



ANALYST-AWARE INCIDENT ASSIGNMENT IN SECURITY OPERATIONS CENTERS: A MULTI-FACTOR PRIORITIZATION AND OPTIMIZATION FRAMEWORK

Eyup Can KILINCDEMİR^{1*}, Baris CELIKTAS¹


¹*Işık University, Institute of Graduate Students, Department of Computer Engineering, 34398, İstanbul, Türkiye*


Abstract: In this paper, 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 incident severity, 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, SLA urgency

*Corresponding author: Işık University, Institute of Graduate Students, Department of Computer Engineering, 34398, İstanbul, Türkiye

E mail: 23sibe5004@isik.edu.tr (E.C.KILINCDEMİR)

Eyup Can KILINCDEMİR  <https://orcid.org/0009-0005-1151-7480>

Baris CELIKTAS  <https://orcid.org/0000-0003-2865-6370>

Received: May 06, 2025

Accepted: June 16, 2025

Published: July 15, 2025

Cite as: Kilincdemir E.C., Celiktas B. 2025. Incident assignment and prioritization framework for security operations centers (SOCs). BSJ Eng Sci, 8(4): 1160-1180.

1. Introduction

The increasing frequency and complexity of cybersecurity incidents demand a structured and adaptive approach to incident management. Security Operations Centers (SOCs), as the frontline infrastructure of organizational defense, are responsible for detecting, analyzing, and mitigating threats in real time. However, the surge in alert volume—combined with limited analyst availability and manual triage—often leads to delays, fatigue, and inefficient resource use. These challenges highlight the need for intelligent, automated incident assignment mechanisms that evaluate factors such as analyst expertise, real-time workload, incident complexity, and service-level agreement (SLA) urgency to ensure timely and effective response.

To address these limitations, we present a novel incident assignment and prioritization framework that consolidates contextual incident attributes—such as severity, SLA urgency, asset criticality, threat intelligence,

correlation, and repetition—into a unified scoring model. Simultaneously, analysts are dynamically profiled through workload and expertise measures, enabling real-time, competency-aware analyst-incident matching.

The main contributions of this study are as follows:

- We propose a multi-factor scoring model integrating technical and contextual incident features.
- We introduce two analyst-centric metrics—Analyst Load Factor (ALF) and Experience Match Factor (EMF).
- We formalize analyst assignment as an optimization task with scoring formulas and examples.
- We validate the model via pseudocode, scoring tables, and a case study.
- We benchmark it against prior work and propose future enhancements such as API integration and reinforcement learning.



- Our dual-sided optimization ensures effective triage and balanced analyst workloads.
- We empirically evaluate the model using CICIDS2017 benchmark data to demonstrate its applicability in real-world SOC environments (see Section 5.2).

The remainder of this paper is organized as follows. Section 2 presents a comprehensive review of related works on incident prioritization and analyst assignment in SOC environments. Section 3 introduces the scoring methodology, explaining the key incident attributes and their contribution to the overall incident score. Section 4 describes the proposed model in detail, including the calculation of incident complexity, the ALF, and the EMF, as well as the final assignment logic. Section 5 presents a simplified case study that demonstrates the practical execution of the proposed model through step-by-step scoring and analyst matching across three incidents and two analysts. Section 6 provides an integrated conclusion that summarizes the framework's key contributions, discusses current limitations, incorporates the case study findings, and outlines directions for future work.

1.2. Related Works

The increasing volume, frequency, and complexity of cybersecurity threats—ranging from ransomware to insider threats—have accelerated the evolution of incident response models in SOCs. As the modern SOC must balance high alert volumes, dynamic attacker behavior, and limited human resources, the need for scalable and intelligent incident handling mechanisms has become more critical than ever. In this context, numerous studies have addressed the challenge by proposing frameworks and algorithms focused on incident classification, prioritization, analyst-task alignment, and intelligent decision support.

The foundational ITIL framework (AXELOS, 2019) offers a process-oriented structure for managing incidents, emphasizing impact, urgency, escalation workflows, and SLAs. While ITIL is widely adopted for standardizing IT operations, it lacks analyst-specific considerations and dynamic task distribution features. Similarly, the Capability Maturity Model proposed by Mooi and Botha (2016) promotes institutional readiness and security governance maturity, but it does not address real-time triage, prioritization scoring, or analyst matching.

From a prioritization perspective, Jalalvand et al. (2024) provided a comprehensive survey of alert triage strategies, including severity-based models and statistical classifiers. Likewise, Chhetri et al. (2024) emphasized human-AI teaming approaches to reduce analyst fatigue through cognitive support. Although these works significantly contribute to understanding prioritization criteria and analyst overload, they fall short of offering analyst-aware assignment or workload balancing mechanisms.

Other researchers have explored task allocation using algorithmic or optimization methods. For instance, Gachnang et al. (2023) employed multi-objective

evolutionary algorithms to match analysts with incidents based on skills and SLAs, but their model incurs high computational complexity. Hou et al. (2022) introduced a graph-based load balancing strategy, which improves matching efficiency but lacks integration with incident severity or threat intelligence. In another dimension, Handri et al. (2025) proposed a culture-centric analyst matching approach using Q-methodology, which addresses human aspects of task assignment but lacks technical prioritization logic.

Automation in SOCs has also been the subject of multiple studies. Alrimawi et al. (2019) introduced automated incident workflows for smart spaces, while Binbeshr et al. (2025) proposed the Cognitive SOC model with AI-powered triage capabilities. However, these models focus more on detection and AI-driven automation than analyst-specific triage or post-assignment optimization. Several works target domain-specific SOC applications. Al-Dhaqm et al. (2020) proposed a forensic incident response model specific to database systems, and Villalón-Huerta et al. (2022) developed a kill-chain model for SOC defense. He et al. (2019) introduced IS-CHEC for real-time incident management but did not incorporate analyst expertise or scoring mechanisms.

Foundational studies such as Vielberth et al. (2020) offered taxonomies and architectural overviews of SOCs, emphasizing integration and role clarity but without actionable assignment strategies. Meanwhile, generic real-time load balancing models (e.g., Liao et al., 2011; Jadon et al., 2024) and SLA-driven frameworks from adjacent domains (e.g., García and Tomás, 2020) provide valuable optimization insights but do not account for security-specific complexity or SOC analyst matching.

A comparative summary of these studies is presented in Table 1. As illustrated, most prior models focus on individual SOC lifecycle components—such as alert severity, task allocation, or analyst workload—without integrating these into a unified, dynamic framework.

In contrast, our study proposes a comprehensive framework that combines seven core incident scoring dimensions—Severity, SLA Urgency, Incident Type, Asset Criticality, Repetition Frequency, Threat Intelligence, and Correlation Score—with analyst-side profiling via the EMF and ALF. Additionally, our model supports real-time operation and includes a feedback loop that dynamically adapts based on outcomes (e.g., reassignment frequency or false positive rates).

This integrated approach fills a critical gap in the literature by offering a scalable, analyst-aware solution for prioritization and assignment in modern SOCs. While previous research has made significant strides in alert filtering, automation, and human-centric support, our contribution lies in synthesizing these dimensions into a cohesive and operationally deployable prioritization engine with quantifiable metrics and formal assignment logic.

Table 1. Comparative summary of related work on SOC incident assignment and prioritization

Author / Study	Model	Key Factors	Assignment Logic	Strengths	Limitations
ITIL Foundation (2019)	Process Oriented Framework	Impact, Urgency, SLAs	Role-Based Static Assignment	Provides structured workflows	Lacks analyst-level adaptation
Mooi and Botha (2016)	Capability Maturity Model	Readiness, Process Stages	Capability Maturity Tracking	Organizational focus	No dynamic scoring
Jalalvand et al. (2024)	Systematic Survey	Severity, Alert Fatigue	Triage Criteria Review	Comprehensive review	No model proposed
Chhetri et al. (2024)	Human-AI Teaming	Analyst Fatigue, Volume	Cognitive Load Allocation	Human-centric focus	Ignores technical priority
Gachnang et al. (2025)	Evolutionary Optimization	SLA, Analyst Skill	Multiobjective Matching	High-quality allocation	High computation cost
Handri et al. (2025)	Q Method + Agile SOC	Culture, Agility	Culture-Based Matching	Organizational perspective	Not technically focused
Alrimawi et al. (2019)	Smart-Space Automation	IoT Threats	Autonomous Triggers	Automation focus	SOC generalization lacking
Binbeshr et al. (2025)	Cognitive SOC	AI Models, Alerts	AI-Based Matching	Uses cognitive AI	Overlooks workload balancing
Aldhaqm et al. (2020)	Forensic IR Model	DB Logs, Activities	Forensic Phases	Structured forensic view	Not real-time
Villal'ón Huerta et al. (2022)	Defensive Kill Chain	Attack Lifecycle	Phase Mapping	Kill-chain based SOC model	No analyst matching
He et al. (2019)	IS-CHEC Framework	Performance Metrics	Real-Time Structured Flow	Real-time focus	Ignores analyst context
Vielberth et al. (2020)	SOC Survey Model	SOC Roles, Taxonomy	Role Description	Broad taxonomy	Not actionable
Hou et al. (2022)	Graph Load Balancing	Analyst Load, Fit	Graph Matching	Balanced matching	Lacks threat modeling
Jadon et al. (2024)	RT Load Balancing	Task Type, RT Needs	Core-Aware Dist.	Effective scheduler	Generic, not SOC-specific
Liao et al. (2011)	Network LB Algorithm	Load, Latency	Network Mapping	Efficient networking	No SOC focus
Garc'ia and Tom'as (2020)	Traffic IR Framework	Incident Risk, SLA	Adaptive Prioritization	SLA-driven incident timing	Transportation domain
This Paper	Score + Matching	Severity, SLA, Threat Intel, Correlation, Repetition, EMF + ALF, Complexity	Real-time, multi-factor analyst-aware assignment	Integrates prioritization, dynamic analyst profiling, feedback loop, correlation-aware triage	Requires tuning for large-scale SOC's

2. Materials and Methods

The proposed framework follows a multi-factor prioritization approach inspired by multi-criteria decision-making (MCDM) to evaluate and prioritize incidents in a SOC context. This strategy is particularly well-suited for environments where various, often conflicting, attributes such as urgency, complexity, and

resource constraints must be simultaneously considered. Each security incident is evaluated against a set of factors that contribute to its overall priority, enabling both structured triage and context-aware analyst assignment. The scoring model integrates the following incident-specific factors, which are formally defined along with their symbols in Table 2.

Table 2. Symbols used in incident score calculation formula

Symbol	Description
S_m	Total score assigned to an incident
S_{sev}	Incident severity level score (1–5)
S_{SLA}	Numerical urgency level based on SLA (1–5)
S_{type}	Score based on type/category of the incident
S_{rep}	Additional score based on frequency of recurrence
S_{asset}	Score reflecting the criticality of the affected system
S_{ti}	Score based on threat intelligence indicators
S_{cor}	Score derived from similarity to past incidents
W_{sev}	Weight coefficient for severity attribute
W_{SLA}	Weight coefficient for SLA urgency
W_{type}	Weight coefficient for incident type
W_{rep}	Weight coefficient for repetition
W_{asset}	Weight coefficient for asset criticality
W_{ti}	Weight coefficient for threat intelligence
W_{cor}	Weight coefficient for correlation

- Incident Score (S_m): Represents the overall priority score assigned to an incident after applying weighted aggregation across all relevant attributes. This cumulative score is used to rank and compare incidents within the SOC, enabling efficient triage and resource allocation. A higher S_m value indicates greater urgency and complexity, directly influencing analyst assignment decisions.
- Incident Severity (S_{sev}): Reflects the potential impact of the incident on organizational assets and operations. More severe incidents are prioritized for faster remediation.
- SLA Urgency (S_{SLA}): Based on predefined SLAs, this dimension reflects the allowable response time for each incident. Lower SLA windows increase incident priority.
- Incident Type (S_{type}): Different types of incidents (e.g., phishing, ransomware, privilege escalation) vary in complexity and risk. A predefined severity level is associated with each category.
- Repetition (S_{rep}): Recurring incidents within a time window suggest unresolved vulnerabilities or ongoing campaigns. Repetition increases priority dynamically.
- Affected Asset (S_{asset}): Incidents involving high-value or critical systems (e.g., SIEM, domain controllers) are weighted more heavily to mitigate business risk.
- Threat Intelligence (S_{ti}): Incorporates contextual data such as blacklisted IPs, malware indicators, and known attack patterns. Threat actor linkage directly raises priority.
- Correlation Score (S_{cor}): Measures incident similarity with past events using attributes like source IP, destination, and user account. This enables detection of patterns and campaign-level

behavior.

- Severity Weight (W_{sev}): Indicates the relative importance assigned to the incident severity attribute in the overall scoring formula.
- SLA Urgency Weight (W_{SLA}): Represents the weight assigned to the SLA urgency factor.
- Incident Type Weight (W_{type}): Specifies the influence of incident type classification (e.g., ransomware, phishing) on the total score.
- Repetition Weight (W_{rep}): Reflects the emphasis placed on the recurrence frequency of incidents.
- Asset Criticality Weight (W_{asset}): Denotes the priority given to the importance of the affected system.
- Threat Intelligence Weight (W_{ti}): Measures the contribution of threat intel indicators to the total score.
- Correlation Weight (W_{cor}): Indicates the significance assigned to correlation scores from past incidents.

To ensure that high-priority incidents are addressed by the most capable personnel, analysts are profiled based on their experience and current workload. An ALF is used to avoid overloading any single analyst, while an EMF assesses how well an analyst's skill level aligns with the complexity of a given incident. Details and formulas for ALF and EMF are provided in Section 4.4.

The final incident score is obtained through a weighted aggregation of the aforementioned attributes, while the final analyst suitability score considers both ALF and EMF. Weights were initially derived using expert judgment and validated through scenario testing. Future iterations may use reinforcement learning to optimize these weights dynamically. This methodology serves as the foundation for the stepwise model described in the following section.

2.1. Proposed Model

The proposed model consists of several sequential steps designed to facilitate intelligent and efficient analyst assignment in SOC operations. Figure 1 provides an overview of this dynamic workflow.

2.1.1. Step 1: Calculate incident score

Each incident is scored using a weighted combination of normalized factors, including severity, SLA urgency, incident type, repetition frequency, asset criticality, threat intelligence, and correlation indicators. The weights were derived from expert evaluations through a structured survey. This composite score reflects the overall contextual and technical priority of each incident and serves as the basis for assignment and triage decisions.

2.1.2. Step 2: Determine incident complexity

The computed score is then used to determine the complexity level of the incident. Incidents are categorized into five levels: Very Low, Low, Medium, High, and Critical. This classification ensures that incidents are assigned to analysts with matching expertise levels.

2.1.3. Step 3: Calculate analyst load factor (ALF)

To avoid overloading any analyst, a load factor is calculated based on each analyst's current number of assigned incidents and their maximum handling capacity. This factor penalizes analysts already close to their workload limit.

2.1.4. Step 4: Calculate experience match factor (EMF)

The EMF determines how closely an analyst's experience level aligns with the complexity of the incident. Higher EMF scores are given to analysts whose expertise level closely matches the required incident complexity.

2.1.5. Step 5: Assign to most suitable analyst

Finally, a suitability score is computed by combining the incident score, EMF, and ALF. The incident is assigned to the analyst with the highest suitability score, ensuring effective and context-aware allocation.

Figure 1 illustrates the core steps of the proposed assignment workflow, including incident scoring, analyst matching, and workload balancing.

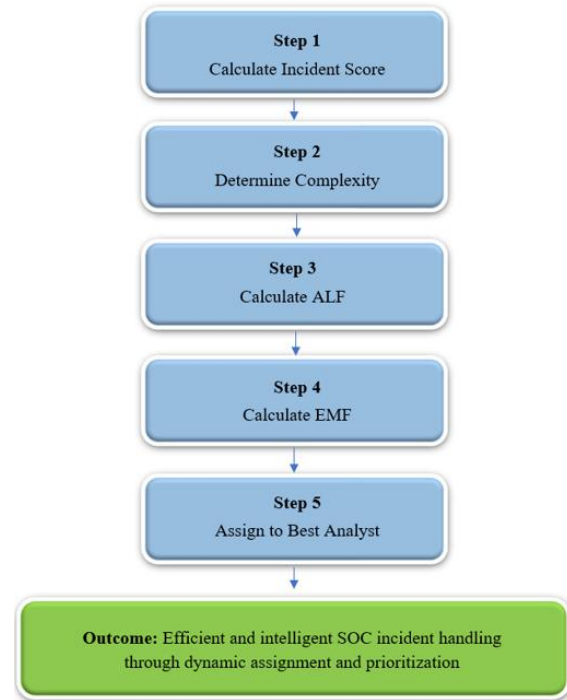


Figure 1. Proposed dynamic incident assignment flow in soc operations. The process ensures intelligent analyst matching and workload balancing.

2.2. Incident Score Calculation Formula

To determine the priority level of an incident, a multi-factor scoring model is employed that consolidates technical and contextual attributes into a single weighted score. Unlike fixed summation methods, this model incorporates factor-specific weights derived from professional evaluations to reflect the relative importance of each attribute more accurately.

The general weighted incident score formula is as follows (equations 1 and 2):

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

Where:

- S_m is the final incident score,
- $S_{sev}, S_{SLA}, S_{type}, S_{rep}, S_{asset}, S_{ti}, S_{cor}$ represent the normalized (0–5 scale) scores for each corresponding incident attribute.
- $W_{sev}, W_{SLA}, W_{type}, W_{rep}, W_{asset}, W_{ti}, W_{cor}$ are the normalized weights assigned to each attribute, such that:

$$W_{sev} + W_{SLA} + W_{type} + W_{rep} + W_{asset} + W_{ti} + W_{cor} = 1 \quad (2)$$

These weights were derived through a structured survey conducted among professionals working in cybersecurity, IT auditing, risk management, and operational SOC roles. Participants were asked to rate the importance of seven core incident attributes on a 1–5

Likert scale. The mean scores were subsequently normalized to compute the final weights used in the model.

The resulting weighted scoring formula is (equations 3):

$$S_m = 0.160 \times S_{sev} + 0.135 \times S_{SLA} + 0.149 \times S_{type} + 0.117 \times S_{rep} + 0.156 \times S_{asset} + 0.149 \times S_{ti} + 0.135 \times S_{cor} \quad (3)$$

These weights help enhance prioritization accuracy by embedding real-world, context-aware professional insights into the incident evaluation process. The detailed survey data and computation steps are presented in Table 3.

Table 3. Expert ratings for incident score weights (Normalized Averages)

Title	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
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

*Sev. = severity, Inc Type = incident type, Ass Cri = asset criticality, TI = threat intel, Re = repetition, Co = correlation, CSE = cyber security engineer, CSM = cyber security manager, IR = incident responder, ISM = information security manager, L2A = L2 cyber security analyst, SS = Security Specialist, SCSE = Senior Cyber Security Expert, SIA = senior information auditor, SOCS = SOC specialist, SOCTL = SOC team lead, Avg = average, Norm. Wt = normalized weight.

2.2.1. Severity score

The incident severity describes the impact of the event on the system. Higher score values correspond to more critical events.

In SOCs, severity plays a crucial role in classifying and prioritizing security incidents according to their urgency and potential impact. Most SOCs adopt a five-level classification model Informational, Low, Medium, High, and Critical to enable consistent and risk-informed incident handling.

This structured categorization directly influences triage operations. Critical incidents involve threats such as data exfiltration, ransomware infections, or nation-state attacks that require immediate response. Conversely, Low or Informational incidents—like brute force attempts or misconfigured settings, are less urgent.

In this paper, each severity level is assigned a numerical score, as shown numerically in Table 4, to support a correct match between the analyst and incident. These scores play a key role in our incident assignment approach by helping prioritize incidents based on their criticality.

Table 4. Severity levels and their associated scores

Level	Description	Score
1	Critical	5
2	High	4
3	Medium	3
4	Low	2
5	Informational	1

The severity score reflects the criticality of an incident's impact on organizational assets. Incidents classified as "Critical" (e.g., ransomware, nation-state attacks) receive the highest score, enabling urgent triage and immediate analyst response. Conversely, informational or low-severity events receive the lowest score.

2.2.2. SLA urgency score

SLAs are essential elements in SOC workflows, defining the maximum allowable time frame for detecting, analyzing, and resolving security incidents based on their severity. These thresholds help minimize risk exposure and ensure operational continuity.

Most SOCs employ a tiered SLA structure that aligns with severity levels. In our proposed framework, incidents are assigned SLA urgency levels that directly influence their prioritization score. For example, a Critical such as a

detected data exfiltration attempt must be addressed within 15 minutes, while a Low such as an unauthorized access attempt can be resolved within two hours or more, depending on operational policies.

To integrate SLA urgency into the incident scoring model, each response tier is converted into a numerical score. Incidents with higher priorities have higher urgency scores, thereby directly affecting the incident's final weight.

The specific mapping between SLA response time and the corresponding urgency score is provided in Table 5.

This score reflects how quickly an incident must be resolved based on its SLA tier. The shorter the SLA response window, the higher the urgency score (via the transformation $6 - \text{SLA Level}$). This transformation ensures SLA-compliant prioritization, minimizing mean time to response for high-criticality threats.

Table 5. SLA urgency levels and corresponding scores

Level	Response Time	Score (6 -SLA)
1	< 15 minutes (Critical)	5
2	< 30 minutes (High)	4
3	< 60 minutes (Medium)	3
4	< 120 minutes (Low)	2
5	> 120 minutes (Informational)	1

2.2.3. Incident type score

The incident type plays a key role in determining the appropriate response strategy for analysts within a SOC. It defines the nature of the security incident, such as ransomware, phishing, or unauthorized access, and reveals the potential risk to the organization. Classifying incidents by type helps analysts better understand the severity, technical complexity, and scope of impact.

In this article, each type of incident is assigned a score that contributes to the overall prioritization mechanism. Table 6 shows how the various incident types are grouped according to their potential risk levels and how scores are assigned. This score assignment contributes to the final incident score and the repetition score.

Table 6. Categorization of information security incidents and corresponding scores

Incident Type	Score
Critical Incident	
Advanced Persistent Threat (APT)	5
Data Exfiltration (Sensitive Data Leakage)	5
Ransomware Infection	5
Nation-State Sponsored Attack	5
Supply Chain Attack	5
High Severity Incidents	
Unauthorized Privilege Escalation	4
SQL Injection Attack	4
Exploitation of Known Vulnerabilities	4
Remote Code Execution (RCE) Attempt	4
Active Directory Compromise	4
Medium Severity Incidents	
Malware Infection	3
Distributed Denial of Service (DDoS) Attack	3
Phishing Attack (Spear Phishing)	3
Credential Stuffing Attack	3
Suspicious Lateral Movement	3
Zero-Day Exploit Detected	3
Insider Threat Activity	3
Low Severity Incidents	
Unauthorized Access Attempt (Brute Force)	2
Social Engineering Attack	2
Unusual Login Behavior	2
Malware Callback (C2 Communication)	2
Informational Severity Incidents	
Port Scanning	1
Misconfigured Security Settings Detected	1
Suspicious File Execution	1
Unusual Network Traffic	1

*The incident types and associated severity scores were manually derived based on their prevalence in SOC environments and their potential impact on confidentiality, integrity, and availability (CIA triad). This taxonomy aims to support structured triage decisions by linking incident categories with appropriate risk levels.

2.2.4. Repetition score

The base incident type score is dynamically adjusted based on how frequently the same type of incident occurs within a defined time frame. Table 7 defines frequency-based modifiers.

Table 7. Repetition-based score adjustment criteria

Repetition Frequency	Modifier Value (R)
More than 5 occurrences within 1 hour	50
More than 5 occurrences within 24 hours	25
More than 3 occurrences within 7 days	10
First occurrence	0

The repetition score adjusts incident priority based on temporal frequency to reflect the potential urgency of

unresolved or recurring threats (e.g., brute force, scanning). The more frequently a threat is observed, the higher the adjustment—while keeping the score bounded.

The final repetition-adjusted score is calculated using the following formula, which caps the result at a maximum of 5 (equations 4):

$$\text{Repetition Score} = \min \left(5, \frac{\text{Incident Type Score} + \frac{(\text{Repetition Score Modifier} + \text{Incident Type Score})}{100}}{1} \right) \quad (4)$$

Example scores calculated based on different scenarios:

- APT Attack (Base Score = 5), occurring 5 times in 1 hour: $\min(5, 5 + (50 + 5) / 100) = \min(5, 5.55) = 5.0$
- Port Scanning (Base Score = 1), occurring 5 times in 24 hours: $\min(5, 1 + (25 + 1) / 100) = \min(5, 1.26) = 1.26$
- Brute Force Attack (Base Score = 2), occurring 3 times in 7 days: $\min(5, 2 + (10 + 2) / 100) = \min(5, 2.12) = 2.12$

This bounded adjustment method ensures that high-frequency but low-severity attacks gain priority appropriately without disproportionately inflating scores for already high-impact incidents such as APTs.

2.2.5. Affected asset score

The criticality of the asset affected by a security incident is a key determinant in prioritizing incident response. Assets are not equal in value or function; for example, an attack on a SIEM or payment processing system poses a much higher risk than one on a guest Wi-Fi network. In the proposed model, affected assets are classified into five levels based on their operational importance and security sensitivity, with each category assigned a corresponding score. This classification enables SOC teams to assess the impact of an incident more accurately and allocate resources more effectively during triage.

Table 8 categorizes affected systems based on operational importance, ranging from mission critical infrastructure to sandbox environments.

Table 8. Asset criticality-based scoring for affected systems

Affected Asset	Score
Critical Security Systems (SIEM, IAM, DB, DC, IDS/IPS)	5
Cloud Infrastructure (Kubernetes Cluster, Virtualization Host)	5
Payment Processing Systems (PCI-DSS Environments)	5
Email Server	4
Public-Facing Web Server	4
VPN Gateway	4
Identity and Authentication Systems (SSO, MFA)	4
Important Application Server	3
Internal Business Applications (ERP, CRM)	3
File Servers	3
Development Environments (CI/CD, Code Repositories)	3
Standard Workstation (Regular Employee Devices)	2
Remote Access Systems (VDI, Remote Desktop)	2
IoT/OT Devices (Industrial Systems, Smart Devices)	2
Self-Contained System (Standalone or Low-Risk System)	1
Guest Wi-Fi Networks	1
Test and Sandbox Environments	1

*The asset criticality scores in this table are manually defined based on their strategic importance, sensitivity level, and potential impact on business continuity in case of compromise.

2.2.6. Threat intelligence score

The threat score evaluates whether the incident originates from a known threat actor or a high-risk entity. Incidents associated with APT groups, botnets, and dark web indicators are given the highest priority.

Table 9 presents a structured classification of threat sources along with their impact-based scores.

Table 9. Threat intelligence-based scoring of detected indicators

Threat Type	Score
Known Threat Actor (APT, Darknet IP, Nation-State Threat Group)	5
Compromised Infrastructure (C2 Servers, Botnets, Malware Hosts)	5
Malicious IP (Blacklist, Repeated Offender)	4
Publicly Known Exploitable Vulnerability (CVE Exploit Source)	4
High-Risk Domain (Phishing, Fake Login Pages, Scam Websites)	4
Suspicious Activity (Unusual Traffic Patterns, Unknown Anomaly)	3
Newly Registered Domains (Potential Phishing or C2 Servers)	3
Geographically Unusual Access (Suspicious Country or TOR Exit Node)	3
Outdated SSL Certificate on External Domain	2
Insecure Protocol Detected (e.g., HTTP Instead of HTTPS)	2
Internal Network Traffic (Unverified but Unlikely to Be Malicious)	1
First-Time Seen Traffic from Internal IPs	1

*The threat scores presented in this table are assigned manually based on expert judgment and domain knowledge to reflect relative risk levels for common threat indicators

2.2.7. Correlation score

The correlation score quantifies how similar a new incident is to previously recorded cases, thus prioritizing repeated or evolving threat patterns. To compute this value, we consider three core indicators commonly used in SOC analysis:

- Source IP (srcIP): Origin of the attack.
- Destination IP (dstIP): Targeted internal address.
- Username (user): Account involved in the incident.

Each indicator is scored based on historical frequency and importance weight. To prevent score inflation, a saturation threshold is defined.

Variables:

- M_i : Number of historical matches for attribute i
- T_i : Saturation threshold for attribute i
- CW_i : Correlation weight assigned to attribute i where $i \in \{\text{srcIP}, \text{dstIP}, \text{user}\}$.

Assigned Values:

$CW_1 = 1.25, T_1 = 2$ (Source IP)
 $CW_2 = 1.75, T_2 = 2$ (Destination IP)
 $CW_3 = 2.0, T_3 = 3$ (Username)

Formula (equations 5):

Correlation Score

$$= CW_1 \times \min\left(1, \frac{M_{\text{srcIP}}}{T_1}\right) + CW_2 \times \min\left(1, \frac{M_{\text{dstIP}}}{T_2}\right) + CW_3 \times \min\left(1, \frac{M_{\text{user}}}{T_3}\right) \quad (5)$$

The correlation score encapsulates the historical similarity of incidents via weighted saturation thresholds over key identifiers (source IP, destination IP, and username). By normalizing frequency contributions and applying capped influence ($\min(1, M/T)$), this metric promotes temporal threat continuity detection while controlling for noise and score accumulation. An example breakdown of how individual attributes contribute to the correlation score is shown in Table 10.

Table 10. Correlation score breakdown example

Attribute	M_i	T_i	CW_i	Formula	Cont
				$1.25 \times$	
Source IP	2	2	1.25	$\min(1, \frac{2}{2})$	1.25
				$1.75 \times$	
Destination IP	1	2	1.75	$\min(1, \frac{1}{2})$	0.875
				$2.0 \times$	
Username	4	3	2.0	$\min(1, \frac{4}{3})$	2.0

* T_i (saturation threshold) and CW_i (correlation weight) are statically defined model parameters based on expert judgment. Cont = contribution.

Total Correlation Score: $1.25 + 0.875 + 2.00 = 4.125$

2.3. Example Incident Score Calculation

The following is an example calculation of an incident score based on a real-world attack scenario.

2.3.1. Incident scenario

An organization's SOC detects multiple failed login attempts from an external IP on their VPN gateway. Over the course of 24 hours, more than five login attempts are observed from the same external IP, targeting different employee accounts. Historical analysis reveals that this same IP address had triggered incidents on three different occasions in the last seven days, including an alert for brute-force attempts and lateral movement attempts on internal systems.

After a few hours, the same IP successfully authenticates using a compromised credential. Shortly after, an abnormal login occurs on a high-privilege account, followed by the execution of a suspicious PowerShell script on a domain controller (DC) from a newly created user account. Threat intelligence also flags the external IP as a known malicious actor linked to previous credential stuffing campaigns.

4.3.2 Incident Details and Score Calculation

A credential stuffing attack is detected on the

organization's VPN gateway. The attacker uses a known malicious IP and successfully compromises a user account. The incident affects the domain controller (DC) and matches previous incidents involving the same IP, destination, and username. The following scoring breakdown is applied:

- Severity: 2 (High) \rightarrow Score = 4, Weight = 0.160 $\rightarrow 0.160 \times 4 = 0.640$ points
- SLA Urgency: 2 (High, <30 minutes) $\rightarrow (6 - 2) = 4$ Score = 4, Weight = 0.135 $\rightarrow 4 \times 0.135 = 0.540$ points
- Incident Type: Credential Stuffing Attack \rightarrow Score = 3, Weight = 0.149 $\rightarrow 3 \times 0.149 = 0.447$ points
- Repetition: More than 5 occurrences in 24 hours \rightarrow Repetition Score = $\min(5, 3 + (25 + 3)/100) = 1.26$, Weight = 0.117 $\rightarrow 1.26 \times 0.117 = 0.147$ points
- Affected Asset: Domain Controller (DC) \rightarrow Score = 5, Weight = 0.156 $\rightarrow 5 \times 0.156 = 0.780$ points
- Threat Intelligence: Malicious IP (Blacklisted) \rightarrow Score = 4, Weight = 0.149 $\rightarrow 4 \times 0.147 = 0.596$ points
- Correlation Score:
 - Source IP: $M_{srcIP} = 3 T_1 = 2 CW_1 = 1.25 \rightarrow 1.25 \times \min(1, \frac{3}{2}) = 1.25$
 - Destination IP: $M_{dstIP} = 2 T_2 = 2 CW_2 = 1.75 \rightarrow 1.75 \times \min(1, \frac{2}{2}) = 1.75$
 - Username: $M_{user} = 4 T_3 = 3 CW_3 = 2.0 \rightarrow 2.0 \times \min(1, \frac{4}{3}) = 2$
- Total Correlation Score: $1.25 + 1.75 + 2.0 = 5$ $5 \times 0.135 = 0.675$ points
- Final Incident Score: $0.640 + 0.540 + 0.447 + 0.147 + 0.780 + 0.596 + 0.675 = 3.825$

To illustrate the practical implications of the scoring model, a credential stuffing attack scenario is examined below. The attack progresses through multiple phases including reconnaissance, credential misuse, and lateral movement. The sequence of these actions is visualized in Figure 2. providing a chronological view of the incident response timeline.

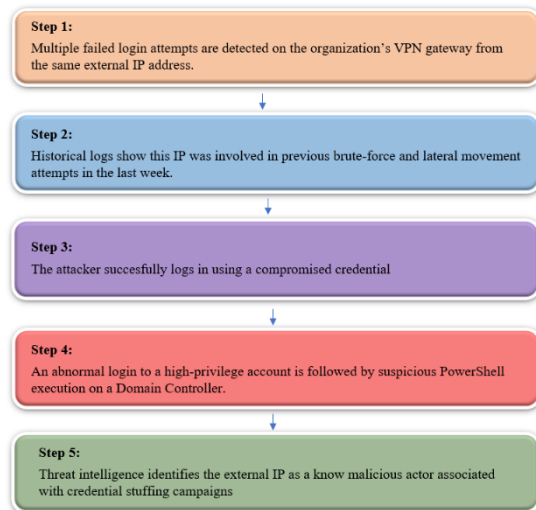


Figure 2. Step-by-step timeline of the credential stuffing attack and detection process in the SOC.

2.4. Analyst Scoring - Incident Assignment Process

To effectively assign incidents to analysts, we use a structured approach considering workload balancing and experience matching.

2.4.1. Step 1: Defining analyst groups and capacity

We categorize analysts into five levels based on expertise:

- Senior Analysts (Level 5): A_i
- Advanced Mid-Level Analysts (Level 4): A_j
- Mid-Level Analysts (Level 3): A_k
- Junior Analysts (Level 2): A_l
- Trainee Analysts (Level 1): A_m

Each analyst has a different maximum capacity and current workload. These capacity constraints across analyst levels are summarized in Table 11.

Table 11. Analyst levels, incident load, and capacity in SOC

Analyst A_n	Level L_n	Current Incidents CI_n	Max Capacity MC_n
A_i (Senior)	5	CI_i	MC_i
A_j (Advanced Mid-Level)	4	CI_j	MC_j
A_k (Mid-Level)	3	CI_k	MC_k
A_l (Junior)	2	CI_l	MC_l
A_m (Trainee)	1	CI_m	MC_m

4.4.2. Step 2: Determining incident complexity from incident score

The calculated incident score S_m is used to determine the complexity level C_m , which guides analyst assignment by aligning incident difficulty with analyst experience. As the scoring model has been normalized to a 0–5 scale, the complexity levels are recalibrated accordingly. equation (6) presents the threshold-based classification of incident complexity levels based on normalized incident scores

$$C_m = \begin{cases} 5, & \text{if } S_m \geq 4.0 \text{ (Critical Complexity)} \\ 4, & \text{if } 3.2 \leq S_m < 4.0 \text{ (High Complexity)} \\ 3, & \text{if } 2.4 \leq S_m < 3.2 \text{ (Medium Complexity)} \\ 2, & \text{if } 1.6 \leq S_m < 2.4 \text{ (Low Complexity)} \\ 1, & \text{if } S_m < 1.6 \text{ (Very Low Complexity)} \end{cases} \quad (6)$$

This classification enables the system to match incidents to analysts with suitable experience levels (as used in the EMF calculation). Table 12 presents examples of incident score values and their associated complexity classes based on this scale.

Table 12. Incident scores and their corresponding complexity levels

Incident I_m	Incident Score S_m	Complexity Level 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)

All scores are computed using the weighted scoring formula described in Section 4.2, ensuring consistency with analyst assignment logic described in Section 4.4.

2.4.3 Step 3: Calculating analyst load factor (ALF)

ALF_n is computed using the following formula (equation 7):

$$ALF_n = 1 + \frac{CI_n}{MC_n} \quad (7)$$

Table 13. ALF calculation and resulting scores

Analyst A_n	Current Incidents CI_n	Max Capacity MC_n	ALF Calculation	ALF Score ALF_n
A_1 (Senior)	4	6	$1 + \frac{4}{6} = 1.67$	1.67
A_2 (Advanced Mid-Level)	3	5	$1 + \frac{3}{5} = 1.60$	1.60
A_3 (Mid-Level)	2	7	$1 + \frac{2}{7} = 1.29$	1.29
A_4 (Junior)	3	6	$1 + \frac{3}{6} = 1.50$	1.50
A_5 (Trainee)	1	6	$1 + \frac{1}{6} = 1.17$	1.17

2.4.4 Step 4: Calculating experience match factor (EMF)

The experience match factor EMF_n determines how well an analyst matches the complexity of an incident. It is calculated by comparing the analyst's experience level L_n with the complexity level C_m of the incident (equation 8):

$$EMF_n = \begin{cases} 1, & \text{if } L_n = C_m \\ 0.75, & \text{if } L_n = C_m + 1 \\ 0.5, & \text{if } L_n = C_m + 2 \\ 0.25, & \text{if } L_n = C_m + 3 \\ 0, & \text{if } L_n < C_m \end{cases} \quad (8)$$

where:

- L_n is the level of analyst A_n , ranging from 1 (Trainee) to 5 (Senior).

where:

- CI_n is the current number of incidents assigned to analyst A_n .
- MC_n is the maximum capacity of analyst A_n .

Table 13 provides sample ALF calculations and resulting scores for various analyst levels.

- C_m is the complexity level of incident I_m , ranging from 1 (Very Low Complexity) to 5 (Critical Complexity).

Table 14 presents EMF scores for selected analyst–incident assignments to illustrate how analyst expertise aligns with incident complexity.

A higher EMF score means the analyst's experience is a better match for the incident complexity. Analysts with levels closer to the incident's complexity will have higher EMF scores, which means they are better suited for handling the incident.

Table 14. Experience Match Factor (EMF) scores for analyst–incident assignments

Incident I_m	Analyst A_n	Analyst Level L_n	Complexity Level C_m	EMF Score EMF_n
I_1 (APT Attack)	A_1 (Senior)	5	5	1.00
	A_3 (Mid-Level)	3	5	0.00
	A_5 (Trainee)	1	5	0.00
I_2 (Phishing)	A_2 (Advanced Mid-Level)	4	3	0.75
	A_4 (Junior)	2	3	0.00
I_3 (Port Scanning)	A_3 (Mid-Level)	3	1	0.50
	A_5 (Trainee)	1	1	1.00

Figure 3 summarizes the full analyst matching logic, incorporating both ALF and EMF calculations for optimal assignment.

The process integrates scoring, complexity evaluation, ALF, and EMF to ensure precise analyst allocation.

The ALF score reduces the assignment priority of analysts with high existing workloads, helping to balance incident distribution across available personnel. The EMF score measures how well an analyst's expertise level aligns with the complexity of an incident. A high EMF combined with a low ALF indicates the most suitable analyst. Together, these scores ensure both operational efficiency and task-competency alignment in incident assignment.

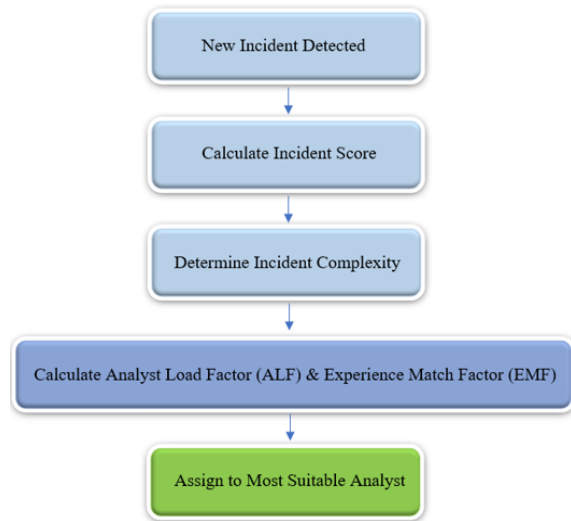


Figure 3. Analyst matching flow: from incident evaluation to optimal assignment.

Additionally, the model supports future extensions such as analyst fatigue metrics, skill-based routing using specialized domain tags (e.g., cloud, endpoint, identity), and AI-driven anomaly clustering, ensuring long-term scalability and personalization.

2.4.5 Step 5: Final analyst suitability score

The final suitability score for an analyst handling a specific incident is given by (equation 9):

$$S_n = \frac{S_m \times EMF_n}{ALF_n} \quad (9)$$

where:

- S_n is the final score for analyst A_n .
- S_m is the incident score for incident I_m .
- EMF_n is the experience match factor for analyst A_n .
- ALF_n is the analyst load factor for analyst A_n .

To demonstrate the scoring mechanism, Tables 15 through 18 show the final suitability scores for different incidents (APT attack, phishing, port scanning, unusual login behavior), evaluated across all analysts. Each table presents detailed ALF, EMF, and final score calculations per analyst.

Table 19 consolidates the results by identifying the analyst with the highest suitability score for each incident, enabling optimized assignment based on both expertise and workload.

Table 15. Final score calculation for incident 1 (APT Attack, Score $S_1 = 4.63$)

Analyst A_n	ALF ALF_n	EMF EMF_n	Final Score Calculation S_n	Suitability Score (S_n)
A_1 (Senior)	1.50	1.00	$\frac{4.63 \times 1.00}{1.50} = 3.08$	3.08
A_2 (Advanced Mid-Level)	1.40	0.00	$\frac{4.63 \times 0.00}{1.40} = 0.00$	0.00
A_3 (Mid-Level)	1.30	0.00	$\frac{4.63 \times 0.00}{1.30} = 0.00$	0.00
A_4 (Junior)	1.60	0.00	$\frac{4.63 \times 0.00}{1.60} = 0.00$	0.00
A_5 (Trainee)	1.20	0.00	$\frac{4.63 \times 0.00}{1.20} = 0.00$	0.00

Table 16. Final score calculation for incident 2 (Phishing, Score $S_2 = 1.92$)

Analyst A_n	ALF ALF_n	EMF EMF_n	Final Score Calculation S_n	Suitability Score (S_n)
A_1 (Senior)	1.50	0.50	$\frac{1.92 \times 0.50}{1.50} = 0.64$	0.64
A_2 (Advanced Mid-Level)	1.40	0.75	$\frac{1.92 \times 0.75}{1.40} = 1.03$	1.03
A_3 (Mid-Level)	1.30	1.00	$\frac{1.92 \times 1.00}{1.30} = 1.47$	1.47
A_4 (Junior)	1.60	0.00	$\frac{1.92 \times 0.00}{1.60} = 0.00$	0.00
A_5 (Trainee)	1.20	0.00	$\frac{1.92 \times 0.00}{1.20} = 0.00$	0.00

Table 17. Final score calculation for incident 3 (Port Scanning, Score $S_3 = 1.45$)

Analyst A_n	ALF ALF_n	EMF EMF_n	Final Score Calculation S_n	Suitability Score (S_n)
A_1 (Senior)	1.50	0.25	$\frac{1.45 \times 0.25}{1.50} = 0.24$	0.24
A_2 (Advanced Mid-Level)	1.40	0.50	$\frac{1.45 \times 0.50}{1.40} = 0.51$	0.51
A_3 (Mid-Level)	1.30	0.75	$\frac{1.45 \times 0.75}{1.30} = 0.83$	0.83
A_4 (Junior)	1.60	1.00	$\frac{1.45 \times 1.00}{1.60} = 0.90$	0.90
A_5 (Trainee)	1.20	0.00	$\frac{1.45 \times 0.00}{1.20} = 0.00$	0.00

Table 18. Final score calculation for incident 4 (Unusual Login Behavior, Score $S_4 = 2.33$)

Analyst A_n	ALF ALF_n	EMF EMF_n	Final Score Calculation S_n	Suitability Score (S_n)
A_1 (Senior)	1.50	0.50	$\frac{2.33 \times 0.50}{1.50} = 0.77$	0.77
A_2 (Advanced Mid-Level)	1.40	0.75	$\frac{2.33 \times 0.75}{1.40} = 1.24$	1.24
A_3 (Mid-Level)	1.30	1.00	$\frac{2.33 \times 1.00}{1.30} = 1.79$	1.79
A_4 (Junior)	1.60	0.00	$\frac{2.33 \times 0.00}{1.60} = 0.00$	0.00
A_5 (Trainee)	1.20	0.00	$\frac{2.33 \times 0.00}{1.20} = 0.00$	0.00

Table 19. Best analyst assignment per incident based on final score

Incident I_m	Best Analyst A_n	Suitability Score (S_n)
I_1 (APT Attack)	A_1 (Senior)	3.08
I_2 (Phishing)	A_3 (Mid-Level)	1.47
I_3 (Port Scanning)	A_4 (Junior)	0.90
I_4 (Unusual Login Behavior)	A_3 (Mid-Level)	1.79

The following pseudocode outlines the full incident scoring and assignment process in two phases.

- Algorithm 1 handles incident evaluation and analyst profiling.
- Algorithm 2 performs analyst–incident matching and assigns each incident to the most suitable analyst based on the computed scores.

Algorithm 1 Part 1 - Incident Scoring and Analyst Profiling

1: Input:

2: $I = \{I_1, I_2, \dots, I_m\}$ \triangleright Set of incidents

3: $A = \{A_1, A_2, \dots, A_n\}$ \triangleright 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_{cor}

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

9: Step 1: Compute Total Incident Score and Complexity Level

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: $C_m \leftarrow 5$ \triangleright Critical

14: else if $S_m \geq 3.2$ then

15: $C_m \leftarrow 4$ \triangleright High

16: else if $S_m \geq 2.4$ then

17: $C_m \leftarrow 3$ \triangleright Medium

18: else if $S_m \geq 1.6$ then

19: $C_m \leftarrow 2$ \triangleright Low

20: else

21: $C_m \leftarrow 1$ \triangleright Very Low

22: end if

23: end for

24: Step 2: Compute Analyst Load Factor (ALF)

25: for $A_n \in A$ do

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

27: end for

Algorithm 2 Part 2 - Analyst Matching and Incident Assignment

1: Step 3: Compute Experience Match Factor (EMF)

2: for $I_m \in I$ do

3: for $A_n \in A$ do

4: if $L_n = C_m$ then


```

5:      EMFn,m ← 1
6:      else if Ln = Cm + 1 then
7:          EMFn,m ← 0.75
8:      else if Ln = Cm + 2 then
9:          EMFn,m ← 0.5
10:     else if Ln = Cm + 3 then
11:         EMFn,m ← 0.25
12:     else
13:         EMFn,m ← 0
14:     : end if
15: end for
16: end for
17: Step 4: Compute Final Suitability and Assign Incidents
18: for Im ∈ I do
19:     best score ← -∞
20:     assigned ← None
21:     for An ∈ A do
22:         Sn,m ← Sm ×  $\frac{EMF_{n,m}}{ALF_n}$ 
23:         if Sn,m > best score then
24:             best score ← Sn,m

```

```

25:             assigned ← An
26:         : end if
27:     end for
28:     Assign Im → assigned
29: end for
30: Return all {Im → An} assignments

```

3. Results and Discussion

This section presents a step-by-step example involving three incidents and two analysts to demonstrate how the scoring and matching logic operates in practice.

To demonstrate the practical applicability of the proposed scoring and assignment framework, we present a simplified case study involving three distinct incidents and two SOC analysts. Each incident is evaluated using the seven scoring factors, and analysts are profiled using the ALF and EMF metrics. The final analyst-incident assignment is performed based on the suitability score.

3.1. Incident Summary

Table 20 summarizes the key attributes of the three sample incidents used in this illustrative case study.

Table 20. Incident characteristics and scoring inputs for case study

Incident ID	Type	Sev	SLA (hrs)	AsC	Rep	TI	Cor
I1	Phishing Email	3	4	2	0	1	1
I2	Ransomware Detected	5	1	5	1	2	3
I3	Privilege Escalation	4	2	4	2	3	2

*Each factor is normalized to a score out of 5. Higher scores mean higher priority. Sev = severity, AsC= asset criticality, Rep = repetition, TI = threat intel, Cor = correlation.

Each incident is characterized based on seven normalized scoring inputs, including severity, SLA urgency, asset criticality, repetition frequency, threat intelligence relevance, and correlation indicators. These structured inputs serve as the foundation for computing incident scores and enable consistent prioritization across diverse alert types. Notably, Incident I2 represents the most critical case, with the highest severity and repetition levels, whereas I1 shows minimal threat indicators, suggesting a lower priority.

3.2. Incident Scoring

To compute the final score for each incident, the proposed framework utilizes a weighted aggregation model that incorporates seven critical incident attributes: severity (Sev), SLA urgency (SLA), asset criticality (AsC), repetition frequency (Rep), threat intelligence (TI), correlation score (Cor), and incident type (Type). Rather than assuming equal importance, this model applies expert-defined weights to each factor, as formalized in Section 4.2.

Incident I1 (Phishing Email):

$$S_{I1} = (0.149 \times 3) + (0.160 \times 3) + (0.135 \times 4) + (0.156 \times 2) + (0.117 \times 0) + (0.149 \times 1) + (0.135 \times 1) = 0.447 + 0.480 + 0.540 + 0.312 + 0.000 + 0.149 +$$

$$0.135 = 2.063$$

Incident I2 (Ransomware Detected):

$$S_{I2} = (0.149 \times 5) + (0.160 \times 5) + (0.135 \times 1) + (0.156 \times 5) + (0.117 \times 1) + (0.149 \times 2) + (0.135 \times 3) = 0.745 + 0.800 + 0.135 + 0.780 + 0.117 + 0.298 + 0.405 = 3.280$$

Incident I3 (Privilege Escalation):

$$S_{I3} = (0.149 \times 4) + (0.160 \times 4) + (0.135 \times 2) + (0.156 \times 4) + (0.117 \times 2) + (0.149 \times 3) + (0.135 \times 2) = 0.596 + 0.640 + 0.270 + 0.624 + 0.234 + 0.447 + 0.270 = 3.081$$

These weighted scores serve as the foundation for determining incident complexity and inform the analyst-assignment process described in subsequent sections. Notably, Incident I2 received the highest score due to its high severity, critical asset impact, and strong correlation indicators, whereas Incident I1 was rated the lowest due to low repetition and threat intelligence relevance.

3.3. Analyst Profiles

Table 21 presents the analyst profiles used in the assignment process, highlighting their technical skill domains, current workload as measured by the ALF, and the EMF for each incident.

Table 21. Analyst profiles with ALF and EMF values

Analyst ID	Skill Tags	Load (ALF)	EMF I1	EMF I2	EMF I3
A1	Email, SIEM	0.3	0.9	0.3	0.5
A2	Malware, Priv. Escal	0.6	0.5	0.8	0.9

*EMF reflects the degree of match between the incident complexity level and the analyst's expertise level. Lower ALF values indicate higher analyst availability and are therefore considered more suitable for assignment.

Analyst A1, who specializes in email and SIEM alerts, shows higher expertise alignment with Incident I1, whereas A2 has stronger alignment with privilege escalation and malware-related threats. The ALF metric reflects analyst availability, favoring A1 for lower workload. These metrics jointly contribute to the final suitability scoring that guides the analyst-incident assignment process.

3.4. Analyst Suitability Scoring

In this step, each analyst's suitability for a given incident is computed using the updated scoring formula defined in Section 4.4.5:

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

The suitability score increases with higher EMF values and decreases with higher ALF values. Table 21 provides the required ALF and EMF values, while the previously calculated incident scores from Section 5.1.2 are used here.

- Incident I1:
A1: $2.063 \times \left(\frac{0.9}{0.3}\right) = 2.063 \times 3.00 = 6.189$

$$A2: 2.063 \times \left(\frac{0.5}{0.6}\right) = 2.063 \times 0.833 = 1.718$$

→ Assigned to A1

- Incident I2:

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

$$A2: 3.280 \times \left(\frac{0.8}{0.6}\right) = 3.280 \times 1.33 = 4.362$$

→ Assigned to A2

- Incident I3:

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

$$A2: 3.081 \times \left(\frac{0.9}{0.6}\right) = 3.081 \times 1.50 = 4.621$$

→ Assigned to A1

3.5. Final Assignment Table

Table 22 presents the final analyst-incident assignment results based on the integrated evaluation model that combines incident scoring and analyst suitability. Each assignment reflects a data-driven match between incident criticality and analyst availability and expertise, as computed through the weighted formulas defined in previous sections.

Table 22. Final analyst-incident assignment decisions with suitability scores

Incident	Incident Score	Assigned Analyst	Suitability Score
I1	2.063	A1	6.189
I2	3.280	A2	4.362
I3	3.081	A1	5.145

Incident I2, which received the highest incident score (S_m) of 3.280, was assigned to Analyst A2, who exhibited a strong expertise alignment (EMF: 0.8) despite a moderate workload. The resulting suitability score of 4.362 confirms that A2 is the most effective option for handling this high-priority ransomware incident.

Incident I3, with a slightly lower score of 3.081, was routed to Analyst A1, whose lower workload (ALF: 0.3) and moderate domain match (EMF: 0.6) resulted in a suitability score of 5.145. This indicates a strategic load distribution, where analyst availability plays a decisive role.

Incident I1, the lowest-priority event (score: 2.063), was also assigned to A1, who demonstrated a high EMF score (0.9) and minimal workload, yielding a strong suitability score of 6.189. This decision reflects the model's preference to match lower-risk incidents with available analysts having domain expertise, thereby conserving specialized resources for more complex threats.

Overall, this assignment strategy achieves a balanced

optimization between incident urgency and analyst fit. By dynamically incorporating both workload and expertise metrics, the framework ensures timely responses to critical incidents while maintaining sustainable analyst capacity across the SOC environment.

To further support the practical relevance of the proposed model, subsequent evaluation scenarios (Section 5.2) utilize labeled attack traces from the CICIDS2017 dataset. These experiments demonstrate the model's scalability and adaptability when applied to real-world SOC data under varying incident and analyst profiles.

3.6. Empirical Evaluation Using Benchmark SOC Data

To validate the real-world applicability of the proposed framework, a benchmark evaluation was conducted using labeled incident samples from the CICIDS2017 dataset. This section presents the scoring outcomes (Section 5.2.1), metadata and attack characteristics (Section 5.2.2), and analyst assignment results based on suitability scores (Section 5.2.3).

3.6.1. Scoring results of benchmark incidents

Table 23 summarizes the raw attribute values for each incident across seven model dimensions, including severity, SLA urgency, asset criticality, repetition, threat intelligence, correlation, and incident type. These unweighted values are used as inputs for the final priority score computation shown in Table 24.

Table 23. Raw Incident Attribute Scores Across Seven Model Dimensions

Inc. ID	Sev.	SLA	Asset	Rep.	TI	Cor.	Inc. Type
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
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

*These are raw scores for each incident dimension. Final weighted prioritization scores are calculated in Table 24. Inc. ID = incident ID, Sev. = severity, Rep. = repetition, TI = threat intel, Cor. = correlation, Inc. Type = incident type.

Table 24. Final weighted incident scores

Incident ID	Final Score
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

*Final scores represent the normalized and weighted prioritization values used for analyst matching and complexity classification.

3.6.2. Incident Metadata and Threat Typology

The selected cases reflect a diverse threat landscape, including brute-force attempts, exploit-based attacks, DDoS campaigns, and infiltration methods. Each incident was mapped to both external and internal hosts within the dataset and aligned with a victim asset class.

Detailed incident metadata, including attacker IP, victim IP, asset, and assigned technique are summarized in Table 25.

3.6.3. Analyst Assignment Outcomes

To support analyst-incident matching, synthetic analyst

In the previous table (Table 23), raw incident attributes such as severity, SLA urgency, asset criticality, and others are listed for comparative visualization. These values represent the original, unweighted scores and are not directly used for final prioritization.

To derive a reliable prioritization outcome, these attributes are normalized and multiplied by their corresponding expert-defined weights, as specified in Section 4.2. The final incident score for each case is then calculated using the following formula:

$$S_m = W_{sev} \times S_{sev} + W_{SLA} \times S_{SLA} + W_{type} \times S_{type} + W_{rep} \times S_{rep} + W_{asset} \times S_{asset} + W_{ti} \times S_{ti} + W_{cor} \times S_{cor} \quad (10)$$

Where the weights (w_i) were empirically determined via expert survey and are normalized to sum to 1. Table 24 summarizes the final weighted scores computed from the raw values.

profiles were defined based on varying levels of expertise and workload. Each analyst was assigned an experience level (L_n) ranging from 1 (Trainee) to 5 (Senior), and an Analyst Load Factor (ALF) value representing the analyst's current workload relative to their maximum handling capacity. These parameters were used to evaluate the suitability of each analyst for the incidents under consideration.

The synthetic analyst profiles used in this evaluation are presented in Table 26.

Table 25. Incident descriptions extracted from CICIDS2017 dataset

Inc. ID	Date	Attack Type	Attacker IP	Victim IP	Asset	Tech.
I1	July 4	FTP-Patator	205.174.165.73	192.168.10.50	Web Server	Brute Force
I2	July 4	SSH-Patator	205.174.165.73	192.168.10.50	Web Server	Brute Force
I3	July 5	DoS Hulk	205.174.165.73	192.168.10.50	Web Server	DoS
I4	July 5	Heartbleed	205.174.165.73	192.168.10.51	Ubuntu12 Server	Exploit
I5	July 6	SQL Injection	205.174.165.73	192.168.10.50	Web Server	Web Attack
I6	July 6	Infiltration (Dropbox)	205.174.165.73	192.168.10.8	Windows Vista	Infiltration
I7	July 6	Infiltration (Cool Disk)	205.174.165.73	192.168.10.25	MAC	Infiltration
I8	July 7	Botnet ARES	205.174.165.73	Multiple Targets	Win 10/8/Vista	Botnet
I9	July 7	Port Scanning	205.174.165.73	192.168.10.50	Ubuntu16	Reconnaissance
I10	July 7	DDoS LOIT	205.174.165.69–71	192.168.10.50	Ubuntu16	DDoS

*This table lists real incident samples extracted from CICIDS2017, which serve as empirical inputs for scoring and assignment. Inc. ID = incident ID, Tech. = technique.

Table 26. Synthetic analyst profiles used in evaluation

Analyst	Experience Level L_n	ALF
A1	5 (Senior)	0.30
A2	4 (Advanced)	0.40
A3	3 (Mid-Level)	0.50
A4	2 (Junior)	0.60
A5	1 (Trainee)	0.70

*The CICIDS2017 dataset does not include analyst metadata. These experience levels and ALF values were synthetically assigned to simulate a realistic analyst pool with varying workloads and expertise.

Using the incident complexity levels (C_m) calculated in Section 5.2.1 and the analyst profiles summarized in

Table 26, the EMF was determined for each analyst–incident pair by comparing the analyst’s experience level (L_n) to the incident’s complexity level. Suitability scores were then computed using the model’s formal suitability function introduced in Section 4.4.5:

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

A higher S_n score indicates a more appropriate match between the analyst and the incident, balancing expertise and workload. The final assignment results, including the selected analyst and computed suitability scores, are presented in Table 27.

Table 27. Analyst Assignment Results Based on Suitability Score

Incident ID	Assigned Analyst	S_m (Normalized)	EMF	ALF	Suitability Score 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	1.678
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

*Suitability scores were computed using the model formula $S_n = (S_m \times EMF_n) / ALF_n$. Each incident was assigned to the analyst with the highest S_n value to ensure optimal alignment of expertise and workload.

As shown in Table 27, analysts with the highest suitability scores were selected for each incident. Notably, high-complexity incidents such as I4, I8, and I10 were consistently assigned to senior or advanced-level analysts with lower ALF values, reflecting the model's effectiveness in balancing analyst capacity and expertise for prioritized incident response.

4. Conclusion

4.1. Summary and Contributions

The incident assignment process ensures that each incident is handled by the most suitable analyst based on multiple factors such as incident severity, SLA urgency, and complexity. Key takeaways from the model include:

- **Shorter SLA Urgency:** Incidents with a shorter SLA (requiring quicker resolution) are prioritized to ensure timely response.
- **Complex Incidents:** Incidents with higher complexity scores are assigned to more experienced analysts (Senior, Advanced Mid-Level), while lower complexity incidents are assigned to Junior or Trainee analysts.
- **Workload Balancing:** Analysts' workloads are carefully managed using the ALF, ensuring no analyst is overloaded with incidents.
- **Experience Matching:** EMF ensures incidents are assigned to analysts whose experience level matches the incident's complexity.
- **Dynamic Assignment:** The assignment process is dynamic and recalculated based on real-time data, ensuring that the most appropriate analyst is always handling the most critical incidents.
- **Threat Intelligence:** Known threat actors and the type of asset affected by the incident are factored into the assignment process to ensure priority is given to high-risk incidents.
- **Final Assignments:** Based on the calculations and factors above, the final assignments are dynamically adjusted, with critical incidents being handled by Senior analysts, medium to high complexity incidents being assigned to Mid-Level or Advanced Mid-Level analysts, and low severity incidents being delegated to Junior or Trainee analysts.
- **Case Study Demonstration:** A synthetic case validated the model's logic, showing that high-priority incidents (e.g., I2, score 2.86) were routed even with moderate analyst suitability, while lower-priority ones (e.g., I1) were matched based on optimal expertise. This illustrates the model's dynamic balancing of priority and analyst fit.

This process guarantees that each incident is assigned to the right analyst, optimizing response time and enhancing overall security operations in the organization.

Empirical validation using CICIDS2017 incidents confirmed that the proposed framework effectively prioritizes and assigns incidents in line with analyst

experience and workload.

4.2. Discussion and Limitations

The proposed incident assignment framework presents a structured and comprehensive approach for prioritizing and allocating incidents in SOC, based on both technical risk indicators and analyst characteristics. By integrating factors such as incident severity, SLA urgency, threat intelligence, and correlation scores with analyst-specific attributes like expertise and workload, the model aims to ensure efficient resource utilization and informed triage decisions. Despite its methodological robustness and practical motivation, several aspects of the current implementation present notable limitations that may constrain its applicability in dynamic operational settings.

One potential enhancement to overcome static weighting is the integration of a reinforcement learning agent that adjusts scoring logic based on historical assignment outcomes, false positive rates, and SOC performance KPIs. A key limitation of the framework lies in its reliance on static weighting schemes across all scoring dimensions. While these weights reflect domain-informed estimations of attribute importance (e.g., severity = 5, SLA = 4), they lack adaptability to real-time contextual factors or organization-specific risk priorities. Such rigidity may undermine the model's responsiveness to evolving threat environments. Weights were initially derived using expert judgment and validated through scenario testing. Future iterations may use reinforcement learning to optimize these weights dynamically. This limitation suggests the need for the integration of adaptive weighting mechanisms, potentially through feedback-driven systems or multi-criteria decision-making techniques such as Analytic Hierarchy Process (AHP), TOPSIS, or reinforcement learning models that allow the scoring logic to evolve over time.

Another important constraint is related to the restricted scope of the correlation component. The current implementation evaluates incident similarity using only three attributes—source IP, destination IP, and username—which, while foundational, do not adequately capture behavioral patterns or adversarial tactics present in sophisticated attacks. Enhancing the correlation score to incorporate richer features, including command-line behavior, timestamp proximity, tool usage patterns (e.g., PowerShell, Mimikatz), and threat actor tactics mapped via the MITRE ATT&CK framework, would improve the model's capacity to identify campaign-level threats and anomaly clusters.

Moreover, the absence of a feedback-driven refinement mechanism restricts the system's capacity for learning and self-improvement. Once incident-to-analyst assignments are made, there is no subsequent evaluation based on resolution outcomes, reassignment frequency, or analyst satisfaction. Without such feedback loops, the system cannot distinguish between effective and suboptimal assignments over time. This limitation could be addressed by incorporating supervised learning

models that continuously recalibrate assignment logic based on analyst input, historical resolution data, and operational performance indicators.

The model's EMF also warrants further refinement. Currently based on predefined distance-based coefficients between incident complexity and analyst experience levels, the EMF metric lacks granularity and fails to consider domain-specific skillsets, fatigue, or recent performance trends. A more nuanced EMF calculation incorporating analyst specialization (e.g., malware analysis, identity attacks), prior success rates, and real-time capacity signals would enhance the fidelity of analyst-incident mapping.

In terms of data integration, the model assumes access to relatively static datasets that describe incident characteristics and analyst capacity. In practice, SOC environments operate in real-time, and decision-making requires continuously updated information. Without integration into live platforms such as SIEMs, CMDBs, or Extended Detection and Response (XDR) systems, the model's outputs risk becoming obsolete or misaligned with the current threat landscape. Establishing API-based data pipelines with tools like Elastic SIEM or IBM QRadar would facilitate real-time decision support and elevate operational relevance.

From a validation perspective, the current work remains conceptual, with no empirical testing conducted in real-world SOC environments or through simulation frameworks. Although a simplified case study was included to demonstrate the model's functionality and logic, full-scale evaluation and longitudinal testing remain future priorities. The absence of experimental results means that the effectiveness, scalability, and latency performance of the model remain unverified. To strengthen its practical credibility, future research should include scenario-based simulations, stress tests using synthetic incident datasets, and controlled pilot deployments in operational SOC contexts.

Finally, the computational efficiency of the proposed assignment algorithm has not been formally examined. Although the scoring and matching mechanisms are designed for clarity and interpretability, large-scale SOCs handling thousands of incidents and dozens of analysts could encounter significant processing overhead. A formal analysis of algorithmic complexity, along with benchmarking under load, would provide essential insights into the model's performance under high-throughput conditions.

In conclusion, while the proposed model introduces a methodologically sound and operationally motivated solution to the incident assignment problem in SOCs, its practical deployment would benefit significantly from adaptive learning capabilities, enriched correlation metrics, analyst feedback integration, real-time data synchronization, and empirical validation. Addressing these limitations would enhance the framework's scalability, resilience, and alignment with modern SOC operational dynamics.

4.3. Code Availability

A reference implementation of the analyst assignment framework (including ALF and EMF scoring logic) is available upon request for academic and research purposes. Please contact the corresponding author.

4.4. Future Work

Building upon the foundational structure of the proposed incident assignment and prioritization framework, several key directions are envisioned to enhance its effectiveness, scalability, and operational alignment within real-world SOCs. These future research pathways are centered around four core improvement domains: adaptability, learning capability, integration, and validation. Such adaptivity would not only improve triage accuracy but also enable SOCs to tailor decision logic according to sector-specific threats, compliance requirements, and organizational maturity.

A critical area for advancement lies in transitioning from static to dynamic weight assignment mechanisms across the incident scoring model. Currently, weights attributed to parameters such as severity, SLA urgency, and threat intelligence are fixed and domain-informed. However, SOCs operate in highly fluid threat environments, where contextual relevance and risk prioritization vary over time. Future iterations of the model should explore adaptive weighting strategies utilizing decision-making frameworks such as Analytic Hierarchy Process (AHP), Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), or reinforcement learning. These approaches can enable the system to reweigh incident attributes in real time based on feedback loops, evolving threat profiles, or analyst performance metrics.

In parallel, enhancing the system's capacity to learn from historical decisions and analyst interactions is essential. Currently, the model lacks a feedback mechanism that captures analyst agreement with incident assignments, reassignment frequencies, or resolution outcomes. Future developments should embed a supervised learning component that utilizes these variables to incrementally adjust the assignment logic, enabling continuous improvement and personalized allocation. This concept is illustrated in Figure 4, which demonstrates the analyst feedback loop as a dynamic reinforcement layer that connects incident outcomes back into the scoring and assignment pipeline. Such feedback integration would allow the system to iteratively evolve and increase its contextual awareness over time.

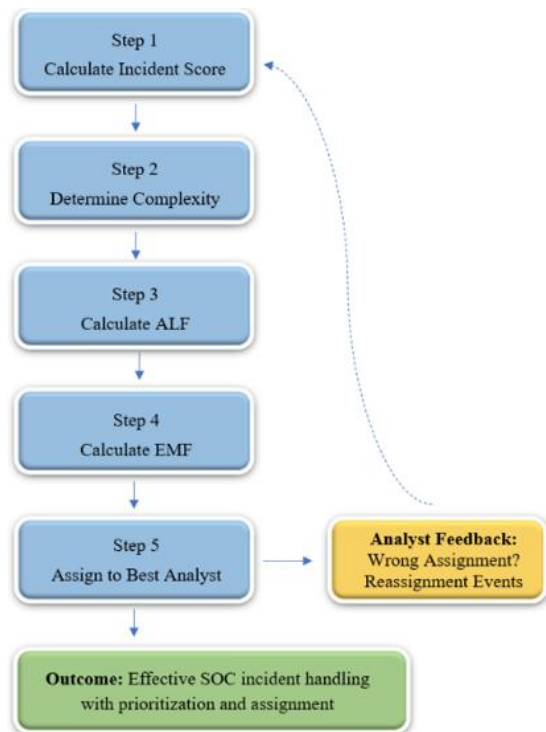


Figure 4. Enhanced dynamic incident assignment flow with analyst feedback loop for learning.

Moreover, the scope of the correlation score mechanism requires significant broadening to improve pattern recognition and campaign-level threat detection. Presently based on a limited set of attributes (source IP, destination IP, and username), future versions should integrate temporal patterns (e.g., frequency bursts), command-line activity indicators, domain names, authentication anomalies, and attack tools. Incorporating MITRE ATT&CK-based tactic and technique mappings into the correlation score can also improve threat classification and enhance alignment with structured adversary behavior frameworks.

Integration with live SOC ecosystems represents another pivotal development trajectory. To ensure operational viability and timeliness, future work should implement real-time data pipelines with external platforms such as SIEM (e.g., Elastic, Splunk), CMDBs, and XDR tools (e.g., SentinelOne, QRadar). API-based synchronization would enable live updates on incident states, analyst capacity, and organizational context, thereby improving responsiveness and reducing reliance on static or outdated data inputs.

Additionally, expanding the EMF to reflect more granular analyst characteristics is a necessary step. Future versions should incorporate analyst specialization

profiles, historical resolution accuracy, domain-based expertise (e.g., cloud security, endpoint threats), and real-time workload fatigue indicators. Such multi-dimensional EMF modeling would support more accurate and equitable incident distribution.

On the validation front, rigorous testing of the model through simulation environments or controlled deployments is imperative. The inclusion of the illustrative case study in this paper was a preliminary step in demonstrating model functionality; however, broader validation with synthetic or real-world datasets remains essential. Generating synthetic incident datasets that simulate realistic SOC alert distributions would allow performance benchmarking under various scenarios (e.g., high alert volume, analyst shortages, APT detection). Time-to-resolution metrics, analyst satisfaction, and reassignment rates could be tracked to evaluate model efficiency and practical benefit. Experimental deployments in enterprise SOC environments, even on a limited scope or shadow mode basis, would offer valuable insights into usability and organizational adoption feasibility.

Finally, a formal computational complexity analysis of the scoring and assignment algorithm should be conducted. In large SOC environments—where n represents the number of incidents and m represents the number of analysts—the overall time complexity of $O(n \times m)$ implies that each incident may need to be evaluated against every analyst. To ensure scalability and maintain low-latency performance under such enterprise-scale conditions, optimization techniques such as batch assignment processing, parallel computation, or heuristic-based filtering should be considered.

In summary, future enhancements to the proposed framework should transform the current theoretical model into a dynamic, intelligent, and integrative decision-support engine capable of adapting to complex SOC environments. By incorporating learning mechanisms, real-time integrations, enriched analytical models, and empirical evaluations, the framework can evolve into a robust operational tool for next-generation cybersecurity incident management.

Ultimately, the proposed framework supports analyst-aware SOC operations by offering a quantifiable and explainable assignment mechanism. Future work will focus on integrating AI-driven adaptivity, real-time SIEM pipelines, and empirical testing to move from conceptual design to full operational deployment.

Author Contributions

The percentages of the authors' contributions are presented below. All authors reviewed and approved the final version of the manuscript.

	E.C.K.	B.C.
C	50	50
D	50	50
S		100
DCP	80	20
DAI	50	50
L	20	80
W	70	30
CR	10	90
SR	50	50
PM	20	80

C=Concept, D= design, S= supervision, DCP= data collection and/or processing, DAI= data analysis and/or interpretation, L= literature search, W= writing, CR= critical review, SR= submission and revision, PM= project management, FA= funding acquisition.

Conflict of Interest

The authors declared that there is no conflict of interest.

Ethical Consideration

Ethics committee approval was not required for this study because of there was no study on animals or humans.

References

- 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., pp. 1-255.
- Binbeshr F, Imam M, Hamdan M, Ghaleb M, Rahim MA,

- Hammoudeh M. 2025. The rise of cognitive SOC: 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, Ehrental 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.
- Vielberth M, Böhm F, Pernul G, Fichtinger I. 2020. Security operations center: A systematic study and open challenges. *IEEE Access*, 8: 227756-227779.
- Villalón-Huerta A, Ripoll-Ripoll I, Marco-Gisbert H. 2022. SOC critical path: A defensive kill chain model. *IEEE Access*, 10: 13570-13581.