T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Eyüp Can KILINÇDEMİR

GÜVENLİK OPERASYONU MERKEZLERİNDE OLAYLARIN ÖNCELİKLENDİRİLMESİ VE ANALİST ATAMASINA YÖNELİK ÇOK KRİTERLİ BİR KARAR DESTEK ÇERÇEVESİ

DANIŞMAN
Dr. Öğr. Üyesi Barış ÇELİKTAŞ

İSTANBUL, Temmuz 2025

T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Eyüp Can KILINÇDEMİR
(23SİBE5004)

GÜVENLİK OPERASYONU MERKEZLERİNDE OLAYLARIN ÖNCELİKLENDİRİLMESİ VE ANALİST ATAMASINA YÖNELİK ÇOK KRİTERLİ BİR KARAR DESTEK ÇERÇEVESİ

DANIŞMAN
Dr. Öğr. Üyesi Barış ÇELİKTAŞ

İSTANBUL, Temmuz 2025

T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Eyüp Can KILINÇDEMİR
(23SİBE5004)

GÜVENLİK OPERASYONU MERKEZLERİNDE OLAYLARIN ÖNCELİKLENDİRİLMESİ VE ANALİST ATAMASINA YÖNELİK ÇOK KRİTERLİ BİR KARAR DESTEK ÇERÇEVESİ

Tezin Savunulduğu Tarih: 01/07/2025

Tez Danışmanı: Dr. Öğr. Üyesi Barış ÇELİKTAŞ / Işık Üniversitesi

Diğer Jüri Üyeleri: Dr. Öğr. Üyesi Ahmet Feyzi ATEŞ / Işık Üniversitesi

Dr. Öğr. Üyesi Mehmet Tahir SANDIKKAYA / İstanbul Teknik Üniversitesi

İSTANBUL, Temmuz 2025

ÖZET

GÜVENLİK OPERASYONU MERKEZLERİNDE OLAYLARIN ÖNCELİKLENDİRİLMESİ VE ANALİST ATAMASINA YÖNELİK ÇOK KRİTERLİ BİR KARAR DESTEK ÇERÇEVESİ

Bu çalışmada, Güvenlik Operasyon Merkezleri (SOC) için olay atama ve önceliklendirme süreçlerine yönelik kapsamlı ve ölçeklenebilir bir çerçeve önerilmektedir. Önerilen model; analist iş yoğunluğu, alarm yoğunluğu ve tutarsız olay yönetimi gibi temel operasyonel zorlukları ele alarak SOC iş akışlarını optimize etmeyi amaçlamaktadır. Geliştirilen çerçeve, her bir olayı; şiddet seviyesi, SLA aciliyeti, olay türü, varlık kritiklik düzeyi, tehdit istihbaratı göstergeleri, tekrar sıklığı ve geçmiş olay verilerine dayalı korelasyon puanı gibi çok sayıda faktörü içeren çok kriterli bir puanlama modeli ile değerlendirmektedir. Bu değerlendirme süreci, dinamik olay puanlarını hesaplayan ve olayın karmaşıklık düzeyini belirleyen matematiksel fonksiyonlar aracılığıyla biçimsel hale getirilmiştir. Eşzamanlı olarak, analist profilleri; iş yükü dağılımını ve uzmanlık uyumunu dikkate alan iki yenilikçi metrik olan Analist Yük Faktörü (ALF) ve Deneyim Uyumluluk Faktörü (EMF) kullanılarak nicelleştirilmiştir. Olay–analist eşleştirme süreci, olay önceliği ile analist uygunluğunu dengeleyen kısıtlı bir optimizasyon problemi olarak tanımlanmıştır. Bu formülasyon; olayların en uygun analistlere, gerçek zamanlı ve otomatik olarak atanmasını sağlarken; operasyonel değerin korunmasını ve triyaj hassasiyetinin sürdürülmesini mümkün kılar. Model, algoritmik yalancı kodlar, puanlama tabloları ve büyük ölçekli SOC ortamlarında modelin karar mantığını ve pratik uygulanabilirliğini gösteren örnek bir vaka çalışması ile doğrulanmıştır. Gerçek dünya koşullarında çerçevenin geçerliliğini değerlendirmek amacıyla, CICIDS2017 benchmark veri setinden seçilen 10

saldırı senaryosu kullanılarak ampirik bir vaka çalışması gerçekleştirilmiştir. Genel olarak, bu çalışmanın katkısı; ikili faktöre dayalı bir analist puanlama şemasının biçimselleştirilmesi ve bağlamsal olay özelliklerinin uyarlanabilir ve kural tabanlı bir yapı çerçevesiyle bütünleştirilmesidir. Operasyonel değeri daha da artırmak amacıyla, gelecekte yapılacak çalışmalarda dinamik ağırlıklandırma mekanizmaları ile gerçek zamanlı SIEM veri akışlarıyla entegrasyon sağlanması planlanmaktadır. Ayrıca, analist geri bildirim döngülerinin ve denetimli öğrenme modellerinin sisteme entegre edilmesiyle olay-atama ve önceliklendirme süreçlerinin sürekli olarak iyileştirilmesi hedeflenmektedir.
Anahtar Kelimeler: Olay Yönetimi, Analist Atama, SOC Optimizasyonu, Olay Önceliklendirme, Korelasyon Puanı

ABSTRACT

A MULTI-CRITERIA DECISION SUPPORT FRAMEWORK FOR INCIDENT PRIORITIZATION AND ANALYST ASSIGNMENT IN SECURITY OPERATIONS CENTERS

In this thesis, we propose a comprehensive and scalable framework for incident assignment and prioritization in Security Operations Centers (SOCs). The proposed model aims to optimize SOC workflows by addressing key operational challenges such as analyst fatigue, alert overload, and inconsistent incident handling. Our framework evaluates each incident using a multi-factor scoring model that incorporates severity level, service-level agreement (SLA) urgency, incident type, asset criticality, threat intelligence indicators, frequency of repetition, and a correlation score derived from historical incident data. We formalize this evaluation through a set of mathematical functions that compute a dynamic incident score and derive incident complexity. In parallel, analyst profiles are quantified using Analyst Load Factor (ALF) and Experience Match Factor (EMF), two novel metrics that account for both workload distribution and expertise alignment. The incident–analyst matching process is expressed as a constrained optimization problem, where the final assignment score is computed by balancing incident priority with analyst suitability. This formulation enables automated, real-time assignment of incidents to the most appropriate analysts, while ensuring both operational fairness and triage precision. The model is validated using algorithmic pseudocode, scoring tables, and a simplified case study, which illustrates the real-world applicability and decision logic of the framework in large-scale SOC environments. To validate the framework under real-world conditions, an empirical case study was conducted using 10 attack scenarios from the CICIDS2017 benchmark dataset. Overall, our contributions lie in the formalization of a dual-factor analyst scoring scheme and the

integration of contextual incident features into an adaptive, rule-based assignment framework. To further strengthen operational value, future work will explore adaptive weighting mechanisms and integration with real-time SIEM pipelines. Additionally, feedback loops and supervised learning models will be incorporated to continuously refine analyst-incident matching and prioritization.
Keywords: Incident Management, Analyst Assignment, SOC Optimization, Incident Prioritization, Correlation Score

TEŞEKKÜR

Bu yüksek lisans tezinin hazırlanmasında, özellikle karşılaşılan güçlüklerin aşılmasında yönlendirici katkılarıyla sürecin her aşamasında sabır ve özveriyle destek sunan değerli danışmanım Dr. Barış Çeliktaş'a en içten teşekkürlerimi sunarım. Kendisinin akademik rehberliği ve çözüm odaklı yaklaşımı, çalışmanın tamamlanmasında belirleyici rol oynamıştır.

Bu süreçte her zaman yanımda olan, anlayışı, sabrı ve sarsılmaz desteğiyle en büyük motivasyon kaynağım haline gelen değerli eşim Canan Kılınçdemir'e en içten şükranlarımı sunarım. Varlığı, bu zorlu yolculuğu daha anlamlı ve sürdürülebilir kılmıştır.

Hayatım boyunca gösterdiği sınırsız fedakârlık, çalışkanlık ve kararlılıkla bana her zaman örnek olan kıymetli annem Sevinç Kılınçdemir'e de minnettarım.

Moral ve neşe kaynağım olan sevgili kardeşim Buse Kılınçdemir'e ve sessiz desteği ve özverili yaklaşımıyla her zaman arkamda duran sevgili babam Mehmet Kılınçdemir'e gönülden teşekkür ederim.

Bu tezin ortaya çıkmasında, ailemin sağladığı manevi güç ve kesintisiz destek temel bir dayanak oluşturmuş; akademik hedeflerime ulaşma yolculuğumu mümkün kılmıştır.

Eyüp Can KILINÇDEMİR

İÇİNDEKİLER

SAYFA NO

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

AHP: Analitik Hiyerarşi Süreci (Analytic Hierarchy Process)

AI: Yapay Zekâ (Artificial Intelligence)

ALF: Analist Yük Faktörü (Analyst Load Factor)

API: Uygulama Programlama Arayüzü (Application Programming Interface)

APT: Gelişmiş Sürekli Tehdit (Advanced Persistent Threat)

CI/CD : Sürekli Entegrasyon / Sürekli Dağıtım (Continuous Integration / Continuous Deployment)

C2: Komut ve Kontrol (Command and Control)

CVE: Bilinen Güvenlik Açıkları (Common Vulnerabilities and Exposures)

DB: Veritabanı (Database)

DC: Etki Alanı Denetleyicisi (Domain Controller)

EMF: Deneyim Uyumluluk Faktörü (Experience Match Factor)

HTTP/HTTPS: Hiper Metin Aktarım İletişim Protokolü (Hypertext Transfer Protocol / Secure)

IAM: Kimlik ve Erişim Yönetimi (Identity and Access Management)

IDS/IPS: Saldırı Tespit / Önleme Sistemleri (Intrusion Detection/Prevention System)

IP: İnternet Protokolü (Internet Protocol)

MITRE ATT&CK: MITRE Saldırgan Taktikleri, Teknikleri ve Ortak Bilgi Çerçevesi (MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework)

MFA: Çok Faktörlü Kimlik Doğrulama (Multi-Factor Authentication)

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

SLA: Hizmet Seviyesi Anlaşması (Service Level Agreement)

SOC: Güvenlik Operasyon Merkezi (Security Operation Center)

SSO: Tek Oturum Açma Sistemi (Single Sign-On)

TOPSIS: İdeal Çözüme Benzerliğe Göre Tercih Tekniği (Technique for Order Preference by Similarity to Ideal Solution)

TOR: Soğan Yönlendirici (The Onion Router)

VPN: Sanal Özel Ağ (Virtual Private Network)

XDR: Genişletilmiş Tespit ve Müdahale (Extended Detection and Response)

SEMBOLLER LİSTESİ

ALF_n: Analist n için Yük Faktörü

CI_n: Analiste atanmış olay sayısı (Current incidents)

C_m: Olay karmaşıklık düzeyi (Complexity of incident)

C_n: Analist n için olay sayısı

CW_i: Öznitelik i için korelasyon ağırlığı

dstIP: Hedef IP adresleri

EMF_n: Analist n'in deneyim uyumluluk faktörü

L_n: Analist deneyim seviyesi (Level of analyst)

MC_n: Analist n için maksimum kapasite (Maximum capacity)

M_i: Öznitelik i için geçmiş eşleşme sayısı

S_m: Olayın toplam skoru (Incident score)

S_n: Nihai analist uygunluk skoru (Final suitability score for analyst)

srcIP: Kaynak IP adresleri

T_i: Öznitelik i için doyum eşiği

BÖLÜM 1

1. GİRİŞ

1.1 ARAŞTIRMANIN AMACI

Siber güvenlik olaylarının artan sıklığı ve karmaşıklığı, yapılandırılmış ve uyarlanabilir bir olay yönetim yaklaşımını zorunlu kılmaktadır. Kurumsal savunmanın ön cephesi olarak konumlanan Güvenlik Operasyon Merkezleri (SOC'ler), tehditlerin gerçek zamanlı olarak tespitinden, analizine ve bertaraf edilmesine kadar olan tüm süreçten sorumludur. Ancak uyarı hacmindeki ciddi artış, sınırlı analist kaynakları ve manuel önceliklendirme süreçleriyle birleştiğinde gecikmelere, analist yorgunluğuna ve kaynakların verimsiz kullanımına neden olmaktadır. Bu zorluklar; olay karmaşıklığı, analist uzmanlığı, iş yükü ve SLA aciliyeti gibi faktörleri değerlendirebilen akıllı ve otomatik olay atama mekanizmalarına olan ihtiyacı göstermektedir.

Bu gereksinimlere yanıt olarak, olayların bağlamsal özniteliklerini (ciddiyet, SLA aciliyeti, varlık kritikliği, tehdit istihbaratı, korelasyon ve tekrar gibi) birleştiren bütünleşik bir skorlama modeline dayalı yeni bir olay atama ve önceliklendirme çerçevesi sunuyoruz. Aynı zamanda, analistler yük ve uzmanlık ölçütleri ile dinamik olarak profillenmekte ve bu sayede olaylarla gerçek zamanlı, yetkinlik odaklı bir eşleştirme sağlanmaktadır.

Bu çalışmanın temel katkıları şunlardır:

- Teknik ve bağlamsal olay özelliklerini bütünleştiren çok faktörlü bir skorlama modeli önerilmiştir.
- Analist odaklı iki yeni metrik sunulmuştur: Analist Yük Faktörü (ALF) ve Deneyim Uyum Faktörü (EMF).
- Analist atama süreci, skorlama formülleri ve örneklerle birlikte bir optimizasyon problemi olarak biçimsel hale getirilmiştir.

- Önerilen model, sahte kodlar, skor tabloları ve bir vaka çalışması aracılığıyla doğrulanmıştır.
- Modelin önceki çalışmalarla karşılaştırmalı analizi yapılmış ve API (Application Programming Interface) entegrasyonu ile pekiştirmeli öğrenme gibi gelecekteki geliştirme önerileri sunulmuştur.
- Çift yönlü optimizasyon yaklaşımımız, etkin olay önceliklendirmesi ile dengeli analist iş yükü arasında denge sağlar.
- Modelin gerçek dünya SOC ortamlarındaki uygulanabilirliğini göstermek amacıyla, CICIDS2017 benchmark verisi kullanılarak ampirik bir değerlendirme gerçekleştirilmiştir (bkz. Bölüm 5.2).

Tezin geri kalan bölümleri şu şekilde yapılandırılmıştır: Bölüm 2, SOC ortamlarında olay önceliklendirme ve analist ataması üzerine yapılmış çalışmaları kapsamlı şekilde ele alır. Bölüm 3, olay skorlama metodolojisini tanıtarak temel öznitelikleri ve bunların toplam skora katkılarını açıklar. Bölüm 4, olay karmaşıklığı, ALF ve EMF hesaplamaları ile birlikte nihai atama mantığını da içerecek şekilde önerilen modeli ayrıntılı olarak sunar. Bölüm 5, üç olay ve iki analistin yer aldığı örnek bir vaka çalışmasıyla modelin adım adım nasıl uygulandığını gösterir. Bölüm 6 ise çerçevenin temel katkılarını özetleyen, mevcut sınırlılıkları tartışan, vaka çalışmasının bulgularını içeren ve gelecekteki çalışmalara yönelik önerileri içeren bütünleşik bir sonuç bölümü sunar.

BÖLÜM 2

2. LİTERATÜR

Siber güvenlik tehditlerinin artan hacmi, sıklığı ve karmaşıklığı—fidye yazılımlarından kurum içi tehditlere kadar uzanan bir yelpazede—SOC'lerde (Güvenlik Operasyon Merkezleri) olay müdahale modellerinin evrimini hızlandırmıştır. Modern bir SOC, yüksek alarm hacmini, dinamik saldırgan davranışlarını ve sınırlı insan kaynağını dengelemek zorunda olduğundan, ölçeklenebilir ve akıllı olay işleme mekanizmalarına olan ihtiyaç her zamankinden daha kritik hâle gelmiştir. Bu bağlamda birçok çalışma; olay sınıflandırması, önceliklendirme, analist-olay eşleştirmesi ve karar destek sistemlerine odaklanan çerçeve ve algoritmalar önermiştir.

Temel ITIL çerçevesi (AXELOS, 2019), olayların yönetimine yönelik süreç odaklı bir yapı sunar ve etki, aciliyet, yükseltme akışları ve SLA'lara (Hizmet Seviyesi Anlaşmaları) vurgu yapar. ITIL, BT operasyonlarının standartlaştırılmasında yaygın olarak benimsenmiş olsa da, analist odaklı değerlendirmeleri ve dinamik görev dağıtım özelliklerini içermemektedir. Benzer şekilde, Mooi ve Botha (2016) tarafından önerilen Yetenek Olgunluk Modeli (Capability Maturity Model), kurumsal hazırlığı ve güvenlik yönetişimi olgunluğunu destekler; ancak gerçek zamanlı önceliklendirme, skorlamaya dayalı triyaj veya analist eşleştirmesi konularına değinmez.

Önceliklendirme perspektifinden bakıldığında, Jalalvand ve arkadaşları (2024), uyarı triyaj stratejilerini—ciddiyete dayalı modeller ve istatistiksel sınıflandırıcılar dahil olmak üzere—kapsamlı şekilde incelemiştir. Benzer şekilde, Chhetri ve arkadaşları (2024), analist yorgunluğunu azaltmak için insan-yapay zekâ iş birliği yaklaşımını vurgulamıştır. Bu çalışmalar, önceliklendirme kriterlerini ve analist üzerindeki yükü anlamaya önemli katkılar sunsa da, analiste duyarlı atama veya iş yükü dengeleme mekanizmaları sağlamamaktadır.

Diğer araştırmacılar, görev dağıtımını algoritmik veya optimizasyon temelli yöntemlerle ele almıştır. Örneğin, Gachnang ve arkadaşları (2023), analistleri becerileri ve SLA'lar doğrultusunda olaylarla eşleştirmek için çok amaçlı evrimsel algoritmalar kullanmış; ancak modelleri yüksek hesaplama maliyetine sahiptir. Hou ve arkadaşları (2022), eşleştirme verimliliğini artıran grafik tabanlı bir yük dengeleme stratejisi geliştirmiştir; fakat bu model, olay ciddiyeti veya tehdit istihbaratı ile bütünleşmemiştir. Farklı bir boyutta, Handri ve arkadaşları (2025), görev atamasının insani yönlerine odaklanan kültür merkezli bir analist eşleştirme yaklaşımını Q metodolojisi ile önermiş; fakat teknik önceliklendirme mantığı eksik kalmıştır.

SOC ortamlarında otomasyon da birçok çalışmanın konusu olmuştur. Alrimawi ve arkadaşları (2019), akıllı alanlar (smart spaces) için otomatik olay iş akışlarını tanıtmış; Binbeshr ve arkadaşları (2025) ise yapay zekâ destekli triyaj yetenekleri içeren Bilişsel SOC (Cognitive SOC) modelini önermiştir. Ancak bu modeller, daha çok tespit ve yapay zekâ odaklı otomasyona yönelmiş olup, analist odaklı triyaj veya atama sonrası optimizasyon süreçlerine odaklanmamaktadır.

Bazı çalışmalar, alan özelinde SOC uygulamalarını hedeflemektedir. Al-Dhaqm ve arkadaşları (2020), veritabanı sistemlerine özgü bir adli olay müdahale modeli önermiştir. Villalón-Huerta ve arkadaşları (2022) ise SOC savunması için bir "kill-chain" modeli geliştirmiştir. He ve arkadaşları (2019) ise gerçek zamanlı olay yönetimi için IS-CHEC yöntemini sunmuştur; fakat analist uzmanlığı veya skor bazlı değerlendirme mekanizmalarını içermemektedir.

Vielberth ve arkadaşları (2020) gibi bazı öncü çalışmalar, SOC mimarilerine dair taksonomiler ve yapısal çerçeveler sunmuş; entegrasyon ve rol netliği gibi konulara vurgu yapmıştır; ancak uygulanabilir olay atama stratejileri önermemiştir. Öte yandan, gerçek zamanlı yük dengeleme için önerilen genel modeller (örneğin, Liao ve ark., 2011; Jadon ve ark., 2024) ve yakındaki alanlardan alınan SLA temelli çerçeveler (örneğin, García ve Tomás, 2020),

optimizasyon açısından değerli içgörüler sunsa da, güvenliğe özgü karmaşıklık ya da SOC analisti eşleşmesini içermemektedir.

Bu çalışmaların karşılaştırmalı özeti Tablo 2.1'de sunulmuştur. Görüldüğü üzere, önceki modellerin çoğu, SOC yaşam döngüsünün yalnızca belirli bileşenlerine—örneğin, uyarı ciddiyeti, görev dağıtımı veya analist iş yükü—odaklanmakta ve bunları birleşik, dinamik bir çerçevede bütünleştirmemektedir.

Buna karşılık, *bu* çalışma; yedi temel olay skorlama boyutunu—Ciddiyet, SLA Aciliyeti, Olay Türü, Varlık Kritikliği, Tekrar Frekansı, Tehdit İstihbaratı ve Korelasyon Puanı—analist tarafındaki profil verileriyle (EMF ve ALF üzerinden) birleştiren kapsamlı bir çerçeve önermektedir. Ayrıca modelimiz, gerçek zamanlı çalışmayı desteklemekte ve yeniden atama sıklığı veya yanlış pozitif oranları gibi çıktılara göre kendini dinamik olarak uyarlayan bir geri besleme döngüsü içermektedir.

Bu bütünleşik yaklaşım, modern SOC ortamlarında önceliklendirme ve atama süreçlerine yönelik ölçeklenebilir, analist-farkındalıklı bir çözüm sunarak literatürdeki önemli bir boşluğu doldurmaktadır. Önceki araştırmalar uyarı filtreleme, otomasyon ve insan merkezli destek konusunda önemli ilerlemeler kaydetmiş olsa da; bizim katkımız, bu boyutları nicel ölçütlere ve biçimsel atama mantığına dayalı, bütüncül ve operasyonel olarak uygulanabilir bir önceliklendirme motorunda sentezlemektir.

Tablo 2.1 SOC Olay Atama ve Önceliklendirme Üzerine İlgili Çalışmaların Karşılaştırmalı Özeti

Yazar / Çalışma	Model	Ana Faktörler	Atama Mantığı	Güçlü Yönler	Sınırlılıklar
ITIL Foundation (2019)	Süreç Odaklı Çerçeve	Etki, Aciliyet, SLA	Rol Bazlı Statik Atama	Yapılandırılmış iş akışları sağlar	Analist düzeyinde uyarlama yok
Mooi ve Botha (2016)	Yetenek Olgunluk Modeli	Kurumsal Hazırlık, Süreç Aşamaları	Olgunluk Takibi	Kurumsal odaklı yaklaşım	Dinamik skor yok
Jalalvand ve ark. (2024)	Sistematik Derleme	Ciddiyet, Uyarı Yorgunluğu	Triyaj Kriterleri	Kapsamlı literatür özeti	Model önerisi sunulmamış
Chhetri ve ark. (2024)	İnsan-YZ İş Birliği	Analist Yorgunluğu, Alarm Hacmi	Bilişsel Yük Dağılımı	İnsan odaklı yaklaşım	Teknik önceliklendirmeyi ihmal eder
Gachnang ve ark. (2025)	Evrimsel Optimizasyon	SLA, Analist Yetkinliği	Çok Amaçlı Eşleştirme	Yüksek kaliteli atama sonuçları	Yüksek hesaplama maliyeti
Handri ve ark. (2025)	Q Yöntemi + Çevik SOC	Kurum Kültürü, Çeviklik	Kültür Tabanlı Eşleştirme	Kurumsal perspektifi ele alır	Teknik odak zayıf
Alrimawi ve ark. (2019)	Akıllı Alan Otomasyonu	IoT Tehditleri	Otonom Tetikleyiciler	Otomasyon odaklı yapı	SOC bağlamı genellenmiş
Binbeshr ve ark. (2025)	Bilişsel SOC	YZ Modelleri, Alarm Verisi	YZ Tabanlı Eşleştirme	Bilişsel YZ kullanır	İş yükü dengelemesini ihmal eder
Al-Dhaqm ve ark. (2020)	Adli Olay Müdahale Modeli	Veritabanı Günlükleri, Aktiviteler	Adli Aşamalar	Yapılandırılmış adli görünüm	Gerçek zamanlı değil
Villalón-Huerta ve ark. (2022)	Savunma Amaçlı Kill Chain	Saldırı Yaşam Döngüsü	Aşama Eşleştirme	Kill-chain tabanlı SOC modeli	Analist eşleştirmesi yok
He ve ark. (2019)	IS-CHEC Çerçevesi	Performans Ölçütleri	Gerçek Zamanlı Yapısal Akış	Gerçek zamanlı odak	Analist bağlamı dışlanmış

Tablo 2.1 (Devamı) SOC Olay Atama ve Önceliklendirme Üzerine İlgili Çalışmaların Karşılaştırmalı Özeti

Vielbert h ve ark. (2020)	SOC İnceleme Modeli	SOC Rolleri, Taksonom i	Rol Tanımı	Geniş kapsamlı taksonomi	Eyleme dökülebilir değil
Hou ve ark. (2022)	Grafik Tabanlı Yük Dengele me	Analist Yükü, Uygunluk	Grafik Eşleştirme	Dengeli atama sağlar	Tehdit modelleme si yok
Jadon ve ark. (2024)	Gerçek Zamanlı Yük Dengele me	Görev Türü, RT Gereksini mi	Çekirdek Farkındalıklı Dağıtım	Etkili zamanlayıcı	Genel yapı, SOC'e özel değil
Liao ve ark. (2011)	Ağ Tabanlı Yük Dengele me	Yük, Gecikme	Ağ Haritalama	Verimli ağ yönetimi sağlar	SOC'e özgü değil
García ve Tomás (2020)	Trafik Tabanlı Müdahale Çerçevesi	Olay Riski, SLA	Uyarlanabilir Önceliklendir me	SLA odaklı zamanlama	Ulaşım sektörü odaklı
Bu Çalışma	Skorlama + Eşleştirm e	Ciddiyet, SLA, Tehdit İstihbaratı, Korelasyo n, Tekrar, EMF + ALF, Karmaşıkl ık	Gerçek zamanlı, çok faktörlü, analist-farkındalıklı atama	Önceliklendir me, dinamik analist profili, geri besleme döngüsü, korelasyon farkındalığı entegre	Büyük ölçekli SOC'ler için ayarlama gerektirir

BÖLÜM 3

3. YÖNTEM

Önerilen çerçeve, Güvenlik Operasyon Merkezi (SOC) bağlamında olayları değerlendirmek ve önceliklendirmek amacıyla çok ölçütlü karar verme (MCDM) yaklaşımından esinlenen çok faktörlü bir önceliklendirme stratejisini izlemektedir. Bu strateji, aciliyet, karmaşıklık ve kaynak kısıtları gibi çoğu zaman birbiriyle çelişen çeşitli niteliklerin aynı anda dikkate alınması gereken ortamlarda özellikle etkilidir. Her bir güvenlik olayı, toplam önceliğine katkı sağlayan bir dizi faktöre göre değerlendirilmekte ve bu sayede hem yapılandırılmış triyaj hem de bağlama duyarlı analist ataması mümkün hâle gelmektedir.

Skorlama modeli, Tablo 3.1'de sembolleriyle birlikte biçimsel olarak tanımlanan aşağıdaki olaya özgü faktörleri bütünleştirir:

- **Olay Puanı (S_m):** Tüm ilgili öznitelikler için ağırlıklı toplam kullanılarak bir olaya atanan genel öncelik puanını temsil eder. Bu toplam puan, Güvenlik Operasyon Merkezi (SOC) içinde olayların sıralanması ve karşılaştırılması amacıyla kullanılır; böylece etkili önceliklendirme ve kaynak tahsisi sağlanır. Daha yüksek bir $\mathbf{S_m}$ değeri, olayın daha acil ve karmaşık olduğunu gösterir ve analist atama kararlarını doğrudan etkiler.
- **Olay Ciddiyeti (S_{sev}):** Olayın kurumsal varlıklar ve operasyonlar üzerindeki potansiyel etkisini yansıtır. Daha ciddi olaylar, daha hızlı müdahale edilmek üzere önceliklendirilir.
- **SLA Aciliyeti (S_{SLA}):** Önceden tanımlanmış Hizmet Seviyesi Anlaşmalarına (SLA) dayalı olarak, olay için izin verilen yanıt süresini ifade eder. Daha kısa SLA süreleri, olayın öncelik düzeyini artırır.
- **Olay Türü (S_{type}):** Oltalama (phishing), fidye yazılımı (ransomware) veya ayrıcalık yükseltme (privilege escalation) gibi farklı olay türleri;

karmaşıklık ve risk düzeyine göre farklılık gösterir. Her kategoriye önceden belirlenmiş bir ciddiyet düzeyi atanır.

- **Tekrarlama (S_{rep}):** Belirli bir zaman dilimi içerisinde yinelenen olaylar, çözülmemiş zafiyetler veya devam eden tehdit kampanyalarının göstergesi olabilir. Bu nedenle tekrarlayan olaylar dinamik olarak daha yüksek öncelik alır.
- **Etkilenen Varlık (S_{asset}):** SIEM, etki alanı denetleyicileri gibi yüksek değerli veya kritik sistemleri etkileyen olaylar, iş sürekliliğini korumak amacıyla daha yüksek ağırlıkla değerlendirilir.
- **Tehdit İstihbaratı (S_{ti}):** Kara listeye alınmış IP adresleri, kötü amaçlı yazılım göstergeleri ve bilinen saldırı kalıpları gibi bağlamsal verileri içerir. Tehdit aktörleriyle olan bağlantılar, olayın önceliğini doğrudan yükseltir.
- **Korelasyon Puanı (S_{cor}):** Kaynak IP, hedef sistem ve kullanıcı hesabı gibi öznitelikler temel alınarak olayın geçmiş vakalarla benzerliğini ölçer. Bu ölçüm, kalıpların ve kampanya düzeyindeki davranışların tespit edilmesine olanak sağlar.
- **Ciddiyet Ağırlığı (W_{sev}):** Olay ciddiyeti özniteliğine genel puanlama formülünde atanan göreli önemi ifade eder.
- **SLA Aciliyeti Ağırlığı (W_{SLA}):** SLA aciliyet faktörüne atanan ağırlığı temsil eder.
- **Olay Türü Ağırlığı (W_{type}):** Olayın türünün (örneğin ransomware veya phishing) toplam puan üzerindeki etkisini belirtir.
- **Tekrarlama Ağırlığı (W_{rep}):** Olayların tekrar etme sıklığına verilen önemi yansıtır.
- **Varlık Kritiklik Ağırlığı (W_{asset}):** Etkilenen sistemin önem derecesine verilen önceliği gösterir.
- **Tehdit İstihbaratı Ağırlığı (W_{ti}):** Tehdit istihbaratı göstergelerinin toplam puana katkısını ölçer.
- **Korelasyon Ağırlığı (W_{cor}):** Geçmiş olaylardan türetilen korelasyon skorlarına atanan önemi ifade eder.

Tablo 3.1 Olay Puanı Hesaplama Formülünde Kullanılan Semboller

Sembol	Açıklama
S_m	Bir olaya atanan toplam puan
S_{sev}	Olayın şiddet düzeyi puanı (1–5 arası)
S_{SLA}	Hizmet Seviyesi Anlaşması (SLA) temelinde sayısal aciliyet düzeyi (1–5)
S_{type}	Olayın türü/kategorisine dayalı olarak verilen puan
S_{rep}	Tekrarlanma sıklığına bağlı olarak verilen ek puan
S_{asset}	Etkilenen sistemin kritiklik düzeyini yansıtan puan
S_{ti}	Tehdit istihbaratı göstergelerine dayalı olarak verilen puan
S_{cor}	Geçmiş olaylarla benzerliğe göre türetilen puan
W_{sev}	Şiddet özniteliği için ağırlık katsayısı
W_{SLA}	SLA aciliyeti için ağırlık katsayısı
W_{type}	Olay türü için ağırlık katsayısı
W_{rep}	Tekrarlanma durumu için ağırlık katsayısı
W_{asset}	Varlık kritiklik düzeyi için ağırlık katsayısı
W_{ti}	Tehdit istihbaratı için ağırlık katsayısı
W_{cor}	Korelasyon için ağırlık katsayısı

Yüksek öncelikli olayların en yetkin personel tarafından ele alınmasını sağlamak amacıyla analistler, deneyim ve mevcut iş yüklerine göre profillenmektedir. Herhangi bir analistin aşırı yüklenmesini önlemek için ALF (Analist Yük Faktörü) kullanılırken, EMF (Deneyim Uyumluluk Faktörü), analistin yetkinlik düzeyinin olayın karmaşıklığıyla ne ölçüde örtüştüğünü değerlendirir. ALF ve EMF ile ilgili ayrıntılar ve formüller Bölüm 4.4'te sunulmaktadır.

Nihai olay puanı, yukarıda belirtilen özniteliklerin ağırlıklı birleştirilmesiyle elde edilirken; analist uygunluk skoru hem ALF hem de EMF bileşenlerini dikkate alır. Bu ağırlıklar başlangıçta uzman görüşüyle belirlenmiş ve senaryo testleriyle doğrulanmıştır. Gelecekteki yinelemelerde bu ağırlıkların dinamik olarak optimize edilmesi için pekiştirmeli öğrenme (reinforcement learning) kullanılabilir. Bu yöntem, bir sonraki bölümde adım adım açıklanan modelin temelini oluşturmaktadır.

BÖLÜM 4

4. ÖNERİLEN MODEL

Önerilen model, SOC operasyonlarında akıllı ve verimli analist atamasını kolaylaştırmak amacıyla tasarlanmış bir dizi ardışık adımdan oluşmaktadır. Şekil 1, bu dinamik iş akışının genel bir görünümünü sunmaktadır.

4.1 OLAY SKORLAMASI VE ANALİST EŞLEŞTİRME ADIMLARI

4.1.1 Adım 1: Olay Skorunun Hesaplanması

Her olay; ciddiyet, SLA aciliyeti, olay türü, tekrarlanma sıklığı, varlık kritiklik düzeyi, tehdit istihbaratı ve korelasyon göstergeleri gibi normalleştirilmiş faktörlerin ağırlıklı birleşimi kullanılarak puanlanır. Ağırlıklar, yapılandırılmış bir anket aracılığıyla uzman değerlendirmelerinden elde edilmiştir. Bu bileşik puan, her bir olayın bağlamsal ve teknik açıdan genel önceliğini yansıtmakta olup atama ve triyaj kararları için temel teşkil eder.

4.1.2 Adım 2: Olay Karmaşıklığının Belirlenmesi

Hesaplanan olay skoru, olayın karmaşıklık düzeyini belirlemek için kullanılır. Olaylar, Çok Düşük, Düşük, Orta, Yüksek ve Kritik olmak üzere beş kategoriye ayrılır. Bu sınıflandırma, olayların uygun uzmanlık seviyesine sahip analistlere atanmasını sağlar.

4.1.3 Adım 3: Analist Yük Faktörünün (ALF) Hesaplanması

Herhangi bir analistin aşırı yüklenmesini önlemek amacıyla, mevcut atanan olay sayısı ve maksimum işleme kapasitesine göre analist bazında bir yük

faktörü hesaplanır. Bu faktör, iş yükü sınırına yaklaşan analistlerin uygunluk skorunu düşürmektedir.

4.1.4 Adım 4: Deneyim Uyumluluk Faktörünün (EMF) Hesaplanması

EMF, bir analistin deneyim seviyesinin olayın karmaşıklığı ile ne ölçüde örtüştüğünü belirler. Olay karmaşıklık seviyesiyle deneyim seviyesi yüksek ölçüde örtüşen analistlere daha yüksek EMF puanı verilir.

4.1.5 Adım 5: En Uygun Analiste Atama Yapılması

Son olarak, olay skoru, EMF ve ALF birleşimiyle bir uygunluk skoru hesaplanır. Olay, en yüksek uygunluk skoruna sahip analiste atanır. Bu yöntem, etkili ve bağlam farkındalığına sahip bir atama yapılmasını garanti eder.

Şekil 1, olay skorlaması, analist eşleştirme ve iş yükü dengelemesini içeren önerilen atama iş akışının temel adımlarını görselleştirir.

4.2 OLAY SKORU HESAPLAMA FORMÜLÜ

Bir olayın öncelik düzeyini belirlemek amacıyla, teknik ve bağlamsal öznitelikleri tek bir ağırlıklı puan içinde birleştiren çok faktörlü bir puanlama modeli kullanılmaktadır. Sabit toplama yöntemlerinden farklı olarak, bu model her bir öznitelik için göreli önemi daha doğru yansıtmak üzere uzman değerlendirmelerine dayalı faktör özgü ağırlıkları içermektedir. Genel ağırlıklı olay puanı formülü aşağıda sunulmuştur:

$$S_m = W_{sev} \times S_{Sev} + W_{SLA} \times S_{SLA} + W_{type} \times S_{type} + W_{rep} \times S_{rep} + W_{asset} \times S_{asset} + W_{ti} \times S_{ti} + W_{cor} \times S_{Cor} \quad (4.1)$$

Burada:

- S_m, nihai olay puanıdır.
- •S_{sev}, S_{SLA}, S_{type}, S_{rep}, S_{asset}, S_{ti}, S_{cor} her bir olaya özgü öznitelik için 0–5 aralığında normalleştirilmiş puanlardır.

- •W_{sev}, W_{SLA}, W_{type}, W_{rep}, W_{asset}, W_{ti}, W_{cor} ilgili özniteliklere atanan ve toplamı 1 olacak şekilde normalize edilmiş ağırlıklardır.

$$W_{sev} + W_{SLA} + W_{type} + W_{rep} + W_{asset} + W_{ti} + W_{cor} = 1 \quad (4.2)$$

Bu ağırlıklar, siber güvenlik, BT denetimi, risk yönetimi ve operasyonel SOC görevlerinde çalışan uzmanlara yönelik olarak yürütülen yapılandırılmış bir anket çalışması aracılığıyla elde edilmiştir. Katılımcılardan, yedi temel olay özniteliğinin önem düzeyini 1–5 Likert ölçeğinde puanlamaları istenmiştir. Elde edilen ortalama puanlar daha sonra normalize edilerek modelde kullanılan nihai ağırlık değerleri hesaplanmıştır.

Ortaya çıkan ağırlıklı puanlama formülü aşağıda sunulmuştur:

$$S_m = 0.160\ x\ S_{Sev} + 0.135\ x\ S_{SLA} + 0.149\ x\ S_{type} + 0.117\ x\ S_{rep} + 0.156\ x\ S_{asset} + 0.149\ x\ S_{ti} + 0.135\ x\ S_{Cor} \quad (4.3)$$

Bu ağırlıklar, olay değerlendirme sürecine gerçek dünya koşullarına duyarlı, bağlamsal uzman görüşlerini entegre ederek önceliklendirme doğruluğunu artırmaktadır. Ayrıntılı anket verileri ve hesaplama adımları Tablo 4.1'te sunulmuştur.

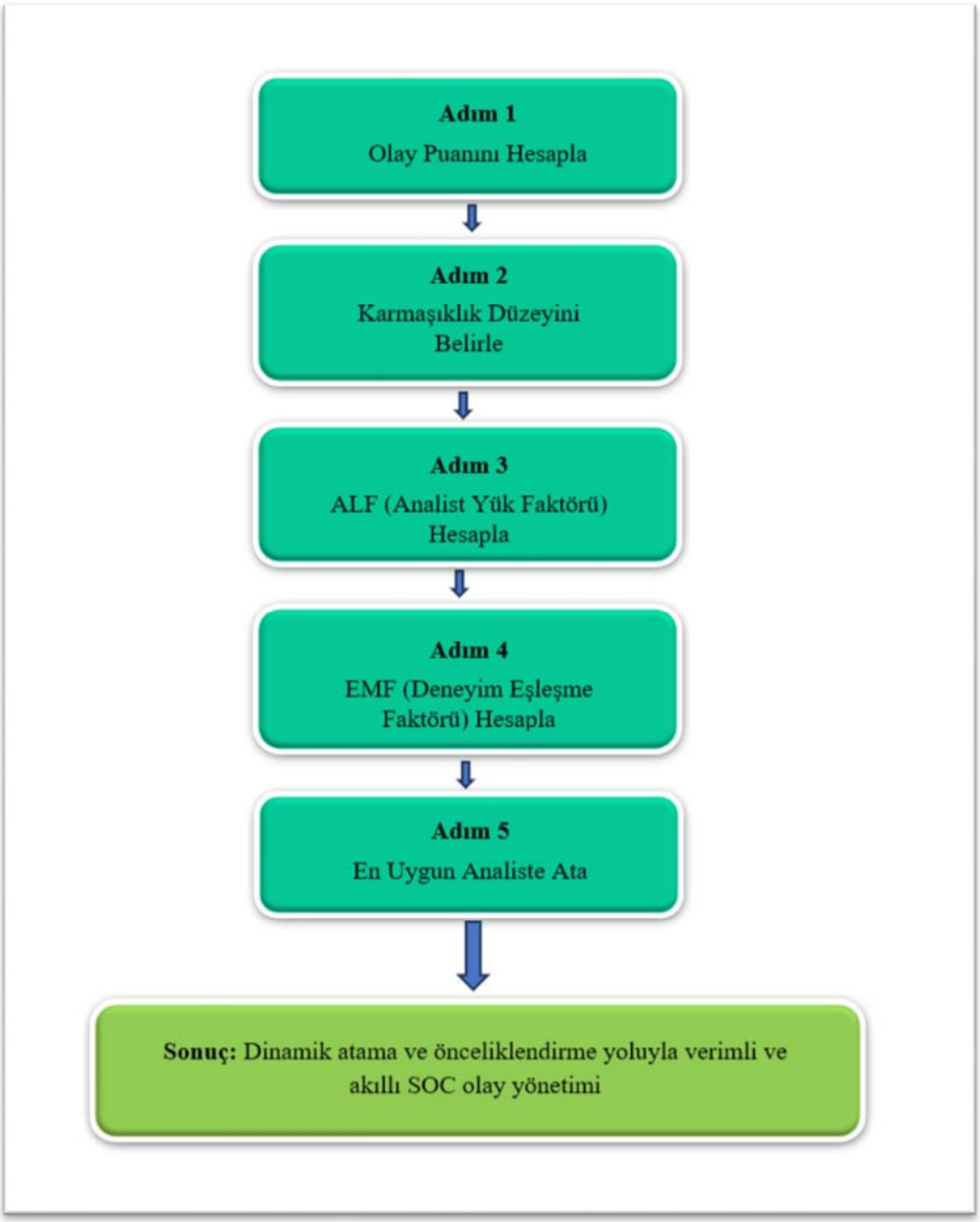
Tablo 4.1. Olay Puanı Ağırlıkları İçin Uzman Değerlendirmeleri (Normalize Edilmiş Ortalama Değerler)

Ünvan	Sev	SLA	Inc Type	Ass Cri	TI	Re	Co
CSE	5	3	5	4	3	4	5
CSM	5	3	4	3	5	2	3
IR	4	2	3	5	4	3	3
ISM	5	5	5	5	5	5	5

Tablo 4.1 (Devamı) Olay Puanı Ağırlıkları İçin Uzman Değerlendirmeleri (Normalize Edilmiş Ortalama Değerler)

L2A	5	4	4	4	5	1	3
SS	1	3	5	4	5	5	4
SCSE	5	5	3	5	4	4	4
SIA	5	5	5	4	4	3	3
SOCS	5	4	4	5	3	3	4
SOCTL	5	4	4	5	4	3	4
Avg	4.5	3.8	4.2	4.4	4.2	3.3	3.8
Norm. Wt	0.160	0.135	0.149	0.156	0.149	0.117	0.135

Not: *Sev. = Ciddiyet, Inc Type = Olay Türü, Ass Cri = Varlık Kritiklik Düzeyi, TI = Tehdit İstihbaratı, Re = Tekrarlanma, Co = Korelasyon, CSE = Siber Güvenlik Mühendisi, CSM = Siber Güvenlik Yöneticisi, IR = Olay Müdahale Uzmanı, ISM = Bilgi Güvenliği Yöneticisi, L2A = Seviye 2 Siber Güvenlik Analisti, SS = Güvenlik Uzmanı, SCSE = Kıdemli Siber Güvenlik Uzmanı, SIA = Kıdemli Bilgi Denetçisi, SOCS = SOC Uzmanı, SOCTL = SOC Takım Lideri, Avg = Ortalama, Norm. Wt = Normalize Edilmiş Ağırlık*



Şekil 4.1 SOC Operasyonlarında Önerilen Dinamik Olay Atama Akışı. Bu süreç, akıllı analist eşleştirmesi ve iş yükü dengesini sağlar

4.2.1 Ciddiyet Skoru (Severity Score)

Ciddiyet seviyesi, olayın sistem üzerindeki etkisini tanımlar. Daha yüksek skor değerleri, daha kritik olaylara karşılık gelir.

SOC (Güvenlik Operasyon Merkezi) ortamlarında, ciddiyet düzeyi, güvenlik olaylarının aciliyetine ve potansiyel etkisine göre sınıflandırılması ve önceliklendirilmesinde kritik bir rol oynar. Çoğu SOC, tutarlı ve riske duyarlı olay yönetimini mümkün kılmak amacıyla Bilgilendirici (Informational), Düşük (Low), Orta (Medium), Yüksek (High) ve Kritik (Critical) olmak üzere beş seviyeli bir sınıflandırma modeli benimsemektedir.

Bu yapılandırılmış kategorizasyon, doğrudan triyaj süreçlerini etkiler. Kritik olaylar; veri sızdırma, fidye yazılımı bulaşmaları veya devlet destekli saldırılar gibi acil müdahale gerektiren tehditleri içerir. Buna karşılık, Düşük veya Bilgilendirici kategorisindeki olaylar—örneğin kaba kuvvet denemeleri veya hatalı yapılandırmalar gibi—daha az aciliyet taşır.

Bu çalışmada, her bir ciddiyet seviyesine Tablo 4.2'te gösterildiği şekilde sayısal bir skor atanmıştır. Bu skorlar, analist ile olay arasında doğru eşleşmenin sağlanmasına katkıda bulunmakta ve olayların kritiklik derecesine göre önceliklendirilmesinde temel rol oynamaktadır.

Tablo 4.2 Ciddiyet Seviyeleri ve İlişkili Skorları

Seviye	Açıklama	Puan
1	Kritik	5
2	Yüksek	4
3	Orta	3
4	Düşük	2
5	Bilgilendirici	1

Ciddiyet skoru, bir olayın kurumsal varlıklar üzerindeki etkisinin kritiklik düzeyini yansıtır. “Kritik” olarak sınıflandırılan olaylar (örneğin, fidye yazılımı saldırıları, devlet destekli tehditler) en yüksek skoru alır ve bu da acil triyaj ve hızlı analist müdahalesi gerektirir. Buna karşılık, Bilgilendirici veya Düşük ciddiyetli olaylar en düşük skoru alır.

4.2.2 SLA Aciliyet Skoru

SLA’lar (Hizmet Seviyesi Anlaşmaları), SOC iş akışlarında temel unsurlar olup, güvenlik olaylarının ciddiyetine göre algılama, analiz etme ve çözümleme işlemleri için izin verilen maksimum zaman aralığını tanımlar. Bu eşikler, risk maruziyetini azaltmaya ve operasyonel sürekliliği sağlamaya yardımcı olur.

Çoğu SOC, ciddiyet seviyeleriyle uyumlu kademeli bir SLA yapısı kullanır. Önerilen çerçevemizde, olaylara atanan SLA aciliyet seviyeleri, doğrudan önceliklendirme skorunu etkiler. Örneğin, Kritik bir olay olan veri sızdırma teşebbüsü, 15 dakika içinde ele alınmalıdır. Buna karşılık, Düşük bir olay olan izinsiz erişim denemesi, operasyonel politikalara bağlı olarak iki saat veya daha uzun sürede çözümlenebilir.

SLA aciliyetini olay skorlama modeline entegre edebilmek için, her yanıt seviyesi sayısal bir skora dönüştürülür. Daha yüksek öncelikli olaylar, daha yüksek aciliyet skoru alır ve bu, olayın nihai ağırlığını doğrudan etkiler.

Tablo 4.3, SLA yanıt süresi ile ilgili aciliyet skorunun eşlemesini sunmaktadır.

Bu skor, bir olayın SLA düzeyine göre ne kadar hızlı çözümlenmesi gerektiğini ifade eder. SLA yanıt süresi ne kadar kısaysa, aciliyet skoru o kadar yüksek olur (bu ilişki “6 − SLA Düzeyi” dönüşümü ile sağlanır). Bu dönüşüm, SLA uyumlu bir önceliklendirme mekanizmasını garanti altına alır ve yüksek kritiklikteki tehditler için ortalama müdahale süresini (MTTR) en aza indirir.

Tablo 4.3 SLA Aciliyet Düzeyleri ve Karşılık Gelen Puanlar

Seviye	Yanıt Süresi	Puan (6 -SLA)
1	< 15 dakika (Kritik)	5
2	< 30 dakika (Yüksek)	4
3	< 60 dakika (Orta)	3
4	< 120 dakika (Düşük)	2
5	> 120 dakika (Bilgilendirici)	1

4.2.3 Olay Türü Skoru (Incident Type Score)

Olay türü, bir SOC (Güvenlik Operasyon Merkezi) içinde analistler için uygun müdahale stratejisinin belirlenmesinde temel bir rol oynar. Ransomware, oltalama (phishing) veya yetkisiz erişim gibi güvenlik olaylarının niteliğini tanımlar ve kuruma yönelik potansiyel riski ortaya koyar. Olayların türlerine göre sınıflandırılması, analistlerin olayın ciddiyetini, teknik karmaşıklığını ve etkisinin kapsamını daha iyi anlamalarına yardımcı olur.

Bu çalışmada, her olay türüne toplam önceliklendirme mekanizmasına katkı sağlayacak şekilde belirli bir skor atanmıştır. Tablo 4.4, farklı olay türlerinin potansiyel risk seviyelerine göre nasıl gruplandığını ve bu türlere hangi skorların verildiğini göstermektedir. Bu skor atamaları hem nihai olay skoruna hem de tekrarlama skoruna katkı sağlamaktadır.

Tablo 4.4 Bilgi Güvenliği Olaylarının Sınıflandırması ve Karşılık Gelen Puanlar

Olay Türü	Puan
Kritik Olaylar	
Gelişmiş Sürekli Tehdit (APT)	5
Veri Sızdırma (Hassas Veri Kaçağı)	5
Fidye Yazılımı Bulaşması	5
Devlet Destekli Saldırı	5
Tedarik Zinciri Saldırısı	5
Yüksek Ciddiyetli Olaylar	
Yetkisiz Ayrıcalık Yükseltme	4
SQL Enjeksiyon Saldırısı	4
Bilinen Zafiyetlerin Sömürülmesi	4
Uzak Kod Çalıştırma (RCE) Girişimi	4
Active Directory Ele Geçirme	4
Orta Ciddiyetli Olaylar	
Zararlı Yazılım Bulaşması	3
Dağıtık Hizmet Engelleme (DDoS) Saldırısı	3
Oltalama Saldırısı (Spear Phishing)	3
Kimlik Bilgisi Doldurma Saldırısı	3
Şüpheli Yanal Hareket	3
Sıfırıncı Gün (Zero-Day) Açığı Tespiti	3
İç Tehdit Kaynaklı Faaliyet	3
Düşük Ciddiyetli Olaylar	
Yetkisiz Erişim Girişimi (Brute Force)	2
Sosyal Mühendislik Saldırısı	2
Olağandışı Oturum Davranışı	2
Zararlı Yazılım Geri Çağrısı (Komuta ve Kontrol İletişimi - C2)	2
Bilgilendirici Düzeyde Olaylar	
Port Taraması	1
Hatalı Yapılandırılmış Güvenlik Ayarları	1
Şüpheli Dosya Çalıştırma	1
Olağandışı Ağ Trafiği	1

Not: *Olay türleri ve bunlara karşılık gelen ciddiyet puanları, Güvenlik Operasyon Merkezleri (SOC) ortamlarında gözlemlenen yaygınlıkları ile gizlilik, bütünlük ve erişilebilirlik (CIA üçlemesi) üzerindeki potansiyel etkileri dikkate alınarak manuel olarak türetilmiştir. Bu taksonomi, olay kategorilerini uygun risk düzeyleriyle ilişkilendirerek yapılandırılmış önceliklendirme (triage) kararlarını desteklemeyi amaçlamaktadır.*

4.2.4 Tekrarlama Puanı (Repetition Score)

Temel olay türü puanı, aynı türdeki olayların tanımlı bir zaman dilimi içerisinde ne sıklıkla meydana geldiğine bağlı olarak dinamik şekilde ayarlanmaktadır. Sıklığa dayalı ayarlayıcı katsayılar Tablo 4.5'te tanımlanmıştır.

Tablo 4.5 Tekrarlama Sıklığına Dayalı Puan Ayarlama Kriterleri

Tekrarlama Sıklığı	Puan Ayarlayıcı (R)
1 saat içinde 5'ten fazla tekrar	50
24 saat içinde 5'ten fazla tekrar	25
7 gün içinde 3'ten fazla tekrar	10
İlk gerçekleşme	0

Tekrarlama puanı, zaman içindeki sıklığa bağlı olarak olayın önceliğini ayarlamakta ve bu yolla çözülmemiş ya da yinelenen tehditlerin (örneğin kaba kuvvet saldırıları, tarama faaliyetleri) potansiyel aciliyetini yansıtmaktadır. Bir tehdit ne kadar sık gözlemlenirse, yapılan ayarlama o ölçüde artar; ancak bu artış, belirli bir üst sınırla sınırlandırılır.

Nihai tekrarlama ayarlı puan, aşağıda verilen ve sonucu en fazla 5 ile sınırlayan formül kullanılarak hesaplanmaktadır:

$$Repetition\ Score = min\left(5,\ Incident\ Type\ Score + \frac{(Repetition\ Score\ Modifier(R) + Incident\ Type\ Score)}{100}\right) \quad (4.4)$$

Farklı olay türleri ve tekrar düzeylerine göre örnek skorlar aşağıdaki şekilde belirlenmiştir.

- APT Saldırısı (Temel Skor = 5), 1 saat içinde 5 kez gerçekleştiğinde

$$\min(5, 5 + (50 + 5) / 100) = \min(5, 5{,}55) = 5{,}0 \quad (4.5)$$

- Port Tarama (Temel Skor = 1), 24 saat içinde 5 kez gerçekleştiğinde

$$\min(5, 1 + (25 + 1) / 100) = \min(5, 1{,}26) = 1{,}26 \quad (4.6)$$

- Brute Force Saldırısı (Temel Skor = 2), 7 gün içerisinde 3 kez gerçekleştiğinde

$$\min(5, 2 + (10 + 2) / 100) = \min(5, 2{,}12) = 2{,}12 \quad (4.7)$$

Bu sınırlandırılmış ayarlama yöntemi, düşük ciddiyetli ancak yüksek frekanslı saldırıların (örneğin port tarama, brute force) uygun şekilde öncelik kazanmasını sağlarken, APT gibi zaten yüksek etkili olayların puanlarının orantısız biçimde artmasını engeller.

4.2.5 Etkilenen Varlık Skoru (Affected Asset Score)

Bir güvenlik olayından etkilenen varlığın kritiklik düzeyi, olay müdahalesinin önceliklendirilmesinde temel belirleyicilerden biridir. Tüm varlıklar değer ve işlev açısından eşit değildir; örneğin bir SIEM sistemi veya ödeme altyapısına yönelik bir saldırı, misafir Wi-Fi ağına yönelik bir saldırıya kıyasla çok daha yüksek risk taşır.

Önerilen modelde, etkilenen varlıklar operasyonel önem ve güvenlik hassasiyeti temelinde beş düzeye ayrılarak sınıflandırılır ve her kategoriye karşılık gelen bir skor atanır. Bu sınıflandırma, SOC ekiplerinin olayın potansiyel etkisini daha doğru değerlendirmesine ve triyaj sürecinde kaynakları daha etkin biçimde tahsis etmesine olanak tanır.

Tablo 4.6, etkilenen sistemleri görev-kritik altyapılardan sandbox ortamlarına kadar operasyonel önem düzeylerine göre kategorize etmektedir.

Tablo 4.6 Etkilenen Sistemler İçin Varlık Kritikliğine Dayalı Puanlama

Etkilenen Varlık	**Puan**
Kritik Güvenlik Sistemleri (SIEM, IAM, DB, DC, IDS/IPS)	5
Bulut Altyapısı (Kubernetes Kümesi, Sanallaştırma Sunucusu)	5
Ödeme İşleme Sistemleri (PCI-DSS Ortamları)	5
E-posta Sunucusu	4
Kamuya Açık Web Sunucusu	4
VPN Geçidi	4
Kimlik ve Kimlik Doğrulama Sistemleri (SSO, MFA)	4
Önemli Uygulama Sunucusu	3
Kurum İçi İş Uygulamaları (ERP, CRM)	3
Dosya Sunucuları	3
Geliştirme Ortamları (CI/CD, Kod Depoları)	3
Standart İş İstasyonu (Genel Çalışan Cihazları)	2
Uzaktan Erişim Sistemleri (VDI, Uzak Masaüstü)	2
IoT/OT Cihazları (Endüstriyel Sistemler, Akıllı Cihazlar)	2
Bağımsız Sistem (Tek Başına Çalışan veya Düşük Riskli Sistem)	1
Misafir Wi-Fi Ağları	1
Test ve Korumalı Alan (Sandbox) Ortamları	1

Not: *Bu tabloda yer alan varlık kritiklik puanları, ilgili sistemlerin stratejik önemi, hassasiyet düzeyi ve güvenlik ihlali durumunda iş sürekliliği üzerindeki potansiyel etkileri dikkate alınarak uzman değerlendirmesiyle manuel olarak tanımlanmıştır.*

4.2.6 Tehdit İstihbaratı Skoru (Threat Intelligence Score)

Tehdit skoru, bir olayın bilinen bir tehdit aktöründen ya da yüksek riskli bir kaynaktan gelip gelmediğini değerlendirir. **APT grupları**, **botnet ağları** ve **dark web** kaynaklı göstergelerle ilişkilendirilen olaylara en yüksek öncelik verilir.

Tablo 4.7, tehdit kaynaklarının yapılandırılmış bir sınıflandırmasını ve bunlara atanan etkiye dayalı skorları sunmaktadır.

Tablo 4.7 Tespit Edilen Göstergelerin Tehdit İstihbaratına Dayalı Puanlaması

Tehtid Türü	**Puan**
Bilinen Tehdit Aktörü (APT, Darknet IP, Devlet Destekli Tehdit Grubu)	5
Ele Geçirilmiş Altyapı (C2 Sunucuları, Botnetler, Zararlı Yazılım Barındırıcıları)	5
Zararlı IP (Kara Liste, Tekrarlayan Saldırgan)	4
Kamuya Açık Bilinen Sömürülebilir Zafiyet (CVE Tabanlı Açıklar)	4
Yüksek Riskli Alan Adı (Oltalama, Sahte Giriş Sayfaları, Dolandırıcılık Siteleri)	4
Şüpheli Aktivite (Olağandışı Trafik Desenleri, Bilinmeyen Anomaliler)	3
Yeni Kaydedilmiş Alan Adları (Olası Oltalama veya C2 Sunucuları)	3
Coğrafi Olarak Olağandışı Erişim (Şüpheli Ülke veya TOR Çıkış Noktası))	3
Dış Alan Adında Geçersiz/Eski SSL Sertifikası	2
Güvensiz Protokol Tespiti (örn. HTTPS yerine HTTP kullanımı)	2
İç Ağ Trafiği (Doğrulanmamış ancak Kötü Amaçlı Olma İhtimali Düşük)	1
İç IP Adreslerinden İlk Kez Görülen Trafik	1

Not: *Bu tabloda sunulan tehdit puanları, yaygın tehdit göstergelerine ilişkin göreli risk düzeylerini yansıtmak amacıyla uzman görüşü ve alan bilgisine dayalı olarak manuel şekilde belirlenmiştir.*

4.2.7 Korelasyon Puanı (Correlation Score)

Korelasyon puanı, yeni bir olayın daha önce kaydedilmiş vakalara olan benzerliğini nicel olarak ifade eder ve bu sayede tekrar eden ya da evrimleşen

tehdit kalıplarının önceliklendirilmesini sağlar. Bu değerin hesaplanmasında, SOC analizlerinde yaygın olarak kullanılan üç temel gösterge dikkate alınmaktadır:

- **Kaynak IP (srcIP):** Saldırının başladığı adres
- **Hedef IP (dstIP):** Hedef alınan iç sistem adresi
- **Kullanıcı Adı (user):** Olayda yer alan kullanıcı hesabı

Her bir gösterge, geçmişteki eşleşme sıklığına ve atanmış önem ağırlığına göre puanlanmaktadır. Skorların yapay biçimde şişmesini önlemek amacıyla her bir gösterge için bir doygunluk eşiği (saturation threshold) tanımlanmıştır.

Değişkenler:

- M_i: Öznitelik i için geçmişteki eşleşme sayısı
- T_i: Öznitelik i için doygunluk eşiği
- CW_i: Öznitelik i için atanan korelasyon ağırlığı

Burada i ∈{srcIP, dstIP, user} kümesindedir.

Atanmış Değerler:

- CW_1=1,25, T_1=2 (Kaynak IP)
- CW_2=1,75, T_2=2 (Hedef IP)
- CW_3=2,0, T_3=3 (Kullanıcı Adı)

Formül:

$$Correlation\ Score = \boldsymbol{CW_1}\ x\ min\left(1, \frac{M_{srcIP}}{T_1}\right) + \boldsymbol{CW_2}\ x\ min\left(1, \frac{M_{drcIP}}{T_2}\right) + \boldsymbol{CW_3}\ x\ min\left(1, \frac{M_{user}}{T_3}\right) \quad (4.8)$$

Korelasyon puanı, olayların tarihsel benzerliğini, temel tanımlayıcılar (kaynak IP, hedef IP ve kullanıcı adı) üzerinden ağırlıklı doygunluk eşikleri aracılığıyla özetlemektedir. Bu metrik, frekans katkılarını normalize ederek ve etki düzeyini sınırlandırılmış biçimde uygulayarak (min(1, M/T)), bir yandan zaman içinde devam eden tehdit kalıplarının tespitini desteklerken, diğer yandan gürültü (noise) ve skor birikimi sorunlarını kontrol altında tutar.

Bireysel özniteliklerin korelasyon puanına nasıl katkı sağladığını gösteren örnek bir dağılım Tablo 4.8'de sunulmaktadır.

Tablo 4.8 Korelasyon Puanı Bileşenlerinin Dağılımı Örneği

Öznitelik	M_i	T_i	CW_i	Formül	Katkı
Kaynak IP	2	2	1.25	$1.25\ x\ min(1,\frac{2}{2})$	1,25
Hedef IP	1	2	1.75	$1.75\ x\ min(1,\frac{1}{2})$	0,875
Kullanıcı Adı	4	3	2.0	$2.0\ x\ min(1,\frac{4}{3})$	2,0

Not: *T_i (doygunluk eşiği) ve CWi (korelasyon ağırlığı), uzman görüşüne dayalı olarak statik biçimde tanımlanmış model parametreleridir.Katkı (Cont) = Öznitelik katkısı*

Toplam Korelasyon Puanı: 1,25 + 0,875 + 2.00 = 4,125

4.3 OLAY SENARYOSU

Bir kuruluşun Güvenlik Operasyon Merkezi (SOC), kamuya açık bir web sunucusu üzerinde, harici bir IP adresinden gelen olağandışı HTTP isteklerini tespit eder. 24 saatlik bir süre içerisinde, söz konusu IP adresi, farklı kullanıcı hesaplarını hedef alan beşten fazla SQL enjeksiyonu denemesi gerçekleştirmiştir. İlgili trafik, uygulama güvenlik duvarı (WAF) tarafından şüpheli olarak işaretlenmiş ve olay SIEM sistemi üzerinde bir alarm olarak tetiklenmiştir.

Tehdit istihbaratı kaynakları, saldırgan IP adresinin daha önce Darknet ortamlarında tanımlanmış, APT grubuna ait kötü niyetli bir aktörle ilişkili olduğunu göstermektedir. Geriye dönük analizler, aynı IP adresinin son yedi gün içinde iki SQL enjeksiyonu ve bir oltalama saldırısına neden olduğunu ortaya koymaktadır. Ayrıca, SIEM kayıtları, bu IP adresinin aynı hedef sistem ve kullanıcı adı ile ilişkilendirilmiş üç farklı olay ile eşleştiğini göstermektedir.

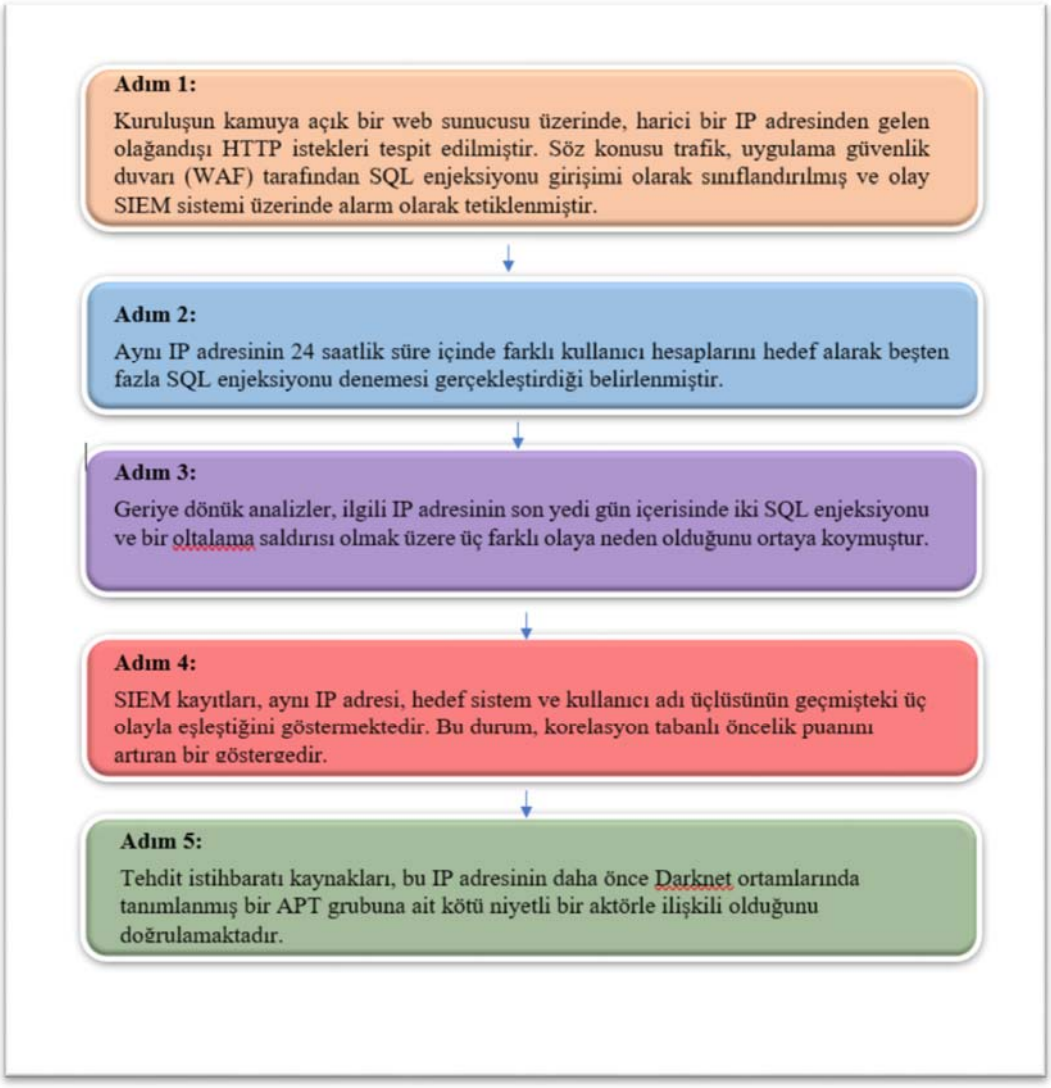
4.3.1 Olay Detayları ve Skor Hesaplaması

Kuruluşun kamuya açık web sunucusu üzerinde gerçekleştirilen bir SQL enjeksiyonu saldırısı tespit edilmiştir. Bu olay, uygulama güvenlik duvarı tarafından alarm olarak tanımlanmış olup saldırgan, daha önce tehdit istihbaratı veritabanlarında kötü niyetli olarak işaretlenmiş bir IP adresi kullanmaktadır. Söz konusu saldırı, önemli bir ERP uygulamasını barındıran sunucuyu hedef almış ve IP adresi, kullanıcı adı ve hedef sistem bilgileri açısından geçmişteki üç ayrı olayla eşleşmiştir. Olayın 24 saat içerisinde tekrarlanma sayısı beşin üzerinde olup, aynı türde saldırıların süreklilik göstermesi nedeniyle önceliklendirme düzeyi artırılmıştır.

Bu duruma ilişkin puanlama aşağıdaki şekilde yapılmaktadır:

- Ciddiyet: 2 (Yüksek) → 4 puan
- SLA Aciliyeti: 2 (Yüksek, <30 dakika) → (6 − 2) = 4 puan
- Olay Türü: SQL Enjeksiyon Saldırısı (SQL Injection) → 4 puan
- Tekrarlama: 24 saat içinde 5'ten fazla tekrar → R değeri 25 olarak belirlenir → min(5, 4 + (4 + 25)/100)) = 4,29 puan
- Etkilenen Varlık: Web Sunucusu (ERP uygulamasını barındıran web sunucusu) → 4 puan
- Tehdit İstihbaratı: Bilinen Tehdit Aktörü (APT ile ilişki) → 5 puan
- Korelasyon Puanı:
    - Kaynak IP: $M_{srcIP} = 3\ T_1 = 2\ CW_1 = 1.0 \rightarrow 1.25 \times \min\left(1, \frac{3}{2}\right) = 1{,}25$
    - Hedef IP: $M_{dstIP} = 3\ T_2 = 2\ CW_2 = 1.5 \rightarrow 1.75 \times \min\left(1, \frac{3}{2}\right) = 1.75$
    - KullanıcıAdı: $M_{user} = 3\ T_3 = 3\ CW_3 = 2.0 \rightarrow 2.0 \times \min\left(1, \frac{3}{3}\right) = 2$
- Toplam Korelasyon Puanı:1,25 + 1,75 + 2,0 = 5 puan
- Nihai Olay Puanı: 0,160 x 4 (Ciddiyet) + 0,135 x 4 (SLA) + 0,149 x 4 (Olay Türü) + 0,117 x 4,29 (Tekrarlama) + 0,156 x 4 (Varlık) + 0,149 x 5 (Tehdit) + 0,135 x 5 (Korelasyon) = 0,64 + 0,54 + 0,596 + 0,501 + 0,624 + 0,725 + 0,675 = 4,301 puan

Puanlama modelinin pratik etkilerini göstermek amacıyla, aşağıda tanımlanan SQL enjeksiyonu saldırısı senaryosu değerlendirilmiştir. Saldırı; keşif, sömürü, izinsiz erişim ve tehdit istihbaratı eşleşmeleri gibi çok aşamalı bir yapıya sahiptir. Bu olayın çok aşamalı yapısı Şekil 2'de görselleştirilmiş olup, olay müdahale zaman çizelgesine ilişkin kronolojik bir bakış sunmaktadır.



Şekil 4.2 SOC içerisindeki SQL enjeksiyonu saldırısı ve tespit sürecine ait adım adım zaman çizelgesi

4.4 ANALİST SKORLAMA – OLAY ATAMA SÜRECİ

Olayların analistlere etkin bir şekilde atanabilmesi için, iş yükü dengesi ve deneyim uyumu esas alınarak yapılandırılmış bir yaklaşım benimsenmiştir.

4.4.1 Adım 1: Analist Gruplarının ve Kapasitelerinin Tanımlanması

Analistler, uzmanlık düzeylerine göre beş kategoriye ayrılmaktadır:

- Kıdemli Analistler (Seviye 5): A_i
- İleri Düzey Orta Seviye Analistler (Seviye 4): A_j
- Orta Seviye Analistler (Seviye 3): A_k
- Yeni Başlayan Analistler (Seviye 2): A_l
- Stajyer Analistler (Seviye 1): A_m

Her analistin sahip olduğu maksimum kapasite ve mevcut iş yükü farklılık göstermektedir. Analist seviyelerine göre bu kapasite kısıtları Tablo 4.9'da özetlenmiştir.

Tablo 4.9 SOC'de Analist Seviyeleri, Olay Yükü ve Kapasite

Analist A_n	**Seviye L_n**	**Mevcut Olay Sayısı CI_n**	**Maksimum Kapasite MC_n**
A_i (Kıdemli)	5	CI_i	MC_i
A_j (İleri Düzey Orta Seviye)	4	CI_j	MC_j
A_k (Orta Seviye)	3	CI_k	MC_k
A_l (Yeni Başlayan)	2	CI_l	MC_l
A_m (Stajyer)	1	CI_m	MC_m

4.4.2 Adım 2: Olay Skoruna Göre Olayın Karmaşıklığını Belirleme

Hesaplanan olay puanı (Sm), olayın karmaşıklık düzeyini (Cm) belirlemek amacıyla kullanılmaktadır. Bu değer, olayın zorluk seviyesinin analist deneyimiyle eşleştirilerek uygun analist atamasını yönlendirmesini sağlar. Skorlama modeli 0–5 aralığında normalleştirildiği için, karmaşıklık düzeyleri de bu ölçekte yeniden kalibre edilmiştir. Eşik tabanlı olay karmaşıklığı sınıflandırması, normalleştirilmiş olay puanlarına göre Denklem (4.9)'da sunulmaktadır.

$$C_m = \begin{cases} 5, & \text{if } Sm \geq 4 \text{ (Kritik Karmaşıklık)} \\ 4, & \text{if } 3{,}2 \leq Sm < 4 \text{ (Yüksek Karmaşıklık)} \\ 3, & \text{if } 2{,}4 \leq Sm < 3{,}2 \text{ (Orta Karmaşıklık)} \\ 2, & \text{if } 1{,}6 \leq Sm < 2{,}4 \text{ (Düşük Karmaşıklık)} \\ 1, & \text{if } Sm < 1{,}6 \text{ (Çok Düşük Karmaşıklık)} \end{cases} \quad (4.9)$$

Bu sınıflandırma, sistemin olayları uygun deneyim düzeyine sahip analistlerle eşleştirmesini (EMF hesaplamasında kullanıldığı şekilde) mümkün kılmaktadır. Tablo 4.10, olay puanı değerleri ve bunlara karşılık gelen karmaşıklık sınıflarına ilişkin örnekleri bu ölçek temelinde sunmaktadır.

Tablo 4.10 Olay Skorları ve Karşılık Geldiği Karmaşıklık Seviyeleri

Olay I_m	**Olay Puanı S_m**	**Karmaşıklık Seviyesi C_m**
I_1	4.3	5 (Critical)
I_2	3.6	4 (High)
I_3	2.7	3 (Medium)
I_4	1.9	2 (Low)
I_5	1.3	1 (Very Low)

4.4.3 Adım 3: Analist Yük Faktörünün (ALF) Hesaplanması

Her bir analist için ALF□ (Analist Yük Faktörü) aşağıdaki formül kullanılarak hesaplanır:

$$\mathrm{ALF_n} = 1 + \frac{\mathrm{CI_n}}{\mathrm{MC_n}} \tag{4.10}$$

Burada:

- CI_n, analist A_n'ye şu anda atanmış olan olay sayısını,
- MC_n, analist A_n'nin maksimum kapasitesini ifade eder.

Tablo 4.11, farklı analist seviyeleri için örnek ALF hesaplamalarını ve elde edilen skorları göstermektedir.

Tablo 4.11 ALF Hesaplaması ve Elde Edilen Skorlar

Analist A_n	**Mevcut Olay Sayısı CI_n**	**Maksimum Kapasite MC_n**	**ALF Hesaplaması**	**ALF Puanı ALF_n**
A_1 (Kıdemli)	4	6	$1 + \frac{4}{6} = 1.67$	1.67
A_2 (İleri Orta Seviye)	3	5	$1 + \frac{3}{5} = 1.60$	1.60
A_3 (Orta Seviye)	2	7	$1 + \frac{2}{7} = 1.29$	1.29
A_4 (Yeni Başlayan)	3	6	$1 + \frac{3}{6} = 1.50$	1.50
A5 (Stajyer)	1	6	$1 + \frac{1}{6} = 1.17$	1.17

4.4.4 Adım 4: Deneyim Uyumluluk Faktörünün (EMF) Hesaplanması

Deneyim Uyumluluk Faktörü (EMF□), bir analistin olayın karmaşıklık düzeyiyle ne ölçüde örtüştüğünü belirler. Bu faktör, analistin deneyim seviyesi L_n ile olayın karmaşıklık seviyesi C_m karşılaştırılarak hesaplanır.

$$EMF_n = \begin{cases} 1, & if\ L_n = C_m \\ 0.75 & if\ L_n = C_m + 1 \\ 0.5, & if\ L_n = C_m + 2 \\ 0{,}25 & if\ L_n = C_m + 3 \\ 0 & if\ L_n < C_m \end{cases} \quad (4.11)$$

Burada:

- L_n, A_n analistinin seviyesini ifade eder ve 1 (Stajyer) ile 5 (Kıdemli) arasında değişir.
- C_m, I_m olayının karmaşıklık seviyesini temsil eder ve 1 (Çok Düşük Karmaşıklık) ile 5 (Kritik Karmaşıklık) aralığındadır.

Tablo 4.12, seçilmiş analist–olay eşleşmeleri için EMF skorlarını sunmakta olup, analist deneyiminin olayın karmaşıklığıyla ne ölçüde örtüştüğünü göstermektedir.

Daha yüksek EMF skorları, analistin deneyim düzeyinin olayın karmaşıklığı ile daha iyi örtüştüğünü gösterir. Analist seviyesi, olayın karmaşıklık seviyesine ne kadar yakınsa, EMF skoru da o kadar yüksek olur; bu da söz konusu analistin olayı ele almak için daha uygun olduğunu ifade eder.

Tablo 4.12 Analist–Olay Eşleştirmeleri İçin Deneyim Uyumluluk Faktörü (EMF) Skorları

Olay I_m	**Analist A_n**	**Analist Seviyesi L_n**	**Karmaşıklık Seviyesi C_m**	**EMF Puanı EMF_n**
I_1 (APT Saldırısı)	A_1 (Kıdemli)	5	5	1.00
	A_3 (Orta Seviye)	3	5	0.00

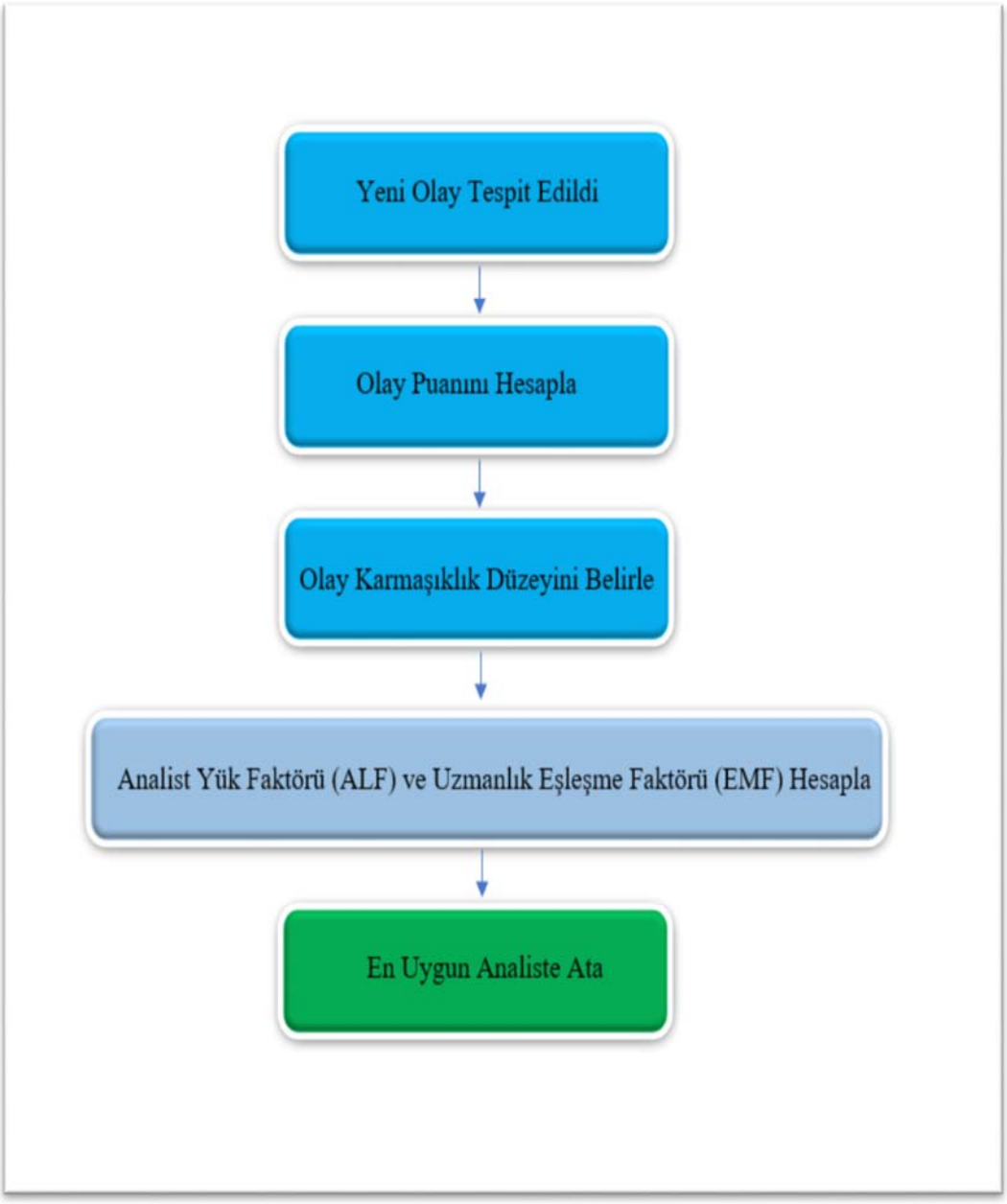
Tablo 4.12 (Devamı) Analist–Olay Eşleştirmeleri İçin Deneyim Uyumluluk Faktörü (EMF) Skorları

I_2 (Oltalama)	A_5 (Stajyer)	1	5	0.00
	A_2 (İleri Orta Seviye)	4	3	0.75
	A_4 (Yeni Başlayan)	2	3	0.00
I_3 (Port Taraması)	A3 (Orta Seviye)	3	1	0.50
	A5 (Stajyer)	1	1	1.00

Şekil 3, en uygun atamayı sağlamak üzere ALF ve EMF hesaplamalarını birleştiren tam analist eşleştirme mantığını özetlemektedir.

Bu süreç, skorlama, olay karmaşıklığı değerlendirmesi, ALF ve EMF hesaplamalarını bütünleştirerek analistlerin doğru biçimde atanmasını sağlar. ALF skoru, mevcut iş yükü yüksek olan analistlerin atama önceliğini düşürerek olayların mevcut personel arasında dengeli şekilde dağıtılmasına katkıda bulunur. EMF skoru ise bir analistin uzmanlık düzeyinin, olayın karmaşıklık seviyesiyle ne derece uyumlu olduğunu ölçer. Yüksek EMF ile düşük ALF değerinin birleşimi, en uygun analisti işaret eder.

Bu iki skor birlikte değerlendirildiğinde, olay atama süreci hem operasyonel verimlilik hem de uygunluk açısından optimize edilmiş olur.



Şekil 4.3 Analist eşleştirme akışı: olay değerlendirmesinden en uygun atamaya kadar olan süreç

Ayrıca, önerilen model; analist yorgunluğu metrikleri, uzmanlık etiketlerine (ör. bulut, uç nokta, kimlik) dayalı beceri yönlendirmesi ve yapay zekâ destekli anomali kümelendirmesi gibi gelecekteki genişletmelere de olanak tanıyarak uzun vadede ölçeklenebilirlik ve kişiselleştirme sağlamaktadır.

4.4.5 Adım 5: Nihai Analist Uygunluk Puanı

Belirli bir olay için bir analiste ait nihai uygunluk skoru, aşağıdaki formülle hesaplanmaktadır:

$$S_n = \frac{S_m \text{x } EMF_m}{ALF_n} \quad (4.12)$$

Burada:

- S_n: Analist A_n için nihai uygunluk skoru,
- S_m: Olay I_m için toplam olay skoru,
- EMF_n: Analist A_n'nin deneyim uyumluluk faktörü,
- ALF_n: Analist A_n'nin yük faktörünü ifade eder.

Bu puanlama mekanizmasını göstermek amacıyla, Tablo 4.13 ila 4.16, farklı olay türleri (APT saldırısı, oltalama, port tarama, olağandışı oturum davranışı) için tüm analistler bazında hesaplanan nihai uygunluk skorlarını sunmaktadır. Her bir tabloda, ilgili analist için ALF, EMF ve nihai skor hesaplamaları ayrıntılı olarak gösterilmektedir

Tablo 4.13 Olay 1 İçin Nihai Skor Hesaplaması (APT Saldırısı, Skor $S_1 = 4,63$)

Analist A_n	**ALF** ALF_n	**EMF** EMF_n	**Nihai Skor Hesaplaması** S_n	**Nihai Puan** (S_n)
A_1 (Kıdemli)	1,50	1,00	$\frac{4,63 \text{ x } 1,00}{1,50} = 3,08$	3,08
A_2 (İleri Orta Seviye)	1,40	0,00	$\frac{4,63 \text{ x } 0,00}{1,40} = 0,00$	0,00
A_3 (Orta Seviye)	1,30	0,00	$\frac{4,63 \text{ x } 0,00}{1,30} = 0,00$	0,00
A_4 (Yeni Başlayan)	1,60	0,00	$\frac{4,63 \text{ x } 0,00}{1,60} = 0,00$	0,00
A_5 (Stajyer)	1,20	0,00	$\frac{4,63 \text{ x } 0,00}{1,20} = 0,00$	0,00

Tablo 4.14 Olay 2 İçin Nihai Skor Hesaplaması (Oltalama Skor, S_2 = 1,92)

Analist A_n	**ALF** ALF_n	**EMF** EMF_n	**Nihai Skor Hesaplaması**	**Nihai Puan** (S_n)
A_1 (Kıdemli)	1,50	0,50	$\frac{1,92 \text{ x } 0,50}{1,50} = 0,64$	0,64
A_2 (İleri Orta Seviye)	1,40	0,75	$\frac{1,92 \text{ x } 0,75}{1,40} = 1,03$	1,03
A_3 (Orta Seviye)	1,30	1,00	$\frac{1,92 \text{ x } 1,00}{1,30} = 1,47$	1,47
A_4 (Yeni Başlayan)	1,60	0,00	$\frac{1,92 \text{ x } 0,00}{1,60} = 0,00$	0,00
A_5 (Stajyer)	1,20	0,00	$\frac{1,92 \text{ x } 0,00}{1,20} = 0,00$	0,00

Tablo 4.15 Olay 3 İçin Nihai Skor Hesaplaması (Port Taraması, Skor S_3 = 1,45)

Analist A_n	**ALF** ALF_n	**EMF** EMF_n	**Nihai Skor Hesaplaması** S_n	**Nihai Puan** (S_n)
A_1 (Kıdemli)	1,50	0,25	$\frac{1,45 \; x \; 0,25}{1,50} = 0,24$	0,24
A_2 (İleri Orta Seviye)	1,40	0,50	$\frac{1,45 \; x \; 0,50}{1,40} = 0,51$	0,51
A_3 (Orta Seviye)	1,30	0,75	$\frac{1,45 \; x \; 0.75}{1,30} = 0,83$	0,83
A_4 (Yeni Başlayan)	1,60	1,00	$\frac{1,45 \; x \; 1,00}{1,60} = 0,90$	0,90
A_5 (Stajyer)	1,20	0,00	$\frac{1,45 \; x \; 0,25}{1,50} = 0,24$	0,24

Tablo 4.16 Olay 4 İçin Nihai Skor Hesaplaması (Olağandışı Oturum Davranışı, Skor S_4 = 2,33)

Analist A_n	**ALF** ALF_n	**EMF** EMF_n	**Nihai Skor Hesaplaması** S_n	**Nihai Puan** (S_n)
A_1 (Kıdemli)	1,50	0,50	$\frac{2,33\ x\ 0,50}{1,50} = 0,77$	0,77
A_2 (İleri Orta Seviye)	1,40	0,75	$\frac{2,33\ x\ 0,75}{1,40} = 1,24$	1,24
A_3 (Orta Seviye)	1,30	1,00	$\frac{2,33\ x\ 1,00}{1,30} = 1,79$	1,79
A_4 (Yeni Başlayan)	1,60	0,00	$\frac{2,33\ x\ 0,00}{1,60} = 0,00$	0,00
A_5 (Stajyer)	1,20	0,00	$\frac{2,33\ x\ 0,00}{1,20} = 0,00$	0,00

Her bir olay için en yüksek uygunluk puanına sahip analisti belirleyerek uzmanlık ve iş yükü dengesini esas alan optimize edilmiş atamaların yapılmasına olanak tanıyan özet sonuçlar, Tablo 4.17'da sunulmaktadır.

Tablo 4.17 Nihai Skora Göre Her Olay İçin En Uygun Analist Ataması

Olay I_m	**En Uygun Analist** A_n	**Nihai Skor** (S_n)
I_1 ((APT Saldırısı)	A_1 (Kıdemli)	3.08
I_2 (Oltalama)	A_3 (Orta Seviye)	1.47
I_3 (Port Taraması)	A_4 (Yeni Başlayan)	0.90
I_4 (Olağandışı Oturum Davranışı)	A_3 (Orta Seviye)	1.79

Aşağıda sunulan yalancı kod (pseudocode), olay skorlama ve atama sürecinin iki aşamalı tam yapısını özetlemektedir:

- Algoritma 1, olay değerlendirmesini ve analist profil oluşturma işlemlerini gerçekleştirir.
- Algoritma 2, analist–olay eşleştirmesini yapar ve her olayı, hesaplanan skorlara dayanarak en uygun analiste atar.

Algoritma 1 Bölüm 1 – Olay Puanlama ve Analist Profilleme

1: Input:

2: $I = \{I_1, I_2, \ldots, I_m\}$ ▯ Set of incidents

3: $A = \{A_1, A_2, \ldots, A_n\}$ ▯ Set of analysts

4: CI_n: Current incident count for analyst A_n

5: MC_n: Max capacity for analyst A_n

6: L_n: Analyst A_n's experience level (1–5)

7: Incident features: S_{sev} , S_{sla}, S_{type}, S_{rep}, S_{asset} , S_{ti}, S_{corr}

8: Feature weights: w_{sev}, w_{sla}, w_{type}, w_{rep}, w_{asset}, w_{ti}, w_{cor}

9: Adım 1: Toplam Olay Puanını ve Karmaşıklık Seviyesini Hesapla

10: for $I_m \in I$ do

11: $S_m \leftarrow (w_{sev} \times S_{sev}) + (w_{sla} \times S_{sla}) + (w_{type} \times S_{type}) + (w_{rep} \times S_{rep}) + (w_{asset} \times S_{asset}) + (w_{ti} \times S_{ti}) + (w_{cor} \times S_{cor})$

12: if $S_m \geq 4$ then

13: $C_m \leftarrow 5$ ▯ Critical

14: else if $S_m \geq 3.2$ then

15: $C_m \leftarrow 4$ ▯ High

16: else if $S_m \geq 2.4$ then

17: $C_m \leftarrow 3$ ▯ Medium

18: else if $S_m \geq 1.6$ then

19: $C_m \leftarrow 2$ ▯ Low

20: else

21: $C_m \leftarrow 1$ ▯ Very Low

22: end if

23: end for

24: Adım 2: Analist Yük Faktörünü (ALF) Hesapla

25: for An ∈ A do

26: $ALFn \leftarrow 1 + \frac{CI_n}{MC_n}$

27: **end for**

Algoritma 2 Bölüm 2 – Analist Eşleştirme ve Olay Atama

1: Adım 3: Deneyim Uyumluluk Faktörünü (EMF) Hesapla

2: for $I_m \in I$ do

3: for $A_n \in A$ do

4: if $L_n = C_m$ then

5: $EMF_{n,m} \leftarrow 1$

6: else if $L_n = C_m + 1$ then

7: $EMF_{n,m} \leftarrow 0.75$

8: else if $L_n = C_m + 2$ then

9: $EMF_{n,m} \leftarrow 0.5$

10: else if $L_n = C_m + 3$ then

11: $EMF_{n,m} \leftarrow 0.25$

12: else

13: $EMF_{n,m} \leftarrow 0$

14 : end if

15: end for

16: end for

17: Adım 4: Nihai Uygunluk Değerini Hesapla ve Olayları Ata

18: for $I_m \in I$ do

19: best score $\leftarrow -\infty$

20: assigned $\leftarrow$ None

21: for $A_n \in A$ do

22: $S_{n,m} \leftarrow S_m \, x \frac{EMF_{n,m}}{ALF_n}$

23: if $S_{n,m}$ > best score then

24: best score $\leftarrow S_{n,m}$

25: assigned $\leftarrow A_n$

26 : end if

27: end for

28: Assign $I_m \rightarrow$ assigned

29: end for

30: Return all $\{I_m \rightarrow A_n\}$ assignments

Bu bölümde, puanlama ve eşleştirme mantığının uygulamada nasıl işlediğini göstermek amacıyla, üç olay ve iki analisti içeren adım adım bir örnek senaryo sunulmaktadır.

Önerilen skorlama ve atama çerçevesinin pratik uygulanabilirliğini göstermek için, üç farklı güvenlik olayı ve iki SOC analistini içeren sadeleştirilmiş bir örnek olay çalışması (case study) sunulmuştur. Her olay, yedi skorlama faktörü kullanılarak değerlendirilmiş; analistler ise ALF ve EMF metrikleriyle profillenmiştir. Nihai analist–olay ataması, uygunluk skoruna dayalı olarak gerçekleştirilmiştir.

BÖLÜM 5

5. OLAY ÖZETİ

Bu bölüm, puanlama ve eşleştirme mantığının pratikte nasıl işlediğini göstermek amacıyla üç olay ve iki analisti içeren adım adım bir örnek sunmaktadır.

Önerilen puanlama ve atama çerçevesinin pratik uygulanabilirliğini göstermek amacıyla, üç farklı olayı ve iki SOC analistini içeren sadeleştirilmiş bir örnek vaka çalışması sunulmuştur. Her bir olay, yedi puanlama faktörü kullanılarak değerlendirilmiş; analistler ise ALF ve EMF metrikleri aracılığıyla profillenmiştir. Nihai analist-olay ataması ise uygunluk skoruna (suitability score) dayalı olarak gerçekleştirilmiştir.

5.1.1 Olay Özeti

Tablo 5.1, bu örnek olay çalışmasında kullanılan üç örnek olayın temel özniteliklerini özetlemektedir.

Tablo 5.1 Vaka Çalışması İçin Olay Özellikleri ve Skorlama Girdileri

Olay ID	Olay Türü	Sev	SLA (saat)	AsC	Tekrarlama	TI	Korelasyon
I1	Oltalama E-postası	3	4	2	0	1	1
I2	Fidye Yazılımı Tespiti	5	1	5	1	2	3
I3	Ayrıcalık Yükseltme	4	2	4	2	3	2

Not: *Her bir faktör, 1-5 aralığında normalize edilmiş bir skordur. Yüksek puanlar daha yüksek öncelik anlamına gelir. Sev = Severity, AsC= Asset Criticality, TI = Threat Intel,*

Her bir olay, ciddiyet, SLA aciliyeti, varlık kritikliği, tekrarlama sıklığı, tehdit istihbaratı ilişkisi ve korelasyon göstergeleri dahil olmak üzere yedi normalleştirilmiş skorlama girdisine dayalı olarak tanımlanmıştır. Bu yapılandırılmış öznitelikler, olay skorlarının hesaplanmasında temel teşkil eder ve farklı alarm türleri arasında tutarlı bir önceliklendirme yapılmasına olanak tanır. Özellikle, Olay I2, en yüksek ciddiyet ve tekrar düzeylerine sahip olması nedeniyle en kritik vakayı temsil ederken; I1, düşük tehdit göstergeleriyle nispeten daha düşük öncelikli bir duruma işaret etmektedir.

5.1.2 Olay Skorlaması

Her bir olay için nihai puanı hesaplamak amacıyla, önerilen çerçeve; ciddiyet (Sev), SLA aciliyeti (SLA), varlık kritiklik düzeyi (AsC), tekrarlama sıklığı (Rep), tehdit istihbaratı (TI), korelasyon skoru (Cor) ve olay türü (Type) olmak üzere yedi kritik olay özniteliğini içeren ağırlıklı bir toplama modeli kullanmaktadır. Bu model, özniteliklerin eşit önemde olduğunu varsaymak yerine, her bir faktöre uzman tanımlı ağırlıklar uygulamakta olup bu yaklaşım Bölüm 4.2'de biçimsel olarak tanımlanmıştır.

Olay I1 (Oltalama E-postası):

$$SI1 = (0.149 \times 3) + (0.160 \times 3) + (0.135 \times 4) + (0.156 \times 2) + (0.117 \times 0) + (0.149 \times 1) + (0.135 \times 1)$$

$$= 0.447 + 0.480 + 0.540 + 0.312 + 0.000 + 0.149 + 0.135 = 2.063$$

Olay I2 (Fidye Yazılımı Tespiti):

$$SI2 = (0.149 \times 5) + (0.160 \times 5) + (0.135 \times 1) + (0.156 \times 5) + (0.117 \times 1) + (0.149 \times 2) + (0.135 \times 3)$$

$$= 0.745 + 0.800 + 0.135 + 0.780 + 0.117 + 0.298 + 0.405 = 3.280$$

Olay I3 (Ayrıcalık Yükseltme):

$$SI3 = (0.149 \times 4) + (0.160 \times 4) + (0.135 \times 2) + (0.156 \times 4) + (0.117 \times 2) + (0.149 \times 3) + (0.135 \times 2)$$

$$= 0.596 + 0.640 + 0.270 + 0.624 + 0.234 + 0.447 + 0.270 = 3.081$$

Bu ağırlıklı puanlar, olayın karmaşıklık düzeyinin belirlenmesinde temel teşkil etmekte ve sonraki bölümlerde açıklanan analist atama sürecine girdi sağlamaktadır. Özellikle, I2 numaralı olay, yüksek ciddiyet seviyesi, kritik varlık üzerindeki etkisi ve güçlü korelasyon göstergeleri nedeniyle en yüksek puanı almıştır. Buna karşılık, I1 numaralı olay, düşük tekrarlama oranı ve tehdit istihbaratıyla zayıf ilişkisi nedeniyle en düşük puanı almıştır.

5.1.3 Analist Profilleri

Bu adımda, her bir analistin belirli bir olaya uygunluğu, Bölüm 4.4.5'te tanımlanan güncellenmiş puanlama formülü kullanılarak hesaplanmaktadır.

Tablo 5.2 ALF ve EMF Değerleriyle Analist Profilleri

Analist Kimliği	Uzmanlık Etiketleri	Yük (ALF)	EMF I1	EMF I2	EMF I3
A1	E-posta, SIEM	0.3	0.9	0.3	0.5
A2	Zararlı Yazılım Ayrıcalık Yükseltme	0.6	0.5	0.8	0.9

Not: *EMF, olayın karmaşıklık düzeyi ile analistin uzmanlık düzeyi arasındaki uyum derecesini yansıtmaktadır. Düşük ALF değerleri, analistin daha yüksek müsaitliğini ifade eder ve bu nedenle atama için daha uygun kabul edilir.*

Analist A1, e-posta ve SIEM uyarıları konusunda uzmanlaşmış olup, Olay I1 ile daha yüksek düzeyde deneyim uyumu göstermektedir. Buna karşılık, A2, ayrıcalık yükseltme ve zararlı yazılım (malware) temelli tehditlerle daha güçlü bir uyum sergilemektedir. ALF metriği, analistin mevcut iş yükünü yansıtarak, daha düşük iş yüküne sahip olan A1'i tercih edilir kılmaktadır. Bu metrikler, analist–olay atama sürecine yön veren nihai uygunluk skorunun hesaplanmasına birlikte katkı sağlamaktadır.

5.1.4 Analist Uygunluk Skorlaması

Bu adımda, her bir analistin belirli bir olaya uygunluğu, Bölüm 4.4.5'te tanımlanan puanlama formülü kullanılarak hesaplanmaktadır.

$$S_n = \frac{S_m x\ EMF_m}{ALF_n} \quad (5.1)$$

Uygunluk skoru, EMF değerinin artmasıyla yükselir, ALF değerinin artmasıyla ise azalır. Tablo 5.2, gerekli ALF ve EMF değerlerini sunmakta olup, burada Bölüm 5.1.2'de daha önce hesaplanan olay puanları kullanılmaktadır.

- Olay I1:

A1: $2.063 \text{ x } \left(\frac{0.9}{0.3}\right) = 2.063 \text{ x } 3.00 = 6.189$

A2: $2.063 \text{ x } \left(\frac{0.5}{0.6}\right) = 2.063 \text{ x } 0.833 = 1.718$ → A1'e atanmıştır

- Olay I2:

A1: $3.280 \text{ x } \left(\frac{0.3}{0.3}\right) = 3.280 \text{ x } 1.00 = 3.280$

A2: $3.280 \text{ x } \left(\frac{0.8}{0.6}\right) = 3.280 \text{ x } 1.33 = 4.362$ → A2'ye atanmıştır

- Olay I3:

A1: $3.081 \text{ x } \left(\frac{0.5}{0.3}\right) = 3.081 \text{ x } 1.67 = 5.145$

A2: $3.081 \text{ x } \left(\frac{0.9}{0.6}\right) = 3.081 \text{ x } 1.50 = 4.621$ → A1'ye atanmıştır

5.1.5 Nihai Atama Tablosu

Tablo 5.3, olay önceliklendirmesi ile analist uygunluğunu birlikte ele alan bütünleşik skorlama modeline dayalı olarak gerçekleştirilen nihai analist–olay atama kararlarını sunmaktadır. Her satır, puanlanmış bir olay ile, operasyonel aciliyet ve mevcut uzmanlık düzeyi dikkate alınarak en uygun analist arasındaki eşleşmeyi yansıtmaktadır.

Tablo 5.3 Uygunluk Skorlarıyla Nihai Analist–Olay Atama Kararları

Olay	Nihai Olay Skoru	Atanan Analist	Uygunluk Skoru
I1	2,063	A1	6,189
I2	3,280	A2	4,362
I3	3,081	A1	5,145

Olay I2, 3,280 ile en yüksek olay puanını (S_m) almış olup, orta düzeyde bir iş yüküne sahip olmasına rağmen güçlü bir uzmanlık uyumu (EMF: 0,8) gösteren Analist A2'ye atanmıştır. Elde edilen uygunluk skoru olan 4,362, bu yüksek öncelikli fidye yazılımı olayını yönetmek için A2'nin en etkili seçenek olduğunu doğrulamaktadır.

Biraz daha düşük bir puana (3,081) sahip olan Olay I3, daha düşük bir iş yüküne (ALF: 0,3) ve orta düzeyde bir uzmanlık uyumuna (EMF: 0,6) sahip olan Analist A1'e yönlendirilmiştir. Bu durum sonucunda elde edilen uygunluk skoru olan 5,145, analist kullanılabilirliğinin belirleyici bir rol oynadığı stratejik bir iş yükü dağılımını ortaya koymaktadır.

En düşük öncelikli olay olan I1 (puan: 2,063), aynı zamanda A1'e atanmıştır. A1'in yüksek bir EMF skoru (0,9) ve minimum düzeyde iş yükü göstermesi, 6,189 gibi güçlü bir uygunluk skoru ile sonuçlanmıştır. Bu karar, modelin daha düşük riskli olayları alanında uzman ve uygun durumda olan analistlerle eşleştirme eğilimini yansıtmakta ve böylece daha karmaşık tehditler için özel kaynakların korunmasını sağlamaktadır.

Genel olarak, bu atama stratejisi, olay önceliği ile analist uyumu arasında dengeli bir optimizasyon gerçekleştirmektedir. İş yükü ve uzmanlık ölçütlerini dinamik biçimde birleştiren bu çerçeve, kritik olaylara zamanında müdahale sağlarken, SOC ortamı genelinde sürdürülebilir bir analist kapasitesini korumaktadır.

Önerilen modelin pratik geçerliliğini daha fazla desteklemek amacıyla, sonraki değerlendirme senaryolarında (Bölüm 5.2), CICIDS2017 veri kümesinden etiketlenmiş saldırı izleri kullanılmaktadır. Bu deneyler, modelin farklı olay ve analist profilleri altında gerçek SOC verileriyle uygulandığında ölçeklenebilirlik ve uyarlanabilirlik özelliklerini ortaya koymaktadır.

5.2 BENCHMARK SOC VERİLERİYLE AMPİRİK DEĞERLENDİRME

Önerilen çerçevenin gerçek dünya uygulamalarına uygunluğunu doğrulamak amacıyla, CICIDS2017 veri kümesinden etiketlenmiş olay örnekleri kullanılarak kıyaslama (benchmark) değerlendirmesi gerçekleştirilmiştir. Bu bölümde; puanlama sonuçları (Bölüm 5.2.1), meta veriler ve saldırı özellikleri (Bölüm 5.2.2) ile uygunluk puanlarına dayalı analist atama sonuçları (Bölüm 5.2.3) sunulmaktadır.

5.2.1 Benchmark Olaylarına Ait Puanlama Sonuçları

Tablo 5.4, her bir olay için ciddiyet, SLA aciliyeti, varlık kritiklik düzeyi, tekrarlama, tehdit istihbaratı, korelasyon ve olay türü olmak üzere yedi model boyutunda yer alan ham öznitelik değerlerini özetlemektedir. Bu ağırlıklandırılmamış değerler, Tablo 5.5'te sunulan nihai öncelik puanı hesaplamasında girdi olarak kullanılmaktadır.

Tablo 5.4 Değerlendirilecek Olaylara Ait Yedi Boyutlu Öznitelik Skorları

Olay Kodu	Ciddiyet	SLA	Varlık	Tekrarlama	Tehtid İstihbaratı	Korelasyon	Olay Türü
I1	3	4	2	2	1	1	2
I2	4	2	2	3	2	3	2
I3	4	2	2	3	3	2	3

I4	5	1	5	1	4	2	5
I5	3	3	2	2	2	1	4

Tablo 5.4 (Devamı) Değerlendirilecek Olaylara Ait Yedi Boyutlu Öznitelik Skorları

I6	4	2	2	1	2	2	4
I7	2	4	1	1	2	1	3
I8	5	1	2	3	4	3	5
I9	2	4	2	2	1	1	1
I10	5	1	2	3	3	3	5

Not: *Bu tablo, her olay için yedi boyutta ölçülen ham öznitelik puanlarını göstermektedir. Ağırlıklı nihai önceliklendirme puanları, Tablo 5.5'te sunulmaktadır.*

Önceki tabloda (Tablo 5.4), karşılaştırmalı görselleştirme amacıyla ciddiyet, SLA aciliyeti, varlık kritiklik düzeyi gibi ham olay öznitelikleri listelenmiştir. Bu değerler, orijinal yani ağırlıklandırılmamış puanları temsil etmekte olup doğrudan nihai önceliklendirme hesaplamasında kullanılmamaktadır.

Güvenilir bir önceliklendirme sonucu elde edebilmek için, bu öznitelikler normalize edilir ve Bölüm 4.2'de belirtilen uzman tanımlı ağırlıklarla çarpılır. Her bir olay için nihai olay puanı (incident score) aşağıdaki formül kullanılarak hesaplanmaktadır:

$$S_m = W_{sev}\, x\, S_{Sev} + W_{SLA}\, x\, S_{SLA} + W_{type}\, x\, S_{type} + W_{rep}\, x\, S_{rep} + W_{asset}\, x\, S_{asset} + W_{ti}\, x\, S_{ti} + W_{cor}\, x\, S_{Cor} \quad (5.2)$$

Buradaki ağırlıklar (w_i), uzman anketleri aracılığıyla ampirik olarak belirlenmiş olup, toplamlarının 1'e eşit olacak şekilde normalize edilmiştir. Tablo 5.5, ham değerlerden hesaplanan nihai ağırlıklı puanları özetlemektedir.

Tablo 5.5 Nihai Ağırlıklı Olay Puanları

Olay Kodu	**N**ihai Puan (S_m)
I1	2.148
I2	2.574
I3	2.737
I4	3.443
I5	2.460
I6	2.503
I7	2.013
I8	3.344
I9	1.839
I10	3.195

Not: *Nihai puanlar (S_m), analist eşleştirme ve olay karmaşıklığı sınıflandırmasında kullanılan normalize edilmiş ve ağırlıklandırılmış önceliklendirme değerlerini ifade etmektedir.*

5.2.2 Olaylara Ait Meta Veriler ve Tehdit Tipolojisi

Seçilen vakalar; kaba-kuvvet girişimleri, açık sömürmeye dayalı saldırılar, DDoS saldırıları ve sızma yöntemleri gibi çeşitli tehdit tipolojilerini yansıtmaktadır. Her olay, veri seti içerisinde hem dış hem de iç sistemlerle eşleştirilmiş ve hedef alınan varlık sınıfına göre konumlandırılmıştır.

Saldırgan IP'si, hedef IP'si, etkilenen varlık ve kullanılan saldırı tekniği gibi olaylara ait ayrıntılı meta veriler Tablo 5.6'te özetlenmiştir.

Tablo 5.6 CICIDS2017 Veri Setinden Elde Edilen Olay Tanımları (Sharafaldin vd., 2018)

Olay Kodu	Tarih	Saldırı Türü	Saldırgan IP Adresi	Hedef IP Adresi	Etkilenen Varlık	Kullanılan Teknik
I1	04.07	FTP-Patator	205.174.165.73	192.168.10.50	Web Server	Kaba Kuvvet
I2	04.07	SSH-Patator	205.174.165.73	192.168.10.50	Web Server	Kaba Kuvvet
I3	05.07	DoS Hulk	205.174.165.73	192.168.10.50	Web Server	Hizmet Engelleme
I4	05.07	Heartbleed	205.174.165.73	192.168.10.51	Ubuntu12 Server	Açık Sömürme
I5	06.07	SQL Injection	205.174.165.73	192.168.10.50	Web Server	Web Saldırısı
I6	06.07	Sızma (Dropbox)	205.174.165.73	192.168.10.8	Windows Vista	Sızma
I7	06.07	Sızma (Cool Disk)	205.174.165.73	192.168.10.25	MAC	Sızma
I8	07.07	Botnet ARES	205.174.165.73	Multiple Targets	Win 10/8/Vista	Botnet
I9	07.07	Port Tarama	205.174.165.73	192.168.10.50	Ubuntu16	Keşif
I10	07.07	DDoS LOIT	205.174.165.69–71	192.168.10.50	Ubuntu16	Dağıtık Hizmet Engelleme

Not: *Bu tablo, CICIDS2017 veri setinden alınan gerçek olay örneklerini listelemekte olup, puanlama ve atama işlemleri için ampirik veri girişi olarak kullanılmaktadır.*

5.2.3 Analist Atama Sonuçları

Analist–olay eşlemesini desteklemek amacıyla, farklı uzmanlık ve iş yükü seviyelerine sahip sentetik analist profilleri tanımlanmıştır. Her bir analiste, 1 (Stajyer) ile 5 (Kıdemli) arasında değişen bir deneyim seviyesi (Ln) atanmış ve mevcut iş yükünü maksimum kapasitesine oranla yansıtan bir Analist Yük Faktörü (ALF) değeri belirlenmiştir. Bu parametreler, her bir analistin değerlendirme kapsamındaki olaylara uygunluğunu ölçmek için kullanılmıştır. Bu değerlendirmede kullanılan sentetik analist profilleri Tablo 5.7'de sunulmaktadır.

Tablo 5.7. Değerlendirmede Kullanılan Analist Profilleri

Analist	Deneyim Seviyesi L_n	ALF
A1	5 (Kıdemli)	0.30
A2	4 (İleri Orta Seviye)	0.40
A3	3 (Orta Seviye)	0.50
A4	2 (Yeni Başlayan)	0.60
A5	1 (Stajyer)	0.70

Not: *CICIDS2017 veri kümesi, analistlere ilişkin meta veriler içermemektedir. Bu nedenle, deneyim seviyeleri ve ALF değerleri, farklı iş yükleri ve uzmanlık düzeylerine sahip gerçekçi bir analist havuzunu simüle etmek amacıyla sentetik olarak atanmıştır.*

Bölüm 5.2.1'de hesaplanan olay karmaşıklık seviyeleri (C_m) ve Tablo 5.7'de özetlenen analist profilleri kullanılarak, her bir analist–olay eşleşmesi için EMF değeri; analistin deneyim seviyesi (L_n) ile olayın karmaşıklık düzeyinin karşılaştırılması yoluyla belirlenmiştir. Uygunluk puanları ise, Bölüm 4.4.5'te tanıtılan modelin resmi uygunluk fonksiyonu kullanılarak hesaplanmıştır.

$$S_n = \frac{S_m x\ EMF_m}{ALF_n}$$

Daha yüksek bir Sn skoru, analist ile olay arasındaki uygunluğun daha yüksek olduğunu, uzmanlık düzeyi ile iş yükü arasında dengeli bir eşleşme sağlandığını göstermektedir. Seçilen analist ve hesaplanan uygunluk puanlarını içeren nihai atama sonuçları Tablo 5.8'de sunulmuştur.

Tablo 5.8 Uygunluk Skoruna Dayalı Analist Atama Sonuçları

Olay Kodu	Atanan Analist	Olay Skoru (S_m)	EMF (Deneyim Uyumu)	ALF (İş Yükü Faktörü)	Uygunluk Skor (S_n)
I1	A3	2.148	1.00	0.50	4.296
I2	A3	2.574	1.00	0.50	5.148
I3	A3	2.737	1.00	0.50	5.474
I4	A2	3.443	1.00	0.40	8.608
I5	A2	2.460	0.75	0.40	4.613
I6	A2	2.503	0.75	0.40	4.692
I7	A4	2.013	0.50	0.60	3,355
I8	A1	3.344	0.75	0.30	8.360
I9	A3	1.839	1.00	0.50	3.678
I10	A2	3.195	1.00	0.40	7.988

Not: *Uygunluk puanları, model formülü olan $S_n = (S_m \times EMF_n) / ALF_n$ kullanılarak hesaplanmıştır. Her bir olay, uzmanlık ve iş yükü dengesinin en uygun şekilde sağlanabilmesi için en yüksek S_n değerine sahip analiste atanmıştır.*

Tablo 5.8'de gösterildiği üzere, her bir olay için en yüksek uygunluk puanına sahip analistler seçilmiştir. Özellikle, I4, I8 ve I10 gibi yüksek karmaşıklığa sahip olayların, daha düşük ALF değerlerine sahip kıdemli veya ileri düzey analistlere tutarlı bir şekilde atanması, modelin öncelikli olaylara müdahalede analist kapasitesi ile uzmanlık arasında denge kurmadaki etkinliğini yansıtmaktadır.

Bu değerlendirmede kullanılan puanlama mantığı, talep üzerine paylaşılabilir (bkz. Sonuç ve Öneriler).

SONUÇ VE ÖNERİLER

Olay atama süreci, her olayın; ciddiyet düzeyi, SLA aciliyeti ve karmaşıklığı gibi çoklu faktörler temelinde en uygun analiste yönlendirilmesini garanti eder. Modelin öne çıkan katkıları şunlardır:

- **Kısa SLA Aciliyeti:** Daha kısa SLA süresine sahip olaylar daha hızlı çözüme ulaştırılması gerektiğinden önceliklendirilir.
- **Karmaşık Olaylar:** Daha yüksek karmaşıklık skoruna sahip olaylar, kıdemli veya ileri düzey orta seviye analistlere atanırken; daha basit olaylar junior veya stajyer analistlere yönlendirilir.
- **İş Yükü Dengeleme:** Analistlerin iş yükü, ALF metriği kullanılarak dengelenir ve hiçbir analistin aşırı yüklenmesine izin verilmez.
- **Deneyim Uyumu:** EMF metriği, olay karmaşıklığı ile analistin deneyim seviyesi arasındaki uyumu sağlar.
- **Dinamik Atama:** Atama süreci gerçek zamanlı verilerle yeniden hesaplanır, böylece her zaman en uygun analist, en kritik olayı ele alır.
- **Tehdit İstihbaratı:** Bilinen tehdit aktörleri ve etkilenen varlıkların türü, yüksek riskli olaylara öncelik verilmesini sağlamak için atama sürecine dâhil edilir.
- **Nihai Atamalar:** Yukarıda belirtilen hesaplamalar doğrultusunda, kritik olaylar kıdemli analistlere, orta düzey olaylar orta seviye analistlere, düşük önem derecesine sahip olaylar ise junior veya stajyer analistlere atanacak şekilde dinamik olarak düzenlenir.
- **Vaka Çalışması Uygulaması:** Yapay olarak oluşturulan bir vaka çalışması, modelin mantığını doğrulamış ve yüksek öncelikli olayların (örneğin I2, skor 2.86) analist uygunluğu mükemmel olmasa da doğru şekilde yönlendirildiğini; düşük öncelikli olayların (örneğin I1) ise uzmanlık temelli eşleşmelerle atandığını göstermiştir. Bu durum, modelin öncelik ve analist uyumu arasındaki dinamik dengeyi başarıyla kurabildiğini ortaya koymaktadır.

Bu süreç, her olayın doğru analiste yönlendirilmesini sağlayarak müdahale süresini optimize eder ve kurumsal güvenlik operasyonlarının bütünsel etkinliğini artırır.

CICIDS2017 olaylarıyla yapılan ampirik doğrulama, önerilen çerçevenin olayları analist deneyimi ve iş yüküyle uyumlu şekilde etkili bir biçimde önceliklendirdiğini ve atadığını doğrulamıştır.

Tartışma ve Sınırlılıklar

Önerilen olay atama çerçevesi, SOC ortamlarında olayların önceliklendirilmesi ve etkin şekilde dağıtılması için hem teknik risk göstergelerine hem de analist niteliklerine dayanan yapılandırılmış ve kapsamlı bir yaklaşım sunmaktadır. Model; ciddiyet düzeyi, SLA aciliyeti, tehdit istihbaratı ve korelasyon skorları gibi olay odaklı faktörleri, analiste özel öznitelikler (örneğin uzmanlık düzeyi ve iş yükü) ile birleştirerek kaynakların verimli kullanımı ve bilinçli triyaj kararları sağlamayı amaçlamaktadır.
Yöntemsel olarak sağlam ve uygulama açısından motive edici olmasına rağmen, mevcut modelin bazı yönleri; dinamik operasyonel ortamlarda uygulanabilirliğini sınırlayabilecek belirli kısıtlar içermektedir.

Statik ağırlıklandırma yaklaşımını aşmak için önerilebilecek potansiyel bir iyileştirme, geçmiş atama sonuçları, yanlış pozitif oranları ve SOC performansına ilişkin KPI'lara (Anahtar Performans Göstergeleri) dayalı olarak puanlama mantığını ayarlayan bir pekiştirmeli öğrenme (reinforcement learning) ajanının entegre edilmesidir. Önerilen çerçevenin temel sınırlılıklarından biri, tüm skorlama boyutlarında statik ağırlık değerlerine bağımlı olmasıdır. Bu ağırlıklar her ne kadar (örneğin: ciddiyet = 5, SLA = 4) alan bilgisine dayalı nitelik önemlerini yansıtsa da, gerçek zamanlı bağlamsal faktörlere ya da kuruma özgü risk önceliklerine karşı uyarlanabilirlikten yoksundur. Bu tür bir katılık, modelin değişen tehdit ortamlarına karşı tepki kabiliyetini zayıflatabilir. Ağırlıklar başlangıçta uzman görüşleriyle belirlenmiş ve senaryo testleriyle doğrulanmıştır. Ancak gelecekteki sürümlerde bu ağırlıkların dinamik biçimde optimize edilmesi için pekiştirmeli öğrenme kullanılabilir. Bu sınırlılık,

puanlama mantığının zamanla evrilebilmesini sağlayacak geribildirim temelli sistemlerin veya Analitik Hiyerarşi Süreci (AHP), TOPSIS ya da uyarlanabilir karar destek algoritmaları gibi çok ölçütlü karar verme tekniklerinin entegrasyonuna olan ihtiyacı ortaya koymaktadır.

Bir diğer önemli sınırlılık, korelasyon bileşeninin dar kapsamıyla ilgilidir. Mevcut uygulama, olay benzerliğini yalnızca üç öznitelik—kaynak IP, hedef IP ve kullanıcı adı—üzerinden değerlendirmektedir. Her ne kadar bu öznitelikler temel olsa da, gelişmiş saldırılarda gözlemlenen davranışsal kalıpları veya düşman taktiklerini yeterince yansıtmamaktadır. Korelasyon puanının, komut satırı davranışları, zaman damgası yakınlığı, kullanılan araç kalıpları (örneğin: PowerShell, Mimikatz) ve MITRE ATT&CK çerçevesi ile eşleşen tehdit aktörü taktikleri gibi daha zengin özellikleri içerecek şekilde genişletilmesi, modelin kampanya düzeyinde tehditleri ve anomali kümelerini tanıma kapasitesini artıracaktır.

Ayrıca, sistemin kendini öğrenme ve iyileştirme yeteneğini sınırlayan bir diğer eksiklik ise geribildirim temelli iyileştirme mekanizmasının bulunmamasıdır. Olay–analist ataması yapıldıktan sonra, bu atamaların sonuçlarına ilişkin (örneğin çözümleme başarısı, yeniden atama sıklığı, analist memnuniyeti) hiçbir değerlendirme yapılmamaktadır. Bu tür bir geribildirim döngüsü olmadan, sistem zaman içinde etkili ve yetersiz atamalar arasında ayrım yapamaz. Bu sınırlılık, analist geri bildirimleri, çözümleme kayıtları ve operasyonel performans göstergelerine dayalı olarak atama mantığını sürekli yeniden kalibre eden gözetimli öğrenme modelleri ile giderilebilir.

Modelin EMF (Deneyim Uyumluluk Faktörü) bileşeni de daha fazla ayrıntılandırılmaya ihtiyaç duymaktadır. Şu anki haliyle, olay karmaşıklığı ile analist deneyimi arasındaki sabit katsayılara dayanmaktadır; ancak alan uzmanlığı, yorgunluk durumu veya güncel performans eğilimlerini dikkate almamaktadır. Analistlerin uzmanlık alanları (ör. zararlı yazılım analizi, kimlik saldırıları), geçmiş başarı oranları ve anlık kapasite sinyalleri gibi faktörleri içeren daha gelişmiş bir EMF hesaplama yöntemi, analist–olay eşlemesinin doğruluğunu artıracaktır.

Veri entegrasyonu açısından model, olay özelliklerini ve analist kapasitesini tanımlayan nispeten statik veri kümelerine erişimi varsaymaktadır. Oysa gerçek dünya SOC ortamları gerçek zamanlı olarak çalışmakta ve karar alma süreçleri sürekli güncellenen bilgilere ihtiyaç duymaktadır. SIEM, CMDB veya XDR (Genişletilmiş Tespit ve Müdahale) sistemleri gibi canlı platformlara entegre edilmediği takdirde, modelin çıktıları güncelliğini kaybedebilir veya mevcut tehdit ortamıyla uyumsuz hale gelebilir. Elastic SIEM veya IBM QRadar gibi araçlarla API tabanlı veri boru hatlarının kurulması, gerçek zamanlı karar destek kapasitesini artırarak modelin operasyonel geçerliliğini yükseltecektir.

Doğrulama açısından, mevcut çalışma kavramsal düzeyde kalmakta olup ne gerçek SOC ortamlarında ne de simülasyon tabanlı test ortamlarında ampirik olarak test edilmiştir. Modelin işleyişini ve mantığını göstermek amacıyla basitleştirilmiş bir vaka çalışması sunulmuş olsa da, tam ölçekli değerlendirmeler ve uzun dönemli testler gelecekteki araştırma öncelikleri arasında yer almaktadır. Deneysel sonuçların eksikliği, modelin etkililiği, ölçeklenebilirliği ve gecikme performansı gibi kritik yönlerinin henüz doğrulanmadığı anlamına gelmektedir. Modelin uygulama güvenilirliğini artırmak için, senaryo temelli simülasyonlar, yapay olay veri kümeleriyle stres testleri ve gerçek SOC ortamlarında kontrollü pilot uygulamalar gibi yöntemler gelecekteki çalışmalarda yer almalıdır.

Son olarak, önerilen atama algoritmasının hesaplama verimliliği henüz resmi olarak analiz edilmemiştir. Skorlama ve eşleştirme mekanizmaları, kavramsal netlik ve yorumlanabilirlik için tasarlanmış olsa da, binlerce olay ve çok sayıda analist yöneten büyük ölçekli SOC'lerde ciddi işlem yükü oluşabilir. Bu nedenle, algoritmanın zaman karmaşıklığına ilişkin biçimsel bir analiz yapılması ve yük altında karşılaştırmalı performans ölçümleri gerçekleştirilmesi, modelin yüksek hacimli ortamlardaki davranışına ilişkin kritik içgörüler sağlayacaktır.

Sonuç olarak, önerilen model SOC'lerde olay atama sorununa metodolojik olarak sağlam ve operasyonel açıdan motive edilmiş bir çözüm sunmakla birlikte, pratik kullanımı açısından;

- Uyarlanabilir öğrenme yetenekleri,
- Zenginleştirilmiş korelasyon metrikleri,
- Analist geribildirim entegrasyonu,
- Gerçek zamanlı veri senkronizasyonu ve ampirik doğrulama süreçleri ile desteklendiğinde önemli ölçüde güç kazanacaktır.

Bu sınırlılıkların giderilmesi, çerçevenin ölçeklenebilirliğini, dayanıklılığını ve modern SOC operasyon dinamiklerine uyumunu önemli ölçüde artıracaktır.

Kod Erişilebilirliği

Analist atama çerçevesinin (ALF ve EMF puanlama mantığı dâhil) referans uygulaması, akademik ve araştırma amaçlı talepler doğrultusunda paylaşılabilir. Lütfen ilgili yazarla iletişime geçiniz.

Gelecek Çalışmalar

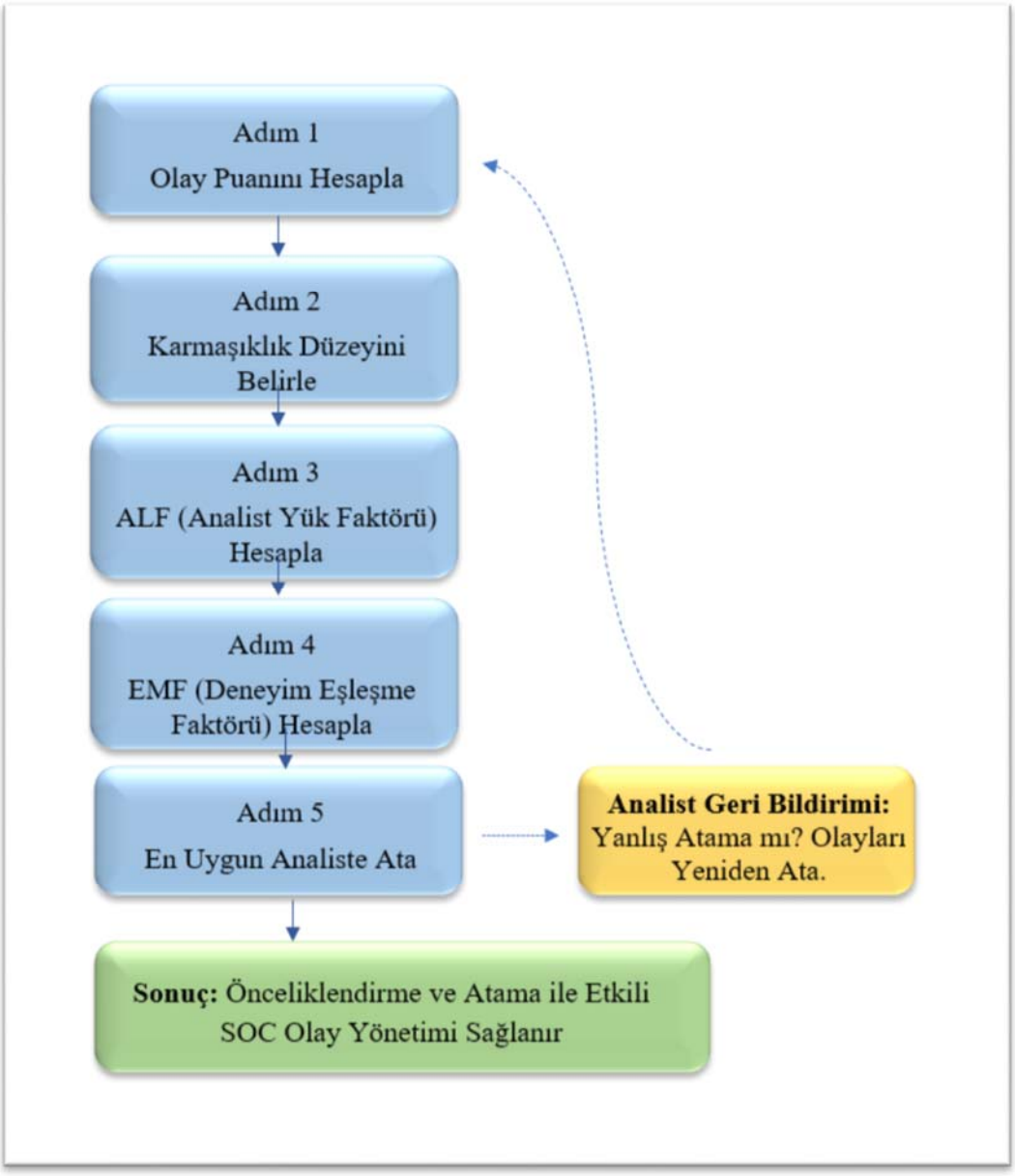
Önerilen olay atama ve önceliklendirme çerçevesinin temel yapısı üzerine inşa edilerek, modelin etkinliğini, ölçeklenebilirliğini ve gerçek dünya SOC operasyonlarıyla uyumunu artırmaya yönelik çeşitli önemli araştırma yönleri öngörülmektedir. Bu gelecek araştırma yolları, dört temel iyileştirme alanı etrafında şekillenmektedir: uyarlanabilirlik, öğrenme yetisi, entegrasyon ve doğrulama. Bu tür bir adaptasyon, yalnızca triyaj doğruluğunu artırmakla kalmayacak, aynı zamanda SOC'lerin karar mantığını sektörlere özgü tehditlere, yasal uyum gerekliliklerine ve kurumsal olgunluk düzeylerine göre özelleştirebilmelerine de olanak tanıyacaktır.

İyileştirmeye yönelik kritik alanlardan biri, olay skorlama modelinde kullanılan statik ağırlık atama mekanizmalarının dinamik ağırlıklandırma yaklaşımlarına dönüştürülmesidir. Halihazırda, ciddiyet, SLA aciliyeti ve tehdit istihbaratı gibi parametrelere atanan ağırlıklar sabit olup, yalnızca alan bilgisini yansıtmaktadır. Ancak, SOC ortamları son derece değişken ve akışkan tehdit dinamiklerine sahiptir; bağlamsal öncelik ve risk algısı zaman içinde farklılaşmaktadır. Bu nedenle, modelin gelecekteki sürümleri; Analitik Hiyerarşi

Süreci (AHP), İdeal Çözüme Benzerliğe Göre Tercih Tekniği (TOPSIS) veya pekiştirmeli öğrenme (reinforcement learning) gibi karar destek yöntemlerini kullanarak uyarlanabilir ağırlıklandırma stratejilerini keşfetmelidir. Bu tür yaklaşımlar, sistemin olay özniteliklerini; geribildirim döngüleri, gelişen tehdit profilleri veya analist performans metriklerine göre gerçek zamanlı olarak yeniden ağırlıklandırmasına olanak sağlayacaktır.

Bununla birlikte, sistemin geçmiş kararlar ve analist etkileşimlerinden öğrenme kapasitesinin artırılması da son derece önemlidir. Mevcut model, analistlerin atamalara verdiği onay, yeniden atama sıklığı ya da çözümleme sonuçları gibi unsurları yakalayan bir geribildirim mekanizmasından yoksundur. Gelecekteki geliştirmelerde, bu değişkenleri kullanarak atama mantığını kademeli biçimde ayarlayacak gözetimli öğrenme bileşenlerinin modele entegre edilmesi gereklidir. Bu sayede sistem, sürekli iyileşme ve kişiselleştirilmiş kaynak tahsisi sağlayabilir.

Bu kavram Şekil 4'te gösterilmektedir; şekil, analist geribildirim döngüsünü olay sonuçlarını skorlama ve atama sürecine yeniden bağlayan dinamik bir pekiştirme katmanı olarak betimlemektedir. Bu tür bir geribildirim entegrasyonu, sistemin zaman içinde bağlamsal farkındalığını artırmasına ve evrilerek gelişmesine olanak tanıyacaktır.



Şekil 6.1 Öğrenme amacıyla analist geri besleme döngüsünü içeren geliştirilmiş dinamik olay atama akışı

Ayrıca, modelin korelasyon puanı mekanizmasının kapsamı, desen tanıma ve kampanya düzeyinde tehdit tespiti yeteneklerini artırmak amacıyla önemli ölçüde genişletilmelidir. Hâlihazırda sadece kaynak IP, hedef IP ve kullanıcı adı gibi sınırlı sayıda öznitelik üzerinde çalışan bu yapı, ilerleyen sürümlerde

zamansal desenler (örneğin, ani frekans artışları), komut satırı aktiviteleri, alan adları, kimlik doğrulama anomalileri ve saldırı araçları gibi daha zengin öznitelikleri kapsamalıdır. Korelasyon puanına MITRE ATT&CK tabanlı taktik ve teknik eşlemeleri dâhil etmek, tehdit sınıflandırma yetkinliğini artıracak ve modelin yapılandırılmış saldırgan davranış çerçeveleriyle uyumunu güçlendirecektir.

Modelin canlı SOC ekosistemleriyle entegrasyonu, kritik bir diğer gelişim yönüdür. Operasyonel geçerlilik ve zamanında müdahale sağlamak adına, ileriki çalışmalarda SIEM (ör. Elastic, Splunk), CMDB ve XDR araçları (ör. SentinelOne, QRadar) gibi dış platformlarla gerçek zamanlı veri akışları uygulanmalıdır. API tabanlı senkronizasyon, olay durumu, analist kapasitesi ve organizasyonel bağlam hakkında canlı güncellemeleri mümkün kılarak, modelin yanıt verme kapasitesini artıracak ve statik/veri güncelliğini yitirmiş girdilere bağımlılığı azaltacaktır.

Bunun yanında, EMF metriğinin (Deneyim Uyumluluk Faktörü) daha ayrıntılı analist niteliklerini yansıtacak şekilde genişletilmesi gerekmektedir. Gelecekteki versiyonlarda, analistlerin uzmanlık profilleri, geçmiş çözüm doğruluğu, alan bazlı yetkinlikleri (ör. bulut güvenliği, uç nokta tehditleri) ve gerçek zamanlı iş yükü/yorgunluk göstergeleri gibi öğeler entegre edilmelidir. Bu tür çok boyutlu EMF modellemesi, daha adil ve isabetli olay dağıtımını destekleyecektir.

Doğrulama (validasyon) açısından, modelin simülasyon ortamlarında veya kontrollü saha uygulamalarında kapsamlı biçimde test edilmesi zorunludur. Bu çalışmada sunulan örnek vaka çalışması, model işleyişini göstermek açısından öncül bir adım teşkil etse de, gerçek dünya verileriyle veya sentetik olay veri kümeleriyle yapılacak daha geniş doğrulama çalışmaları elzemdir. Gerçekçi SOC alarm dağılımlarını taklit eden sentetik veri kümeleri oluşturarak; yüksek alarm hacmi, analist yetersizliği veya APT tespiti gibi senaryolar altında performans karşılaştırmaları yapılabilir. Çözüm süresi, analist memnuniyeti ve yeniden atama oranları gibi metrikler, modelin operasyonel verimliliğini değerlendirmek açısından kullanılabilir. Gerçek kurumsal SOC ortamlarında,

hatta sınırlı kapsamlı veya gölge modlu deneysel uygulamalar bile, modelin kullanılabilirliği ve kurumsal benimsenme potansiyeli hakkında değerli içgörüler sağlayacaktır.

Son olarak, olay skorlama ve atama algoritmasının hesaplama karmaşıklığına ilişkin biçimsel bir analiz gerçekleştirilmelidir. Büyük ölçekli SOC ortamlarında—n olay sayısını, m ise analist sayısını temsil ettiğinde—O(n×m) olan zaman karmaşıklığı, her olayın tüm analistlerle karşılaştırılarak değerlendirileceğini gösterir. Bu nedenle, kurumsal düzeyde düşük gecikmeli ve ölçeklenebilir performans sağlamak için; toplu atama işlemleri (batch processing), paralel hesaplama teknikleri veya sezgisel filtreleme yaklaşımları gibi optimizasyon stratejileri dikkate alınmalıdır.

Sonuç olarak, gelecekte önerilen çerçevenin geliştirilmesi; mevcut teorik modeli, dinamik, akıllı ve entegre bir karar destek motoruna dönüştürmeli ve karmaşık SOC ortamlarına uyarlanabilir hale getirmelidir. Öğrenme mekanizmalarının, gerçek zamanlı entegrasyonların, gelişmiş analiz modellerinin ve deneysel değerlendirmelerin dâhil edilmesiyle, bu çerçeve, gelecek nesil siber güvenlik olay yönetimi için sağlam bir operasyonel araca evrilebilecektir.

Özetle, önerilen model; analist-farkındalıklı SOC operasyonlarını destekleyen, nicel ve açıklanabilir bir atama mekanizması sunmaktadır. Gelecek çalışmalar; yapay zekâ destekli adaptasyon, gerçek zamanlı SIEM entegrasyonları ve ampirik testler ile bu kavramsal yapıyı tam anlamıyla uygulanabilir bir çözüm haline getirmeyi hedeflemektedir

KAYNAKLAR

Al-Dhaqm A, Siddique K, Abd Razak S, Ikuesan RA, Kebande VR. 2020. Towards the development of an integrated incident response model for database forensic investigation field. *IEEE Access*, 8: 145018 - 145032.

Alrimawi F, Pasquale L, Nuseibeh B. 2019. On the automated management of security incidents in smart spaces. *IEEE Access*, 7: 111513 – 111527.

AXELOS. 2019. ITIL Foundation: ITIL 4 Edition. *The Stationery Office (TSO)*, London, UK, 1st ed., 1–255.

Binbeshr F, Imam M, Hamdan M, Ghaleb M, Rahim MA, Hammoudeh M. 2025. The rise of cognitive SOCs: A systematic literature review on AI approaches. *IEEE Open J Comput Soc*, 6: 360 – 379.

Chhetri MB, Tariq S, Singh R, Jalalvand F, Paris C, Nepal S. 2024. Towards human-AI teaming to mitigate alert fatigue in security operations centres. *ACM Comput Surv*, 24(3): 1 – 22.

Gachnang P, Ehrenthal J, Telesko R, Hanne T. 2023. Determination of weights for multiobjective combinatorial optimization in incident management with an evolutionary algorithm. *IEEE Access*, 11: 138502 – 138514.

García LA, Tomás VR. 2020. A framework for enhancing the operational phase of traffic management plans. *IEEE Access*, 8: 204483 – 204493

Handri EY, Sensuse DI, Tarigan A. 2025. Developing an agile cybersecurity framework with organizational culture approach using Q methodology. *IEEE Access*, 13: 108835 – 108850.

He Y, Luo C, Evans M, Zamani E, Maglaras LA, Yevseyeva I, Janicke H. 2019. Real-time information security incident management: A case study using the IS-CHEC technique. *IEEE Access*, 7: 142147 – 142175.

Hou W, Meng L, Ke X, Zhong L. 2022. Dynamic load balancing algorithm based on optimal matching of weighted bipartite graph. *IEEE Access*, 10: 127225 – 127236.

Jadon S, Kannan PK, Gupta K, Kalaria U, Honnavalli PB, Varsha KR. 2024. A comprehensive study of load balancing approaches in real-time multi-core systems for mixed real-time tasks. *IEEE Access*, 12: 53373 – 53395.

Jalalvand F, Chhetri MB, Nepal S, Paris C. 2024. Alert prioritisation in security operations centres: A systematic survey on criteria and methods. ACM Comput Surv, 57(2): 1 – 36

Liao S, Wu C, Yang Q, Wang B, Jiang M. 2011. A resource-efficient load balancing algorithm for network virtualization. Chin J Electron, 20(4): 765–770.

Mooi RD, Botha RA. 2016. A management model for building a computer security incident response capability. *SAIEE Afr Res J*, 107(2): 78 – 91.

Sharafaldin I, Habibi Lashkari A, Ghorbani AA. 2018. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: Proceedings of the 4th *International Conference on Information Systems Security and Privacy (ICISSP)*, Funchal, Portugal, 22–24 January 2018, 108–116.

Villalón-Huerta A, Ripoll-Ripoll I, Marco-Gisbert H. 2022. SOC critical path: A defensive kill chain model. *IEEE Access*, 10: 13570 - 13581.

Vielberth M, Böhm F, Pernul G, Fichtinger I. 2020. Security operations center: A systematic study anda open challenges. *IEEE Access*, 8: 227756 – 227779.

ÖZGEÇMİŞ