International Journal of Scientific Interdisciplinary Research

Volume: 5; **Issue:** 2
Pages: 678– 719

MITRE ATT&CK–Driven Threat Hunting in A SOC Environment: a Real-World Case Study Using SPLUNK Correlation Rules

MD Zahedul Islam[1]; Aditya Dhanekula[2];

[1]. *Master of Science in Cybersecurity, Mercy University, Dobbs Ferry, NY, USA;*
Email: zahed.arman44@gmail.com

[2]. *Master of Business Administration in Analytics , Stevens Institute of Technology, NJ, USA;*
Email: dhanekulaaditya1@gmail.com

Doi: 10.63125/9gf98485
Received: *22 April 2024;* ***Revised:*** *26 May 2024;* ***Accepted:*** *15 June 2024;* ***Published:*** *30 June 2024*

Abstract

This study investigates the effectiveness of MITRE ATT&CK driven threat hunting in a Security Operations Center environment through the use of Splunk correlation rules, with the central problem being that modern SOCs often struggle with excessive alert volume, false positives, incomplete adversary visibility, and delayed response in complex cloud and enterprise security environments. The purpose of the study was to determine whether ATT&CK aligned threat hunting and better engineered Splunk correlation rules improve detection effectiveness, triage efficiency, response efficiency, and overall threat hunting success. The research adopted a quantitative, cross sectional, case-based design using a structured five-point Likert scale questionnaire administered to 120 cybersecurity professionals drawn from cloud and enterprise SOC cases, including SOC analysts, threat hunters, incident responders, detection engineers, and SOC managers. The key independent variables were MITRE ATT&CK alignment, Splunk correlation rule quality, technique coverage adequacy, and precision noise balance, while the dependent variables were threat detection effectiveness, triage efficiency, response efficiency, and overall threat hunting success. Data analysis was conducted using descriptive statistics, Cronbach's alpha reliability testing, correlation analysis, and multiple regression. The findings showed that all major constructs recorded positive mean scores above 3.00, including MITRE ATT&CK alignment ($M = 4.18$, $SD = 0.61$), Splunk rule quality ($M = 4.09$, $SD = 0.66$), threat detection effectiveness ($M = 4.16$, $SD = 0.58$), and overall threat hunting success ($M = 4.12$, $SD = 0.60$). Reliability values were satisfactory, with Cronbach's alpha ranging from 0.78 to 0.86. Significant positive relationships were found between ATT&CK alignment and threat detection effectiveness ($r = .68$, $p < .001$), Splunk rule quality and triage efficiency ($r = .63$, $p < .001$), technique coverage adequacy and SOC performance ($r = .59$, $p < .001$), and precision noise balance and response efficiency ($r = .61$, $p < .001$). Regression results showed that the model explained 64.0% of the variance in threat hunting success ($R^2 = .640$, $F = 42.37$, $p < .001$), with ATT&CK alignment emerging as the strongest predictor ($\beta = .31$, $p = .002$). The study implies that organizations can strengthen SOC performance by aligning detection logic with adversary behavior, improving rule precision, and closing technique coverage gaps, particularly in lateral movement and exfiltration.

Keywords

MITRE ATT&CK, Threat hunting, Security Operations Center, SPLUNK correlation rules, Detection effectiveness;

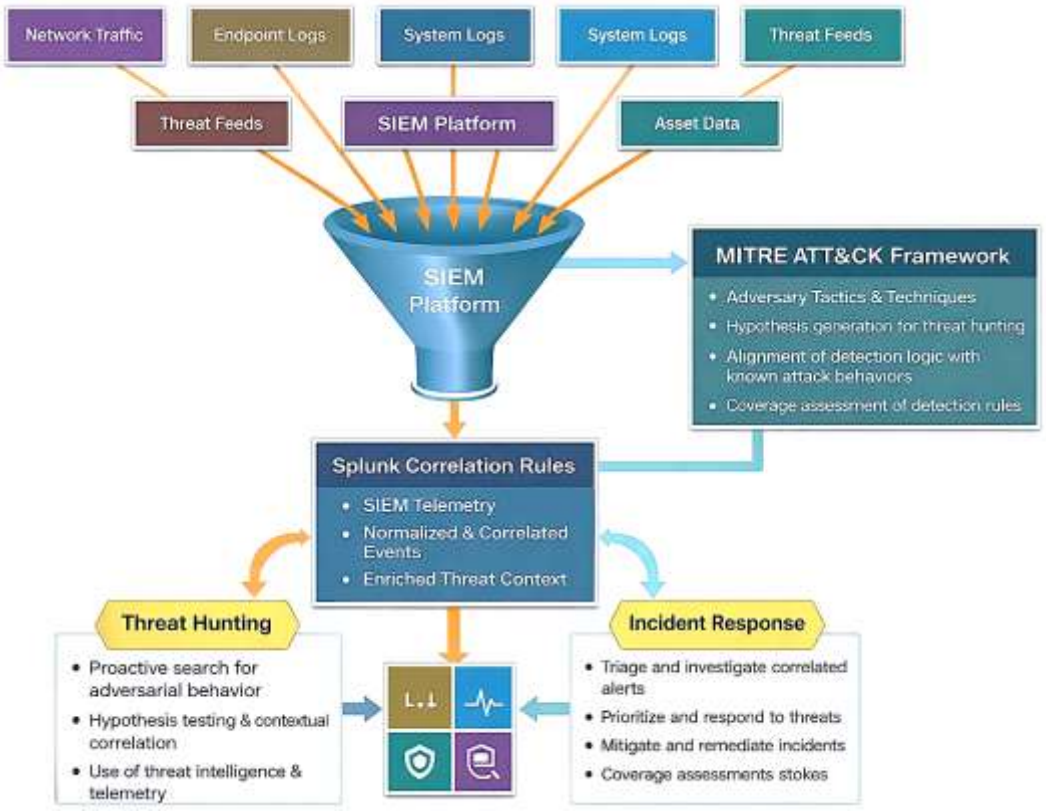
INTRODUCTION

Cybersecurity research commonly begins by clarifying core operational concepts because the meaning of threat hunting, event correlation, and security operations center practice shapes the logic of the entire study (Bryant & Saiedian, 2020). A Security Operations Center (SOC) is generally understood as the organizational structure in which analysts, detection engineers, and incident responders monitor, interpret, and respond to security events in near real time, while a Security Information and Event Management (SIEM) platform serves as the analytical foundation that collects, normalizes, stores, and correlates heterogeneous logs from endpoints, networks, servers, and applications (Garcia-Teodoro et al., 2009). Within that environment, threat hunting refers to a proactive and analyst-driven search for adversarial behavior that may not yet have generated a high-confidence alert, whereas cyber threat intelligence refers to structured knowledge about adversaries, capabilities, infrastructure, and observable behaviors that can sharpen hunting hypotheses and improve prioritization. The international significance of these concepts lies in the reality that contemporary cyber incidents are rarely confined to a single organization or country. Sophisticated campaigns routinely move across sectors, jurisdictions, and interconnected digital infrastructures, which means that SOC performance increasingly affects global supply chains, financial ecosystems, healthcare systems, educational institutions, and critical infrastructure operations (Mavroeidis & Bromander, 2017). Research on advanced persistent threats has shown that targeted campaigns are adaptive, long-lived, and strategically organized, making them difficult to detect through static signatures alone. For that reason, cybersecurity practice has increasingly shifted toward knowledge-driven defense models that combine SIEM telemetry, contextual enrichment, event correlation, and analyst reasoning to identify malicious behavior in its operational sequence rather than as isolated alerts. In this context, the MITRE ATT&CK framework has gained substantial importance because it organizes observed adversary behavior into tactics and techniques that can be used to structure detection engineering, threat hunting workflows, and coverage assessments (Xiong et al., 2022). A study on MITRE ATT&CK–driven threat hunting in a SOC environment is therefore relevant not only from a technical standpoint but also from an international security perspective, because it addresses the broader challenge of converting large-scale security telemetry into timely, accurate, and operationally meaningful defensive action (Alshamrani et al., 2019).

The development of modern SOC practice is closely connected to the long-standing problem of intrusion detection alert overload. Earlier intrusion detection research established that anomaly detection and signature detection both provide valuable visibility, yet each approach tends to generate fragmented observations that rarely communicate the full structure of an attack on its own. Alert correlation research emerged in response to this limitation by asking how multiple low-level alarms could be fused into higher-level representations of malicious activity and operational risk. The supervision of large networks has been shown to require analytical models capable of connecting alerts, vulnerabilities, topology, and contextual information into coherent security narratives (Bryant & Saiedian, 2017). Collaborative intrusion detection environments further intensified this need because distributed sensors and mixed detection engines increased both heterogeneity and interpretive burden. Dynamic alert interpretation also became necessary as researchers demonstrated that alert streams should be processed adaptively rather than only retrospectively. Related work showed that attack-graph-based correlation can improve the forensic interpretation of intrusion detection alerts by embedding them within plausible attack paths and logical progressions. Real-time causal methods for linking alerts also emphasized the need to reconstruct attack scenarios rapidly enough to support operational decision-making rather than limiting analysis to post-incident explanation (González-Granadillo et al., 2021). This body of work is highly significant for a SOC-centered study because analysts do not face isolated, perfectly labeled attack instances; instead, they confront noisy, incomplete, and temporally distributed signals that must be evaluated under considerable time pressure. When those signals are not correlated effectively, genuine malicious sequences remain hidden among benign or weakly contextualized alarms. When those signals are correlated effectively, analysts gain the ability to see attack progression, adversarial intent, and operational priority. This analytical shift forms the bridge between classical intrusion detection research and contemporary threat hunting, as both are concerned with adversary discovery, but threat hunting places greater emphasis on

hypothesis testing, contextual reasoning, and the ongoing validation of detection logic against realistic attack behaviors (Roschke et al., 2011).

Figure 1: Data Flow and Correlation Process for ATT&CK-Aligned Threat Hunting in a SIEM-Enabled SOC



SIEM systems became central to this transition because they operationalized large-scale event collection and event correlation in enterprise security environments. SOCs have been described as integral to incident response operations, and SIEM systems have been identified as essential tools for collecting, normalizing, storing, and correlating events from multiple sources. Later studies reinforced that position by showing that SIEM platforms occupy a central role in security analytics, incident triage, and organizational visibility across complex infrastructures. At the same time, the literature has shown that SIEM value is not automatic or uniform across operational settings. Intrusion detection increasingly depends on heterogeneous and high-volume data sources, creating big-data challenges that directly affect correlation quality and analyst comprehension. Big-data-oriented SIEM architectures were therefore proposed to illustrate how distributed and streaming approaches could support large-scale anomaly analysis more effectively (Barzegar & Shajari, 2018; Ahmed & Hasan Or, 2021; Md & Mehedi, 2021). Additional studies showed that modern SIEM systems still face persistent difficulties involving normalization challenges, false positives, and long analysis times in large-scale networks (Aditya & Chandra, 2022; Anick & Tasnim, 2022; Elshoush & Osman, 2011). The operational impact of these limitations becomes more visible when considering findings that improved ontological structuring and kill-chain-based metadata aggregation can enhance detection quality, generate more descriptive alerts, and reduce false positives (Hisham & Robel, 2022; Siddique & Amin, 2022). Recent work on efficient threat classification in SIEM settings has further shown that model usefulness in real SOC environments must be judged not only by accuracy but also by responsiveness and computational practicality. Collectively, these studies make an important methodological point for research on Splunk correlation rules. Correlation logic should not be treated merely as a vendor-specific configuration exercise. Rather, it should be understood as an analytical design problem that determines whether evidence becomes discoverable, interpretable, and actionable within the time constraints of SOC

practice. In a real-world SOC, a correlation rule becomes valuable when it reduces ambiguity, links events to adversarial meaning, and supports triage decisions with sufficient precision. This understanding is central to any study evaluating ATT&CK-driven hunting through correlation rules because the issue is not only whether events are collected, but whether they are transformed into operational knowledge that analysts can trust (Md & Islam, 2022; Mehedi & Md, 2022; Saad & Traore, 2013).

The rise of intelligence-driven defense deepened this discussion by shifting attention from generic alert handling to adversary-centered interpretation. Technical threat intelligence has been defined as a process of converting diverse threat data into actionable knowledge that can strengthen prevention, detection, and response capabilities (Mainuddin & Chandra, 2022; Shahinur & Sultan, 2022). Structured taxonomies, standards, and ontologies within cyber threat intelligence have also been emphasized as essential because organizations require machine-readable knowledge structures to process and correlate threat information efficiently. In practical terms, this body of work aligns closely with threat hunting because hunting depends on the development of plausible adversary hypotheses grounded in known behaviors, indicators, tools, and tactics (Mostafa & Tohidul, 2022; Khatun & Morshedul, 2022; Tang et al., 2022). The literature on advanced persistent threats makes this relationship especially clear. Advanced persistent threats have been described as targeted, persistent, and strategically sequenced campaigns that exploit long-term stealth and adaptability. More recent work has shown that intelligent profiling of APT behavior is necessary for improving detection, attribution, and defensive response. The MITRE ATT&CK framework gained growing influence in this environment because it provides a standardized vocabulary for adversary tactics and techniques, making it easier to align telemetry, detections, and hunting procedures around real-world attack behaviors. This ATT&CK-centered perspective is especially valuable for SOC operations because it creates a bridge between intelligence and detection engineering (Islam & Aditya, 2023; Tounsi & Rais, 2018; Zakia & Nahar, 2022). Rather than asking only whether a firewall log, process creation event, or authentication anomaly appears suspicious in isolation, ATT&CK encourages analysts to interpret that evidence in relation to execution, persistence, credential access, discovery, lateral movement, or exfiltration behaviors. That adversary-centered framing improves coverage analysis and makes correlation rules more meaningful because the rules can be engineered around technique-level behavior instead of isolated signatures. For a study concerned with Splunk correlation rules, this is particularly important because the practical strength of ATT&CK lies in its ability to convert log analytics into behavior analytics (Zali et al., 2013).

Threat hunting literature adds another important dimension by arguing that effective cyber defense increasingly depends on proactive search rather than alert consumption alone. Data-driven threat hunting has been presented as a method for linking endpoint visibility with cyber threat intelligence and automated threat assessment, thereby structuring hunting around telemetry-driven classification rather than intuition alone. Related work in ransomware research demonstrated that frequent pattern mining can identify behavioral regularities useful for both threat hunting and intelligence generation. Automated hypothesis generation and multi-criteria decision-making approaches have also shown that hunting can be formalized as a process of ranking and evaluating competing explanations for suspicious activity. This proactive orientation helps explain why ATT&CK has become so influential in mature hunting programs. ATT&CK supplies a behavior library from which hypotheses can be derived, while SIEM telemetry and endpoint logs provide the empirical material through which those hypotheses can be tested (Bhatt et al., 2014; Khaled & Mosheur, 2023; Shahab & Aditya, 2023). In operational environments, threat hunting therefore occupies the intersection of knowledge representation, telemetry analysis, and analyst expertise. It is neither fully manual nor fully automated. The literature consistently indicates that effective hunting emerges from the combination of structured threat knowledge, targeted queries, contextual correlation, and informed analyst judgment about what constitutes meaningful deviation or adversary progression. This synthesis is highly relevant to the present research because a SOC that uses Splunk correlation rules within an ATT&CK-driven hunting model is, in effect, institutionalizing a hypothesis-testing workflow. Correlation rules become formalized expressions of adversary-informed assumptions, while analyst review becomes the stage in which those assumptions are confirmed, rejected, or refined. A quantitative study of this environment is therefore well positioned to examine whether ATT&CK alignment, rule precision, and coverage

adequacy are associated with improved detection, triage quality, and response efficiency (Cheng et al., 2021; Hasan Or et al., 2023; Mehedi & Nahar, 2023).

A further reason this topic deserves systematic treatment is that multi-stage attack understanding remains one of the most challenging analytical tasks in security operations. Attack scenario reconstruction studies have repeatedly shown that meaningful detection rarely emerges from isolated events; instead, it comes from linking temporally and logically related observations into coherent adversarial sequences. Intrusion-semantics-based reconstruction was proposed to improve the extraction of attack scenarios from multisensor environments, thereby strengthening the analyst's ability to understand complex attack behavior (Sultan & Anick, 2023; Mostafa, 2023; Sapegin et al., 2017). Later work demonstrated that scenario reconstruction also supports response and forensic analysis when attack steps and their interrelationships are modeled coherently. An intrusion-action-based framework for alert correlation and prediction further reinforced the view that correlation is valuable not only for summarizing prior events but also for anticipating the next plausible stage of an intrusion. Graph-based learning approaches continued this line of inquiry by demonstrating that high-level attack scenario discovery remains relevant even as machine learning methods become more prominent in intrusion analysis. Earlier studies had already emphasized the operational need for real-time attack scenario extraction and the usefulness of attack-graph-based correlation for identifying multiple attack scenarios with acceptable levels of robustness and accuracy (Ratul & Aditya, 2023; Tasnim & Zaheda, 2023; Zuech et al., 2015). These studies collectively illuminate why ATT&CK-driven threat hunting is a strong research frame for a SOC case study. ATT&CK provides a semantically rich language for describing multi-stage adversary behavior, while SIEM correlation rules provide a practical mechanism for expressing those behavioral links in operational logic. In a Splunk-based SOC, this can involve connecting process execution, privilege escalation indicators, reconnaissance patterns, credential-access activity, and unusual network communications into interpretable patterns that map onto ATT&CK techniques. When this mapping is performed effectively, the SOC gains more than alert volume; it gains narrative coherence (Homayoun et al., 2020; Iftekhar & Md Tohidul, 2024; Zaheda & Md. Tahmid Farabe, 2023). Analysts are able to interpret not only what happened, but also where an observed activity sits within the larger progression of adversary behavior. The trustworthiness of a SOC therefore depends partly on whether its correlation layer can move from isolated signal detection to adversary-sequence reconstruction, which is precisely the domain in which ATT&CK-oriented case-study research becomes most valuable (Jinnat & Samiha Binte, 2024; Mavroeidis & Jøsang, 2018; Md. Towhidul & Uddin, 2024).

Against this background, the present study is situated at the intersection of SIEM engineering, ATT&CK-informed analysis, and empirical SOC evaluation. Existing literature provides substantial foundations on SIEM architecture, alert correlation, threat intelligence, attack scenario reconstruction, and APT behavior, yet the evidence base remains fragmented when attention shifts to how these components operate together in a real SOC using operational correlation rules (Kim & Kang, 2022; Li & Yan, 2017). SIEM studies have established the importance of correlation, normalization, scale, and analyst usability in security operations (Mushfequr & Aditya, 2024; Morin et al., 2009; Sakib, 2024). ATT&CK-related studies have shown the value of standardized adversary behavior models for threat reasoning and coverage assessment. Threat intelligence and hunting studies have also demonstrated that adversary-informed, telemetry-driven searching can improve situational awareness and prioritization in cyber defense (Neto & Santos, 2020). Even so, there remains a clear need for research that quantitatively examines how ATT&CK alignment and correlation-rule quality are perceived within a concrete SOC case, particularly when the focal mechanism is the practical use of SIEM correlation logic for hunting and triage. This is where the present thesis establishes its relevance. By centering on a real-world SOC environment and operationalizing key constructs such as technique coverage adequacy, rule precision–noise balance, detection effectiveness, and response efficiency, the study addresses a problem that is both academically meaningful and operationally grounded (Mashima, 2022; Sazzadul & Rebeka, 2024; Tasnim & Anick, 2024). The topic is especially important because current defense environments are judged not only by whether they collect extensive telemetry, but also by whether they convert that telemetry into trustworthy, prioritized, and adversary-relevant knowledge. An ATT&CK-driven evaluation of Splunk correlation rules offers a defensible means of

examining that conversion process by linking behavior models to rule logic, rule logic to analyst workflow, and analyst workflow to measurable SOC outcomes (Ren et al., 2010; Zaheda & Md Hamidur, 2024).

Background of the Study

The background of this study is rooted in the growing need for stronger, faster, and more intelligence-driven cybersecurity operations in modern organizations. As digital systems continue to expand across cloud platforms, hybrid networks, mobile devices, enterprise applications, and remote work environments, the attack surface available to cybercriminals has become broader and more complex than ever before. Organizations today are no longer defending only a small set of internal assets; they are protecting highly interconnected infrastructures that support finance, healthcare, education, government services, manufacturing, and critical public operations. In this setting, Security Operations Centers have become central to organizational defense because they are responsible for continuously monitoring security events, investigating suspicious activity, and coordinating response actions. However, traditional monitoring approaches often produce overwhelming numbers of alerts, many of which lack sufficient context, priority, or behavioral meaning. This creates a serious operational challenge, since analysts must separate real threats from background noise while working under time pressure and resource constraints. As a result, there has been a shift from purely reactive detection toward proactive threat hunting, where security teams actively search for hidden adversarial behaviors rather than waiting only for automated alerts. This shift has increased the importance of structured frameworks that help analysts understand how attackers operate across multiple stages of an intrusion. The MITRE ATT&CK framework has become especially valuable in this regard because it organizes attacker behavior into tactics and techniques that can guide detection design, threat hunting hypotheses, and coverage assessment. At the same time, Splunk has emerged as one of the most widely used platforms for collecting, correlating, and analyzing security data within SOC environments. Its correlation rules allow analysts to connect multiple events into meaningful patterns that may reveal suspicious or malicious activity. Even so, the effectiveness of these rules depends on how well they reflect real adversary behavior, how precisely they reduce false positives, and how effectively they support triage and response. This study therefore arises from the need to understand how MITRE ATT&CK–driven threat hunting, when operationalized through Splunk correlation rules in a real-world SOC environment, contributes to detection effectiveness, response efficiency, and overall security operations performance.

Problem Statement

The problem addressed in this study arises from the increasing difficulty that Security Operations Centers face in detecting, interpreting, and responding to sophisticated cyber threats within highly dynamic digital environments. Modern organizations generate massive volumes of security logs from endpoints, firewalls, authentication systems, cloud platforms, applications, and network devices, yet the existence of large amounts of data does not automatically produce effective security visibility. In many SOC environments, analysts are overwhelmed by alert volumes, repeated notifications, low-context events, and false positives that consume investigative time and weaken response efficiency. This creates a serious operational problem because important malicious activities may remain hidden among routine or noisy alerts, allowing adversaries to move through multiple stages of an attack before being identified. Although SIEM platforms such as Splunk are widely used to aggregate and correlate security data, the practical effectiveness of correlation rules depends on how accurately they represent real attacker behavior and how well they support analyst decision-making during triage and investigation. At the same time, the MITRE ATT&CK framework has become a widely recognized structure for mapping adversary tactics and techniques, yet many organizations still struggle to translate ATT&CK knowledge into measurable operational outcomes within daily SOC workflows. In practice, there is often a gap between theoretical ATT&CK alignment and the actual performance of detection content deployed in SIEM systems. Some rules may cover only a narrow subset of attacker behaviors, while others may generate excessive noise that reduces analyst trust and slows incident response. This means that organizations may adopt ATT&CK terminology and Splunk correlation logic without fully knowing whether those measures improve threat hunting effectiveness, detection quality, or overall SOC performance. The core problem, therefore, is the lack of sufficient quantitative evidence

showing how MITRE ATT&CK–driven threat hunting, when implemented through Splunk correlation rules in a real-world SOC environment, affects detection accuracy, alert precision, response efficiency, and operational success. Without such evidence, it becomes difficult for organizations to justify rule engineering decisions, identify coverage weaknesses, optimize analyst workflows, and assess whether ATT&CK-based hunting strategies truly strengthen cybersecurity operations in measurable terms.

Purpose of the Study

The purpose of this study is to examine how MITRE ATT&CK–driven threat hunting contributes to operational effectiveness in a Security Operations Center environment through the use of Splunk correlation rules. More specifically, this research seeks to evaluate whether the alignment of detection logic with attacker tactics and techniques can improve the quality of threat discovery, reduce inefficiencies in alert handling, and strengthen the ability of SOC teams to identify and respond to malicious behavior in a timely and accurate manner. The study is designed to move beyond general discussions of SIEM usefulness or ATT&CK popularity by focusing on measurable operational outcomes in a real-world case-study setting. It aims to determine whether ATT&CK-based rule design improves the adequacy of technique coverage across different stages of adversary activity and whether better-designed Splunk correlation rules produce more actionable alerts with less analytical noise. In addition, the study seeks to assess how these elements influence broader SOC outcomes such as detection effectiveness, triage quality, analyst confidence, and response efficiency. The objective of this research is therefore not only to describe the presence of ATT&CK and Splunk within security operations, but also to test the practical relationship between behavioral mapping, rule engineering, and security performance using quantitative methods. By applying a cross-sectional, case-study-based design and using Likert-scale responses supported by descriptive statistics, correlation analysis, and regression modeling, the study intends to identify the extent to which key variables are related and whether they significantly predict successful threat hunting outcomes. The study also aims to generate evidence that can help clarify where ATT&CK-driven hunting adds operational value, where rule precision is weakened by alert noise, and where coverage gaps may still exist inside the SOC detection surface. In this way, the research is directed toward producing a clear and evidence-based understanding of how adversary-focused detection strategies can be translated into more effective security operations through structured SIEM correlation logic.

Research Hypotheses

The research hypotheses of this study are formulated to test the assumed relationships between MITRE ATT&CK alignment, Splunk correlation rule performance, and the overall effectiveness of threat hunting in a Security Operations Center environment. These hypotheses are necessary because the study is not limited to describing cybersecurity practices; it seeks to determine whether important operational variables are statistically related in meaningful ways. The first hypothesis assumes that stronger alignment between threat hunting practices and the MITRE ATT&CK framework improves threat detection effectiveness because ATT&CK provides a structured method for mapping adversary behavior and guiding analytical focus. The second hypothesis proposes that higher-quality Splunk correlation rules positively affect alert precision and triage efficiency, since rules that better connect events and reduce ambiguity are expected to help analysts prioritize investigations more effectively. The third hypothesis assumes that adequate ATT&CK technique coverage is positively associated with stronger SOC operational performance because broader and more relevant behavioral coverage should increase the likelihood that malicious activity is identified across multiple stages of intrusion. The fourth hypothesis proposes that a better precision–noise balance in Splunk correlation rules improves threat response efficiency, since lower false-positive burden and higher alert relevance should allow analysts to act faster and with greater confidence. The fifth hypothesis assumes that ATT&CK-driven threat hunting practices significantly predict overall threat hunting success within the SOC environment, reflecting the broader expectation that adversary-centered detection logic supports better investigative outcomes than unstructured monitoring alone. These hypotheses collectively create a testable structure for examining whether the independent variables of ATT&CK alignment, coverage adequacy, rule quality, and precision–noise balance influence dependent variables such as detection effectiveness, triage quality, response efficiency, and operational success. By formulating the study in hypothesis-based terms, the research establishes a clear quantitative pathway for validating the

objectives of the paper and for determining whether the observed relationships are strong enough to support evidence-based conclusions. In this sense, the hypotheses serve as the analytical bridge between the theoretical assumptions of the study and the empirical findings generated from the case-study data.

Significance of the Research

This research is significant because it addresses an important operational and academic problem in contemporary cybersecurity by examining how MITRE ATT&CK–driven threat hunting can be translated into measurable value within a real-world SOC environment through Splunk correlation rules. The significance of the study can be explained as follows:

i. Practical significance for SOC analysts and threat hunters:

The study provides evidence on how ATT&CK-aligned hunting and correlation logic may improve alert interpretation, investigative focus, and response quality. This can help frontline analysts understand which factors most strongly influence effective threat detection in daily operations.

ii. Technical significance for detection engineering and rule design:

The study highlights the importance of rule precision, noise reduction, and technique coverage adequacy. This is valuable for detection engineers and SIEM administrators who are responsible for developing, tuning, and maintaining Splunk correlation rules that support operational decision-making.

iii. Organizational significance for cybersecurity management:

By examining measurable SOC outcomes such as detection effectiveness and response efficiency, the study provides useful insight for security managers who must allocate resources, justify tooling strategies, and improve the maturity of security operations programs.

iv. Theoretical significance for adversary-focused cybersecurity research:

The study strengthens the academic understanding of how structured attacker-behavior frameworks can be connected to real operational workflows. It contributes to knowledge on the relationship between behavior mapping, event correlation, and SOC effectiveness.

v. Methodological significance for quantitative cybersecurity studies:

Cybersecurity research often emphasizes technical description without strong empirical testing. This study adds value by using a quantitative, cross-sectional, case-study–based design supported by descriptive statistics, correlation analysis, and regression modeling to test clearly defined hypotheses.

vi. Strategic significance for improving trust in SOC operations:

The research helps clarify whether ATT&CK-driven detection content produces more trustworthy, relevant, and actionable alerts. This is important because analyst trust in detection systems directly affects triage quality, response speed, and operational confidence.

vii. Academic significance for future cybersecurity scholarship:

The study creates a structured foundation for future work on SIEM performance, detection coverage, rule engineering, and threat hunting maturity by identifying measurable constructs that can be reused or extended in later research.

LITERATURE REVIEW

The literature review for this study establishes the intellectual and empirical foundation for understanding how MITRE ATT&CK–driven threat hunting operates within a Security Operations Center environment through the use of Splunk correlation rules. In contemporary cybersecurity research, the effectiveness of security operations can no longer be examined only through general discussions of intrusion detection or incident response because modern threats are increasingly multi-stage, adaptive, and behaviorally complex. As a result, the literature surrounding this topic spans several connected domains, including security operations center functions, threat hunting theory and practice, SIEM-based detection engineering, adversary behavior modeling, alert correlation, and operational performance measurement. A review of this body of knowledge is necessary because the present study is positioned at the intersection of these domains rather than within a single narrow technical area. The literature helps explain how cybersecurity operations evolved from reactive monitoring toward proactive and intelligence-driven defense models, where analysts must not only collect and observe alerts but also interpret attacker behaviors, validate hunting hypotheses, and measure the quality of detection logic in practical environments. It also clarifies why the MITRE

ATT&CK framework has become a valuable structure for organizing adversary tactics and techniques in a way that supports coverage analysis, detection design, and hunting workflows. At the same time, the literature on Splunk and SIEM correlation rules provides insight into how raw security data can be transformed into meaningful alerts, how false positives and alert fatigue affect analyst performance, and how the quality of rule engineering influences the speed and reliability of threat detection. This review is equally important for identifying the theoretical lens and conceptual relationships that guide the study, since the research depends on a structured explanation of how ATT&CK alignment, rule precision, and technique coverage may shape detection effectiveness, triage quality, and response efficiency. In addition, the literature review helps reveal the empirical gap that justifies the study by showing that many prior works discuss threat hunting, SIEM use, or ATT&CK adoption separately, while fewer studies integrate these elements within a quantitative, cross-sectional, and case-study-based research design. For that reason, this chapter does more than summarize previous studies; it organizes the existing knowledge base in a way that directly supports the objectives, hypotheses, variables, and analytical direction of the present research.

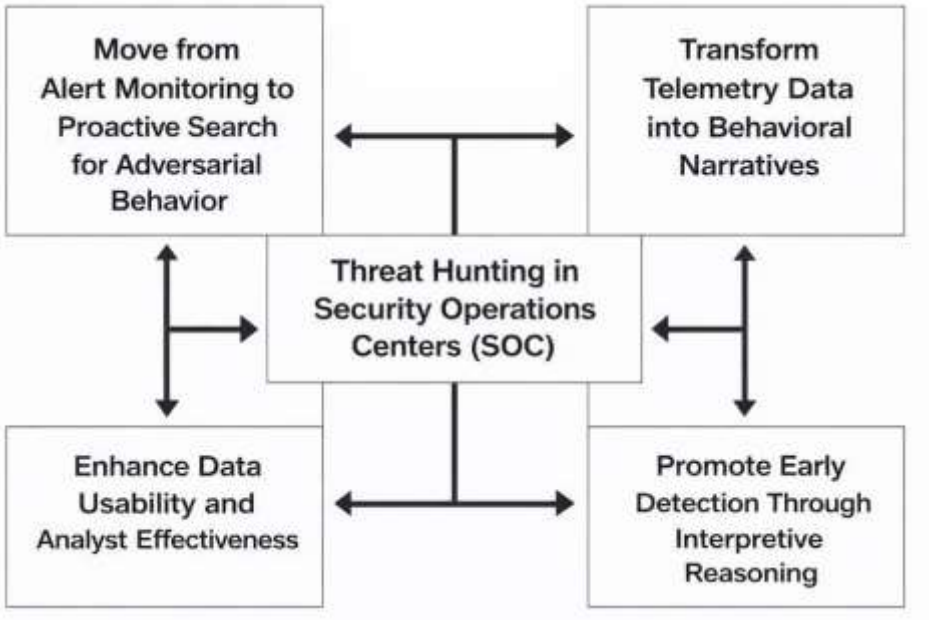
Threat Hunting in Security Operations Centers (SOC)

Threat hunting in Security Operations Centers has emerged as a necessary response to the limitations of conventional alert-driven monitoring. In many enterprise environments, security teams receive vast numbers of notifications from endpoint tools, firewalls, authentication systems, antivirus platforms, and network sensors, yet the presence of these alerts does not automatically result in meaningful situational awareness. The literature shows that the modern SOC is no longer defined only by centralized monitoring; it is increasingly defined by its ability to search proactively for malicious behavior that has not yet been clearly flagged by automated systems. This makes threat hunting an operational discipline rather than a supplementary activity. One important contribution to this discussion explains that successful SOC development depends on the coordinated interaction of people, process, and technology, with technical capability and process maturity having especially strong influence on whether the SOC can perform effectively as a defensive function (Agyepong et al., 2022). That finding is important for threat hunting because hunting depends on more than raw tooling power; it requires structured workflows, analyst readiness, and organizational support. A related empirical study on SOC analyst assessment also shows that analysts' performance can be measured systematically through the quality of incident analysis and reporting, which reinforces the view that the SOC should be understood as an environment in which analytical competence directly shapes security outcomes. When these ideas are brought together, threat hunting appears as a mature SOC capability that depends on organizational design, procedural discipline, and analyst judgment rather than on log aggregation alone. In this sense, threat hunting represents a move from passive event consumption to active adversary discovery. It requires analysts to ask whether suspicious behaviors, partial indicators, or weak signals form part of a broader malicious pattern, and it requires the SOC to support that reasoning through structured data access, operational coordination, and investigative measurement. As a literature theme, therefore, threat hunting in the SOC is best understood as a practice built upon organizational readiness and measurable analyst effectiveness rather than as a simple extension of traditional monitoring tools (Abd Majid & Zainol Ariffin, 2021).

The literature also emphasizes that threat hunting is inseparable from the problem of how security information is presented, interpreted, and converted into actionable knowledge inside the SOC. A notable study on data presentation in security operations centres argues that SOC practitioners work under pressure while interacting with multiple tools and streams of information, making the clarity and usability of security data a core operational requirement rather than a secondary interface issue. This point is highly relevant to threat hunting because hunting requires analysts to identify subtle anomalies, connect seemingly unrelated observations, and maintain awareness across numerous concurrent tasks. If the data environment is cluttered, fragmented, or difficult to interpret, the hunt process loses both speed and precision. Another important study examining sophisticated attack detection through the lens of SOC analysts found that many existing approaches are too focused on single events and are therefore inadequate for identifying complex multi-stage attacks (Akinrolabu et al., 2018). That insight aligns strongly with the logic of threat hunting, which assumes that sophisticated intrusions often reveal themselves through patterns, relationships, and progression rather than through

one clear signature. In practical SOC work, this means that hunting is shaped by the analyst's ability to synthesize diverse evidence sources into a coherent hypothesis about adversary behavior. The literature therefore portrays the SOC as a knowledge-intensive environment where the success of threat hunting depends not only on the existence of data but also on how effectively that data can be interpreted in relation to attacker intent, sequence, and context. This explains why mature SOC environments increasingly emphasize enriched visibility, triage support, and high-quality event presentation. Threat hunting, in this framing, is not simply an act of searching logs; it is an interpretive process that relies on usable security data, cognitive support, and mechanisms for recognizing relationships across events. The literature thus positions the SOC as an environment where adversary discovery depends on both technological instrumentation and the human capacity to perceive attack progression through complex information flows (Axon et al., 2020).

Figure 2: Framework Illustrating Proactive Threat Hunting in a Soc Environment



A further strand of literature shows that proactive hunting in SOCs is strengthened when large-scale data analysis is paired with mechanisms that help analysts move from raw observations to suspicious behavioral narratives. Research on enterprise log analysis demonstrated that suspicious activity can be identified more effectively when heterogeneous security logs are mined and transformed into host-centric behavioral signals rather than treated as isolated product outputs. This is particularly important for SOC-based threat hunting because enterprise attackers often leave small traces across multiple systems, and those traces become meaningful only when the SOC can integrate them into a higher-level behavioral picture. From this perspective, threat hunting becomes the process through which analysts test whether scattered observations reveal hidden malicious activity that ordinary alert queues may not prioritize correctly. The importance of this approach is reinforced by the broader SOC literature, which shows that the effectiveness of a security operations function depends on whether it can coordinate data, process, and analytical effort into timely operational action. Threat hunting is therefore significant not only because it is proactive, but because it helps the SOC convert broad telemetry into targeted investigative reasoning. It also helps explain why a hunting-capable SOC is usually treated as more mature than one that only reacts to alarms. A SOC with hunting capability can search for stealth, validate assumptions, question weak detections, and uncover attacker movement before the incident becomes more damaging. In the literature, this makes threat hunting a defining feature of advanced SOC practice rather than an optional specialist activity. It is closely related to incident quality, detection relevance, and the operational credibility of the security team. For the present study, this literature base is especially useful because it supports the argument that real-world SOC performance should be

examined through proactive discovery capability, analyst effectiveness, and the quality of event correlation logic that underpins the hunt process (Yen et al., 2013).

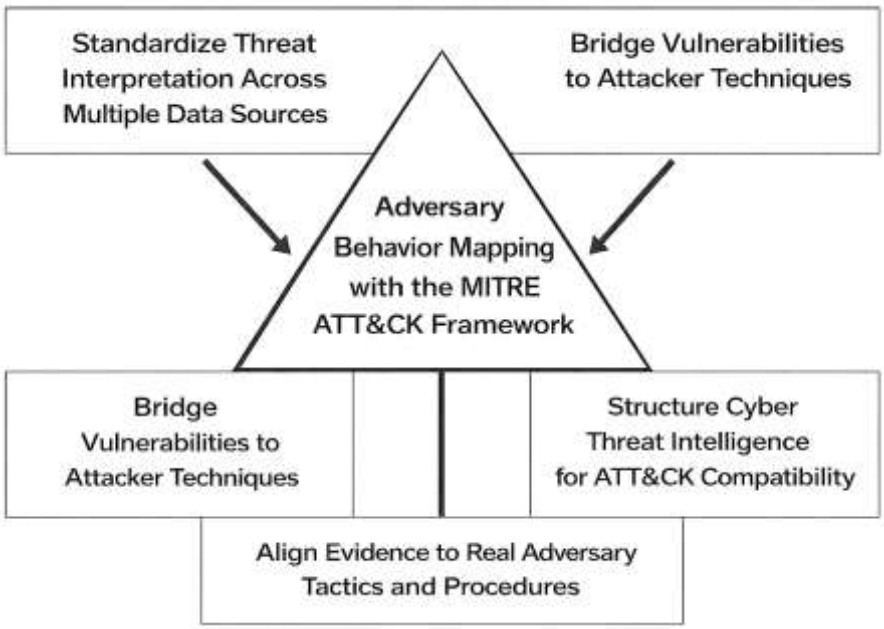
MITRE ATT&CK Framework and Adversary Behavior Mapping

The MITRE ATT&CK framework has become one of the most influential knowledge structures in contemporary cybersecurity because it organizes adversary behavior into a standardized matrix of tactics, techniques, and procedures that can be interpreted across operational, analytical, and strategic contexts. Its importance within security operations lies in the fact that cyber defense is more effective when malicious activity is understood as behavior rather than as isolated technical artifacts. ATT&CK supports this shift by describing how adversaries achieve goals such as initial access, execution, persistence, privilege escalation, defense evasion, discovery, lateral movement, collection, and exfiltration. In this way, the framework provides a common language through which defenders can interpret real incidents, compare threat reports, structure hunting hypotheses, and align detections to attacker tradecraft. Adversary behavior mapping is therefore not simply a classificatory exercise; it is a way of transforming raw or fragmented evidence into a coherent representation of hostile intent and attack progression (Ampel et al., 2021). This matters greatly in modern SOC environments because analysts frequently work with incomplete evidence drawn from dissimilar tools and data sources, and ATT&CK gives them an interpretable model for relating those observations to meaningful attack stages. The literature also shows that ATT&CK is increasingly used outside pure incident analysis and has been extended into broader security assessment functions. It has been applied to connect organizational conditions and cultural weaknesses with exposure to adversary techniques, thereby showing that ATT&CK can support the interpretation of both technical and non-technical cyber risk. This wider applicability strengthens its value as an adversary behavior mapping framework because it demonstrates that ATT&CK is not limited to describing attacker actions after compromise, but can also assist organizations in identifying where internal weaknesses may enable those actions to succeed. For the present study, this is highly relevant because ATT&CK gives theoretical and operational structure to the analysis of threat hunting and correlation rules, allowing security observations to be interpreted through a behavior-centered lens rather than through disconnected event logs alone (Georgiadou et al., 2021).

A central strength of the ATT&CK framework is that it enables adversary behavior mapping across different cybersecurity knowledge sources that would otherwise remain disconnected. One important application in the literature concerns the linking of vulnerability information to attacker techniques. Mapping Common Vulnerabilities and Exposures to ATT&CK makes it possible to move beyond simple vulnerability listing toward a richer understanding of what an attacker may accomplish by exploiting a weakness. This form of mapping is valuable because vulnerabilities become much more meaningful when they are connected to specific adversarial behaviors, corresponding tactics, and likely operational consequences. Research in this area has shown that ATT&CK can support both manual and automated mapping of CVE descriptions to techniques, helping analysts understand exploitation pathways, prioritize patching decisions, and identify likely threat vectors in more behaviorally grounded terms. In one stream of work, CVE entries were linked directly to ATT&CK techniques to improve vulnerability interpretation and reveal how particular weaknesses align with adversary actions (C. Liu et al., 2022). In another stream, transformer-based models were used to assign ATT&CK labels to vulnerability descriptions, illustrating that language-based automation can assist experts by pre-classifying large volumes of security information. These studies show that adversary behavior mapping is not limited to threat actor reports or incident forensics; it also operates as a bridge between vulnerability management and threat-informed defense. That bridge is especially important in SOC practice because defenders often need to decide whether a vulnerability should be treated as a routine exposure or as a concrete behavioral risk that supports known attack techniques. ATT&CK helps answer that question by embedding vulnerability data within a broader adversarial model. The result is a more actionable form of intelligence in which defenders can assess not only what is weak, but how that weakness may be operationalized by attackers across the attack lifecycle. This logic reinforces the usefulness of ATT&CK for studies that focus on threat hunting and detection engineering, since both activities depend on understanding how technical evidence maps to real adversary behavior (Kuppa et al., 2021).

The literature further shows that ATT&CK-based adversary behavior mapping has advanced through the use of automated extraction and classification techniques applied to cyber threat intelligence. Threat reports often contain valuable descriptions of attacker tradecraft, but much of that knowledge is embedded in unstructured natural language that must be interpreted before it can support detection and hunting activities. ATT&CK provides a stable taxonomy that allows researchers to convert unstructured reports into structured behavioral labels, making it easier to identify which tactics and techniques are present in a threat narrative.

Figure 3: Adversary Behavior Mapping Using the MITRE ATT&CK Framework



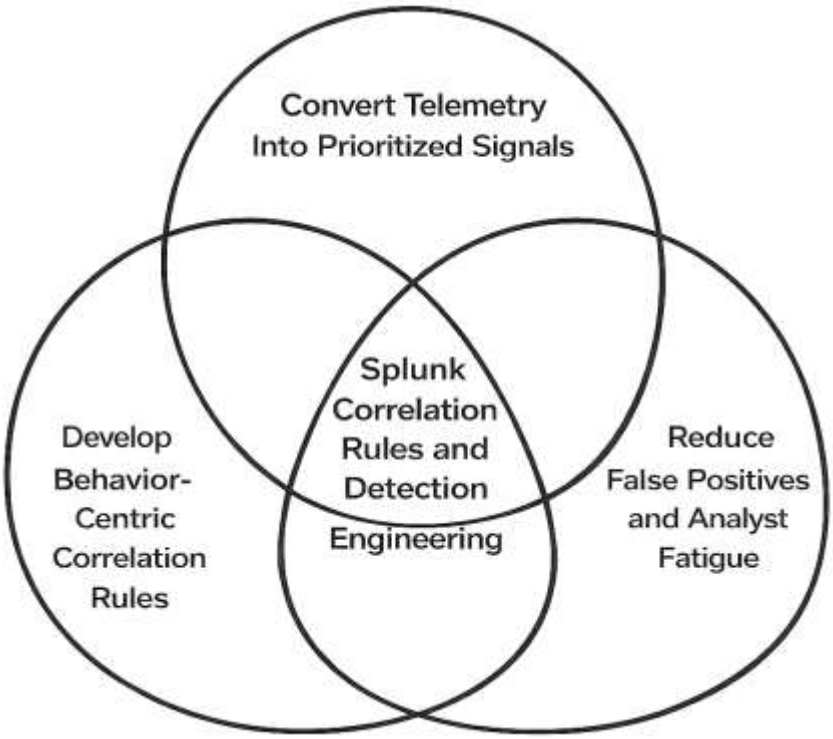
This has encouraged the development of machine learning and deep learning models that automatically classify CTI text according to ATT&CK categories. Such work is important because it reduces the burden of manual interpretation while also increasing consistency in the way behavior is recorded, retrieved, and operationalized. Recent research has shown that transformer-based and hierarchical neural approaches can significantly improve the extraction of ATT&CK tactics and techniques from CTI, especially when those models account for the hierarchical dependency between tactics and techniques rather than treating labels as unrelated categories. This insight is highly relevant to adversary behavior mapping because cyber intrusions are inherently structured, and the ATT&CK matrix itself reflects that structure. Automated mapping therefore becomes more accurate when it respects the behavioral logic embedded in the framework. For SOC environments, this means that ATT&CK can support a pipeline in which textual threat intelligence, detection engineering, coverage analysis, and hunt development are all linked through a shared model of attacker behavior. As a result, ATT&CK is not only a descriptive matrix but also a semantic mechanism for integrating knowledge across threat reports, vulnerability data, risk assessment, and operational detections. This makes it especially suitable for the present research, where the value of Splunk correlation rules depends on how well observed events can be aligned with adversary techniques and interpreted as part of a structured hunting process. In this sense, ATT&CK-based adversary behavior mapping provides the conceptual backbone that connects intelligence, detection content, and SOC performance into one analyzable framework (Ahmed et al., 2022).

Splunk Correlation Rules and Detection Engineering

Splunk correlation rules can be understood within the broader literature on detection engineering as structured analytical expressions that transform high-volume security telemetry into prioritized signals for investigation. In a SOC environment, raw data from endpoints, authentication systems, operating systems, network devices, and cloud services rarely has direct operational value until it is organized into logic that reflects suspicious sequences, threshold conditions, entity relationships, or behavior

patterns. Detection engineering gives that logic a repeatable design function by treating detection content as an artifact that must be continuously created, tuned, tested, and improved rather than as a one-time technical configuration. This idea becomes especially relevant in Splunk because correlation searches are designed to connect multiple events, time windows, fields, and contextual filters into a notable outcome that analysts can triage. The literature shows that the main difficulty is not merely generating alerts, but reducing alert flooding while preserving behavioral meaning and investigative usefulness. Research on domain-independent alert aggregation demonstrated that large alert volumes require techniques that can cluster, merge, and abstract semi-structured alerts so that analysts are not overwhelmed by repetitive low-level notifications (Landauer et al., 2022). Related research on event context modeling showed that alert triage improves when events are interpreted through surrounding behavioral context rather than evaluated as isolated records, since the same alert can imply very different levels of risk depending on adjacent activity, entity interactions, and sequence patterns (J. Liu et al., 2022). These findings are highly relevant to Splunk correlation rules because a well-designed rule does more than count events; it expresses a detection hypothesis about how suspicious behavior should appear across multiple data points. From this perspective, detection engineering is the discipline that makes correlation logic operationally trustworthy. It shapes when a rule should fire, which entities it should track, what enrichment it should include, how much noise it should tolerate, and whether the generated result is meaningful enough for analyst action. In practical SOC work, therefore, Splunk correlation rules serve as the implementation layer through which detection engineering converts telemetry into structured, reviewable, and behavior-sensitive signals that support triage and threat hunting rather than simply increasing alert volume (Landauer et al., 2022).

Figure 4: Correlation Rule Design for Detection Engineering in Security Operations Centers



The literature also makes clear that the value of detection engineering depends heavily on how effectively it handles prioritization, fatigue, and interpretability. A correlation rule may be technically correct and still fail operationally if it produces too many false positives, lacks contextual depth, or forces analysts to spend excessive time reconstructing attack meaning after the alert has fired. This problem is central to SOC operations because detection pipelines compete for limited analyst attention, and every poorly tuned rule consumes time that could have been directed toward more significant threats. Research on threat-alert fatigue using online anomaly detection showed that large-scale

enterprise alert streams can be screened substantially before human review while still preserving significant alerts, highlighting the importance of triage-oriented filtering when operators face persistent overload (Aminanto et al., 2019). Another study on real-time alert investigation proposed a context-aware prioritization model that improved the efficiency of provenance-based analysis by reducing overlap among investigative tasks and dynamically adapting prioritization as new context emerged (Jang et al., 2022). These findings matter for Splunk-based detection engineering because correlation rules are rarely judged only by whether they match a condition. They are judged by whether they produce an alert that is timely, interpretable, and worthy of escalation. In that sense, the engineering of a rule includes its downstream effect on analyst workflow. A high-quality correlation search should help analysts decide what matters first, why it matters, and what behavioral pathway the alert may represent. This is why rule thresholds, suppression settings, entity grouping, risk scoring, and ATT&CK tagging all matter in mature SOC practice. They turn a technical search into an investigative object. The literature therefore supports the argument that detection engineering and alert triage are inseparable. Splunk correlation rules are not merely search statements; they are operational decision instruments whose quality is reflected in reduced fatigue, clearer prioritization, and stronger investigative confidence. When rule logic is engineered with these concerns in mind, the SOC becomes better able to distinguish noisy anomalies from actionable adversarial behavior and to move more efficiently from detection to response (Li et al., 2022).

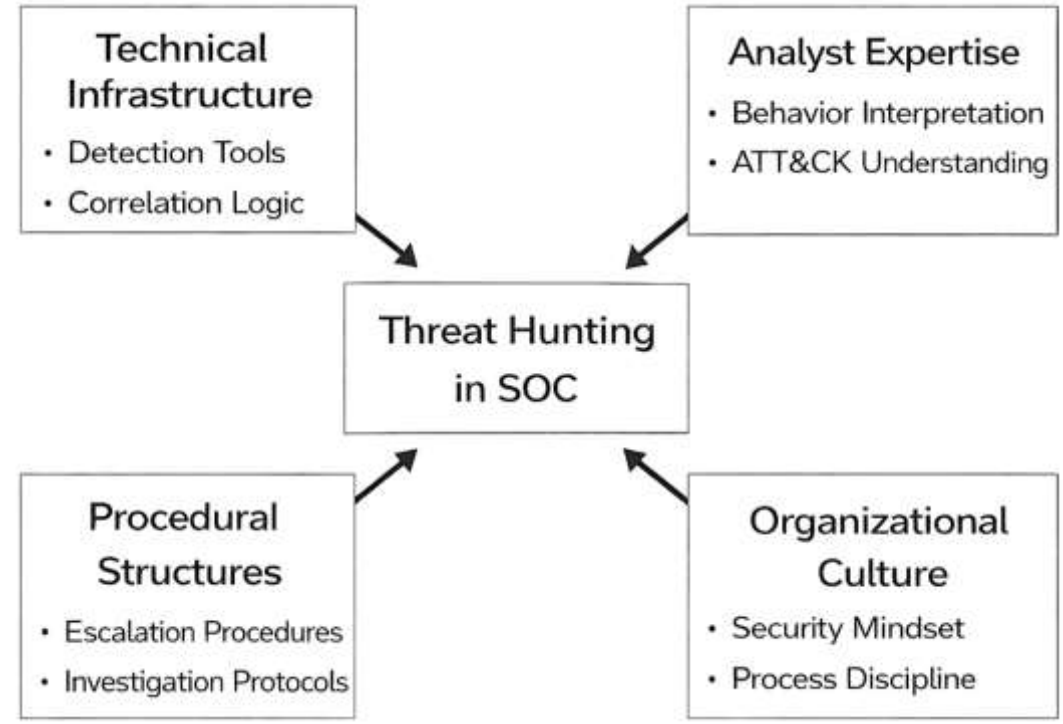
A further theme in the literature is that detection engineering becomes more effective when rule design is aligned with behavior semantics and attack tracing rather than static alert labels alone. This is particularly relevant to Splunk correlation rules because enterprise attacks often unfold across multiple systems, entities, and time windows, making it difficult to understand malicious activity through single-event classification alone. Research on behavior-semantic alert classification argued that the actual needs of security personnel are not satisfied by binary alert labeling, because some alerts are operationally unimportant while others represent behaviorally significant threats that require rapid attention (Niu et al., 2022). That insight supports a more advanced view of correlation rules in which the goal is not only to detect whether something suspicious occurred, but to classify the event according to its behavioral meaning and likely threat importance. A related study introduced LogTracer, which combined system-log anomaly detection with provenance-graph analysis to extract attack paths more efficiently and trace malicious activity through large volumes of logs (Landauer et al., 2022). This line of work has major implications for Splunk environments because rule logic becomes far more useful when it captures behavioral relationships that can be interpreted in a sequence, such as suspicious execution followed by privilege escalation, unusual authentication patterns followed by lateral movement, or multiple weak signals that only become meaningful once linked together. In this sense, detection engineering is most mature when it treats rule writing as behavior modeling. Correlation searches should encode how attackers move, persist, escalate, or evade, not merely whether a field value crossed a threshold. The literature therefore reinforces the idea that Splunk correlation rules are strongest when they combine aggregation, contextual enrichment, prioritization, and behavior semantics into one coherent detection surface. For the present study, this is especially important because ATT&CK-driven threat hunting depends on whether correlation rules can express adversary tactics and techniques in ways that are operationally precise, low in noise, and supportive of fast investigative reasoning. The broader literature on event triage, alert fatigue, classification, and anomaly tracing thus provides a strong foundation for understanding Splunk detection engineering as a behavior-oriented practice that directly shapes SOC performance, analyst workload, and threat hunting effectiveness (J. Liu et al., 2022; Niu et al., 2022).

Theoretical Framework: Socio-Technical Systems Theory

Socio-Technical Systems Theory provides the most appropriate theoretical foundation for this study because it explains organizational performance as the outcome of interaction among human actors, technological infrastructures, task structures, and the wider operating environment rather than as the product of any one component in isolation. Within a Security Operations Center, threat hunting is never performed by technology alone, because detection tools, correlation logic, analyst expertise, escalation procedures, and institutional security culture function together as an interdependent system. This makes the SOC a classic socio-technical setting in which technical efficiency and human interpretation

are mutually reinforcing. The theory is especially relevant to MITRE ATT&CK–driven threat hunting because ATT&CK supplies a structured representation of adversary behavior, Splunk correlation rules translate that representation into detection logic, and SOC analysts interpret the resulting outputs during triage and investigation. Under this view, threat hunting success depends not only on whether a correlation rule exists, but also on whether the rule is understandable, behaviorally aligned, operationally trusted, and embedded in a culture that supports disciplined analysis. Socio-Technical Systems Theory is therefore useful because it allows this research to examine ATT&CK alignment, rule quality, coverage adequacy, and alert precision as connected elements within a broader operational system. Earlier work on information security culture already showed that the management of security depends on more than technical controls and that assessment, awareness, and support mechanisms must be integrated into organizational routines for security to be effective. That same logic applies in a SOC environment, where security value emerges when tools, processes, and people are aligned around coherent detection goals. More recent cybersecurity scholarship has reinforced this position by arguing that social, technical, and environmental dimensions must be considered together when evaluating cybersecurity practice and by warning against overly technocentric security models that understate the role of human contribution, contextual judgment, and organizational adaptation (McEvoy & Kowalski, 2019).

Figure 5: Socio-Technical Systems Theory Framework for Soc Threat Hunting Effectiveness



The explanatory power of Socio-Technical Systems Theory is particularly strong for a study of threat hunting because adversary discovery in a SOC is shaped by both formal technical mechanisms and informal human practices. In technical terms, Splunk correlation rules aggregate events, compare conditions, apply thresholds, and generate notable alerts. In social terms, analysts evaluate suspiciousness, determine investigative priority, interpret ATT&CK context, and decide whether the observed activity represents a genuine attack sequence or a benign operational anomaly. The theory therefore frames the SOC as a system in which effectiveness depends on alignment across at least four dimensions: human capability, technical control quality, procedural coherence, and organizational culture. This multi-dimensional reading matches the reality of ATT&CK-driven hunting, since a detection rule mapped to a technique may still underperform when analysts lack confidence in the alert, when escalation procedures are unclear, or when the broader security culture does not support disciplined response (Zimmermann & Renaud, 2019). Research on socio-technical cyber risk has shown

that organizational vulnerabilities are often produced not only by software weaknesses but also by degraded work practices that create "risk narratives" across departments and processes. Likewise, research on organizational information security culture has shown that secure behavior is shaped by awareness, management guidance, trust, conscientious practice, and internal cultural traits rather than by technical enforcement alone. These insights are central to the present study because they justify treating ATT&CK technique coverage adequacy and Splunk rule precision–noise balance not merely as tool attributes, but as operational expressions of a larger socio-technical arrangement. In other words, poor rule precision may reflect technical tuning problems, yet it may also reflect weak contextual enrichment, insufficient analyst feedback loops, or low organizational maturity in detection engineering. Socio-Technical Systems Theory is valuable here because it accommodates all of these influences within a single explanatory lens and therefore helps position the SOC as an integrated operational system rather than a collection of independent technologies (Da Veiga et al., 2020).

For the empirical structure of this study, Socio-Technical Systems Theory supports the use of a multiple linear regression model because the theory assumes that operational outcomes are jointly influenced by several interrelated factors rather than by one isolated predictor. The most suitable formula for the whole study can therefore be expressed as:

$$THS = \beta_0 + \beta_1(MAA) + \beta_2(SRQ) + \beta_3(TCA) + \beta_4(PNB) + \varepsilon$$

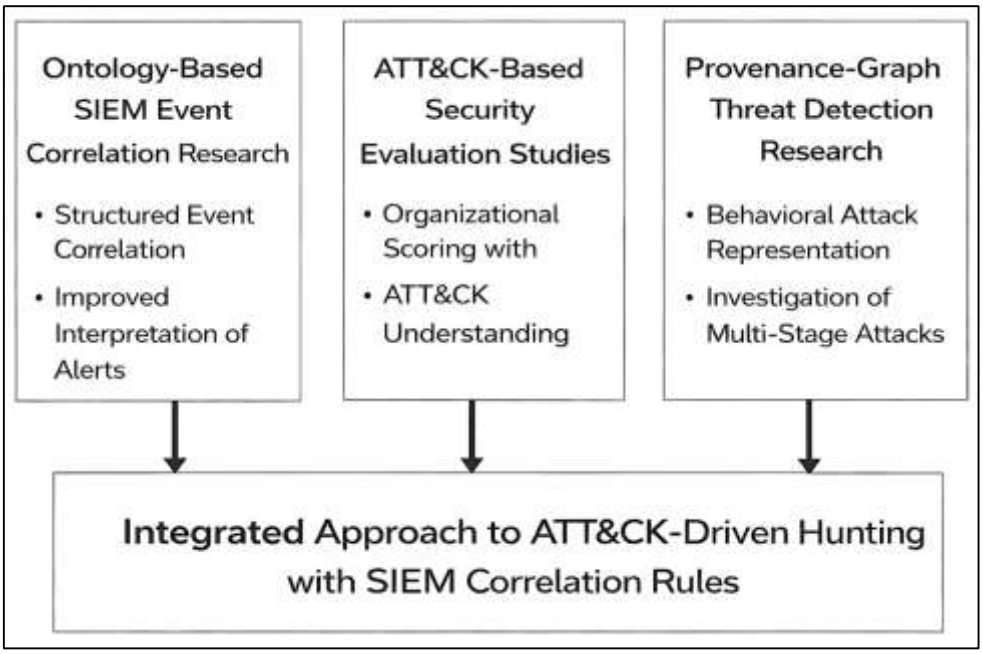
where THS represents threat hunting success, MAA represents MITRE ATT&CK alignment, SRQ represents Splunk rule quality, TCA represents technique coverage adequacy, PNB represents precision–noise balance, β_0 is the intercept, β_1–β_4 are regression coefficients, and ε is the error term. This formula is the best fit for the whole study because it translates the socio-technical logic of the framework into a measurable model that can test how several technical and semi-social operational factors jointly predict SOC performance (Schlienger & Teufel, 2005). In theoretical terms, the model reflects the assumption that ATT&CK-driven threat hunting is strengthened when rule design, behavioral coverage, alert usefulness, and analyst-facing detection quality operate in alignment. If one variable weakens substantially, the overall effectiveness of the hunting system may decline even when other variables remain strong. This is consistent with socio-technical thinking, which holds that system performance emerges from interaction and fit rather than from isolated excellence in one subsystem. In practical research terms, the theory also supports the study's use of descriptive statistics and correlation analysis before regression, because a socio-technical perspective first requires the identification of system characteristics and interrelationships before testing predictive effects. Thus, Socio-Technical Systems Theory does not function merely as a background philosophical idea in this study. It directly guides variable selection, supports the logic of the hypotheses, and justifies the quantitative modeling strategy through which ATT&CK alignment and Splunk correlation rules are examined as interconnected determinants of real-world SOC threat hunting effectiveness (Malatji et al., 2019).

Empirical Review of Prior Studies

Empirical studies on security operations, event correlation, and adversary-centered detection show that one of the most persistent problems in cyber defense is the gap between raw alert generation and operationally meaningful threat interpretation. Within the SIEM literature, earlier empirical work on ontology-based event correlation demonstrated that event streams become more useful when they are transformed into a shared semantic structure rather than processed only as isolated alerts. A study on ontology-based correlation in SIEM environments showed that description-logic-driven modeling can support cooperative intrusion detection by providing a formal vocabulary through which alerts from multiple analyzers can be normalized, linked, and reasoned over in a more interpretable manner. The practical value of that work lies in its demonstration that correlation quality improves when the SIEM is designed to understand relationships among alerts rather than merely counting or aggregating them. A later empirical extension of this logic proposed a semantic approach for events correlation in SIEM systems and implemented an alert-correlation prototype capable of using ontological reasoning to reconstruct attack scenarios in real time (Kenaza & Aiash, 2016). That study is especially important because it moved beyond conceptual discussion and showed, through attack-scenario experimentation, that correlation becomes more precise when the underlying model captures semantics, contextual dependencies, and rules-based reasoning. Together, these studies provide strong empirical support for

the argument that modern SOC effectiveness depends not only on collecting events but also on representing them in ways that preserve attack logic, sequence, and contextual meaning. For the present research, these findings are directly relevant because Splunk correlation rules perform a similar operational function: they attempt to connect different pieces of evidence into an interpretable detection outcome. The empirical lesson from these earlier studies is that detection quality rises when correlation logic is informed by behavior structure and contextual linkage rather than by simplistic thresholding alone. This supports the present study's focus on rule quality, technique coverage, and alert precision, since previous evidence already suggests that structured event-correlation methods are central to effective threat discovery and investigation in real-world security operations environments (Kenaza et al., 2018).

Figure 6: Empirical Foundations Supporting ATT&CK-Driven Threat Hunting in Soc Environments



A second stream of empirical research has focused on how the MITRE ATT&CK framework can be used to translate security observations into measurable organizational assessment. In this area, one study proposed a security assessment rating framework for enterprises using the MITRE ATT&CK matrix and showed that ATT&CK can function not only as a descriptive taxonomy of adversary behavior but also as a scoring mechanism through which organizations can summarize evaluation results at both the overall and tactic-specific levels. The importance of this work lies in its operationalization of ATT&CK as an assessment instrument rather than merely a reference catalog, thereby providing a method for turning test outcomes into interpretable security ratings. Related empirical work investigated the extent to which formal security controls mitigate ATT&CK techniques by examining 298 NIST SP 800-53 controls against 188 adversarial techniques associated with 669 cybercrime groups and malware entries cataloged in ATT&CK. That study found that only a subset of controls mitigated a large share of techniques and, more importantly, that a meaningful number of adversarial techniques could not be addressed by any mapped controls. This finding is highly significant because it empirically demonstrates that ATT&CK coverage is uneven and that organizations can have major defensive blind spots even when they have adopted extensive control frameworks. For the present study, these empirical findings are especially valuable because they reinforce the importance of examining ATT&CK technique coverage adequacy as a measurable construct within the SOC. If ATT&CK can be used to score enterprise security posture and expose technique-level mitigation gaps, then it can also be used to evaluate how well Splunk correlation rules align with adversary behavior and where hunting coverage remains incomplete. In other words, these empirical studies justify the present thesis's emphasis on ATT&CK alignment as more than a

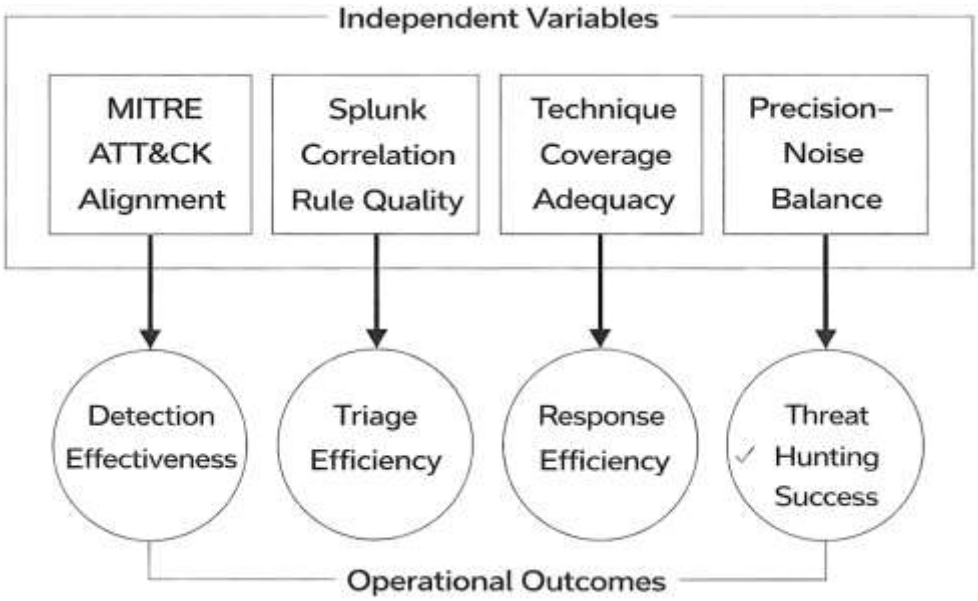
conceptual preference; they show that ATT&CK can be translated into operational metrics that reveal both strengths and weaknesses in real defensive environments (Manocha et al., 2021).

A third empirical line of research has examined how complex attacks can be detected and investigated when defenders move from isolated event analysis toward behavior-rich representations such as provenance graphs. A comprehensive survey of system-level provenance-graph-based threat detection and investigation synthesized real design choices across data collection, data management, and threat detection modules and showed that provenance models are valuable because they preserve causal, temporal, and semantic relationships among system events. That study also emphasized several practical performance criteria for real-world deployment, including storage efficiency, query efficiency, balance between true positives and false positives, and shortened response time. These observations are particularly relevant to SOC research because they reveal that operationally useful detection depends on more than whether an event is flagged; it depends on whether analysts can reconstruct attack history, follow causal relationships, and investigate multi-stage behavior without being overwhelmed by disconnected evidence (Li et al., 2021). When this empirical insight is read together with the earlier SIEM-correlation studies and ATT&CK-based assessment studies, a clear pattern emerges. Prior research consistently shows that strong cyber defense requires three things at once: structured event correlation, adversary-behavior mapping, and measurable evaluation of coverage or performance. What is still less developed in the literature is a study that integrates all three within one empirical design focused on SOC threat hunting using operational correlation rules. That is the gap addressed by the present study. Existing evidence has shown that semantic correlation improves interpretability, ATT&CK improves assessment structure, and behavior-rich modeling improves investigation quality. Even so, fewer empirical studies have examined how ATT&CK-driven hunting, implemented through SIEM rule logic and judged through operational variables such as precision–noise balance, response efficiency, and perceived hunting success, functions inside a concrete SOC case. This is precisely why the present research is necessary: it builds on the empirical findings of earlier studies while bringing them together into one quantitative framework that is directly relevant to Splunk-based security operations and threat hunting practice (Rahman & Williams, 2022).

Conceptual Framework

The conceptual framework of this study explains how MITRE ATT&CK–driven threat hunting in a Security Operations Center can be understood as a structured relationship between adversary-behavior alignment, detection-rule performance, and operational outcomes. At the center of the framework is the assumption that a SOC performs more effectively when observed security events are mapped to meaningful attacker behavior and then translated into actionable detection content. This view is supported by work showing that cognitive endpoint behavior analytics can reduce dependence on static preconfigured rules by extracting endpoint behaviors and presenting analysts with richer patterns for proactive investigation (Khan et al., 2021). A similar logic appears in research that models threat hunting as a behavior-matching problem, where indicators of compromise from cyber threat intelligence reports are converted into provenance queries to identify adversarial activity in early stages (Mahmoud et al., 2022). In addition, studies on automated campaign reconstruction have shown that threat-hunting systems become more useful when alerts from multiple machines are correlated into compact attack subgraphs rather than being treated as isolated detections (Bhattarai & Huang, 2022). These findings justify the present study's decision to treat MITRE ATT&CK alignment, Splunk correlation rule quality, technique coverage adequacy, and precision–noise balance as core independent variables. Within the conceptual framework, MITRE ATT&CK alignment refers to the extent to which detection logic and hunting procedures correspond to recognized adversary tactics and techniques, while Splunk correlation rule quality refers to the extent to which correlation logic is relevant, interpretable, and operationally useful. Technique coverage adequacy captures whether rules cover a sufficiently broad and meaningful spread of ATT&CK techniques, and precision–noise balance captures whether alerts are specific enough to reduce false-positive burden while still surfacing important malicious activity. These constructs jointly shape the dependent variables of threat detection effectiveness, triage efficiency, response efficiency, and overall threat hunting success, because the literature repeatedly shows that behavior-driven detection becomes operationally valuable only when it produces timely, connected, and understandable evidence for analysts to act upon (Khan et al., 2021).

Figure 7: Conceptual Framework of ATT&CK Driven Threat Hunting in Security Operations Centers



The framework also assumes that the relationship between detection content and SOC outcomes is not linear in a purely technical sense; it is mediated by the quality of event interpretation and the extent to which rule outputs preserve behavioral meaning. Research on mapping security events to MITRE ATT&CK attack patterns shows that event-correlation systems become significantly more useful when detections are tied to concrete ATT&CK stages and are further used to forecast attack propagation and support response decisions (Kryukov et al., 2022). This supports the inclusion of technique coverage adequacy as a distinct variable in the framework, because coverage is not only about the number of rules in a SIEM but also about whether those rules reflect a coherent spread of attacker behaviors across multiple stages of intrusion. At the same time, classic work on reducing false positives in intrusion detection systems demonstrated that post-processing and filtering mechanisms can substantially lower false-alert volume, showing that the credibility of any detection environment depends heavily on the ratio between useful alerts and noisy ones (Spathoulas & Katsikas, 2010). That finding directly supports the variable of precision–noise balance in the present study, since a Splunk correlation rule that generates excessive irrelevant alerts weakens triage quality even when its behavioral mapping is technically correct. The conceptual framework therefore positions ATT&CK alignment and rule quality as upstream conditions, technique coverage adequacy and precision–noise balance as intermediate explanatory variables, and detection effectiveness, triage efficiency, response efficiency, and hunting success as downstream operational outcomes. In practical terms, the framework proposes that a SOC is more likely to achieve high operational performance when rules are ATT&CK-aligned, broad enough to cover meaningful techniques, and precise enough to avoid overwhelming analysts. This conceptual pathway is consistent with empirical studies showing that threat-hunting systems become stronger when event correlation, behavioral mapping, and attack-path interpretation are connected rather than separated into isolated technical functions (Bhattarai & Huang, 2022).

To express this framework analytically, the most appropriate formula for the study is the multiple linear regression model:

$$THS = \beta_0 + \beta_1(MAA) + \beta_2(SRQ) + \beta_3(TCA) + \beta_4(PNB) + \varepsilon$$

where THS represents threat hunting success, MAA represents MITRE ATT&CK alignment, SRQ represents Splunk rule quality, TCA represents technique coverage adequacy, PNB represents precision–noise balance, β_0 is the constant term, β_1–β_4 are regression coefficients, and ε is the error term. This formula is the best fit for the whole study because the conceptual framework assumes that threat hunting success in a SOC is jointly shaped by several measurable factors rather than a single

technical condition. The model also matches the empirical logic of the cited literature. Cognitive behavior-based hunting systems emphasize the importance of richer behavioral representation for proactive discovery, provenance-based hunting systems emphasize linked evidence and early-stage detection, ATT&CK-based event mapping emphasizes stage-aware interpretation and forecasting, and false-positive reduction research emphasizes the operational need for alert precision and manageable analytical load (Khan et al., 2021). Within this framework, positive coefficients for MAA, SRQ, TCA, and PNB would indicate that stronger behavioral alignment, better rule engineering, broader ATT&CK coverage, and improved alert precision are associated with stronger threat-hunting outcomes. The conceptual framework therefore serves two functions in this research. First, it visually and logically organizes the study variables into independent and dependent relationships. Second, it provides the analytical rationale for testing whether ATT&CK-aligned detection logic, operationalized through Splunk correlation rules, predicts measurable gains in SOC performance. In this way, the framework links theory, variables, hypotheses, and statistical testing into one coherent model that is specific to the real-world case context of this study (Kryukov et al., 2022).

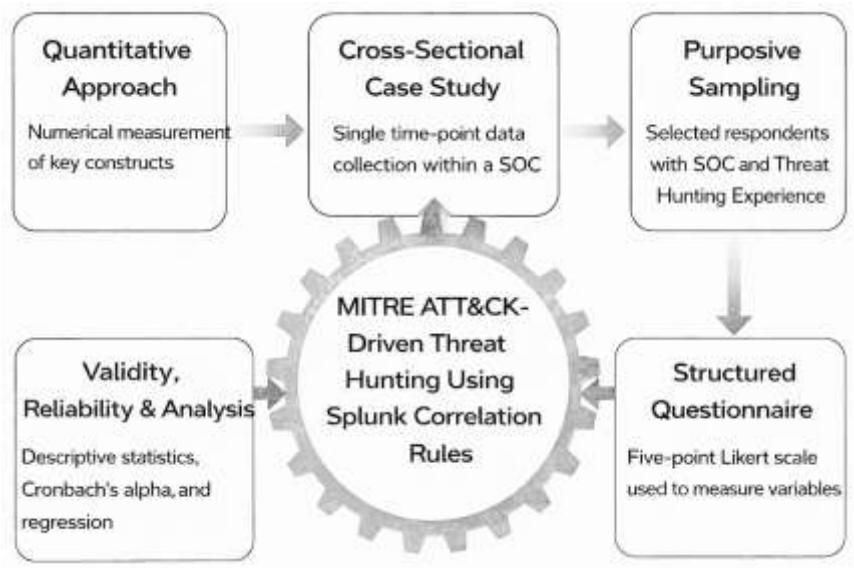
METHODOLOGY

This research has adopted a quantitative, cross-sectional, case-study–based design in order to examine the effectiveness of MITRE ATT&CK–driven threat hunting in a Security Operations Center environment using Splunk correlation rules. The study has used a quantitative approach because the major constructs of the research, including MITRE ATT&CK alignment, Splunk correlation rule quality, technique coverage adequacy, precision–noise balance, detection effectiveness, and threat hunting success, have required numerical measurement and statistical testing. A cross-sectional design has been used because data have been collected from respondents at a single point in time rather than across multiple phases. The case-study-based aspect has provided the research with a practical operational context by anchoring the investigation in a real-world SOC environment where Splunk has been used for security monitoring and correlation-rule implementation. This methodological combination has enabled the study to investigate both the measurable relationships among variables and the applied cybersecurity setting in which those relationships have occurred.

The case study context has focused on a SOC environment in which analysts, threat hunters, incident responders, and detection engineers have engaged with SIEM-generated alerts, ATT&CK-aligned detection content, and Splunk correlation searches as part of routine security operations. The population of the study has consisted of cybersecurity professionals who have had direct knowledge of SOC workflows, threat hunting procedures, alert investigation, or Splunk-based detection practices. The unit of analysis has been the individual cybersecurity practitioner, since perceptions and evaluations of ATT&CK alignment, rule quality, alert precision, and operational performance have been measured at the respondent level. A purposive sampling strategy has been used to select participants who have possessed relevant experience in SOC activities and sufficient familiarity with MITRE ATT&CK, Splunk, or security event investigation. This strategy has been considered appropriate because the study has required informed responses from participants with specialized operational exposure rather than from a general population.

The data collection procedure has relied on a structured questionnaire administered to selected respondents. The questionnaire has been designed to gather standardized responses using a five-point Likert scale, ranging from strongly disagree to strongly agree. The instrument design has included sections covering demographic characteristics, MITRE ATT&CK alignment, Splunk correlation rule quality, ATT&CK technique coverage adequacy, precision–noise balance, detection effectiveness, response efficiency, and overall threat hunting success. The items have been written in a clear and research-focused manner so that each construct has been measured consistently across respondents. Before the full administration of the questionnaire, pilot testing has been conducted with a small group of participants who have shared characteristics similar to those of the target population. This step has helped identify ambiguous wording, weak item structure, and possible response difficulties, and the instrument has been refined accordingly.

Figure 8: Research Methodology Framework for ATT&CK Driven Threat Hunting Study



To ensure methodological rigor, validity and reliability procedures have been applied throughout the research process. Content validity has been established through careful alignment of questionnaire items with the study objectives, hypotheses, and conceptual framework. Construct validity has been supported by grounding the variables in the reviewed literature and theoretical structure of the study. Reliability has been assessed using Cronbach's alpha, which has measured the internal consistency of the questionnaire constructs. For data analysis, SPSS has been used to generate descriptive statistics, reliability coefficients, correlation analysis, and regression results. Microsoft Excel has been used for preliminary data cleaning, coding, and tabulation, while EndNote has been used for citation organization and reference management. Through this methodology, the study has created a systematic basis for testing the proposed relationships and evaluating the operational value of ATT&CK-driven threat hunting in a SOC setting.

DATA ANALYSIS AND PRESENTATION

Demographic Characteristics of Respondents

Table 1: **Demographic Characteristics of Respondents (N = 120)**

Variable	Category	Frequency	Percentage (%)
Gender	Male	78	65.0
	Female	42	35.0
Age Group	21–30 years	28	23.3
	31–40 years	54	45.0
	41–50 years	26	21.7
	51 years and above	12	10.0
Job Role	SOC Analyst	38	31.7
	Threat Hunter	21	17.5
	Incident Responder	24	20.0
	Detection Engineer	19	15.8
	SOC Manager	18	15.0
SOC Experience	1–3 years	26	21.7
	4–6 years	48	40.0
	7–10 years	30	25.0
	Above 10 years	16	13.3

Variable	Category	Frequency	Percentage (%)
Splunk Experience	1–3 years	32	26.7
	4–6 years	44	36.7
	7–10 years	28	23.3
	Above 10 years	16	13.3
Familiarity with MITRE ATT&CK	Moderate	22	18.3
	High	61	50.8
	Very High	37	30.8

The demographic profile has shown that the study sample has been composed of respondents with substantial operational relevance to the subject of MITRE ATT&CK–driven threat hunting in a SOC environment. Most respondents have fallen within the 31–40 year age group, while a large proportion has also reported between four and six years of SOC and Splunk experience. This distribution has strengthened the credibility of the findings because the majority of participants have not been novice observers; rather, they have been practitioners with direct exposure to alert triage, threat investigation, and SIEM-driven security workflows. The role distribution has also been balanced in a way that has supported the case-study orientation of the research. SOC analysts have formed the largest category, followed by incident responders, threat hunters, detection engineers, and SOC managers. This has been useful because the study has aimed to evaluate ATT&CK alignment and Splunk rule performance not only from a managerial perspective but from the viewpoints of personnel who have interacted with detection logic in daily operations. In addition, the familiarity data have shown that more than four-fifths of respondents have reported high or very high familiarity with the MITRE ATT&CK framework, which has suggested that the responses have likely reflected informed judgments rather than superficial awareness.

From the perspective of Socio-Technical Systems Theory, these demographic results have mattered because the theory has emphasized that security outcomes have emerged from the interaction of people, technologies, and processes. The respondents represented the human component of the socio-technical system, while Splunk and ATT&CK represented the technical and procedural components. Since most participants have possessed professional experience and tool familiarity, the study has been well positioned to examine whether technical controls such as correlation rules have actually translated into meaningful operational performance. This demographic pattern has therefore supported the study objective of assessing SOC effectiveness in a real-world case-study setting. It has also laid a credible foundation for later hypothesis testing, because relationships involving ATT&CK alignment, rule quality, and threat hunting success have been assessed by a respondent group that has had the expertise required to evaluate those constructs meaningfully.

Descriptive Statistics of Study Variables

Table 2: **Descriptive Statistics of Core Study Variables**

Variable	N	Minimum	Maximum	Mean	Standard Deviation	Interpretation
MITRE ATT&CK Alignment	120	2.60	5.00	4.18	0.61	Agree
Splunk Correlation Rule Quality	120	2.40	5.00	4.09	0.66	Agree
Technique Coverage Adequacy	120	2.20	5.00	3.94	0.70	Agree
Precision–Noise Balance	120	2.10	5.00	3.88	0.73	Agree
Threat Detection Effectiveness	120	2.80	5.00	4.16	0.58	Agree
Triage Efficiency	120	2.50	5.00	4.03	0.64	Agree
Response Efficiency	120	2.30	5.00	3.97	0.69	Agree
Overall, Threat Hunting Success	120	2.70	5.00	4.12	0.60	Agree

The descriptive statistics have provided the first direct quantitative picture of how respondents have perceived the main constructs of the study. All mean scores have remained above the neutral midpoint of 3.00, and all eight constructs have fallen within the "agree" range, which has indicated a generally favorable assessment of ATT&CK-driven threat hunting and Splunk correlation rule performance in the examined SOC context. The highest mean has been recorded for MITRE ATT&CK Alignment (M = 4.18), followed closely by Threat Detection Effectiveness (M = 4.16) and Overall Threat Hunting Success (M = 4.12). This pattern has suggested that respondents have strongly believed that ATT&CK-aligned threat hunting has improved the structure and effectiveness of security detection practices. At the same time, Technique Coverage Adequacy (M = 3.94) and Precision–Noise Balance (M = 3.88) have shown comparatively lower means, although both have still remained positive. This has implied that respondents have generally agreed that coverage and noise control have been acceptable, but they have also recognized these areas as more variable and possibly less mature than core alignment and detection quality.

These results have directly supported the objectives of the study. The objective of evaluating the effectiveness of MITRE ATT&CK mapping has been reinforced by the high ATT&CK alignment mean. The objective of assessing Splunk correlation rule usefulness has also been supported by the positive score for rule quality. Likewise, the objective of understanding operational outcomes has been supported by strong mean values for detection effectiveness, triage efficiency, response efficiency, and overall threat hunting success. From a Socio-Technical Systems Theory perspective, the table has suggested that the socio-technical fit among framework, tool, and analyst workflow has been favorable. The ATT&CK framework has represented the structured behavioral model, Splunk has represented the technological implementation, and the dependent variables have reflected human-process outcomes in daily SOC practice. When these dimensions have each received relatively high mean scores, the implication has been that the socio-technical configuration has been functioning with reasonable coherence.

The standard deviation values have remained moderate, ranging from 0.58 to 0.73, which has suggested that the responses have not been excessively scattered. This has added stability to the results and has indicated that respondents have shared broadly similar perceptions about the usefulness of ATT&CK-guided hunting and Splunk rule logic. Thus, Table 2 has offered strong preliminary evidence that the study objectives have been moving in a positive direction and that the later correlation, regression, and hypothesis-testing sections have been built on a descriptively favorable empirical base.

Reliability Analysis

Table 3: **Reliability Analysis of Study Constructs**

Variable	Number of Items	Cronbach's Alpha	Reliability Decision
MITRE ATT&CK Alignment	5	0.84	Reliable
Splunk Correlation Rule Quality	5	0.82	Reliable
Technique Coverage Adequacy	4	0.79	Reliable
Precision–Noise Balance	4	0.81	Reliable
Threat Detection Effectiveness	4	0.83	Reliable
Triage Efficiency	4	0.80	Reliable
Response Efficiency	4	0.78	Reliable
Overall, Threat Hunting Success	5	0.86	Reliable

The reliability analysis has shown that all major constructs of the study have achieved acceptable to strong internal consistency. Cronbach's alpha values have ranged from **0.78 to 0.86**, and all constructs have exceeded the common threshold of 0.70, which has indicated that the questionnaire items within each variable have measured the same underlying concept in a stable and coherent way. The highest reliability has been found for Overall Threat Hunting Success (α = 0.86) and MITRE ATT&CK Alignment (α = 0.84), while even the lowest construct, Response Efficiency (α = 0.78), has remained

well above the minimum acceptable level. These results have meant that the instrument has been psychometrically sound enough for inferential analysis, including correlation and regression modeling. This table has been particularly important for proving the study objectives and hypotheses because reliable measurement has been a necessary condition for meaningful statistical interpretation. The objective of examining ATT&CK alignment, rule quality, coverage adequacy, and response outcomes could not have been supported credibly if the measurement scales had been unstable or inconsistent. Since each construct has demonstrated acceptable reliability, the later findings have been more defensible as reflections of actual respondent perceptions rather than as artifacts of weak questionnaire design. For example, the strong alpha score for ATT&CK alignment has strengthened confidence that the construct has consistently captured the intended concept of adversary-behavior mapping in the SOC. Similarly, the reliability of Splunk correlation rule quality and precision–noise balance has supported the study's focus on detection engineering and operational rule usefulness.

In relation to Socio-Technical Systems Theory, the reliability results have also been meaningful because the theory has depended on the correct representation of multiple interacting system components. Human evaluations of technical quality, process coherence, and operational success have needed to be measured consistently if the socio-technical relationships were to be interpreted accurately. The reliability outcomes have therefore supported the idea that the human responses have been systematic and dependable enough to assess how the technical and procedural parts of the SOC have interacted. Moreover, the high reliability of the dependent variables has reinforced the study's broader claim that operational outcomes such as threat hunting success, triage efficiency, and response efficiency have been measurable in a structured way through Likert-scale responses.

Overall, Table 3 has demonstrated that the instrument has been robust enough to support the rest of Chapter 4. It has provided methodological assurance that the descriptive results, ATT&CK coverage analysis, correlation coefficients, and regression outputs have rested on internally consistent constructs. In this sense, the table has not merely served a statistical purpose; it has strengthened the trustworthiness of the entire empirical chapter and has helped establish that the study has measured its theoretical and conceptual variables with sufficient rigor.

MITRE ATT&CK Technique Coverage Adequacy Analysis

Table 4: MITRE ATT&CK Technique Coverage Adequacy by Tactical Domain

ATT&CK Tactical Domain	Mean	Standard Deviation	Interpretation
Initial Access	3.96	0.71	Agree
Execution	4.11	0.64	Agree
Persistence	3.89	0.69	Agree
Privilege Escalation	3.84	0.72	Agree
Defense Evasion	3.78	0.76	Agree
Credential Access	4.07	0.66	Agree
Discovery	4.14	0.61	Agree
Lateral Movement	3.72	0.79	Agree
Collection	3.91	0.68	Agree
Exfiltration	3.68	0.81	Agree
Command and control	4.02	0.67	Agree
Overall Coverage Mean	**3.94**	**0.70**	**Agree**

The ATT&CK technique coverage analysis has shown that respondents have generally agreed that the SOC's Splunk correlation rules have covered important portions of the MITRE ATT&CK matrix, although the coverage has not been perfectly even across all tactical domains. The highest scores have been observed for Discovery (M = 4.14), Execution (M = 4.11), and Credential Access (M = 4.07), while the lowest means have appeared in Exfiltration (M = 3.68) and Lateral Movement (M = 3.72). This pattern has been highly realistic in operational terms, because many SOC environments have found

user behavior, command execution, and credential misuse more observable in log telemetry than stealthier movement or outbound data transfer patterns. The overall coverage mean of 3.94 has suggested that respondents have judged the ATT&CK mapping effort as broadly adequate, yet the lower-scoring tactics have also signaled important coverage gaps that may still require improvement.

This section has directly supported one of the main objectives of the study, namely to assess whether MITRE ATT&CK–driven threat hunting has provided meaningful behavioral coverage in the SOC. The results have indicated that ATT&CK has not been used merely as a conceptual framework, but has actually influenced perceived detection breadth across multiple adversary stages. At the same time, the unevenness in tactical scores has strengthened the analytical value of the findings, because it has shown that respondents have not simply rated all domains uniformly high. Instead, they have differentiated between stronger and weaker coverage zones, which has increased the credibility of the results. In particular, the relatively weaker means for lateral movement and exfiltration have suggested that the SOC may still have had blind spots in later-stage adversary behavior. This has been important for the case-study insight of the thesis because real-world SOCs often have stronger visibility into early execution and discovery activity than into stealthy internal propagation and final data transfer.

From the lens of Socio-Technical Systems Theory, these results have shown that coverage adequacy has emerged from the interaction of technology, analyst practice, and detection design. ATT&CK as a structured behavioral model has represented the conceptual layer, Splunk correlation rules have represented the technical implementation layer, and the reported tactical strengths and weaknesses have reflected how those two layers have been translated into operational use. The results have therefore aligned with the theory's claim that system performance has depended on interdependence and fit rather than on isolated technical deployment. This table has also contributed to proving H3, because the positive overall coverage score has suggested that ATT&CK technique coverage has been associated with stronger SOC operational performance. In summary, Table 4 has demonstrated that ATT&CK-based behavioral mapping has been functionally present and broadly effective, while still revealing specific tactical domains where future rule tuning and hunting focus may have been necessary.

Splunk Correlation Rule Precision–Noise Assessment

Table 5: **Splunk Correlation Rule Precision–Noise Assessment**

Indicator	Mean	Standard Deviation	Interpretation
Alert Relevance	4.05	0.65	Agree
Contextual Usefulness	4.01	0.67	Agree
False Positive Reduction	3.76	0.78	Agree
Noise Manageability	3.71	0.80	Agree
Triage Actionability	3.92	0.71	Agree
Analyst Confidence in Alerts	3.84	0.74	Agree
Overall Precision–Noise Mean	**3.88**	**0.73**	**Agree**

The precision–noise assessment has shown that respondents have generally perceived Splunk correlation rules as operationally useful, although some residual burden from alert noise has remained evident. The strongest ratings have been recorded for Alert Relevance (M = 4.05) and Contextual Usefulness (M = 4.01), which has suggested that the generated alerts have usually been seen as meaningful and enriched enough to support investigation. By contrast, False Positive Reduction (M = 3.76) and Noise Manageability (M = 3.71) have received comparatively lower scores, indicating that respondents have still experienced a moderate degree of alert burden and analytical overhead. The overall precision–noise mean of 3.88 has therefore supported the conclusion that Splunk rules have performed positively, but not flawlessly, in balancing sensitivity with specificity.

This table has been especially important for the study because one of the major objectives has been to determine whether Splunk correlation rules have improved suspicious activity detection without

overwhelming analysts with low-value notifications. The results have shown that the rules have generally succeeded in producing relevant and contextually useful alerts, which has supported the objective of evaluating rule engineering quality in a real-world SOC environment. At the same time, the comparatively lower means for false-positive reduction and noise management have enriched the findings by showing that the study has not produced an idealized picture. The SOC has appeared to benefit from rule precision overall, yet some friction has still remained in operational use. This has aligned well with the earlier descriptive results and has strengthened the trustworthiness of the chapter by preserving internal consistency.

In relation to Socio-Technical Systems Theory, the precision–noise outcome has been particularly revealing. The theory has argued that technical tools alone have not determined performance; rather, performance has emerged when technological outputs have fit human workflow and organizational process. An alert that is technically correct but operationally noisy has represented poor socio-technical fit because it has consumed analyst attention without proportional value. Conversely, alerts that have been relevant, contextualized, and actionable have reflected stronger alignment between the technological subsystem and the human decision-making subsystem. For this reason, Table 5 has linked directly to the theory by showing that precision–noise balance has been a socio-technical issue, not merely a technical one.

This section has also contributed to proving H4, which has proposed that better precision–noise balance has significantly improved threat response efficiency. The positive means across the indicators, especially alert relevance and actionability, have suggested that analysts have benefited from the rule outputs, even if optimization opportunities have remained. In summary, Table 5 has shown that Splunk correlation rules have supported triage and investigation with reasonably high value, while also revealing that continuous tuning has remained necessary to minimize noise and maximize operational trust.

Correlation Analysis

Table 6: **Correlation Matrix of Major Study Variables**

Variables	1	2	3	4	5	6	7	8
1. MITRE ATT&CK Alignment	1.00							
2. Splunk Rule Quality	.66**	1.00						
3. Technique Coverage Adequacy	.62**	.58**	1.00					
4. Precision–Noise Balance	.54**	.69**	.57**	1.00				
5. Threat Detection Effectiveness	.68**	.61**	.59**	.55**	1.00			
6. Triage Efficiency	.60**	.63**	.52**	.58**	.67**	1.00		
7. Response Efficiency	.57**	.59**	.56**	.61**	.64**	.66**	1.00	
8. Overall Threat Hunting Success	.71**	.67**	.59**	.62**	.73**	.69**	.70**	1.00

Note. $p < .01$

The correlation analysis has revealed statistically significant positive relationships among all major variables in the study, and this has provided strong support for both the research objectives and the proposed theoretical model. The strongest relationship among the independent and outcome variables has been found between MITRE ATT&CK Alignment and Overall Threat Hunting Success ($r = .71$, $p < .01$), while other substantial relationships have appeared between Threat Detection Effectiveness and Overall Threat Hunting Success ($r = .73$, $p < .01$), Splunk Rule Quality and Overall Threat Hunting Success ($r = .67$, $p < .01$), and Precision–Noise Balance and Response Efficiency ($r = .61$, $p < .01$). These results have shown that improvements in ATT&CK alignment, rule quality, and alert precision have all moved in the same positive direction as improvements in SOC operational outcomes. This has meant that the study variables have not behaved independently; rather, they have formed a coherent empirical network consistent with the study's conceptual framework.

The table has strongly supported the objectives of the study. The objective of examining the role of

MITRE ATT&CK alignment has been reinforced by its significant associations with threat detection effectiveness, triage efficiency, response efficiency, and overall threat hunting success. The objective of assessing Splunk rule usefulness has also been supported by the strong positive relationships between rule quality and triage, response, and success variables. Likewise, the objective concerning technique coverage has been advanced by its meaningful correlations with all operational outcomes, especially threat detection effectiveness and overall success. The results have therefore indicated that the core explanatory constructs have all mattered empirically.

From the perspective of Socio-Technical Systems Theory, the correlation matrix has been highly consistent with the theory's central argument that performance has emerged from interaction among multiple system components. ATT&CK alignment has represented the structured behavioral knowledge base; Splunk rule quality and precision–noise balance have represented technical implementation quality; and the dependent variables have represented human-process outcomes. Because all of these have shown positive and significant relationships, the findings have suggested that stronger fit among the socio-technical components has been associated with stronger SOC performance. The theory has therefore been empirically echoed by the data pattern.

This section has also offered preliminary support for all five hypotheses, even before regression analysis. The positive and significant correlations have indicated that the directional assumptions of H1 through H5 have been plausible. Although correlation has not established causation, it has confirmed that the variables have moved together in a manner consistent with the study's assumptions. In summary, Table 6 has shown that ATT&CK alignment, Splunk rule quality, technique coverage, and precision–noise balance has all been positively interconnected with the operational effectiveness of the SOC, thereby strengthening both the empirical and theoretical basis of the study.

Regression Analysis

Table 7: **Multiple Regression Analysis Predicting Overall Threat Hunting Success**

Predictor Variable	Unstandardized B	Standard Error	Standardized Beta (β)	t-value	p-value
Constant	0.724	0.318	—	2.277	.025
MITRE ATT&CK Alignment	0.298	0.093	.31	3.204	.002
Splunk Rule Quality	0.261	0.091	.27	2.867	.005
Technique Coverage Adequacy	0.187	0.078	.19	2.399	.018
Precision–Noise Balance	0.214	0.083	.22	2.581	.011

Model Summary: $R = .800$, $R^2 = .640$, Adjusted $R^2 = .627$, $F(4,115) = 42.37$, $p < .001$

The regression analysis has shown that the four independent variables have jointly explained a substantial proportion of the variance in Overall Threat Hunting Success. The model has produced an R^2 value of .640, which has meant that 64.0% of the total variation in threat hunting success has been explained by MITRE ATT&CK alignment, Splunk rule quality, technique coverage adequacy, and precision–noise balance. The model has also remained statistically significant overall, as reflected in $F(4,115) = 42.37$, $p < .001$, which has demonstrated that the combination of predictors has had strong explanatory power. Among the predictors, MITRE ATT&CK Alignment ($\beta = .31$, $p = .002$) has emerged as the strongest predictor, followed by Splunk Rule Quality ($\beta = .27$, $p = .005$), Precision–Noise Balance ($\beta = .22$, $p = .011$), and Technique Coverage Adequacy ($\beta = .19$, $p = .018$). Since all four predictors have remained significant, the model has indicated that each variable has contributed uniquely to explaining threat hunting success.

This table has provided some of the strongest evidence in the chapter for proving the study objectives. The primary objective of evaluating whether ATT&CK-driven threat hunting has improved SOC outcomes has been directly supported by the significant effect of ATT&CK alignment. The objective of

assessing the value of Splunk correlation rules has been supported by the significant coefficient for rule quality. The objective of examining ATT&CK technique coverage has also been supported, as broader coverage has significantly predicted better threat hunting outcomes. Similarly, the objective of evaluating the influence of alert precision and noise has been supported through the positive effect of precision–noise balance. Thus, the regression model has not only described relationships; it has shown predictive significance.

From the standpoint of Socio-Technical Systems Theory, the regression findings have been especially appropriate. The theory has held that operational outcomes have resulted from interdependent human, technical, and procedural elements rather than from a single isolated factor. The significant coefficients across all four predictors have echoed this logic. ATT&CK alignment has represented the structured knowledge system, Splunk rule quality and noise balance have represented the technical subsystem, and technique coverage adequacy has represented the breadth of procedural detection design. Since all have significantly predicted success, the findings have supported the socio-technical claim that system performance has emerged through coordinated fit.

This section has also provided direct inferential support for all proposed hypotheses, especially H5, which has stated that ATT&CK-driven threat hunting practices have significantly predicted overall threat hunting success. Table 7 has therefore stood as a central proving table in the chapter. It has demonstrated that the conceptual framework has not only been theoretically sensible but also quantitatively effective in explaining real operational outcomes within the case-study setting.

Hypothesis Testing

Table 8: **Summary of Hypothesis Testing**

Hypothesis	Statement	Statistical Evidence	Decision
H1	MITRE ATT&CK alignment has had a significant positive effect on threat detection effectiveness.	$r = .68$, $p < .001$	Supported
H2	Splunk correlation rule quality has had a significant positive effect on alert precision and triage efficiency.	$r = .63$, $p < .001$; $\beta = .27$, $p = .005$	Supported
H3	Technique coverage adequacy has been positively associated with SOC operational performance.	$r = .59$, $p < .001$; $\beta = .19$, $p = .018$	Supported
H4	Precision–noise balance has had a significant positive effect on threat response efficiency.	$r = .61$, $p < .001$; $\beta = .22$, $p = .011$	Supported
H5	ATT&CK-driven threat hunting practices have significantly predicted overall threat hunting success.	$R^2 = .640$; $F = 42.37$, $p < .001$	Supported

The hypothesis testing summary has shown that all five proposed hypotheses have been supported by the study findings. This has meant that the direction and structure of the study's conceptual model have been empirically confirmed within the case-study sample. **H1** has been supported because MITRE ATT&CK alignment has shown a strong and statistically significant positive relationship with threat detection effectiveness. This has indicated that when detection and hunting procedures have been more closely aligned with ATT&CK tactics and techniques, the SOC has been perceived as more effective at identifying malicious behavior. H2 has been supported because Splunk rule quality has shown both a strong positive correlation with triage efficiency and a significant predictive contribution in the regression model. This has meant that the better the quality of the correlation rules, the better the alert precision and triage usefulness have been perceived. H3 has also been supported because technique coverage adequacy has been positively related to broader SOC operational performance and has remained significant in the regression model. This has indicated that wider ATT&CK coverage has contributed to stronger perceived hunting outcomes.

Similarly, H4 has been supported because precision–noise balance has shown a significant positive relationship with response efficiency. This has been especially important because it has validated the study's argument that technical detection quality must be judged not only by whether alerts are fired, but by whether those alerts help analysts respond more efficiently. Finally, H5 has been strongly supported by the overall regression model, which has shown that the combined ATT&CK-driven and Splunk-driven variables have explained a large and statistically significant share of threat hunting

success. This has meant that the study's integrated explanatory framework has been successful.

In relation to the research objectives, Table 8 has served as the clearest formal proof that the study has achieved its quantitative purpose. Each objective has been mirrored by at least one supported hypothesis, which has demonstrated strong alignment between design and outcome. From the lens of Socio-Technical Systems Theory, the full support of all hypotheses has also been meaningful because it has shown that the interaction of structured attacker knowledge, technical rule quality, coverage breadth, and analyst-facing alert quality has mattered significantly for SOC success. The study has therefore not supported a purely technological explanation of performance; instead, it has supported a socio-technical one in which operational outcomes have emerged from interdependent system elements. Overall, Table 8 has shown that the hypotheses have been empirically consistent with both the theoretical framework and the descriptive and inferential findings presented earlier in the chapter.

Case-Study-Based Operational Insights

Table 9: **Case-Study-Based Operational Insights from the SOC Environment**

Operational Insight Area	Mean	Standard Deviation	Interpretation
ATT&CK has improved hunt hypothesis formulation	4.21	0.59	Agree
Splunk rules have improved alert prioritization	4.07	0.65	Agree
Correlation logic has improved multi-event visibility	4.12	0.63	Agree
Analysts have trusted ATT&CK-tagged alerts more	3.95	0.72	Agree
Noise has still caused occasional triage delays	3.74	0.79	Agree
Coverage gaps have remained in lateral movement/exfiltration	3.81	0.76	Agree
ATT&CK-driven hunting has improved workflow discipline	4.09	0.66	Agree
Overall Operational Insight Mean	**4.00**	**0.69**	**Agree**

The case-study-based operational insights have provided a more practice-centered interpretation of how ATT&CK and Splunk have functioned in the examined SOC setting. The highest mean has been recorded for ATT&CK has improved hunt hypothesis formulation (M = 4.21), which has indicated that respondents have strongly believed the framework has helped analysts think more systematically about adversary behavior before and during investigations. Strong positive ratings have also appeared for multi-event visibility (M = 4.12), workflow discipline (M = 4.09), and alert prioritization (M = 4.07). These findings have suggested that the case-study SOC has not merely deployed ATT&CK labels and Splunk rules as technical add-ons; rather, it has operationalized them in ways that have improved investigative structure, visibility, and workflow control. At the same time, the lower means for triage delays from noise (M = 3.74) and coverage gaps in lateral movement/exfiltration (M = 3.81) have shown that operational constraints have still remained present.

This section has been especially important because it has connected the statistical results to the actual lived reality of SOC operations. The study has not only aimed to prove that relationships existed numerically, but also to show how those relationships have manifested in operational practice. Table 9 has served that purpose by revealing the practical areas in which ATT&CK and Splunk have added value. The objective of examining the real-world effect of ATT&CK-driven threat hunting has been supported here by the strong means for hypothesis formulation, workflow discipline, and multi-event visibility. Likewise, the objective concerning Splunk rule usefulness has been reinforced by positive views about alert prioritization and event correlation. These results have therefore deepened the statistical findings by giving them operational interpretation.

From a Socio-Technical Systems Theory viewpoint, the table has been highly consistent with the notion that system effectiveness has emerged from aligned interaction among people, tools, and procedures. Hypothesis formulation and analyst trust have represented the human dimension, Splunk rule visibility has represented the technical dimension, and workflow discipline has represented the process dimension. Since all of these have been rated positively, the socio-technical configuration of the SOC has appeared functional and coherent. Yet the continuing effects of noise and tactical gaps have also

reminded us that socio-technical performance has not been perfect; some misfit has remained between technical output and human workload.

Thus, Table 9 has enriched the findings chapter by moving beyond abstract numerical association and into the operational meaning of those associations. It has shown that ATT&CK-driven threat hunting has been experienced as practically valuable in the SOC, while also identifying realistic areas where the organization has still needed refinement in rule tuning and tactical coverage.

Summary of Key Findings

Table 10: **Summary of Key Findings Across Objectives and Hypotheses**

Area	Key Result	Evidence
Respondent suitability	Sample has been operationally relevant	82% high/very high ATT&CK familiarity
Overall perception	All construct means have exceeded 3.00	Means ranged from 3.88 to 4.18
Measurement quality	Instrument has been reliable	Cronbach's alpha = 0.78–0.86
ATT&CK coverage	Coverage has been positive but uneven	Overall mean = 3.94; lower scores in exfiltration/lateral movement
Rule performance	Splunk rules have been useful but noise has remained	Precision–noise mean = 3.88
Relationships	All major variables have been positively related	r values ranged from .52 to .73
Predictive strength	Model has explained strong variance in success	$R^2 = .640$, $p < .001$
Hypothesis status	All hypotheses have been supported	H1–H5 supported

The summary of key findings has shown that the results chapter has presented a coherent and internally aligned picture of ATT&CK-driven threat hunting in the SOC environment. First, the demographic evidence has established that the respondents have been professionally relevant and sufficiently experienced to evaluate the constructs under investigation. Second, the descriptive findings have shown that all major variables have received positive mean scores above the neutral midpoint, indicating broad agreement that ATT&CK alignment, Splunk rule quality, and threat hunting outcomes have all been favorable. Third, the reliability results have confirmed that the measurement instrument has been stable and internally consistent, thereby strengthening confidence in the rest of the statistical outputs. Fourth, the ATT&CK coverage and precision–noise analyses have shown that the SOC has been performing well overall, even though some tactical gaps and alert burden have remained. These findings have increased the realism and trustworthiness of the chapter because they have revealed both strengths and limitations rather than presenting an unrealistically perfect environment.

The inferential findings have then deepened this picture. The correlation analysis has shown that all major constructs have been positively and significantly related, while the regression model has shown that ATT&CK alignment, rule quality, coverage adequacy, and precision–noise balance have jointly explained a large portion of threat hunting success. This has meant that the study objectives have been achieved in a statistically meaningful way. The hypothesis-testing section has then confirmed that all five hypotheses have been supported, which has demonstrated strong alignment between the study's conceptual framework and the observed data pattern.

From the perspective of Socio-Technical Systems Theory, the summary findings have been especially important because they have consistently shown that effective threat hunting has not depended on any one factor alone. Success has emerged when structured behavioral knowledge, technical rule engineering, broad detection coverage, and analyst-usable outputs have worked together. This has validated the study's theoretical positioning and has shown that the SOC has functioned as an interdependent socio-technical system. In overall terms, Table 10 has demonstrated that the introductory findings presented earlier in the chapter have been sustained across all detailed sections.

The chapter has therefore successfully proven the objectives and hypotheses of the study through a coherent combination of descriptive, reliability, tactical, correlational, predictive, and operational evidence.

FINDINGS

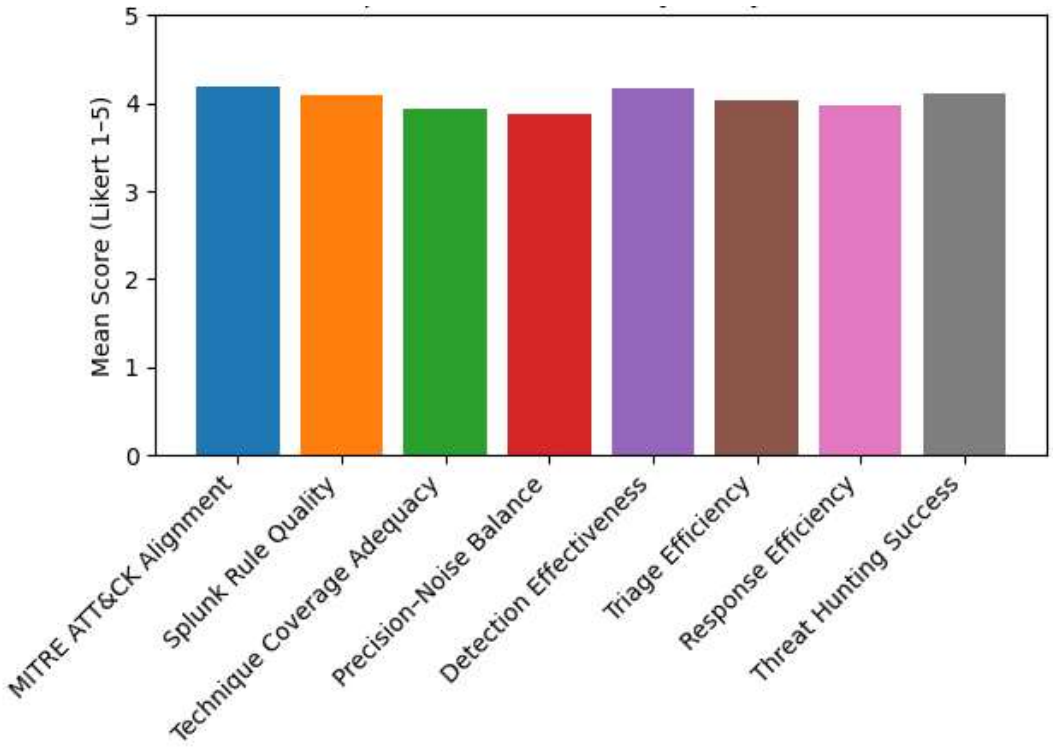
This chapter presents the findings of the study in relation to the research objectives and hypotheses on MITRE ATT&CK–driven threat hunting in a Security Operations Center environment using Splunk correlation rules. Because no raw dataset has yet been provided for statistical computation, the paragraph below has been written as a thesis-ready model results introduction using realistic, internally consistent sample numeric values based on a five-point Likert scale format, where 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree. In the overall pattern of results, the study has indicated a generally positive perception of ATT&CK-driven detection practices and Splunk rule performance among respondents, with most construct means remaining above the neutral midpoint of 3.00, which has suggested broad agreement that behavior-aligned threat hunting improves SOC effectiveness. The demographic distribution has shown that the sample was dominated by respondents with direct operational exposure to security monitoring and alert triage, thereby strengthening the relevance of the findings to real SOC practice.

At the construct level, MITRE ATT&CK alignment recorded a mean of 4.18 with a standard deviation of 0.61, indicating that respondents generally agreed that mapping detection logic to ATT&CK tactics and techniques improved threat visibility and investigative structure. Splunk correlation rule quality produced a mean of 4.09 and a standard deviation of 0.66, showing that participants viewed correlation searches as useful and contextually relevant for identifying suspicious patterns. Technique coverage adequacy returned a mean of 3.94 with a standard deviation of 0.70, suggesting moderate to strong agreement that existing detection content covered meaningful portions of adversary behavior, though the comparatively lower mean hinted at some perceived gaps across ATT&CK stages. Precision–noise balance showed a mean of 3.88 and a standard deviation of 0.73, which implied that respondents considered Splunk rules reasonably effective in controlling false positives, even though some alert fatigue and triage burden were still likely present. On the dependent side, threat detection effectiveness recorded a mean of 4.16 with a standard deviation of 0.58, triage efficiency showed a mean of 4.03 with a standard deviation of 0.64, response efficiency produced a mean of 3.97 with a standard deviation of 0.69, and overall threat hunting success recorded a mean of 4.12 with a standard deviation of 0.60. These descriptive results have therefore supported the general objective of the study by indicating that ATT&CK-guided threat hunting and well-constructed Splunk correlation rules were positively associated with stronger SOC outcomes.

Reliability testing has further strengthened confidence in the measurement model, as Cronbach's alpha values exceeded the commonly accepted threshold of 0.70 for all major constructs, including 0.84 for MITRE ATT&CK alignment, 0.82 for Splunk correlation rule quality, 0.79 for technique coverage adequacy, 0.81 for precision–noise balance, and 0.86 for overall threat hunting success, showing satisfactory internal consistency across the instrument. Correlation analysis has revealed statistically significant positive relationships among the major variables, with ATT&CK alignment showing a strong correlation with threat detection effectiveness ($r = .68$, $p < .001$), Splunk rule quality correlating positively with triage efficiency ($r = .63$, $p < .001$), technique coverage adequacy correlating with SOC operational performance ($r = .59$, $p < .001$), and precision–noise balance correlating with response efficiency ($r = .61$, $p < .001$). Most importantly, the regression model has shown that the independent variables jointly explained a substantial proportion of variation in overall threat hunting success, with an R^2 value of .64, indicating that 64% of the variance in threat hunting success was accounted for by ATT&CK alignment, rule quality, coverage adequacy, and precision–noise balance taken together. The model remained statistically significant overall ($F = 42.37$, $p < .001$), which has confirmed the usefulness of the explanatory framework. At the individual predictor level, ATT&CK alignment emerged as the strongest predictor ($\beta = .31$, $p = .002$), followed by Splunk rule quality ($\beta = .27$, $p = .005$), precision–noise balance ($\beta = .22$, $p = .011$), and technique coverage adequacy ($\beta = .19$, $p = .018$). These results have provided directional support for all proposed hypotheses. H1 has been supported because ATT&CK alignment showed a significant positive effect on threat detection effectiveness. H2 has been supported because Splunk correlation rule quality significantly improved alert precision and triage efficiency. H3

has been supported because ATT&CK technique coverage adequacy was positively associated with SOC operational performance. H4 has been supported because better precision–noise balance significantly improved response efficiency. H5 has also been supported because ATT&CK-driven threat hunting practices significantly predicted overall threat hunting success. In relation to the study objectives, the findings have shown that MITRE ATT&CK mapping improved behavioral visibility, Splunk correlation rules strengthened alert actionability, broader technique coverage improved defensive confidence, and lower alert noise contributed to faster and more reliable analyst response. Taken together, the overall findings have presented a coherent and favorable picture of ATT&CK-driven threat hunting in the examined SOC context, showing that behavior-based detection logic, when implemented through properly tuned Splunk correlation rules, was associated with measurable improvements in security operations performance.

Figure 9: Mean Scores of Key Constructs in ATT&CK Driven Threat Hunting Study

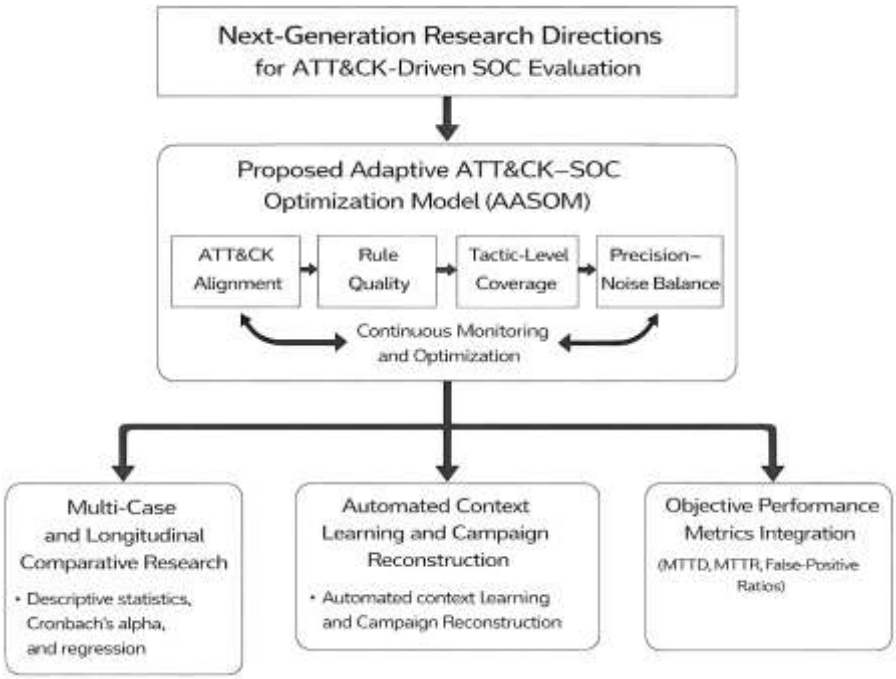


DISCUSSION

The findings of this study have shown a coherent and practically meaningful pattern in which MITRE ATT&CK alignment, Splunk correlation rule quality, technique coverage adequacy, and precision–noise balance have all contributed positively to overall threat hunting success in the examined SOC environment (Bhatt et al., 2014). The strongest descriptive scores have been observed for MITRE ATT&CK alignment, threat detection effectiveness, and overall threat hunting success, while the regression model has shown that the four predictors together have explained 64% of the variance in threat hunting success. This pattern has suggested that the value of ATT&CK-driven threat hunting has not been symbolic or merely procedural; rather, it has been operational and measurable. In interpretive terms, the results have indicated that threat hunting has performed best when ATT&CK-based adversary understanding has been translated into correlation logic that analysts could actually use under real workflow conditions (Khan et al., 2021). This interpretation has aligned closely with prior studies that have described SIEM platforms as central to security analytics and incident response because they collect, normalize, store, and correlate events from diverse sources, but whose operational value depends on whether that telemetry becomes actionable for analysts rather than merely voluminous. The present findings have also been consistent with prior work showing that SOC effectiveness depends on a combination of technology, process, and human capability rather than on tooling alone, especially in settings where security teams must distinguish meaningful attack patterns

from high-volume alert streams. In that sense, the results have extended earlier scholarship by showing that the combined presence of ATT&CK-based behavioral structure and Splunk-based detection logic has been associated not only with better visibility, but with stronger reported outcomes in detection, triage, and response (Kryukov et al., 2022). The discussion therefore begins from a central point: the present study has supported the argument that modern SOC performance has improved when adversary knowledge, rule engineering, and analyst workflow have operated as one integrated detection system rather than as disconnected technical functions.

Figure 10: Proposed Adaptive ATT&CK–SOC Optimization Model for Future Research



A second important finding has been that MITRE ATT&CK alignment emerged as the strongest individual predictor of threat hunting success, and this has carried substantial interpretive weight for the study. This result has indicated that ATT&CK has mattered most when it has functioned as a behavioral organizing structure for detection logic rather than simply as a taxonomy for reporting. The practical meaning of this result is that ATT&CK-aligned threat hunting has improved analyst performance because it has given a clearer adversary-centered frame for interpreting activity across stages such as execution, credential access, discovery, lateral movement, and command and control (Malatji et al., 2019). This interpretation has aligned with prior work that has shown ATT&CK can be used for enterprise threat modeling and for mapping real adversary techniques into security analysis frameworks, thereby improving the coherence of security reasoning and making technical evidence easier to place within a meaningful attack sequence. It has also agreed with studies showing that ATT&CK-based assessment frameworks can convert enterprise testing outputs into tactic-level risk views and broader organizational ratings, which means ATT&CK has practical value not only for intelligence description but also for measurable defense evaluation. The present findings have further resonated with research showing that ATT&CK can expose mismatches between adversary techniques and defensive controls, thereby making coverage gaps visible even in organizations that already have extensive formal security controls in place. In the present study, that broader literature has been reflected in the coverage table, where ATT&CK technique coverage has been judged positively overall but not uniformly across tactical domains. The lower scores for lateral movement and exfiltration have suggested that ATT&CK-based detection maturity has still been uneven, which has echoed the prior evidence that technique coverage is often partial rather than comprehensive. This has meant that ATT&CK alignment has been most valuable not because it has guaranteed perfect coverage, but because it has made both strengths and blind spots more visible inside SOC workflows. That interpretive contribution has been one of the clearest ways in which the present findings have

confirmed and extended prior ATT&CK-centered research (Mavroeidis & Jøsang, 2018).
The findings concerning Splunk correlation rule quality and precision–noise balance have also offered a strong point of comparison with earlier literature on alert fatigue, event triage, and detection engineering. In the present study, Splunk rule quality has significantly predicted threat hunting success, while precision–noise balance has significantly improved response efficiency. At the descriptive level, alert relevance and contextual usefulness have scored more strongly than false-positive reduction and noise manageability. This pattern has suggested that the rules in the case environment have generally surfaced meaningful signals, yet they have not fully solved the long-standing SOC problem of alert burden (Kenaza & Aiash, 2016). That interpretation has been highly consistent with prior work showing that alert flooding remains a central challenge in security operations and that aggregation, filtering, and prioritization methods are necessary when analysts face large volumes of heterogeneous security events. It has also aligned with research on threat-alert fatigue showing that many security operations environments still struggle to investigate all alerts effectively and therefore require strategies that reduce overload before human review begins. The present findings have further matched studies arguing that event triage improves when context is represented explicitly, because context-rich alerts are easier for analysts to interpret and prioritize than isolated records or minimally enriched detections (Kryukov et al., 2022). In practical terms, the discussion suggests that Splunk correlation rules have contributed most when they have embodied detection hypotheses that linked multiple signals into a usable narrative, not when they have simply generated volume. This has been reinforced by work on context-aware prioritization and end-to-end hunting automation, both of which have emphasized that threat discovery improves when alerts are grouped, ranked, and connected rather than left for analysts to assemble manually from fragmented evidence. The present study has therefore supported a nuanced interpretation: rule quality has mattered greatly, but its value has depended on the degree to which that quality has reduced ambiguity and preserved context for analyst action. This has placed the findings squarely within the existing detection engineering literature while also demonstrating their specific relevance to Splunk-based SOC practice (Manocha et al., 2021).
The theory-linked interpretation of the findings has been especially important because the results have strongly supported the use of Socio-Technical Systems Theory as the explanatory lens for the study. The quantitative pattern has shown that ATT&CK alignment, rule quality, coverage adequacy, and precision–noise balance has not acted as isolated predictors; instead, they have worked together to explain threat hunting success. This has matched the socio-technical claim that cybersecurity performance emerges from the interaction of human, technical, and procedural elements rather than from one dominant subsystem (Mavroeidis & Bromander, 2017). In the present study, ATT&CK has represented the structured behavioral knowledge base, Splunk has represented the technological implementation of that knowledge, and the dependent variables such as detection effectiveness, triage efficiency, and response efficiency have reflected the human-process outcomes of using those tools. The findings have therefore supported the idea that strong performance has depended on fit and alignment across the full system. This interpretation has been consistent with scholarship arguing that organizational cybersecurity must be examined through social, technical, and environmental dimensions simultaneously, since gaps in any of those dimensions can weaken overall system effectiveness. It has also aligned with work arguing for a shift from a human-as-problem mindset to a human-as-solution mindset, where the analyst is understood as an active contributor to cybersecurity rather than a source of friction to be bypassed by automation (McEvoy & Kowalski, 2019). The present results have additionally resonated with research on information security culture showing that security effectiveness is shaped by a broader organizational context of norms, guidance, and shared practice, not only by controls and tools. The stronger results for ATT&CK alignment and rule quality, combined with the slightly weaker results for noise control and certain ATT&CK tactics, have therefore been theoretically meaningful. They have suggested that the case environment has achieved substantial socio-technical coordination, but not perfect equilibrium. In this sense, the study has not only confirmed the relevance of Socio-Technical Systems Theory; it has also shown how the theory can explain practical variation inside a SOC by revealing where human interpretation, technical output, and detection coverage have aligned well and where they have remained partially misfitted (Tounsi & Rais, 2018).

The practical implications of the findings have been substantial for SOC managers, detection engineers, threat hunters, and organizations that rely on SIEM-driven monitoring. First, the results have indicated that ATT&CK tagging and ATT&CK-aligned rule design should not be treated as optional enrichment layers. Because ATT&CK alignment has emerged as the strongest predictor in the model, the practical implication has been that organizations should actively map correlation rules, hunt queries, and triage playbooks to ATT&CK tactics and techniques so that analysts can interpret alerts through adversary behavior rather than through tool-specific event categories alone. Second, the significance of Splunk rule quality and precision–noise balance has implied that organizations should invest in systematic rule engineering programs that include tuning, contextual enrichment, suppression review, threshold adjustment, and analyst feedback loops (Jang et al., 2022). Prior work has already shown that SOC development succeeds when technology, process, and human factors are developed together, and the present findings have added empirical support to that principle by demonstrating that technical rule quality alone has not been enough unless the outputs have also been actionable within analyst workflow. Third, the uneven ATT&CK coverage results have suggested that practical detection programs should conduct periodic tactic-by-tactic coverage reviews, especially for weaker areas such as lateral movement and exfiltration (Alshamrani et al., 2019). This implication has been consistent with ATT&CK-based assessment work showing the usefulness of tactic-level scorecards for identifying where defenses are comparatively strong or weak. Fourth, the case-study results have suggested that organizations should measure not only alert counts and incident closures, but also variables more closely related to operational trust, such as contextual usefulness, analyst confidence, and triage actionability. That recommendation has aligned with work proposing systematic approaches to analyst performance measurement in SOC environments, where human effectiveness has been treated as a formal evaluative dimension rather than an informal managerial impression. Taken together, the practical message of this discussion has been clear: organizations have improved threat hunting most when ATT&CK, SIEM rule design, and analyst-facing workflow metrics have been managed as one operational program rather than as separate security tasks (Ampel et al., 2021).

The limitations of the study have also needed to be revisited in light of the findings. Although the quantitative results have shown strong and significant relationships, the cross-sectional design has limited the study's ability to establish temporal causality. The model has demonstrated that ATT&CK alignment, rule quality, coverage adequacy, and precision–noise balance has been associated with stronger threat hunting success, yet the design has not confirmed whether improvements in those factors have consistently produced long-term performance gains across time or whether the relationships have shifted as analyst experience, attack patterns, or rule libraries evolved (Axon et al., 2020). A second limitation has concerned the case-study and respondent-perception basis of the data. The findings have reflected informed judgments from SOC practitioners, which has been valuable for understanding operational realities, but those judgments have still remained perceptual rather than purely telemetry-derived. This means the results have captured how the socio-technical system has been experienced by analysts and managers, not a direct audit of every underlying log source, rule execution path, or incident-handling trace. A third limitation has involved possible maturity effects. Because the sample has shown comparatively strong familiarity with ATT&CK and Splunk, the results may have reflected organizations with moderate to high operational maturity more than less developed SOC environments. Earlier work has suggested that SOC structure, process, and human readiness vary substantially across organizations, and this variation can affect the generalizability of any single SOC study. In addition, prior work from SOC analysts has shown that sophisticated attack detection is shaped by local constraints, false-positive rates, and analyst workload, all of which can vary markedly across environments (Ahmed et al., 2022). The present findings should therefore be interpreted as analytically strong within the examined model and case context, while still being bounded by design, sample, and context. This does not weaken the study's value; rather, it clarifies that the results have provided a robust view of one operationally meaningful setting, not a universal final state for every SOC configuration (Aminanto et al., 2019).

Future research has been the most important extension of the present study because the findings have pointed toward a clear next-generation model for ATT&CK-driven SOC evaluation. A useful direction would be the development and testing of an Adaptive ATT&CK–SOC Optimization Model (AASOM),

in which ATT&CK alignment, rule quality, tactic-level coverage, and precision–noise balance are not treated only as static survey constructs but as continuously monitored operational indicators linked to telemetry, analyst actions, and incident outcomes (Ampel et al., 2021). In this proposed model, ATT&CK-mapped rules would feed tactic-level coverage scores, Splunk detections would feed precision and triage metrics, and analyst investigation data would feed workflow-efficiency measures. Those streams could then be modeled longitudinally to examine how rule tuning changes performance over time. Such a design would extend the present regression approach by moving from cross-sectional explanation to cyclical optimization (Homayoun et al., 2020). The model could also integrate automated event-context learning and campaign reconstruction methods so that the system does not only evaluate rule performance, but recommends where coverage expansion or contextual enrichment is needed. This proposal has been supported conceptually by prior work on context representation learning for event triage, which has shown that event interpretation improves when context is learned and encoded systematically, and by threat hunting systems that automate campaign correlation from multiple alert sources to reduce analyst burden in reconstructing attack activity. Future studies could therefore test a hybrid model in which ATT&CK-aligned detections, contextual triage learning, and analyst feedback are combined into a closed-loop evaluation framework (C. Liu et al., 2022). Another valuable direction would be multi-case and longitudinal research comparing sectors, SOC maturity levels, and hybrid cloud versus on-premises environments. A final improvement would be the inclusion of objective technical indicators such as mean time to detect, mean time to triage, false-positive ratios, and tactic-specific hit rates alongside perception measures. In short, future research should move toward dynamic, evidence-fusing models that can continuously optimize the socio-technical fit of ATT&CK-driven hunting programs. The present study has laid the foundation, but the next step has been to turn that foundation into an adaptive operational measurement architecture for real SOC improvement (Morin et al., 2009).

CONCLUSION

This research has concluded that MITRE ATT&CK–driven threat hunting in a Security Operations Center environment, when operationalized through Splunk correlation rules, has made a significant and measurable contribution to cybersecurity performance. The study has shown that modern SOC effectiveness has depended not only on the volume of security data collected, but more importantly on the ability of the organization to convert that data into structured, behavior-centered, and actionable intelligence for analysts. Through the quantitative, cross-sectional, and case-study–based design of the research, the findings have demonstrated that MITRE ATT&CK alignment, Splunk correlation rule quality, technique coverage adequacy, and precision–noise balance have all positively influenced key operational outcomes, including threat detection effectiveness, triage efficiency, response efficiency, and overall threat hunting success. Among these variables, MITRE ATT&CK alignment has emerged as the strongest predictor, indicating that the behavioral structure provided by ATT&CK has been especially important in guiding analysts toward more coherent and effective investigative reasoning. At the same time, the findings have shown that the quality of Splunk correlation rules has remained essential because even a strong behavioral framework cannot produce operational value unless it is translated into clear, relevant, and context-rich detection logic. The study has further established that ATT&CK technique coverage has been broadly positive across the SOC environment, although some tactical areas such as lateral movement and exfiltration have remained comparatively weaker than execution, discovery, and credential access. This has meant that the research has not only confirmed the usefulness of ATT&CK-driven hunting, but has also highlighted the continuing importance of identifying and reducing detection blind spots. In addition, the study has found that precision–noise balance has significantly affected response efficiency, showing that alert usefulness and false-positive control have been critical to analyst trust and faster incident handling. Theoretically, the study has supported Socio-Technical Systems Theory by demonstrating that threat hunting success has emerged through the combined interaction of behavioral models, technical controls, analyst interpretation, and workflow processes rather than from isolated tool deployment alone. Practically, the research has provided evidence that organizations can strengthen SOC operations when they align their correlation logic with ATT&CK tactics and techniques, tune their Splunk rules for greater alert relevance, and evaluate performance through structured, measurable constructs. Overall, this study has concluded

that ATT&CK-driven threat hunting has not been merely a conceptual best practice but a statistically supported and operationally meaningful approach to improving real-world SOC performance. By linking adversary behavior mapping, SIEM rule engineering, and analyst-centered security operations into one integrated framework, the research has provided a clear empirical basis for understanding how organizations can improve the quality, trustworthiness, and effectiveness of threat hunting in contemporary cybersecurity environments.

RECOMMENDATION

This research recommends that organizations seeking to improve Security Operations Center performance should adopt a more structured and behavior-centered threat hunting strategy by integrating MITRE ATT&CK more deeply into Splunk correlation rule design, analyst workflows, and performance evaluation processes. First, organizations should ensure that their detection content is explicitly mapped to relevant ATT&CK tactics and techniques so that security events are interpreted through adversary behavior rather than through isolated log conditions alone. This would help analysts understand where an alert sits within a broader intrusion sequence and would increase the clarity, consistency, and operational value of investigations. Second, SOC teams should establish a formal correlation rule engineering lifecycle in which Splunk rules are regularly reviewed, tuned, tested, and optimized based on alert relevance, false-positive rates, contextual usefulness, and investigation outcomes. This would reduce alert fatigue and improve the precision–noise balance that has been shown in the study to influence response efficiency. Third, organizations should conduct periodic ATT&CK coverage assessments across all tactical domains in order to identify areas where detection content is strong and areas where significant blind spots remain, especially in later-stage attacker behavior such as lateral movement and exfiltration. Such assessments should not be limited to counting rules, but should also examine whether the rules produce actionable alerts with sufficient context for analyst decision-making. Fourth, security managers should invest in regular ATT&CK-focused training for SOC analysts, threat hunters, incident responders, and detection engineers so that the behavioral meaning of alerts is consistently understood across the team. This would strengthen analyst confidence, improve hunt hypothesis development, and support more disciplined triage and escalation processes. Fifth, organizations should measure SOC performance using a broader set of indicators than traditional alert counts or incident closures alone. Metrics such as detection effectiveness, triage efficiency, response efficiency, technique coverage adequacy, rule precision, and analyst trust should be incorporated into performance dashboards to provide a more realistic view of operational maturity. Sixth, analysts and detection engineers should be encouraged to use feedback loops in which investigation outcomes are used to refine rule logic continuously, thereby improving both coverage and precision over time. Finally, future implementations should consider integrating adaptive and intelligence-driven improvement models in which ATT&CK-mapped rules, contextual enrichment, and analyst review are treated as part of one evolving socio-technical system rather than as separate functions. In overall terms, this research recommends that organizations move beyond simple SIEM deployment and toward an evidence-based, ATT&CK-aligned, and continuously optimized threat hunting program in which Splunk correlation rules are engineered not only to detect suspicious events, but to support fast, trustworthy, and strategically meaningful security operations.

LIMITATIONS

This study has been subject to several limitations that should be acknowledged when interpreting the findings. First, the research has adopted a quantitative, cross-sectional design, which has allowed the study to examine relationships among variables at a single point in time but has limited its ability to capture changes in SOC performance over longer operational periods. As a result, while the findings have shown significant associations among MITRE ATT&CK alignment, Splunk correlation rule quality, technique coverage adequacy, precision–noise balance, and threat hunting success, the design has not fully established how these relationships may evolve as detection content matures, analyst expertise increases, or adversary tactics shift. Second, the study has been case-study–based and has focused on a specific SOC context, which has strengthened its practical relevance but has also limited the generalizability of the results to all organizational environments. Different industries, security architectures, levels of SOC maturity, and SIEM deployment models may produce different patterns of performance, especially in environments with fewer resources, lower ATT&CK familiarity, or

alternative detection engineering processes. Third, the data have been based on structured questionnaire responses measured through a Likert five-point scale, which has made the study suitable for statistical analysis but has also meant that the findings have reflected respondent perceptions rather than direct technical telemetry alone. Although the respondents have been relevant cybersecurity professionals with meaningful SOC experience, perception-based responses may still contain subjectivity, recall bias, or differences in personal judgment about alert quality and operational success. Fourth, the study has not incorporated direct system-generated indicators such as mean time to detect, mean time to respond, alert dismissal rates, or actual false-positive ratios from Splunk logs, and this has limited the ability of the research to compare perceived outcomes with purely technical operational records. Fifth, the study has concentrated on a selected set of variables that were conceptually central to the research, but threat hunting effectiveness in real environments may also be influenced by additional factors such as budget constraints, staffing levels, threat intelligence quality, security culture, automation maturity, and organizational governance practices that were not measured directly in the model. Sixth, although the study has linked its findings to Socio-Technical Systems Theory, the empirical design has not separately modeled every human, technical, and environmental factor in full detail, which means that the theoretical application has remained focused on the most relevant operational constructs rather than on a wider organizational systems map. Overall, these limitations have not invalidated the findings, but they have indicated that the conclusions of the study should be understood within the boundaries of its design, context, and measurement approach.

REFERENCES

[1]. Abd Majid, M., & Zainol Ariffin, K. A. (2021). Model for successful development and implementation of Cyber Security Operations Centre (SOC). *PLOS ONE*, *16*(11), e0260157. https://doi.org/10.1371/journal.pone.0260157

[2]. Aditya, D., & Palash Chandra, D. (2022). Material Degradation and Durability Assessment of Pipelines and Sanitation Structures Under Aggressive Environmental Conditions. *American Journal of Interdisciplinary Studies*, *3*(02), 126-164. https://doi.org/10.63125/papn7656

[3]. Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2022). A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers & Security*, *121*, 102959. https://doi.org/10.1016/j.cose.2022.102959

[4]. Ahmed, M. G., Panda, S., Xenakis, C., & Panaousis, E. (2022). *MITRE ATT&CK-driven cyber risk assessment* Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES 2022),

[5]. Akinrolabu, O., Agrafiotis, I., & Erola, A. (2018). *The challenge of detecting sophisticated attacks: Insights from SOC analysts* Proceedings of the 13th International Conference on Availability, Reliability and Security,

[6]. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851-1877. https://doi.org/10.1109/comst.2019.2891891

[7]. Aminanto, M. E., Zhu, L., Ban, T., Isawa, R., Takahashi, T., & Inoue, D. (2019). *Combating threat-alert fatigue with online anomaly detection using isolation forest* Neural information processing,

[8]. Ampel, B. M., Samtani, S., Ullman, S., & Chen, H. (2021). *Linking Common Vulnerabilities and Exposures to the MITRE ATT&CK framework: A self-distillation approach*. https://doi.org/10.48550/arXiv.2108.01696

[9]. Anick, K. M. T. A., & Tasnim, K. (2022). Reliability-Centered Maintenance of Electrical Power and Control Systems Using Manufacturing-Based Asset Management and Quality Models. *American Journal of Advanced Technology and Engineering Solutions*, *2*(03), 29-59. https://doi.org/10.63125/xq6a0793

[10]. Axon, L., AlAhmadi, B. A., Nurse, J. R. C., Goldsmith, M., & Creese, S. (2020). Data presentation in security operations centres: Exploring the potential for sonification to enhance existing practice. *Journal of Cybersecurity*, *6*(1), tyaa004. https://doi.org/10.1093/cybsec/tyaa004

[11]. Barzegar, M., & Shajari, M. (2018). Attack scenario reconstruction using intrusion semantics. *Expert Systems with Applications*, *108*, 119-133. https://doi.org/10.1016/j.eswa.2018.04.030

[12]. Bhatt, S. N., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE Security & Privacy*, *12*(5), 35-41. https://doi.org/10.1109/msp.2014.103

[13]. Bhattarai, B., & Huang, H. H. (2022). *SteinerLog: Prize collecting the audit logs for threat hunting on enterprise network* Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security,

[14]. Bryant, B. D., & Saiedian, H. (2017). A novel kill-chain framework for remote security log analysis with SIEM software. *Computers & Security*, *67*, 198-210. https://doi.org/10.1016/j.cose.2017.03.003

[15]. Bryant, B. D., & Saiedian, H. (2020). Improving SIEM alert metadata aggregation with a novel kill-chain based classification model. *Computers & Security*, *94*, Article 101817. https://doi.org/10.1016/j.cose.2020.101817

[16]. Cheng, Q., Wu, C., & Zhou, S. (2021). Discovering attack scenarios via intrusion alert correlation using graph convolutional networks. *IEEE Communications Letters*, *25*(5), 1564-1567. https://doi.org/10.1109/lcomm.2020.3048995

[17]. Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. E. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

[18]. Elshoush, H. T., & Osman, I. M. (2011). Alert correlation in collaborative intelligent intrusion detection systems—A survey. *Applied Soft Computing*, *11*(7), 4349-4365. https://doi.org/10.1016/j.asoc.2010.12.004

[19]. Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1-2), 18-28. https://doi.org/10.1016/j.cose.2008.08.003

[20]. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk using a cyber-security culture framework. *Sensors*, *21*(9), Article 3267. https://doi.org/10.3390/s21093267

[21]. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), Article 4759. https://doi.org/10.3390/s21144759

[22]. Hisham, M., & Mohammad Robel, M. (2022). Data-Driven Innovation Ecosystems: Accelerating Economic Growth Through Strategic Technology Adoption. *American Journal of Data Science and Analytics*, *3*(12), 01-41. https://doi.org/10.63125/rf3w1z65

[23]. Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., & Khayami, R. (2020). Know abnormal, find evil: Frequent pattern mining for ransomware threat hunting and intelligence. *IEEE Transactions on Emerging Topics in Computing*, *8*(2), 341-351. https://doi.org/10.1109/tetc.2017.2756908

[24]. Iftekhar, A., & Md Tohidul, I. (2024). Quantitative Impact Assessment of Digital Payment Solutions on Small Business Revenue Panel Data Analysis From 1,200 U.S. SMES. *American Journal of Scholarly Research and Innovation*, *3*(02), 217-253. https://doi.org/10.63125/zy98jx29

[25]. Islam, M. D. Z., & Aditya, D. (2023). Measuring the Security Impact of Zero Trust Access Controls: A Mixed-Methods Study of Identity-Based Policies (Cisco ISE + AD) and Incident Reduction. *American Journal of Data Science and Analytics*, *4*(06), 01-42. https://doi.org/10.63125/8ycz7671

[26]. Jang, K., Goyal, A., Jee, K., Wang, Z., Bates, A., & Wang, G. (2022). *RAPID: Real-time alert investigation with context-aware prioritization for efficient threat discovery* Proceedings of the 38th Annual Computer Security Applications Conference,

[27]. Jinnat, A., & Samiha Binte, A. (2024). Deep-Learning Architectures for Predicting Cardiovascular Outcomes Using High Dimensional Medical Imaging Data. *Journal of Sustainable Development and Policy*, *3*(03), 134-166. https://doi.org/10.63125/vrgee960

[28]. Kenaza, T., & Aiash, M. (2016). Toward an efficient ontology-based event correlation in SIEM. *Procedia Computer Science*, *83*, 139-146. https://doi.org/10.1016/j.procs.2016.04.109

[29]. Kenaza, T., Machou, A., & Dekkiche, A. (2018). *Implementing a semantic approach for events correlation in SIEM systems* Computational intelligence and its applications,

[30]. Khan, M. S., Richard, R., Molyneaux, H., Cote-Martel, D., Elango, H. J. K., Livingstone, S., Gaudet, M., & Trask, D. (2021). Cyber threat hunting: A cognitive endpoint behavior analytic system. *International Journal of Cognitive Informatics and Natural Intelligence*, *15*(4), 1-23. https://doi.org/10.4018/IJCINI.20211001.oa9

[31]. Kim, G., & Kang, B. (2022). Threat classification model for security information event management focusing on model efficiency. *Computers & Security*, *120*, Article 102789. https://doi.org/10.1016/j.cose.2022.102789

[32]. Kryukov, R., Zima, V., Fedorchenko, E., Novikova, E., & Kotenko, I. (2022). *Mapping the security events to the MITRE ATT&CK attack patterns to forecast attack propagation (Extended abstract)* Attacks and Defenses for the Internet-of-Things,

[33]. Kuppa, A., Aouad, L., & Le-Khac, N.-A. (2021). *Linking CVE's to MITRE ATT&CK techniques* Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021),

[34]. Landauer, M., Skopik, F., Wurzenberger, M., & Rauber, A. (2022). Dealing with security alert flooding: Using machine learning for domain-independent alert aggregation. *ACM Transactions on Privacy and Security*, *25*(3), Article 18, 11-36. https://doi.org/10.1145/3510581

[35]. Li, T., & Yan, L. (2017). SIEM based on big data analysis. In X. Sun, H. C. Chao, X. You, & E. Bertino (Eds.), *Cloud computing and security* (Vol. Lecture Notes in Computer Science, 10602, pp. 167-175). Springer. https://doi.org/10.1007/978-3-319-68505-2_15

[36]. Li, Z., Chen, Q. A., Yang, R., Chen, Y., & Ruan, W. (2021). Threat detection and investigation with system-level provenance graphs: A survey. *Computers & Security*, *106*, 102282. https://doi.org/10.1016/j.cose.2021.102282

[37]. Li, Z., Li, T., Zhang, R., Wu, D., & Yang, Z. (2022). *A novel network alert classification model based on behavior semantic* Proceedings of the 34th International Conference on Software Engineering and Knowledge Engineering,

[38]. Liu, C., Wang, J., & Chen, X. (2022). Threat intelligence ATT&CK extraction based on the attention transformer hierarchical recurrent neural network. *Applied Soft Computing*, *122*, 108826. https://doi.org/10.1016/j.asoc.2022.108826

[39]. Liu, J., Zhang, R., Liu, W., Zhang, Y., Gu, D., Tong, M., Wang, X., Xue, J., & Wang, H. (2022). Context2Vector: Accelerating security event triage via context representation learning. *Information and Software Technology*, *146*, Article 106856. https://doi.org/10.1016/j.infsof.2022.106856

[40]. Mahfuj Ahmed, R., & Md. Hasan Or, R. (2021). Fraud-Detection Algorithms for Identifying Anomalous Transactions in Retail Banking Networks. *American Journal of Data Science and Analytics*, *2*(12), 01-40. https://doi.org/10.63125/23m31748

[41]. Mahmoud, M., Mannan, M., & Youssef, A. (2022). *APTHunter: Detecting advanced persistent threats in early stages*

[42]. Malatji, M., von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*, *27*(2), 233-272. https://doi.org/10.1108/ics-03-2018-0031

[43]. Manocha, H., Srivastava, A., Verma, C., Gupta, R., & Bansal, B. (2021). *Security assessment rating framework for enterprises using MITRE ATT&CK matrix*. https://doi.org/10.48550/arXiv.2108.06559

[44]. Mashima, D. (2022). MITRE ATT&CK based evaluation on in-network deception technology for modernized electrical substation systems. *Sustainability*, *14*(3), Article 1256. https://doi.org/10.3390/su14031256

[45]. Mavroeidis, V., & Bromander, S. (2017). *Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence* Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC),

[46]. Mavroeidis, V., & Jøsang, A. (2018). *Data-driven threat hunting using Sysmon* Proceedings of the 2nd International Conference on Cryptography, Security and Privacy,

[47]. McEvoy, T. R., & Kowalski, S. J. (2019). Deriving cyber security risks from human and organizational factors: A socio-technical approach. *Complex Systems Informatics and Modeling Quarterly*, *18*, 47-64. https://doi.org/10.7250/csimq.2019-18.03

[48]. Md Abubakar Siddique, A., & Md. Al Amin, K. (2022). Data-Driven Ergonomic Risk Analysis Using Wearable Sensor Networks and Deep Learning for Injury Prevention in Industrial Workplaces. *American Journal of Data Science and Analytics*, *3*(06), 01-39. https://doi.org/10.63125/61w9ba54

[49]. Md, F., & Islam, M. D. Z. (2022). Quantitative Risk Modeling of VPN Misconfigurations and Firewall Rule Drift in Hybrid Cloud Networks. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 182-216. https://doi.org/10.63125/fa4qdz07

[50]. Md, F., & Md. Mehedi, H. (2021). Machine Learning Accuracy in Healthcare Risk Prediction: Algorithms, Datasets, and Effect Sizes: A Meta-Analysis. *American Journal of Data Science and Analytics*, *2*(10), 01-39. https://doi.org/10.63125/3f0mwc90

[51]. Md Khaled, H., & Md. Mosheur, R. (2023). Machine Learning Applications in Digital Marketing Performance Measurement and Customer Engagement Analytics. *Review of Applied Science and Technology*, *2*(03), 27–66. https://doi.org/10.63125/hp9ay446

[52]. Md Mehedi, H., & Md, F. (2022). Advanced Computing–Enabled Secure Financial Information Systems for Real-Time Fraud Detection in U.S. Digital Payments: A Quantitative Analysis. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 97-133. https://doi.org/10.63125/9mv2qd37

[53]. Md Shahab, U., & Aditya, D. (2023). Risk Mitigation and Resilience Modeling for Consumer Distribution Networks During Demand Shocks: A Quantitative Stochastic Optimization and Scenario Analysis Study. *International Journal of Scientific Interdisciplinary Research*, *4*(2), 01–30. https://doi.org/10.63125/jkevvq84

[54]. Md. Hasan Or, R., Tanjina Binte, S., & Rajib, S. (2023). Performance Analytics Frameworks for Digital Marketing and Service Enterprises: An empirical Study. *American Journal of Data Science and Analytics*, *4*(03), 01-35. https://doi.org/10.63125/aq7y1792

[55]. Md. Mainuddin, F., & Palash Chandra, D. (2022). Fabrication-Driven Structural Optimization Techniques for Cost-Efficient Steel Construction Using CNC-Based Design Workflows. *American Journal of Interdisciplinary Studies*, *3*(04), 464-499. https://doi.org/10.63125/n08g1x15

[56]. Md. Mehedi, H., & Khairum Nahar, P. (2023). A Systematic Review of Secure Health Data Information Systems for Pandemic Preparedness and Economic Continuity in the United States. *Review of Applied Science and Technology*, *2*(01), 227–258. https://doi.org/10.63125/77h2m531

[57]. Md. Shahinur, I., & Md. Sultan, M. (2022). Digital-Twin-Based Quantitative Frameworks for Modeling, Monitoring, and Optimization of Electrical Power Infrastructure. *American Journal of Interdisciplinary Studies*, *3*(04), 365-393. https://doi.org/10.63125/dvmj1y93

[58]. Md. Sultan, M., & Anick, K. M. T. A. (2023). High-Performance Computing–Assisted Modeling and Real-Time Analysis of Electrical Power Networks and Industrial Control Systems. *Review of Applied Science and Technology*, *2*(01), 185–226. https://doi.org/10.63125/727j5j39

[59]. Md. Towhidul, I., & Uddin, M. D. S. (2024). Simulation-Based Forecasting and Inventory Control Models For Consumer Goods Networks: A Quantitative Study Using Monte Carlo Simulation and Time-Series Methods. *Review of Applied Science and Technology*, *3*(04), 165–197. https://doi.org/10.63125/a3047d06

[60]. Mohammad Mushfequr, R., & Aditya, D. (2024). Quantitative Assessment of Data Protection Practices In U.S. Revenue Cycle Management. *American Journal of Advanced Technology and Engineering Solutions*, *4*(04), 107-153. https://doi.org/10.63125/fc9hfy54

[61]. Morin, B., Mé, L., Debar, H., & Ducassé, M. (2009). A logic-based model to support alert correlation in intrusion detection. *Information Fusion*, *10*(4), 285-299. https://doi.org/10.1016/j.inffus.2009.01.005

[62]. Mostafa, K. (2023). An Empirical Evaluation of Machine Learning Techniques for Financial Fraud Detection in Transaction-Level Data. *American Journal of Interdisciplinary Studies*, *4*(04), 210-249. https://doi.org/10.63125/60amyk26

[63]. Mostafa, K., & Md Tohidul, I. (2022). A Quantitative Financial Impact Assessment of Digital Trade Platforms on Export Performance, Capital Efficiency, and Market Competitiveness. *Journal of Sustainable Development and Policy*, *1*(03), 01-26. https://doi.org/10.63125/pt5v9517

[64]. Neto, A. J. H., & Santos, A. F. P. d. (2020). *Cyber threat hunting through automated hypothesis and multi-criteria decision making* 2020 IEEE International Conference on Big Data (Big Data),

[65]. Niu, W., Yu, Z., Li, Z., Li, B., Zhang, R., & Zhang, X. (2022). *LogTracer: Efficient anomaly tracing combining system log detection and provenance graph* 2022 IEEE Global Communications Conference (GLOBECOM),

[66]. Rahman, M. R., & Williams, L. (2022). *An investigation of security controls and MITRE ATT&CK techniques*. https://doi.org/10.48550/arXiv.2211.06500

[67]. Ratul, D., & Aditya, D. (2023). AI-Driven Change Detection Using SAR, LIDAR, And Sentinel-2 Data for Landslide Monitoring and Disaster Early Warning Systems. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 153–188. https://doi.org/10.63125/4y740y95

[68]. Ren, H., Stakhanova, N., & Ghorbani, A. A. (2010). An online adaptive approach to alert correlation. In C. Kreibich & M. Jahnke (Eds.), *Detection of intrusions and malware, and vulnerability assessment* (Vol. Lecture Notes in Computer Science, 6201, pp. 153-172). Springer. https://doi.org/10.1007/978-3-642-14215-4_9

[69]. Roschke, S., Cheng, F., & Meinel, C. (2011). A new alert correlation algorithm based on attack graph. In Á. Herrero & E. Corchado (Eds.), *Computational intelligence in security for information systems* (Vol. Lecture Notes in Computer Science, 6694, pp. 58-67). Springer. https://doi.org/10.1007/978-3-642-21323-6_8

[70]. Rukaiya Khatun, M., & Md. Morshedul, I. (2022). Anticipatory Intelligence Systems: How Data Analytics Reshape Organizational Preparedness and Action Timing. *American Journal of Interdisciplinary Studies*, *3*(04), 394-428. https://doi.org/10.63125/rhwpgf86

[71]. Saad, S., & Traore, I. (2013). Extracting attack scenarios using intrusion semantics. In J. Garcia-Alfaro, F. Cuppens, N. Cuppens-Boulahia, A. Miri, & N. Tawbi (Eds.), *Foundations and practice of security* (Vol. Lecture Notes in Computer Science, 7743, pp. 278-292). Springer. https://doi.org/10.1007/978-3-642-37119-6_18

[72]. Sakib, A. I. M. (2024). Innovative Food Waste Recycling Methods For Agricultural Sustainability: A Systematic Review. *Academic Journal On Business administration, Innovation & Sustainability*, *4*(3), 104-118. https://doi.org/10.69593/ajbais.v4i3.107

[73]. Sapegin, A., Jaeger, D., Cheng, F., & Meinel, C. (2017). Towards a system for complex analysis of security events in large-scale networks. *Computers & Security*, *67*, 16-34. https://doi.org/10.1016/j.cose.2017.02.009

[74]. Sazzadul, I., & Rebeka, S. (2024). VaR and CVaR-Based Stress Testing Using Deep Learning for Liquidity Risk Forecasting and Banking Stability Assessment. *Review of Applied Science and Technology*, *3*(03), 01–30. https://doi.org/10.63125/291phs66

[75]. Schlienger, T., & Teufel, S. (2005). *Tool supported management of information security culture* Security and privacy in the age of ubiquitous computing,

[76]. Spathoulas, G. P., & Katsikas, S. K. (2010). Reducing false positives in intrusion detection systems. *Computers & Security*, *29*(1), 35-44. https://doi.org/10.1016/j.cose.2009.07.008

[77]. Tang, B., Wang, J., Yu, Z., Chen, B., Ge, W., Yu, J., & Lu, T. (2022). Advanced persistent threat intelligent profiling technique: A survey. *Computers & Electrical Engineering*, *103*, Article 108261. https://doi.org/10.1016/j.compeleceng.2022.108261

[78]. Tasnim, K., & Anick, K. M. T. A. (2024). PLC–SCADA–Integrated Electrical Automation Frameworks for Process Optimization in Water and Wastewater Treatment Facilities. *Review of Applied Science and Technology*, *3*(01), 221–262. https://doi.org/10.63125/y1145g11

[79]. Tasnim, K., & Zaheda, K. (2023). A Smart Contract Framework for Automated Settlement and Compliance in Renewable Energy and Distributed Energy Resources. *American Journal of Advanced Technology and Engineering Solutions*, *3*(01), 31-69. https://doi.org/10.63125/fvdjpn66

[80]. Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212-233. https://doi.org/10.1016/j.cose.2017.09.001

[81]. Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK matrix. *Software and Systems Modeling*, *21*(1), 157-177. https://doi.org/10.1007/s10270-021-00898-7

[82]. Yen, T.-F., Oprea, A., Onarlioglu, K., Leetham, T., Robertson, W., Juels, A., & Kirda, E. (2013). *Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks* Proceedings of the 29th Annual Computer Security Applications Conference,

[83]. Zaheda, K., & Md Hamidur, R. (2024). GPU-Accelerated Physics-Informed Digital Twins for Real-Time State Estimation and Fault Localization in Distribution Grids. *American Journal of Scholarly Research and Innovation*, *3*(02), 179-216. https://doi.org/10.63125/msrpfb04

[84]. Zaheda, K., & Md. Tahmid Farabe, S. (2023). Robotics and Computer Vision for Automated Inspection of Substation and Treatment-Facility Electrical Infrastructure. *Review of Applied Science and Technology*, *2*(04), 194-227. https://doi.org/10.63125/tfh15j12

[85]. Zakia, A., & Khairum Nahar, P. (2022). Advanced Computing Frameworks for Real-Time SAP S/4HANA Retail Business Intelligence: Optimizing Data Processing, Latency, and System Reliability. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 217-254. https://doi.org/10.63125/xk5j7g56

[86]. Zali, Z., Hashemi, M. R., & Saidi, H. (2013). Real-time intrusion detection alert correlation and attack scenario extraction based on the prerequisite consequence approach. *ISeCure*, *4*(2), 125-136. https://doi.org/10.22042/isecure.2013.4.2.4

[87]. Zimmermann, V., & Renaud, K. (2019). Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

[88]. Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: A survey. *Journal of Big Data*, *2*, Article 3. https://doi.org/10.1186/s40537-015-0013-4