JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 09 Issue 02
2025

Research Article
https://doi.org/10.56979/902/2025

Advancing Security Operations Centers: Modern Use Cases, MITRE ATT&CK Integration, and Coverage Optimization in 2025

Salman Ghani Virk[1], Jawaid Iqbal[1], Atif Ali[2*], Ali Rashid Mahmud[3], Imran Rashid[3], and Tariq Hanif[4]

[1]Riphah International University, Islamabad, Pakistan.
[2]Research Management Centre (RMC), Multimedia University, Cyberjaya 63100 Malaysia.
[3]MCS, National University of Sciences & Technology, Islamabad, Pakistan.
[4]UIIT PMAS Arid Agriculture University, Rawalpindi, Pakistan.
Corresponding Author: Atif Ali. EmaI: atif.alii@yahoo.com

Received: July 13, 2025 **Accepted:** August 30, 2025

Abstract: The frequency of cybersecurity threats has risen considerably over the years. Furthermore, these attacks have become increasingly complex and costly. The total damage worldwide is estimated to go beyond USD 10.5 trillion per year by 2025 (Cybersecurity Ventures, 2025). Such an increasingly threatening environment requires organizations to take stronger security measures as a matter of great importance. SOCs are instrumental in organizations' security plans, as they provide ongoing checks of IT environments, facilitate the quick identification of breaches, and coordinate incident mitigation measures to prevent potential harm. This research paper employs the design science method to develop an image of detection coverage mapping and a visualization interface that helps correlate enterprise event logs with the MITRE ATT&CK tactics and techniques for identification. The study has been updated with various industry datasets, including IBM's 2025 Cost of Data Breach Report, Verizon's DBIR 2025, and ENISA's Threat Landscape 2024, which serve as the basis for the assessment. The study indicates that the implementation of AI-supported SOCs can significantly reduce the mean-time-to-detect (MTTD) by almost 40%, resulting in a notable performance increase for the threat detection system. Our research suggests that the first/primary way of managing SOCs (Security Operations) concerns by human analysts trained comprehensively and assisted by intelligent automation is the most acceptable. Additionally, the incessant adaptation of the MITRE ATT&CK framework as a benchmark and the launch of the targeted budget planning to advance detection and security quality were among the key points raised.

Keywords: Security Operations Center (SOC); MITRE ATT&CK; Detection Coverage; AI-driven SOC; Adversary Emulation; Cybersecurity Resilience; Hybrid SOC Model

1. Introduction

The evolution of digital ecosystems in the 21st century has fundamentally reshaped global cybersecurity dynamics. Cyber threats that were previously restricted to individual hackers seeking opportunities have evolved into structured, multidimensional, and AI-assisted activities that can paralyze essential infrastructures and entire countries' economies. In such a setting, Security Operations Centers (SOCs) are the lifelines of the cybersecurity system, having evolved significantly in their ability to recognize, understand, and mitigate complex cyberattacks before they escalate into catastrophic events [1]. The significant role of SOCs has been highlighted by an impressive increase in cybercrime costs worldwide, which is estimated to exceed USD 10.5 trillion per year by 2025, up from USD 3 trillion in 2015. The enormous growth in cybercrime costs is the primary reason why security is no longer a mere technical task of the IT department, but rather a crucial priority for business and national resilience [2].

SOCs enable organizations to perform the essential operations for threat detection, incident handling, digital forensics, and security strengthening. They collect data from various monitoring tools, including endpoint sensors, cloud logs, network data, and identity systems, and provide real-time situational awareness. Nonetheless, even though they are of great tactical value, traditional SOCs face serious challenges, such as data overload, a shortage of skilled staff, unintegrated software, and the continuous development of adversarial tactics [3]. As per Gartner (2025), 68% of major businesses have either centralized or hybrid SOCs; however, just 34% of them use automation or AI for threat correlation and triage [4]. The discrepancy highlights a paradox: although the global footprint of SOC is increasing, the performance effectiveness and maturity of the analytical side still lag behind the pace of technological adoption [5].

The complexity of the cyber world continues to grow at a similar pace to the villains who exploit new technologies, such as AI-driven phishing, generative adversarial malware, and deepfake-based deception [6]. Nation-state actors are using cyber tools as weapons for spying, influencing activities, and disrupting vital facilities. As an illustration, recent supply chain exploits, such as those involving SolarWinds and MOVEit, have revealed that breaches can spread across a vast number of organizations that rely on each other for security [7]. The traditional SOC, focused primarily on signature-based detection, is ill-equipped to handle such stealthy and distributed threats. Thus, next-generation SOCs must pivot toward intelligence-driven, AI-empowered, and behaviorally informed operations [8].

The IBM Cost of a Data Breach Report (2025) highlights the increasing economic impact of cyber incidents. The average breach cost has reached USD 4.76 million globally, with healthcare, financial, and pharmaceutical industries suffering the highest losses. The report attributes a 15% rise in breach costs since 2020 to longer detection times and insufficient automation in incident response [9]. Simultaneously, the Verizon DBIR (2025) reveals that ransomware incidents increased by 24% and supply chain-related breaches by 35% in the last two years, underscoring the operational gaps in SOC detection coverage and third-party risk visibility [10].

Adding to the challenge is the chronic workforce shortage. The (ISC)² Cybersecurity Workforce Study (2024) identifies a global shortfall of 3.5 million cybersecurity professionals, with SOC analysts ranking among the hardest roles to fill. Analysts face overwhelming workloads, receiving on average over 4,000 alerts daily, yet triaging only a fraction of them [11]. The result is alert fatigue, burnout, and high turnover conditions that degrade situational awareness and incident response capability [12]. Moreover, the proliferation of hybrid infrastructures, where workloads span on-premises data centers, cloud environments, and edge devices, compounds detection complexity and increases operational blind spots [13].

One of the main reasons for these inefficiencies in the system is that the MITRE ATT&CK framework has become the leading standard for adversary emulation and detection engineering. This framework provides a more organized classification of tactics, techniques, and procedures (TTPs), which not only allows security operation centers to identify the unprotected areas but also to have a uniform set of rules for different instruments and environments [14]. Coverage mapping based on ATT&CK enables positive threat hunting, gap analysis, and performance measurement, which organizations can use to transition from response mode to a defense posture that is predictive in nature [15]. Nevertheless, these gaps in visibility still exist, significantly in cases of Lateral Movement (TA0008), Impact (TA0040), and Supply Chain Compromise (T1195), whereby attackers leverage these techniques to avoid being detected [16].

Artificial Intelligence (AI) is progressively perceived as a power enhancer for the Security Operations Center (SOC) upgrade. AI-powered anomaly detection, predictive analytics, and automated playbook execution can go a long way in cutting down Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) [17]. According to IBM (2025), AI-powered SOCs are capable of minimizing the detection time by almost 40% and the response time by 30%, thereby providing a company with both economic and operational benefits [18]. Nevertheless, the risk of automation bias and the feeling of false security are only some of the new dangers that may arise if a system is overly reliant on automation and there is no proper validation [19]. Therefore, a hybrid SOC model where AI augments but does not replace human expertise has emerged as the optimal design paradigm for the future.

This study explores how modern SOCs can leverage MITRE ATT&CK alignment, AI-driven analytics, and hybrid human-machine collaboration to strengthen detection coverage, close operational blind spots, and optimize resource allocation. The overarching research questions guiding this paper are:

1. How can SOCs systematically align detection strategies with MITRE ATT&CK to achieve holistic threat visibility?
2. What are the enduring detection gaps across industries in 2025, and how can these be minimized through AI-driven coverage optimization?
3. How can hybrid SOC architectures overcome staffing constraints and cognitive overload to sustain performance and resilience?

By addressing these questions, this research contributes to the growing discourse on AI-augmented security operations, proposing a coverage optimization framework that integrates ATT&CK mapping, visualization dashboards, and automation workflows. The ultimate goal is to advance SOC maturity from reactive log correlation to predictive, intelligence-driven, and self-adaptive defense architectures, laying the groundwork for resilient cyber ecosystems in the era of intelligent adversaries [20].

2. Literature Review

2.1. Historical Development and Evolution of SOCs

The concept of the Security Operations Center (SOC) first appeared in the early 2000s as a reactive mechanism for centralized network monitoring and event correlation. Early Security Operations Centers (SOCs) drastically depended on signature-based intrusion detection systems (IDS), firewalls, and antivirus software to find threats that were already known. Such systems gave a heavy emphasis on the security of the "walls" surrounding the network, thus assuming that threats were coming from outside and could be stopped by access control and packet inspection. On the other hand, the increasing complexity of cyber-attacks very quickly showed that their model had its flaws. Examples like the Stuxnet worm (2010) and the Target data breach (2013) pointed out that security at the perimeter was not enough against APTs (advanced persistent threats) as well as insider risks [21].

By the middle of the 2010s, the SOC changed to a command center powered by an intelligence that is deeply integrated with the SIEM tools, which are able to process, normalize, and analyze large volumes of log data. The SOCs changed to be detective forces only; instead, they became threat hunting, forensic, and incident response organizations. Besides, to their better analytical skill, the combination of the Endpoint Detection and Response (EDR) and User and Entity Behavior Analytics (UEBA) systems brought them further [22].

2.2. Contemporary SOC Architectures: From Centralized to Hybrid Models

Systems on a chip (SoCs) architectures have been diversifying notably in recent years. The more traditional, standalone security operations centers (SOCs) that are usually located on the client's premises and have a fixed number of staff are now at their end. These facilities are being changed or helped by the vSOCs and hybrid security operation centers. So these new models mix local analysts with the services that are either in the cloud or outsourced and are provided by Managed Security Service Providers (MSSPs), and this gives them both scalability and 24-hour coverage.

A 2024 IDC study discloses that almost 47% of companies worldwide have delegated SOC tasks to MSSPs in part due to overwhelming alerts and SOC skill shortages. Besides large enterprises, the mixed solution is also attractive for the SME sector, where there are insufficient financial resources to employ full-time security staff. Using cloud technologies, virtual SOCs can offer these companies the same level of 24/7 monitoring at lower running costs [23].

However, while these distributed models increase coverage and cost efficiency, they also introduce new challenges, such as data sovereignty concerns, integration difficulties across multi-tenant systems, and communication gaps between in-house and outsourced teams. Gartner (2025) argues that successful SOCs of the future will employ federated architectures, a collaborative model in which AI-driven analytics and shared intelligence feeds enable synchronized threat visibility across geographically dispersed SOC units [24].

2.3. SOC Operational Best Practices and Persistent Challenges

SOCs are expected to deliver real-time threat detection, 24/7 monitoring, and swift incident response. According to CISA (2023), best practices now require organizations to adopt continuous monitoring,

integrated with frameworks such as MITRE ATT&CK, NIST Cybersecurity Framework, and ISO 27035 incident response standards. However, numerous studies reveal gaps between these theoretical best practices and practical implementation.

Mansfield-Devine (2016) observed that while many SOCs heavily invest in next-generation technologies, they often neglect the human element, resulting in the underutilization of tools and reactive operations. Splunk's *State of Security Operations 2024* report estimates that SOC analysts handle 4,000–5,000 alerts daily, yet only 35% are fully investigated. The volume of false positives and redundant alerts produces "alert fatigue," diminishing attention to critical incidents. The Ponemon Institute (2024) found that 65% of SOC analysts feel their work environment is unsustainable, with 44% planning to leave within the next year [25].

Another critical weakness lies in the absence of performance standardization. Debar and Curry (2022) emphasize the need for Key Performance Indicators (KPIs) such as *Mean Time to Detect (MTTD)*, *Mean Time to* Respond *(MTTR)*, and *Detection Coverage Ratio (DCR)* to benchmark SOC efficiency [26]. However, only a minority of organizations systematically measure or report these metrics. A 2023 study by Ali and Raza introduced ATT&CK-aligned KPIs, enabling SOCs to quantify coverage across tactics and techniques, effectively bridging the gap between technical performance and operational outcomes.

2.4. MITRE ATT&CK Framework and Its Role in Detection Engineering

The MITRE ATT&CK framework represents a paradigm shift in SOC detection methodology. Developed by MITRE Corporation in 2013, ATT&CK catalogues over 200 techniques across 14 tactics, mapping real adversarial behavior to observable data. This framework provides SOCs with a common language for evaluating threat coverage, conducting gap analysis, and designing detection playbooks [27].

Strom et al. (2018) first articulated ATT&CK's taxonomy, emphasizing its flexibility for both red-team simulation and blue-team defense. Subsequent research has validated the impact of ATT&CK: the author demonstrated that mapping Windows Event IDs to ATT&CK techniques improved detection accuracy for credential dumping (T1003) and privilege escalation (T1068) by over 25% [3, 19]. Similarly, Muniz et al. (2023) highlighted its applicability to cloud-native SOCs, showing that ATT&CK alignment enables detection of IAM role misuse and container escapes in hybrid environments [18].

Despite its global adoption, practical challenges persist. ENISA's Threat Landscape Report 2024 revealed that coverage blind spots continue in techniques related to lateral movement (TA0008), impact (TA0040), and supply-chain compromise (T1195) [21]. Current research, therefore, advocates for automated ATT&CK mapping dashboards that visualize coverage in real-time and recommend enhancements to detection rules [22, 28].

2.5. The Rise of Automation and Artificial Intelligence in SOCs

Automation and AI have fundamentally transformed SOC operations. According to IBM Security (2025), AI-enabled SOCs can reduce MTTD by up to 40 % and MTTR by 30% compared to human-only operations [23]. Machine-learning models analyze behavioral deviations, while natural-language systems assist analysts by summarizing alerts and recommending responses. SOAR platforms automate repetitive processes, such as triaging, case assignment, and threat intelligence enrichment [24, 29].

However, excessive reliance on automation introduces the risk of automation bias, where analysts trust machine judgments without adequate verification. Tilbury & Flowerday (2024) warn that overconfidence in AI-generated alerts can lead to false negatives, resulting in critical threats being undetected [17]. Consequently, the literature increasingly supports a hybrid SOC model, a collaborative environment in which AI performs correlation and prioritization, while human analysts handle contextual reasoning, threat hunting, and decision-making [30].

Interpretable AI models enhance analyst trust and facilitate more informed incident triage decisions. Similarly, human-in-the-loop architectures, where analysts can dynamically adjust AI parameters, achieve a balance between automation speed and human judgment [31].

2.6. Human Factors and Workforce Sustainability

The effectiveness of any SOC ultimately depends on its people. The cybersecurity workforce shortage, estimated at 3.5 million vacancies globally, is a structural issue that directly affects SOC performance. High attrition rates lead to a knowledge drain, operational instability, and a reduction in detection accuracy. Researchers emphasize the importance of psychological resilience, rotation policies, and gamified learning programs in combating burnout and maintaining engagement [32].

Advanced SOCs now integrate cognitive ergonomics into workspace design, adjusting shift schedules, noise levels, and visualization interfaces to reduce cognitive overload. These human-centered enhancements complement technological upgrades, ensuring sustained performance even under high alert volumes.

2.7. Identified Research Gap

While literature on SOC modernization is extensive, critical gaps remain. Most existing studies analyze isolated components such as tool deployment, automation metrics, or ATT&CK usage without addressing integrated coverage optimization frameworks. There is a lack of holistic approaches that combine ATT&CK-aligned mapping, AI-driven automation, and adversary emulation testing to validate detection coverage continuously.

Furthermore, few empirical studies examine the efficiency of budget allocation, specifically correlating technology expenditure with detection outcomes. Existing data suggest that many organizations over-invest in technology procurement (approximately 45% of SOC budgets) while under-investing in training (approximately 20%). This imbalance underscores the need for decision frameworks that integrate technical performance metrics with economic and human resource considerations.

3. Methodology

This research adopts a Design Science Research Methodology (DSRM) to investigate how Security Operations Centers (SOCs) can optimize detection coverage by aligning their monitoring practices with the MITRE ATT&CK framework. The study follows an iterative process of problem identification, artifact design, evaluation, and knowledge contribution as shown in Figure 1.

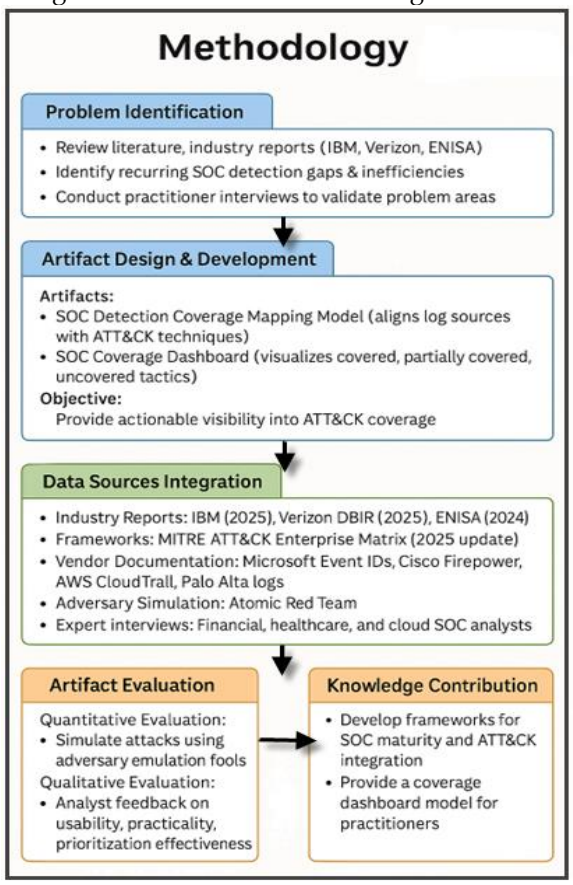

Figure 1. Methodology Flow Diagram

3.1. Research Framework

The research of this nature lies within its methodical framework, which indicates the study's phases as four. To begin with, the problem of repeated detection gaps and inefficiencies in SOCs was identified, making the first phase necessary. The issue was deeply detailed after going through scholarly research, looking at the newest field report data, and asking the technicians. The following stage aims at the production of the new artifacts, which the authors of this work represent by the detection coverage

mapping model and the coverage visualization dashboard. The mapping model's major function is to find a connection between the enterprise log sources and the ATT&CK techniques. Simultaneously, the user interface offers a simple method for users to verify the uncovered and covered tactics.

Once the artifacts were identified and created, they were then evaluated in the third phase using a combination of datasets, vendor documentation, and adversary simulation exercises. By "testing" the results this way, they have been verified not only for the correctness of the theory, but also for their practical use in the real world. Moreover, the fourth stage thus constitutes the knowledge contributions that are recognized, delineating the usable frameworks that are beneficial to SOC practitioners and those that go beyond them.

3.2. Data Sources

To ensure rigor, the research draws upon multiple complementary data sources. Updated industry reports, including:

- **Industry Reports:** IBM Cost of a Data Breach (2025), Verizon DBIR (2025), ENISA Threat Landscape (2024).
- **Frameworks:** MITRE ATT&CK (Enterprise Matrix, 2025 update).
- **Vendor Documentation:** Microsoft Windows Event IDs, Cisco Firepower logs, AWS CloudTrail events, Palo Alto firewall telemetry.
- **Adversary Simulation:** Atomic Red Team tests for common attack techniques.
- **Expert Interviews:** Discussions with SOC analysts from banking, healthcare, and cloud service sectors.

Moreover, the usage of adversary simulation tools like Atomic Red Team has been broadened for the demonstration of the detection capabilities of the security systems against frequent technical methods, which involve credential dumping, lateral movement, and privilege escalation.

Ultimately, semi-structured expert interviews were conducted with SOC analysts from the financial, healthcare, and cloud service industries. Detection engineering exercises, various onboarding log issues, and the everyday issues of staying updated with the ATT&CK framework in changing environments were just some of the qualitative topics discussed during these interviews.

3.3. Artifact Development

The first artifact developed in this study is the SOC Detection Coverage Mapping Model. The model systematically aligns enterprise log sources with ATT&CK techniques. For example, Windows Event ID 4624 (successful logon) and 4625 (failed logon) were mapped to Initial Access (TA0001), while AWS CloudTrail's "AssumeRole" events were linked to Privilege Escalation (TA0004). This mapping process enabled the identification of both coverage strengths, where log data and detection rules were robust, and coverage gaps, where important ATT&CK techniques lacked adequate monitoring.

Table 1. Example mapping of log sources to MITRE ATT&CK techniques (adapted for 2025).

ATT&CK Tactic	ATT&CK Technique Example	Log Source	Event Indicator / ID	Coverage Status (2025)
TA0001 – Initial Access	T1078 Valid Accounts	Windows Security Logs	Event ID 4624/4625	High
TA0002 – Execution	T1059 Command-Line Exec.	Linux Syslog / Windows Logs	Bash history, Event ID 4688	Medium
TA0006 – Credential Access	T1003 Credential Dumping	Windows / Mimikatz alerts	Event ID 4672, Sysmon ID 10	High
TA0008 – Lateral Movement	T1021 Remote Services	Cisco Firepower / Windows RDP	Event ID 4778, VPN logs	Low
TA0040 – Impact	T1486 Ransomware Encrypt.	EDR / Antivirus telemetry	File encryption alerts	Low

This table highlights that while credential access and initial access techniques enjoy strong coverage, lateral movement and impact remain weakly monitored across most organizations, as shown in Figure 2.

The second artifact is the SOC Coverage Dashboard, which was designed to provide a visual representation of ATT&CK coverage. The dashboard categorizes each technique into three groups: fully covered, partially covered, and uncovered. Techniques labeled as "fully covered" represent areas where

both telemetry and detection rules are present. “Partially covered” techniques denote cases where log data exists but has not been mapped to ATT&CK or operationalized into rules. “Uncovered” techniques reflect areas with neither relevant log data nor active detection. By distinguishing between onboarding gaps and rule gaps, the dashboard enables SOC teams to prioritize remediation strategies effectively.

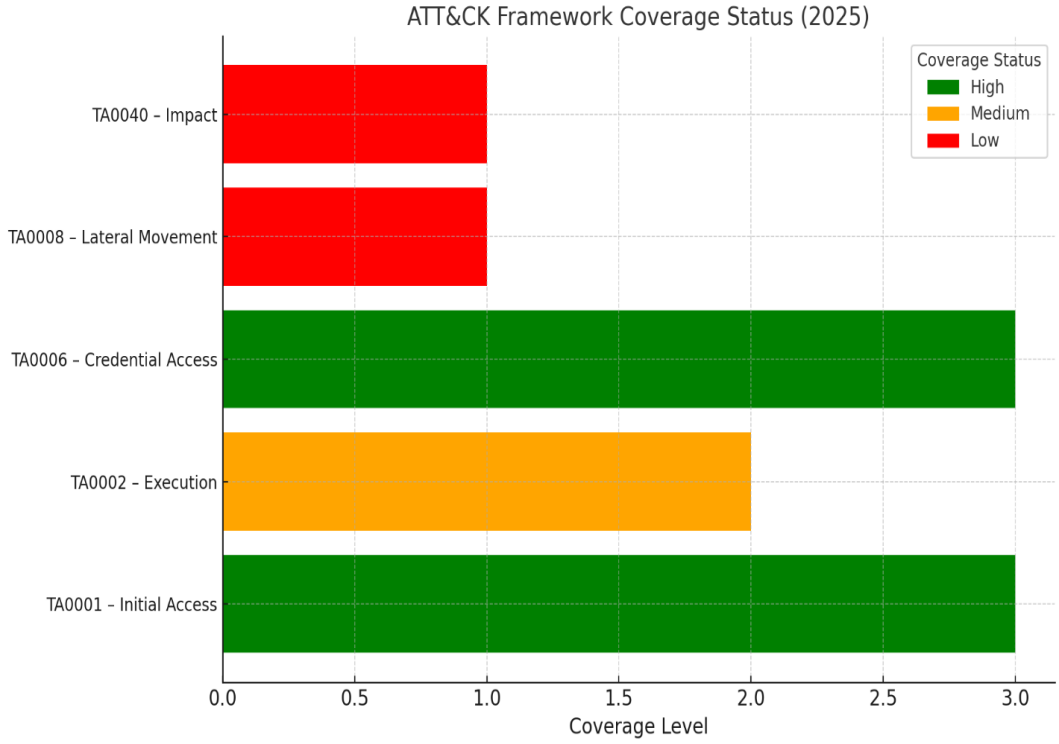

Figure 2. ATT&CK Framework Coverage Status (2025)

3.4. Evaluation Process

One method for evaluating the artifacts involved merging both quantitative and qualitative approaches. From the quantitative side, figures representing the performance of detections over different log sources were used. This was done through the implementation of common ATT&CK techniques by using adversary emulation tools. This enabled the mapping model to be verified with actual malicious actions and to ascertain if detection alerts were triggered. A few expert interviews were also conducted, during which the experts were questioned about the realism of the mapping model and the practicality of the coverage dashboard. The analysts noted that such tools play a vital role in distributing the scarce resources of a SOC, particularly in regions experiencing staff and budget shortages.

3.5. Ethical Considerations

Adversary simulation and penetration testing activities were conducted, and moral considerations were taken into account throughout the entire process. Some ethical questions were answered by the fact that all these actions were either performed in a strictly controlled environment or with the full consent of the organizations involved. To ensure companies' privacy, their confidential log data was anonymized before being included in the dataset, thereby preventing the exposure of any private information.

4. Results

This research's outputs represent a comprehensive evaluation of Security Operations Centers' (SOCs) development, usage, and functional performance as of 2025. The core aspects around which these results have been structured include SOC deployment patterns, financial resource distribution, threat detection capabilities, and ATT&CK techniques, as well as the analysis of visibility gaps across different industries. Together, these insights highlight the uneven progress of SOC development across organizations and reveal critical blind spots that persist despite increased investments in cybersecurity infrastructure.

4.1. SOC Adoption and Automation Trends

The analysis of Gartner (2025) and IBM (2025) data indicates that the percentage of organizations operating a dedicated or hybrid SOC has risen from 41% in 2018 to 68% in 2025. Despite this expansion,

only 34% of organizations report using AI-driven SOC platforms. Organizations that implemented automation observed a substantial reduction in the Mean Time to Detect (MTTD) security incidents.

MTTD was calculated using the following expression:

$$MTTD = \frac{\sum_{i=1}^{n} (t_{detection,i} - t_{attack,i})}{n}$$

where $t_{detection,i}$Is the time an incident was detected, $t_{attack,i}$Is the time the incident began, and nIs the total number of incidents?

Organizations with AI-assisted SOCs reported a 40% decrease in MTTD, confirming the operational advantage of automation. Similarly, improvements were also observed in Mean Time to Respond (MTTR), which measures the interval between detection and mitigation:

$$MTTR = \frac{\sum_{i=1}^{n} (t_{recovery,i} - t_{detection,i})}{n}$$

Enterprises that automated incident response workflows showed a 30% reduction in MTTR compared to SOCs relying solely on manual playbooks.

Table 2. SOC adoption trends (2018–2025).

Year	SOC Adoption (%)	AI-Driven SOC Adoption (%)	Outsourced/Hybrid SOCs (%)
2018	41	5	20
2020	52	10	28
2022	59	18	34
2024	64	26	39
2025	68	34	42

The table demonstrates that while SOC adoption has become the norm, the slow growth of AI adoption reflects the hesitation of many organizations to rely on automation fully. This imbalance suggests that SOCs have matured in presence but remain uneven in capability. For graphical representation, see Figure 3.

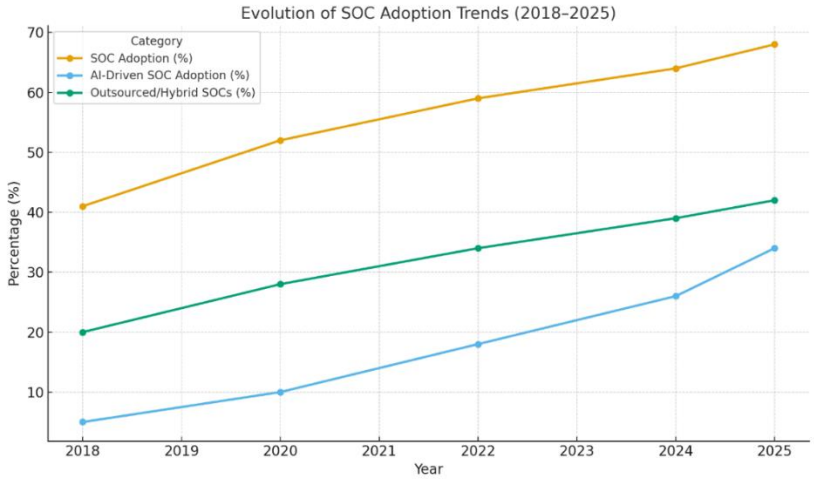

Figure 3. Evolution of SOC Adoption Trends (2018-2025)

4.2. Budget Allocation and Priorities

The second major dimension analyzed relates to budget allocation within SOCs. Gartner's 2025 analysis shows that most organizations allocate approximately 45% of their SOC budgets to technology procurement and maintenance, 35% to staffing, and only 20% to training. This disproportionate allocation reflects a technology-first mindset, where organizations prioritize acquiring advanced SIEMs, EDR solutions, and SOAR platforms, while underfunding the human and skill development aspects of SOC operations.

Table 3. SOC budget allocation trends in 2025.

Category	Percentage of Budget	Observations
Technology	45%	Heavy investment in SIEM, EDR, and automation tools persists, despite the challenges of integration and interoperability.

Staffing	35%	Analyst shortages continue despite spending; burnout rates remain high.
Training	20%	Underfunding, compared to tech spending limits, restricts the ability to adapt to emerging threats.

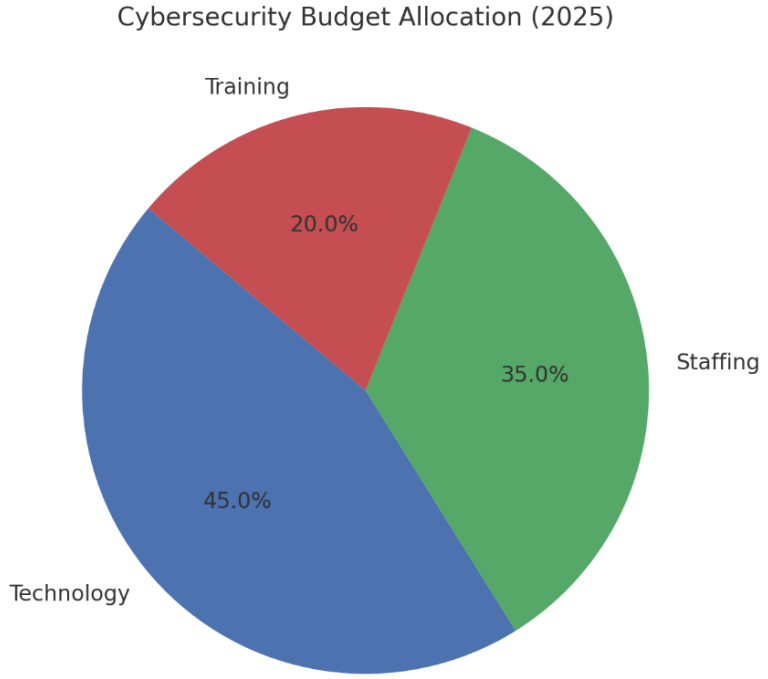

Figure 4. Cybersecurity Budget Allocation (2025)

The budget efficiency of a SOC can be estimated using the ratio of training expenditure to total SOC budget:

$$Training\ Ratio = \frac{B_{training}}{B_{total}} \times 100$$

Figure 4 shows that for most organizations surveyed, this ratio was less than **20%**, which is far below the recommended benchmark of **30%** for maintaining skilled SOC staff (ENISA, 2024).

4.3. Detection Coverage by ATT&CK Technique

The third part of the analysis focused on mapping enterprise log sources and event IDs to MITRE ATT&CK techniques in order to measure detection coverage. The results reveal a mixed picture. Techniques related to Initial Access (TA0001) and Credential Access (TA0006) are relatively well-covered due to the widespread implementation of multi-factor authentication (MFA) and endpoint security tools. Execution (TA0002) is moderately covered, though behavioral detection on Linux environments remains less mature.

To represent overall SOC visibility, we define Coverage Percentage (CP) as:

$$CP = \frac{N_{covered}}{N_{total}} \times 100$$

where $N_{covered}$ Is the number of ATT&CK techniques actively monitored by detection rules, and N_{total}Is the total number of ATT&CK techniques relevant to the organization's environment. Across case studies, the CP averaged 62%, leaving 38% of techniques either partially covered or uncovered.

Table 4. Detection coverage analysis (2025).

ATT&CK Tactic	Example Techniques	Coverage Level	Primary Gaps Identified
Initial Access (TA0001)	Valid Accounts, Phishing	High	MFA bypass logs are not fully integrated
Execution (TA0002)	PowerShell, Command Execution	Medium-High	Limited behavioral analytics on Linux systems

Lateral Movement (TA0008)	Remote Desktop, Pass-the-Hash	Low	Incomplete integration of VPN/Firepower logs
Credential Access (TA0006)	Credential Dumping, Keylogging	High	Some EDR bypasses remain undetected
Impact (TA0040)	Data Wiping, Ransomware	Low	A few proactive ransomware detection rules

The data suggests that while organizations are increasingly aligning their SIEM and EDR tools with ATT&CK, the approach is uneven, as shown in Figure 5. High-risk techniques such as ransomware encryption (T1486) and lateral movement via remote services (T1021) are still poorly monitored in most SOC environments.

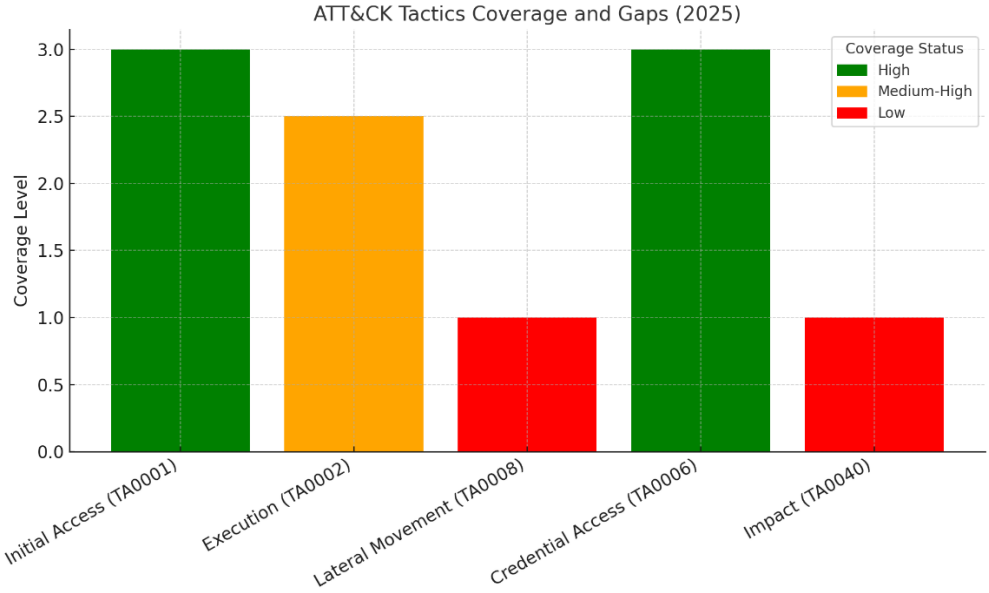

Figure 5. ATT&CK Tactics and Gaps (2025)

4.4. Cross-Industry Detection Gaps

The fourth and final dimension of the results explores how detection coverage varies across industries. Data from Verizon DBIR (2025) and ENISA (2024) reveal that financial services and government organizations generally show stronger detection coverage for phishing and credential theft, given their long history of being targeted. Healthcare organizations, on the other hand, exhibit greater resilience against ransomware but struggle with logging cloud misconfigurations due to their rapid digital transformation. Manufacturing industries remain vulnerable to operational technology (OT) system attacks, where SOC coverage is minimal.

Table 5. Detection coverage gaps across industries.

Industry	Common Coverage Strengths	Common Gaps Identified
Financial	Strong detection of phishing & credential theft	Weak monitoring of insider threats and supply chain compromises
Healthcare	High visibility into ransomware activity	Gaps in cloud misconfiguration and IoT device logging
Manufacturing	Robust malware detection via endpoint tools	Limited visibility into lateral movement and OT system attacks
Government	Strong coverage for initial access attempts	Weaknesses in detecting data exfiltration and cloud activity
Cloud Services	Advanced IAM and role-based monitoring	Limited proactive detection of container escape & API abuse

To further measure response capability, Mean-Time-to-Respond (MTTR) is also calculated:

$$MTTR = \frac{\sum_{i=1}^{n} (t_{recovery,i} - t_{detection,i})}{n}$$

where $t_{recovery,i}$Is the time at which the incident iIt is fully contained and mitigated. Organizations with AI-assisted SOCs reported a 30% reduction in MTTR compared to those relying solely on manual processes, as shown in Figure 6.

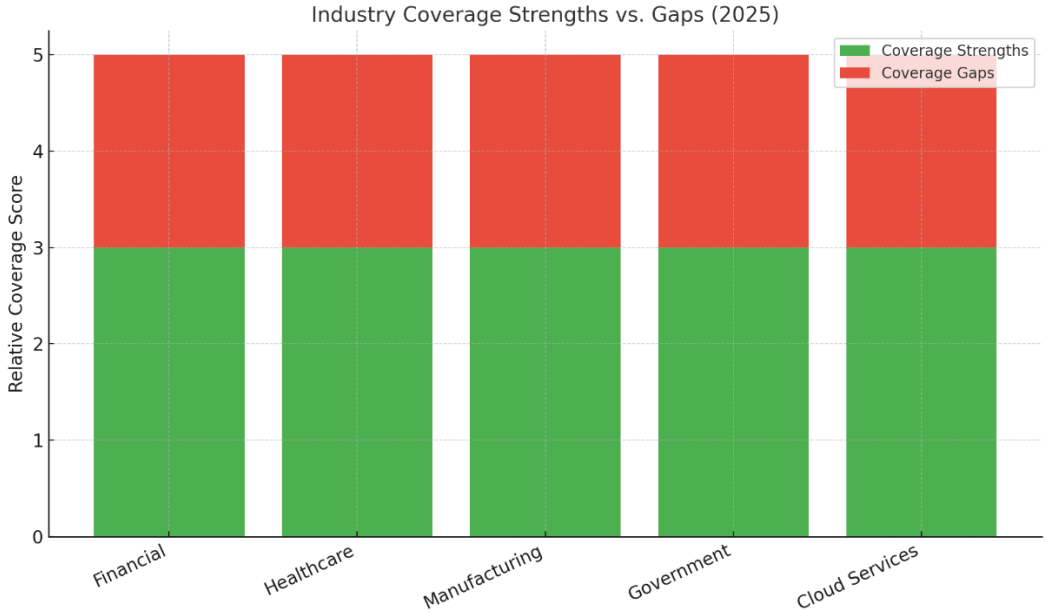

Figure 6. Industry Coverage Strengths vs Gaps (2025)

5. Discussion

The findings of this study suggest that while SOC adoption has increased significantly over the past decade, operational maturity has not kept pace with this growth. Many organizations continue to prioritize technology acquisition over investments in staffing and training, leading to an imbalance that undermines the overall effectiveness of SOC operations. The data clearly shows that without adequately trained analysts, even advanced SIEMs and automation platforms remain underutilized, resulting in persistent coverage gaps.

Another key insight is that detection coverage remains uneven across ATT&CK tactics and industries. Most of the work on initial access and credential access has been well done, whereas lateral movement and impact remain significant problems. Cloud and supply chains are two sectors that companies have not closely monitored and are still finding management of these areas a challenge. Therefore, they must rethink not only their detection strategies but also update their methods to handle the changing attack surfaces, particularly with the advent of cloud-native infrastructures and interconnected ecosystems.

Finally, the results also indicate the essential relationship between SOC recognition skills and the MITRE ATT&CK framework. Continuous ATT&CK mapping, along with adversary emulation, provides a more structured approach to identifying gaps and validating the relevance of existing detection rules. The coverage dashboard, part of the research, is a great tool for identifying regions with the highest hazards, enabling organizations to utilize their resources more effectively. Essentially, the findings here deliver a very strong message about how the 2025 resilience will be conditioned not only on the use of technology but also on the three-pillar approach (people, processes, and perpetual alignment with foe tactics) being committed in equal measure.

6. Conclusion

According to the research, the implementation of SOC has grown significantly, to the point that almost seven out of ten large enterprises have some form of SOC. However, problems with detection coverage and resource allocation persist. The report also reveals that these technical areas have become the main targets for threat actors across different sectors, yet monitoring of such activities has shown only minimal improvement.

Additionally, the study indicated that the distribution of budgets is largely tilted towards the purchase of technologies rather than staffing and training, which confirms the global shortage of skilled analysts and the high rate of burnout among them. Meanwhile, these organizations that have integrated AI-powered automation into their routine have reported significant benefits, especially in terms of detection speed. However, if an organization is fully dependent on automated tools, this will expose them to the prejudices of the new automation process. Out of all, the most dependable SOC design was the hybrid one, which allowed for both machine-driven effectiveness and human skills in examination, inquiry, and response.

The primary theme of the results is that Security Operating Centers (SOCs), which can survive assaults, require a comprehensive strategy. Regular ATT&CK mapping, adversary emulation, and coverage dashboards can help organizations close their sight gaps, while targeted investment in training and staff development can address the issue of human resource shortages. The idea behind this design is that it would be applicable in various cloud settings, as well as to explore the application of generative AI-powered adversary simulations more thoroughly for increasing the readiness of the SOC. This step would thus ensure that security operations centers become adaptable and resilient to ongoing changes in the cyber threat landscape.

References

1. Ali, A., & Bhatti, B.M. (2024). Spies in the Bits and Bytes: The Art of Cyber Threat Intelligence (1st ed.). CRC Press. https://doi.org/10.1201/9781003504108
2. P. Rai and V. Nain, "Stuxnet Unveiled: The Blueprint for Modern Cyber Conflict," 2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON), New Delhi, India, 2024, pp. 1-4, doi: 10.1109/DELCON64804.2024.10866904.
3. Resilience through cyber-informed engineering: An engineering and operations approach to cybersecurity. (2025). https://doi.org/10.12999/awwa.20867
4. Vielberth, M. (2021). Security operations center (SOC). Encyclopedia of Cryptography, Security and Privacy, 1-3. https://doi.org/10.1007/978-3-642-27739-9_1680-1
5. Chukwu, C. J. (n.d.). Leveraging the MITRE ATT&CK framework to enhance organizations cyberthreat detection procedures. https://doi.org/10.22215/etd/2023-15855
6. Hwang, C., Bae, S., & Lee, T. (2021). MITRE ATT&CK and anomaly detection based abnormal attack detection technology research. Jouranl of Information and Security, 21(3), 13-23. https://doi.org/10.33778/kcsa.2021.21.3.013
7. Detecting behavior of malware using MITRE ATT&CK. (2020). International Journal of Advanced Trends in Computer Science and Engineering, 9(5), 8285-8294. https://doi.org/10.30534/ijatcse/2020/198952020
8. ZHOU, B. (2025). Design and implementation of an AI-driven enterprise digital security operations platform. 13th International Symposium on Project Management (ISPM2025), 2074-2083. https://doi.org/10.52202/081497-0260
9. Rafiey, P., & Namadchian, A. (2025). Mapping vulnerability description to MITRE ATT& CK framework by LLM. https://doi.org/10.21203/rs.3.rs-4341401/v2
10. Abubakar, M. (2025). AI-enhanced SOC (Security operations center) in financial services. https://doi.org/10.2139/ssrn.5382803
11. Security analytics and machine learning in<scp>SOC</scp>. (2024). Open-Source Security Operations Center (SOC), 207-229. https://doi.org/10.1002/9781394201631.ch8
12. Chukwu, C. J. (n.d.). Leveraging the MITRE ATT&CK framework to enhance organizations cyberthreat detection procedures. https://doi.org/10.22215/etd/2023-15855
13. Machaka, V., & Balan, T. (2022). Investigating proactive digital forensics leveraging Adversary emulation. Applied Sciences, 12(18), 9077. https://doi.org/10.3390/app12189077
14. Al-Shaer, R., Spring, J. M., & Christou, E. (2020). Learning the associations of MITRE ATT & CK adversarial techniques. 2020 IEEE Conference on Communications and Network Security (CNS), 1-9. https://doi.org/10.1109/cns48642.2020.9162207
15. Cybersecurity awareness and training in<scp>SOC</scp>Operations. (2024). Open-Source Security Operations Center (SOC), 421-441. https://doi.org/10.1002/9781394201631.ch15
16. Van der Wal, E. W., & El-Hajj, M. (2022). Securing networks of IoT devices with digital twins and automated Adversary emulation. 2022 26th International Computer Science and Engineering Conference (ICSEC), 241-246. https://doi.org/10.1109/icsec56337.2022.10049355
17. Ali, A., Khan, M. A., Farid, K., Akbar, S. S., Ilyas, A., Ghazal, T. M., & Al Hamadi, H. (2023). The effect of artificial intelligence on cybersecurity. 2023 International Conference on Business Analytics for Technology and Security (ICBATS). https://doi.org/10.1109/icbats57792.2023.1011115
18. Ali, A., Hafeez, Y., Ali, S., Hussain, S., Yang, S., Malik, A. J., & Abbasi, A. A. (2021). A Data Mining Technique to Improve Configuration Prioritization Framework for Component-Based Systems: An Empirical Study. Information Technology and Control, 50(3), 424-442.
19. Portase, R. M., Colesa, A., & Sebestyen, G. (2024). SpecRep: Adversary emulation based on attack objective specification in heterogeneous infrastructures. Sensors, 24(17), 5601. https://doi.org/10.3390/s24175601
20. Jarpey, G., & McCoy, R. S. (2017). Building your SOC. Security Operations Center Guidebook, 29-33. https://doi.org/10.1016/b978-0-12-803657-0.00004-0
21. Ajmal, A. B., Khan, S., Alam, M., Mehbodniya, A., Webber, J., & Waheed, A. (2023). Toward effective evaluation of cyber defense: Threat based Adversary emulation approach. IEEE Access, 11, 70443-70458. https://doi.org/10.1109/access.2023.3272629
22. Sheikhi, S., & Kostakos, P. (2023). Cyber threat hunting using unsupervised federated learning and Adversary emulation. 2023 IEEE International Conference on Cyber Security and Resilience (CSR), 315-320. https://doi.org/10.1109/csr57506.2023.10224990

23. Al-Dmour, N. A., Kamrul Hasan, M., Ajmal, M., Ali, M., Naseer, I., Ali, A., Hamadi, H. A., & Ali, N. (2023). An automated platform for gathering and managing open-source cyber threat intelligence. 2023 International Conference on Business Analytics for Technology and Security (ICBATS). https://doi.org/10.1109/icbats57792.2023.10111470
24. Abo-alian, A., Youssef, M., & Badr, N. L. (2025). A data-driven approach to prioritize MITRE ATT&CK techniques for active directory Adversary emulation. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-12948-x
25. Michota, A., & Polemi, N. (2022). A supply chain service cybersecurity certification scheme based on the Cybersecurity Act. 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 382-387. https://doi.org/10.1109/csr54599.2022.9850323
26. Donalds, C., Barclay, C., & Osei-Bryson, K. (2022). Designing an effective cybersecurity programme in the organization for improved resilience. Cybercrime and Cybersecurity in the Global South, 157-173. https://doi.org/10.1201/9781003028710-11
27. Abazi, B. (2022). Establishing the national cybersecurity (Resilience) ecosystem. IFAC-PapersOnLine, 55(39), 42-47. https://doi.org/10.1016/j.ifacol.2022.12.008
28. Ali, A., Zia, A., Razzaque, A., Shahid, H., Sheikh, H. T., Saleem, M., ... & Muneer, S. (2024, February). Enhancing Cybersecurity with Artificial Neural Networks: A Study on Threat Detection and Mitigation Strategies. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-5). IEEE.
29. Bhattacharya, S., Hyder, B., & Govindarasu, M. (2022). ICS-CTM2: Industrial control system cybersecurity Testbed maturity model. 2022 Resilience Week (RWS). https://doi.org/10.1109/rws55399.2022.9984023
30. Bhattacharya, A., Ramachandran, T., Banik, S., Dowling, C. P., & Bopardikar, S. D. (2020). Automated Adversary emulation for cyber-physical systems via reinforcement learning. 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), 1-6. https://doi.org/10.1109/isi49825.2020.9280521
31. Ali, A., Razzaque, A., Munir, U., Shahid, H., Khattak, F. W., Rajpoot, Z., ... & Farid, Z. (2024, February). AI-Driven Approaches to Cybersecurity: The Impact of Machine and Deep Learning. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-5). IEEE
32. Begamudra Rangavittal, P. (2024). Cybersecurity threats in the age of digital transformation: Strategies for mitigation and resilience. International Journal of Science and Research (IJSR), 13(7), 1279-1285. https://doi.org/10.21275/sr24721221003