doğrultuda uzman görüşü almak için anket çalışması yapılmıştır. Yapılan anket çalışmasından elde edilen bilgiler ile özgün bir veri seti oluşturulmuştur. Bu veri seti, XGBOOST, Decision Tree, SVM, Random Forest ve Logistic Regression makine öğrenmesi algoritmaları kullanılarak, SOC analistlerinin verimine etki eden özelliklere göre, verimlilik yönünden değerlendirilmiş bir tahminleme modeli kurulmuştur. Kullanılan algoritmalarda başarım olarak XGBoost Algoritması en iyi performans göstererek 0.90 Precision, 0.92 Recall, 0.99 Accuracy ve 0.98 F1-Score elde edilmiştir.

Siber güvenlik analistlerinin iyi bir teknolojiye/donanıma sahip olması, iş yükünün dengeli olması, sektör ile ilgili gerekli eğitimlerin verilmesi, maddi olanaklarının sektör piyasasına göre iyi bir seviyede olması, SOC izleme ürünlerinin ve kurallarının olgun yapıda olması, alarmların az olması (False-positive (Yanlış alarm)) verimlilik açısından önemli unsurlardır. Analistlerin, analiz sırasında kullanabileceği lisanslı uygulamaların sağlanması da verimliliği arttıran etmenlerdendir. Analistlerin üst yönetim ile olan ilişkileri ve üst yönetimin analistlerin fikrine önem vermesi, analistlerin kendi ekip arkadaşlarıyla olan uyumlulukları da verimlilik açısından önemli etmenlerdendir. L1 analistler için raporların (günlük / haftalık / aylık) otomatize hazırlanması verimlilik açısından önemlidir. Siber güvenlikte, zaman çok önemli bir etmen olduğundan, kuruluşlar arasındaki hizmet seviyesi sözleşmelerinde büyük önem arz etmektedir. Bu sözleşme de hizmet şartlarına göre, her seviye analistin

kendisi için belirlenen sürede olayı incelemeye başlaması gerekmektedir. Bu sebeple verimliliği arttıran unsurlar, zaman yönetimi açısından da analistlere katkıda bulunmaktadır.

KAYNAKLAR

1. Cavelty, M. D., "Cyber-security and threat politics, US efforts to ensure the information age", ***Routledge***, 192 (2008).

2. Peterson, D., "Offensive cyber weapons: construction, development, and employment", ***The Journal of Strategic Studies***, 36 (1): 120-124 (2013).

3. Alcaraz, C. and Zeadally, S., "Critical infrastructure protection: requirements and challenges for the 21st century", ***International Journal of Critical Infrastructure Protection***, 8, 53-66 (2015).

4. Alruwaili, F. F. and Gulliver, T. A., "SOCaaS: Security operations center as a service for cloud computing environments", ***International Journal of Cloud Computing and Services Science***, 3 (2): 87-96 (2014).

5. Palvi, A., Maqbool, Z., Grover, A., Pammi, V. S. C., Singh, S. and Dutt, V., "Cyber security: A game-theoretic analysis of defender and attacker strategies in defacing-website games", ***2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)***, London, 1-8 (2015).

6. EY, "Security operations centres against cybercrime, top 10 considerations for success", ***EY's Global Information Security Survey***, (2013).

7. İnternet: UBM Tech. (2015), "Information Security Trends E-paper Report; Hewlett Packard Enterprise", **http://www.webcitation.org/query?url=https://www.hpe.com/h20195/V2/getpdf.aspx/4AA6-3636ENW.pdf&date=2017-07-09** (2016).

8. Eminağaoğlu, M., Uçar, E. ve Eren, Ş., "The positive outcomes of information security awareness training in companies- A case study", ***Information security technical report, Elsevier Advanced Technology Publications***, 14 (4): 223-229 (2009).

9. Moussa, B., Mostafa, M. and El-Khouly, M., "XML Schema-Based Minification for Communication of Security Information and Event Management (SIEM) Systems in Cloud Environments", ***(IJACSA) International Journal of Advanced Computer Science and Applications***, 5 (9): 74-82 (2014).

10. Suarez-Tangil, G., Palomar, E., Ribagorda, A. and Sanz, I., "Providing SIEM systems with self-adaptation", ***Information Fusion***, 21: 145–158 (2015).

11. Cerullo, G., Formicola, V., Iamiglio, P. and Sgaglione, L., "Critical Infrastructure Protection: Having SIEM Technology Cope With Network Heterogeneity", ***Arxiv Cornell University***, (2014).

12. Sarkar, K.R., "Assessing Insider Threats To Information Security Using Technical, Behavioural And Organisational Measures", ***Information Security Technical Report, Elsevier Advanced Technology Publications Oxford***, 15 (3): 112-133 (2010).

13. Elmrabit, N., Yang, S. and Yang, L., "Insider Threats in Information Security Categories and Approaches*"*, ***21st International Conference on Automation and Computing (ICAC)***, Glasgow UK, (2015).

14. İnternet: Medium, "SOC Nedir ? Bu Merkezde Neler Oluyor ?", **https://medium.com/hepsiburadatech/soc-nedir-bu-merkezde-neler-oluyor-4f8ff4167ea3** (2020).

15. Munshi, A., Dell, P. and Armstrong, H., "Insider Threat Behavior Factors: A comparison of theory with reported Incidents", ***45th Hawaii International Conference on System Sciences***, USA, 2402-2411 (2012).

16. Oliver, B., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E. and Ducheneaut, N., "Proactive Insider Threat Detection through Graph Learning and Psychological Context. In Security and Privacy Workshops (SPW)", ***2012 IEEE Symposium on San Francisco***, USA, 142-149 (2012).

17. Alkan M., Atalay, A. H., Bilirgen, C., vd., "Ulusal Siber Güvenlik Stratejisi", ***T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi Güvenliği Derneği,*** Türkiye (2012).

18. Henrie, M., "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment", ***Engineering Management Journal***, (25): 38-40 (2013).

19. Albayrak, A., "Bilgisayar ağlarında güvenlik politikaları ve bulut bilişim", Yüksek Lisans Tezi, ***Beykent Üniversitesi Sosyal Bilimler Enstitüsü***, (2015).

20. Bellovin, S. M., "The Insider Attack Problem Nature and Scope", ***Advances in Information Security***, Boston, 1-4 (2008).

21. Fung, C., "Collaborative Intrusion Detection Networks and Insider Attacks", ***Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications***, 2 (1): 63-74 (2011).

22. Çalı, H. H. ve Altunbaş, F., "Güvenlik Hizmetlerinde Yönetişim Aracı Olarak Sosyal Medya Platformları", ***Ekev Akademi Dergisi***, 50: 1-10 (2012).

23. Halchin, L.Elaine, “Electronic Government: Government Capability and Terrorist Resource”, ***Government Information Quarterly Dergisi***, 21: 406-419 (2004).

24. Mitnick, K. D., Simon, L. W. and Wozniak, S., “The Art of Deception: Controlling the Human Element of Security”, ***New York: Wiley Publishing***, (2003).

25. Anderson, R., Lum, B. and Walha, B., “Offense Vs Defense”, ***Washington: University of Washington***, (2005).

26. McGee, S., Sabett, R. V. and Shah, A., “Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense”, ***8 J. Bus. & Tech***, L 1 (2013).

27. Lachow, I., “Active Cyber Defense A Framework for Policymakers”, ***Center for a New American Security***, (2013).

28. Lu, W., Xu, S. and Yi, X., “Optimizing Active Cyber Defense. Decision and Game Theory for Security. ***4th International Conference, GameSe***, Fort Worth Texas USA**,** 206 - 225 (2013).

29. Pingree, L., MacDonald, N. and Firstbrook, P., “Best Practices for Mitigating Advanced Persistent Threats”, ***Gartner***, (2013).

30. Hutchins, E. M., Cloppert, M. J. and Amin, R. M., “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, ***Leading Issues in Information Warfare & Security Research***, (2011).

31. Al-Shaer, R., Spring, J. M. And Christou, E., “Learning the Associations of MITRE ATT&CK Adversarial Techniques”, ***Arxiv Cornell University***, (2020).

32. Internet: MITRE ATT&CK, “ATT&CK for Industrial Control Systems”, **https://collaborate.mitre.org/attackics/index.php/Main_Page** (2022).

33. Internet: Mandiant Fireeye, “Advanced Persistent Threats (APTs)”, **https://www.mandiant.com/resources/insights/apt-groups** (2021).

34. Internet: CISA, “Stuxnet Malware Mitigation (Update B)”, **https://www.cisa.gov/uscert/ics/advisories/ICSA-10-238-01B** (2014).

35. Hemsley, K. E. and Fisher, D. R. E., “History of Industrial Control System Cyber Incidents”, ***Idaho National Lab***, 37 (2018).

36. Shrivastava, S., “BlackEnergy -Malware for Cyber-Physical Attacks”, ***Itrust***, (2016).

37. Nelson, N., “The Impact of Dragonfly Malware on Industrial Control Systems”, ***SANS Inst. InfoSec Read. Room***, 1–25 (2016).

38. Internet: Youtube Digital Bond Labs, “Havex Deep Dive”, **https://www.youtube.com/watch?v=SyupAcnURtA** (2018).

39. İnternet: Siber Portal, “Bilgi Güvenliği Bakış Açısıyla Tehdit Modelleme”, **https://www.siberportal.org/white-team/governance/bilgi-guvenligi-bakis-acisiyla-tehdit-modelleme** (2020).

40. İnternet: Endüstri4.0, “Yapay Zeka, Makine Öğrenimi ve Derin Öğrenme Arasındaki Farklar”, **https://www.endustri40.com/yapay-zeka-makine-ogrenimi-ve-derin-ogrenme-arasindaki-farklar** (2021).

41. Halchin, L. E., “Electronic Government: Government Capability and Terrorist Resource”, ***Government Information Quarterly***, 21 (4): 406-419 (2004).

42. Henrie, M., “Cyber Security Risk Management in the SCADA Critical Infrastructure Environment”, ***Engineering Management Journal***, 25: 38-45 (2015).

43. Hodos, R. F., “Computerization Of Public Administration To E-government: Between Goal And Reality”, ***Juridical Current***, 59: 119-127 (2014).

44. Hub, M. and Capek, J., “Security Evaluation of Passwords Used on Internet”, ***Journal of Algorithms & Computational Technology***, 5 (3): 437-449 (2011).

45. Karakuş, B. A., “Derin öğrenme ve büyük veri yaklaşımları ile metin analizi”, Doktora Tezi, ***Fırat Üniversitesi Fen Bilimleri Enstitüsü***, Elazığ, (2018).

46. Patil, S., Jangra, A., Bhale, M., Raina A. and Kulkarni, P., "Ethical hacking: The need for cyber security", ***2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)***, Chennai, 1602-1606 (2017).

47. Jordan, T., “Hacking and power: Social and technological determinism in the digital age”, ***First Monday***, 14 (7): (2009).

48. Rounds, M. and Pendgraft, N., “Diversity in network attacker motivation: A literature review”, ***In 2009 International Conference on Computational Science and Engineering***, Vancouver, 319-323 (2009).

49. Kshetri, N., “The simple economics of cybercrimes”, ***IEEE Security & Privacy***, 4 (1): 33-39 (2006).

50. Yihunie, F., Abdelfattah E. and Odeh, A., "Analysis of ping of death DoS and DDoS attacks", ***2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)***, Farmingdale, 1-4 (2018).

51. İnternet: Vatansever Bilişim, "Güvenlik Bilgi ve Olay Yönetimi (SIEM) Çözümleri", **https://www.vatanseverbilisim.com/guvenlik-bilgi-ve-olay-yonetimi-siem-cozumleri**, Erişim Tarihi: 04.09.2021.

52. Internet: Rapid7, "User and Entity Behavior Analytics (UEBA)", **https://www.rapid7.com/fundamentals/user-behavior-analytics**, Erişim Tarihi: 20.10.2021.

53. Internet: Forcepoint, "Forcepoint Behavioral Analytics", **https://www.forcepoint.com/tr/product/ueba-user-entity-behavior-analytics**, Erişim Tarihi: 20.10.2021.

54. Karabatak, M. ve Mustafa, T., "Performance comparison of classifiers on reduced phishing website dataset", ***In 2018 6th International Symposium on Digital Forensic and Security (ISDFS)***, IEEE, 1-5, (2018).

55. Internet: Techtarget, "SOAR (security orchestration, automation and response)", **https://www.techtarget.com/searchsecurity/definition/SOAR** (2021).

56. Internet: Mcafee, "What Is Endpoint Detection and Response (EDR)?", **https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html,** Erişim Tarihi: 20.11.2021.

57. İnternet: Siber Eğitmen, "Honeypot (Bal Küpü Teknolojisi) Nedir?", **https://www.siberegitmen.com/bal-kupu-teknolojisi-nedir** (2021).

58. İnternet: Kaspersky, "Bal küpü (honeypot) nedir?", **https://www.kaspersky.com.tr/resource-center/threats/what-is-a-honeypot**, Erişim Tarihi: 10.03.2022.

59. Internet: Skyhigh Security, "What Is a CASB?", **https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-a-casb.html**, Erişim Tarihi: 15.04.2022.

60. İnternet:Beyaznet, "Soc Nedir ve Soc'da Hizmet Sürekliliği Nasıl Sağlanır?", **https://www.beyaz.net/tr/guvenlik/makaleler/soc_nedir_ve_soc_da_hizmet_surekligi_nasil_saglanir.html** (2019).

61. Avcı, İ., Özarpa, C., Kınacı, B. F., Koca, M., Yıldırım, M. ve Yıldırım, E. "Siber Ölüm Zinciri ve Saldırı Önleme Yöntemlerinin İncelenmesi", ***IX. International Advanced Technologies Symposium (IATS'21)***", Elazığ, 202-213 (2021).

62. Avcı, İ. ve Yıldırım, M. "Görme Engelli Bireyler İçin Derin Öğrenme Tabanlı Nesne Tanıma Modeli", ***Avrupa Bilim ve Teknoloji Dergisi***, (28): 220-227 (2021).

63. Chamkar, S. A., Maleh, Y. and Gherabi, N., "The Human Factor Capabilities in Security Operation Center (SOC)", ***EDPACS***, 66: 1-14 (2021).

64. Majid, M. A. and Ariffin, K. A. Z., "Model for successful development and implementation of Cyber Security Operations Centre (SOC)", ***PLOS ONE***, 16 (11): 1-24 (2021).

65. Avcı, İ., Koca, M., Yıldırım, E. ve Yıldırım, M., " COVID-19 Pozitif Vakaları Tahmin Etmek İçin Derin Öğrenme Yöntemleri ve Analizi", ***IX. International Advanced Technologies Symposium (IATS'21)***", Elazığ, 162-170 (2021).

66. Bernhard E. B., Guyon, I. M. and Vapnik, V. N., "A Training Algorithm for Optimal Margin Classiers", ***Proceedings of the 5th Annual ACM Workshop on Computational***, 144-152 (1992).

67. Jacob, J., Mathew, J. C., Mathew, J. and Issac, E., "Diagnosis of Liver Disease Using Machine Learning Techniques", ***International Research Journal of Engineering and Technology***, 5 (4): 4011 - 4014(2018).

68. Carlos A. C., Bromberg F. and Garino, C. G., "An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection", ***Expert Systems with Applications ELSEVIER***, 39 (2): 1822-1829 (2012).

69. Tsai, C. F., Hsu, Y. F., Lin, C. Y. and Lin, W. Y., "Intrusion detection by machine learning: A review", ***Expert Systems with Applications ELSEVIER***, 36 (10): 11994-12000 (2009).

70. Chen T. and Guestrin, C., "XGBoost: A Scalable Tree Boosting System", ***KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,*** 785–794 (2016).

71. İnternet: Veri Bilimi Okulu, "XGBoost Nasıl Çalışır? Neden İyi Performans Gösterir?", **https://www.veribilimiokulu.com/xgboost-nasil-calisir** (2020).

72. Farid, D. M., Zhang, L., Hossain, A., Rahman, C. M., Strachan, R., Sexton, G. and Dahal, K., "An Adaptive Ensemble Classifier for Mining Concept-Drifting Data Streams", ***Expert systems with Applications ELSEVIER***, 40 (15): 5895-5906 (2013).

73. Mitchell, T., "Machine learning", ***MacHraw Hill***, New York, (1997).

74. İnternet: Veri Bilimcisi, "Destek Vektör Makineleri (Support Vector Machine)", **https://veribilimcisi.com/2017/07/19/destek-vektor-makineleri-support-vector-machine**, Erişim Tarihi: 13.05.2022.

75. Lakshmi, S. V., Meena, M. K. and Kiruthika, N. S., "Diagnosis of Chronic Kidney Disease using Random Forest Algorithms", ***International Journal of Research in Engineering, Science and Management***, 2 (3): 559-562 (2019).

76. VijiyaKumar, K., Lavanya, B., Nirmala, I. and Caroline, S. S., “Random Forest Algorithm for the Prediction of Diabetes”, ***2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)***, Pondicherry, (2019).

EK AÇIKLAMALAR A.

KATILIMCI BİLGİ FORMU

Merhaba, Siber güvenlik analistlerinin verimini arttırıcı yöntemlerin belirlenmesi amaçlanan bu ankette, analistlerin gerçek problemlerinin ne olduğu ve bunları çözmeye yönelik etkenlerin belirlenmesi hedeflenmiştir. Siber güvenlik analisti değilseniz lütfen bu formu doldurmayınız. Kişisel bilgileriniz yüksek lisans tez çalışması haricinde kesinlikle üçüncü şahıslarla paylaşılmayacaktır. Katkılarınızdan dolayı teşekkür ederiz.

1-) Cinsiyet:

a. Kadın
b. Erkek

2-) Yaş

a. 18-25
b. 26-32
c. 33-42
d. 43 ve üzeri

3-) Eğitim Durumu

a. İlköğretim
b. Lise
c. Ön Lisans
d. Lisans
e. Yüksek Lisans
f. Doktora

4-) İş Tecrübesi

a. 0-2 Yıl
b. 3-5 Yıl
c. 5-10 Yıl
d. 10 Yıl ve üzeri

5-) Unvan

a. L 1 Analist
b. L 2 Analist
c. L 3 Analist

EK AÇIKLAMALAR B.

SİBER GÜVENLİK ANALİSTLERİNİN VERİM ARTTIRICI YÖNTEMLERİNİN BELİRLENMESİ ANKETİ

1-) Bir olayın analizi için ne kadar süre harcanır? *

a. 2 dakika
b. 5 dakika
c. 10 dakika
d. 10 dakikadan fazla

2-) Siber güvenlik analistinin manuel olarak yaptığı işlemleri otomatize olarak yapmak verimlilik açısından faydalı mıdır? Örnek olarak, günlük, haftalık, aylık raporlar.*

a. Faydalı Değil
b. Faydalı

3-) Çalıştığınız kurum/kuruluş tarafından any run, browserling gibi lisanslı threat intelligence (tehdit istihbaratı) ürünlerinin satın alınıp analiz sırasında kullanılması verimlilik açısından faydalı mıdır? *

a. Faydalı Değil
b. Faydalı

4-) SOAR ile izleme (monitoring) yapmak, SIEM izleme yapmaya göre verimliliği olumlu yönde etkiler mi? *

a. Etkilemez
b. Etkiler

5-) Alarmın geldiği süre ile, alarmı inceleme süresi arasındaki zaman, ortalama ne kadar olmalıdır?

a. 1 dakika
b. 3 dakika
c. 5 dakika

d. 5 dakikadan fazla

6-) Siber Güvenlik analistinin verimliliğini düşüren etkenlere örnek(ler) veriniz. *

a. False Positive oranı yüksek kurallar,
b. Gereğinden fazla iş yükü,
c. Çevre baskısı ve üs yönetimin yetersiz desteği,
d. Takdir görmeme.

7-) Siber güvenlik analistinin verimliliğini arttıracak etkenlere örnek(ler) veriniz. *

a. İş yükünün gerektiği kadar olması,
b. F/P oranı düşük kurallar,
c. Analiz için yeterli süre,
d. Üst yönetimin desteği ve takdiri.

8-) Psikolojik olarak siber güvenlik analistinin verimliliğini olumsuz etkileyen faktörlere örnek(ler) veriniz. *

a. Offense bildirimlerinde SLA sürelerinin kısa olması,
b. Ekip içindeki sorunlar,
c. destek alınamaması, bir hata sonucu oluşan durumda yalnız kalmak,
d. İş yükünün fazla olması,
e. Zaman problemi

9-) Psikolojik olarak siber güvenlik analistinin verimliliğini olumlu etkileyen faktörlere örnek(ler) veriniz. *

a. Üst yönetimin ve takım arkadaşlarının desteği,
b. yapılan eleştirilerin yapıcı olması,
c. Takdir edilme.
d. Hataların çözümü için açıklayıcı bilgi verilmesi.

10-) Maaş skalasının sektör piyasasının altında olması siber güvenlik analistinin verimliliğini olumsuz yönde etkiler mi? *

a. Etkilemez
b. Etkiler

11-) İş yükünüzün artması verimliliğinizi olumsuz yönde etkiler mi? *

a. Etkilemez
b. Etkiler

12-) Çalıştığınız firmanın SLA (Hizmet Seviyesi Anlaşması) süreleri (zaman açısından) iş yükünüze uygun mudur?

a. Uygun Değil
b. Uygun

13-) Zamanın hayati öneme sahip olduğu analiz sürecinde, firmanızın kurum veya kuruluşlarla yaptığı anlaşmalarda, aksiyon alma sürelerine (SLA) bağlı kalındığında analizlerdeki verimliliğiniz düşer mi? *

a. Düşmez
b. Düşer

14-) Takım içerisindeki uyumsuzluk analist üzerinde verimlilik açısından olumsuz etki oluşturur mu? *

a. Oluşturmaz
b. Oluşturur

15-) Donanımın kaliteli olması verimliliği olumlu yönde etkiler mi? *

a. Etkilemez
b. Etkiler

16-) Monitör sayısı verimlilik açısından önemli midir? *

a. Önemsiz
b. Önemli

17-) Takım liderleri veya yöneticilerle iletişim içerisinde olmak verimlilik açısından önemli midir? *

a. Önemsiz
b. Önemli

18-) Çalıştığınız kurumda/kuruluşta verilen sektörel eğitimler verimliliğinizi arttırır mı? *

a. Arttırmaz
b. Arttırır

19-) İş yükü/yoğunluğu kendinizi geliştirmede engel midir? *

a. Engel Değil
b. Engel

20-) False-Positive alarmlar izleme sürecinin verimini ne yönde etkiler? *

a. Olumsuz
b. Olumlu

21-) Çalıştığınız kurumda/kuruluşta yöneticilerin, analistlerin isteklerini/fikirlerini dikkate almaları verimlilik açısından önemli midir? *

a. Önemli Değildir
b. Önemlidir

22-) Alarm triyajının otomatize olması zaman kazanmak açısından faydalı mıdır? *

a. Faydalı Değil
b. Faydalı

ÖZGEÇMİŞ

Mehmet Yıldırım ilk, orta ve lise öğrenimini aynı yerde tamamladı. Türkan Ömer Okan Lisesi Fen Bilimleri Bölümü'nden mezun oldu. 2014 yılında Bilgisayar Mühendisliği Bölümü'nde öğrenime başlayıp 2019 yılında onur öğrencisi olarak mezun oldu. 2019 yılında Karabük Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans öğrenimine birincilikle yerleşti ve tamamladı. 2020 yılında özel bir siber güvenlik şirketinde siber güvenlik analisti olarak göreve başladı ve halen aynı şirkette tehdit tespit mühendisi (SIEM Danışmanı) olarak çalışmaya devam etmektedir.