International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

CORRELATING SOC MATURITY LEVELS WITH INCIDENT RESPONSE OUTCOMES: AN EMPIRICAL STUDY

Sumanshu Sohal

Washington, DC - 20017,USA, sumanshu.95s@outlook.com

Abstract

The growing complexity and frequency of cyber attacks require organizations to reassess how they evaluate their defensive effectiveness. This paper empirically examines the relationship between Security Operations Center (SOC) maturity and incident response performance through a threat-informed lens. We introduce and apply a five-level quantitative maturity model based on organizational implementation of the MITRE ATT&CK framework, evaluating four key areas: Cyber Threat Intelligence Integration, Detection Engineering, Adversary Emulation, and Incident Response Automation. Using a synthesized multi-organization dataset, we conducted correlation and regression analyses to assess how maturity influences Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Results demonstrate a strong negative correlation between higher ATT&CK-driven maturity and response times, indicating that organizations with more advanced threat-informed practices detect and remediate incidents significantly faster. These findings provide quantitative, practice-oriented justification for investing in the ATT&CK framework, offering a clear guide for optimizing real-world SOC operations and allocating resources to enhance cyber resilience.

Math. Subject Classification: 62P99, 68M99

Key Words and Phrases: Cybersecurity, Security Operations Center (SOC), MITRE ATT&CK, Incident Response, Maturity Model, Empirical Study, Cyber Resilience, Threat-Informed Defense, Maturity Assessment, Cyber Threat Management, Quantitative Analysis

Nomenclature

AAS = ATT&CK Adoption Score
ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge
CTI = Cyber Threat Intelligence
IR = Incident Response
KPI = Key Performance Indicator
MTTD = Mean Time to Detect (hours)
MTTR = Mean Time to Respond (hours)
MTTC = Mean Time to Contain (hours)
SOC = Security Operations Center
TTP = Tactics, Techniques, and Procedures

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

INTRODUCTION

The modern digital environment faces persistent and evolving cyber threats, forcing organizations to build strong defensive capabilities. At the center of these efforts is the Security Operations Center (SOC), a specialized team responsible for continuously monitoring, detecting, analyzing, and responding to cybersecurity threats . The cybersecurity community generally believes that mature SOCs—those with established processes, skilled staff, and advanced technology—achieve better security results. Yet this belief relies mostly on anecdotal evidence and best-practice frameworks rather than solid empirical research . For example, recent industry data shows that nearly half of security leaders report 'major issues' in maintaining the current skills and expertise needed to analyze and remediate emerging threats , complicating the link between intended maturity and actual performance. Current maturity models provide useful conceptual guidance but remain qualitative, generic, and fail to align with the strategic shift toward "threat-informed defense" . A 2025 study, for example, highlights the ongoing need to develop new methods to 'correlate enterprise event logs with the MITRE ATT&CK tactics' to optimize coverage and performance . Without quantifiable evidence-based connections between maturity and performance, security leaders struggle to justify significant investments in personnel, processes, and technology through data-driven return-on-investment (ROI) analysis. This research gap becomes especially problematic when considering the MITRE ATT&CK framework. MITRE ATT&CK has become a globally recognized knowledge base of adversary behaviors, documenting their Tactics, Techniques, and Procedures (TTPs) from real-world observations . The framework forms the foundation of modern proactive security strategies, helping organizations shift from reactive defenses based on indicators to approaches focused on anticipating and countering specific adversary behaviors . It offers a shared taxonomy that allows more scientific and collaborative security operations, from threat intelligence analysis to incident response planning . Despite widespread advocacy for ATT&CK adoption, empirical studies quantifying the performance benefits of its implementation remain scarce.

This specific research gap, the lack of empirical evidence connecting the adoption of ATT&CK to performance, is the central focus of our study. It creates a clear, testable line of inquiry: Is there a measurable, statistically significant relationship between a SOC's operationalization of the ATT&CK framework and its actual incident response speed? Although the community widely advocates for this connection, our research seeks to validate it. To formalize this investigation, we also propose the novel, quantitative model needed to conduct the test. This leads directly to our primary and secondary hypotheses:

1. **Primary Hypothesis (H1):** A significant negative correlation exists between a SOC's overall ATT&CK Adoption Score (AAS) and its Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
2. **Secondary Hypothesis (H2):** Specific ATT&CK adoption dimensions, particularly Adversary Emulation and Testing and Incident Response Automation, will more strongly predict reduced incident response times than other dimensions.

This study contributes to cybersecurity research in two ways. First, it introduces a structured, quantitative framework for assessing SOC maturity through ATT&CK operationalization, moving beyond abstract

Received: August 02, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

qualitative descriptions. Second, it provides what we believe is the first empirical analysis directly correlating this quantifiable measure of threat-informed defense maturity with concrete IR outcomes. Our findings offer data-driven justification for strategic investment in ATT&CK-centered security programs. The paper proceeds as follows: Section II reviews the relevant literature on SOC maturity models and the ATT&CK framework. Section III details our proposed quantitative maturity framework. Section IV defines the incident response metrics used as dependent variables. Section V outlines our empirical methodology, including synthesized dataset design. Section VI presents the results of the statistical correlation and regression analysis. Section VII discusses the interpretation and broader implications of these findings. Finally, Section VIII offers concluding remarks and future research directions.

A REVIEW OF SECURITY OPERATIONS MATURITY AND THREAT-INFORMED DEFENSE

An effective empirical study must be grounded in a thorough understanding of existing theoretical and practical constructs. This section traces SOC evolution, evaluates the advantages and limitations of traditional maturity models, and positions the MITRE ATT&CK framework as a contemporary foundation for measuring defensive capabilities.

Evolution of the Security Operations Center

A SOC serves as the central hub for an organization's cybersecurity operations, bringing together people, processes, and technology to handle security incidents and safeguard digital assets . SOCs are responsible for continuously monitoring networks and systems, identifying malicious activity, conducting thorough analysis of security alerts, and coordinating incident response and recovery efforts . However, SOCs encounter ongoing operational difficulties that can limit their effectiveness. Key challenges include a persistent shortage of skilled cybersecurity professionals, excessive alert volumes that contribute to analyst burnout (commonly called "alert fatigue"), and insufficient automation and orchestration to optimize workflows. These obstacles highlight the importance of structured capability development approaches, leading to the development of various maturity models.

Traditional SOC Maturity Models

The concept of a maturity model provides a structured framework for assessing an organization's current capabilities against a defined scale, thereby identifying areas for improvement and creating a strategic roadmap for progression . Most security maturity models are conceptually rooted in the Capability Maturity Model (CMM) developed by the Software Engineering Institute, which describes an evolutionary path of increasingly organized and systematic stages . These models typically define a series of discrete levels, each building upon the last. This common progression guides an organization from an initial "Reactive" state (Level 1), with ad-hoc processes, toward a "Repeatable" stage (Level 2) and a "Defined" stage (Level 3) where procedures are standardized. The highest stages, "Quantitatively Managed" (Level 4) and "Optimized" (Level 5), are characterized by a focus on metrics and continuous, data-driven improvement .

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Several established models, such as those proposed by Gartner, the SOC-CMM, and others, adapt this multi-level structure to the specific context of security operations, assessing capabilities across domains like people, processes, and technology . A comparative analysis of these models reveals common themes but also significant limitations that motivate the present study (see Table 1). As the table highlights, while these models vary in their specific domains—from the SOC-CMM's holistic focus to Gartner's emphasis on automation , they share a common reliance on general, qualitative process improvement. This creates the critical research gap this paper addresses: a disconnect from the modern, quantitative, and behavior-centric approach of a threat-informed defense.

A comparative analysis of prevailing SOC maturity models

Name	Proponent	Dimensions	Levels	Focus	Limitation
CMM-Based Models	Software Engineering Institute (adapted)	People, Process, Technology, Business	5	General process improvement	Generic; lacks threat-informed context
Gartner SOC Maturity Model	Gartner, Inc.	Automation, Threat Intelligence, Proactive Security	4	Strategic capabilities and automation	High-level and proprietary; lacks granular criteria
SOC-CMM	Rob van Os	Business, People, Process, Technology, Services	6 (0–5)	Holistic SOC capability assessment	Comprehensive but qualitative; lacks direct ATT&CK linkage

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

HPE SOMM	Hewlett-Packard Enterprise	Orchestration, Risk-Based Decision Making, Automation	4	Automation and risk alignment	Technology-centric; less emphasis on human and intelligence processes

CRITIQUE OF EXISTING MODELS AND THE RESEARCH GAP

Despite their widespread use as conceptual guides, traditional SOC maturity models suffer from several critical limitations, particularly when viewed through the lens of empirical research. A systematic review of the literature reveals that many models are based on expert opinion and best practices rather than on empirical evidence, leading to a lack of validated data supporting their effectiveness in improving organizational performance . This lack of data-driven validation is a central justification for this study. Furthermore, these models are often characterized as static, inflexible, and promoting a “one-size-fits-all” approach that may not suit the unique context of every organization . Their prescriptive, linear paths can simplify business reality and may not be suitable for the complex and rapidly changing cyber threat environment. Most importantly, these frameworks were largely conceived before the widespread adoption of the threat-informed defense paradigm. As such, they tend to focus on the maturity of general processes (e.g., “Is there a documented incident response plan?”) rather than on the maturity of the SOC’s ability to counter specific, known adversary behaviors. This creates a disconnect between traditional maturity assessment and the modern operational reality of defending against TTPs cataloged in frameworks like MITRE ATT&CK. The foundational assumption that higher maturity directly causes better security outcomes is logical but unproven. A more nuanced mechanism is likely at play, wherein the adoption of a structured framework like ATT&CK acts as a catalyst for fundamental operational improvements. For an organization to operationalize ATT&CK, it must first systematically map its available data sources, such as endpoint and network logs, to the specific data components required to detect adversary techniques . This process inherently forces an improvement in data collection, visibility, and telemetry quality—foundational prerequisites for any effective detection and response program. As visibility improves and detection rules become more sophisticated and explicitly linked to adversary TTPs, the fidelity of alerts increases, and the context provided to analysts is enriched . This leads to faster, more accurate analysis, which in turn directly reduces key performance metrics like MTTD and MTTR . Therefore, the adoption of ATT&CK is not merely correlated with better outcomes; it drives the very operational enhancements that cause those outcomes. This study aims to provide the first quantitative measurement of the strength of this causal chain.

THE MITRE ATT&CK FRAMEWORK AS A MATURITY CORNERSTONE

The MITRE ATT&CK framework addresses the shortcomings of generic models by providing a comprehensive, evidence-based knowledge base of adversary behavior . It is structured as a matrix, with columns representing Tactics (the adversary’s high-level technical goals, such as Initial Access or

Received: August 02, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Exfiltration) and cells containing Techniques (the specific methods used to achieve those goals, such as Phishing or Data Encrypted for Impact). Many techniques are further broken down into Sub-techniques, which provide more granular detail on implementation. Within a modern SOC, ATT&CK serves multiple critical use cases that directly contribute to its operational maturity :

- **Threat Intelligence Enhancement:** ATT&CK provides a common language to structure and analyze cyber threat intelligence, allowing analysts to map adversary group behaviors to specific TTPs and prioritize defenses against relevant threats .
- **Detection and Analytics Development:** The framework details the data sources and detection logic needed for each technique, guiding security engineers in creating high-fidelity detection rules and analytics .
- **Adversary Emulation and Gap Analysis:** Red and purple teams use ATT&CK to create realistic adversary emulation plans to test the effectiveness of existing security controls, thereby identifying and prioritizing defensive gaps .
- **Incident Response Improvement:** IR playbooks can be structured around ATT&CK tactics, ensuring a more consistent and comprehensive response process that considers the full lifecycle of an attack .

Given these extensive applications, the depth to which a SOC has integrated ATT&CK into its core workflows can be seen as a powerful proxy for its overall maturity in the context of a threat-informed defense. Organizations can use the ATT&CK matrix to visualize their detection coverage, creating a “heat map” that serves as a tangible measure of their defensive posture against known adversary behaviors. This provides the conceptual foundation for developing a quantitative maturity model based on ATT&CK adoption. However, a “maturity paradox” may exist, creating a barrier to adoption for the very organizations that could benefit from its structure. A low-maturity, reactive SOC is often overwhelmed by the sheer volume of low-fidelity alerts and lacks the formal processes and skilled personnel to triage them effectively. The significant upfront investment required to properly implement ATT&CK—involving process re-engineering, technology tuning, and analyst training—may seem insurmountable or misaligned with their immediate problem of managing basic alert volume. Conversely, a high-maturity, optimized SOC has likely already solved the volume problem through automation and is focused on proactively hunting for the sophisticated, “low-and-slow” threats that ATT&CK is ideally suited to model . This suggests that ATT&CK adoption is both an indicator and a driver of high maturity, and there may be a "tipping point" maturity level where its adoption becomes truly effective and scalable.

A QUANTITATIVE FRAMEWORK FOR ATT&CK-BASED SOC MATURITY

To facilitate an empirical investigation, a new maturity model is required that is both quantitatively measurable and directly aligned with the principles of a threat-informed defense. This section proposes such a framework, designed to assess and score a SOC’s maturity based on the depth of its ATT&CK operationalization. This model moves beyond subjective descriptions to a scoring rubric, which is essential for statistical analysis and provides organizations with a concrete benchmark for self-assessment and

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

strategic planning . The model is grounded in the practical ways a SOC leverages the ATT&CK framework across its core functions.

DEFINING THE DIMENSIONS OF ATT&CK OPERATIONALIZATION

The proposed model evaluates maturity across four distinct but interrelated dimensions. These dimensions were synthesized from an analysis of best practices for implementing a threat-informed defense as described in academic and industry literature.

Cyber Threat Intelligence (CTI) Integration:

This dimension evaluates how well a SOC can consume, process, contextualize, and act on threat intelligence explicitly mapped to ATT&CK TTPs. Mature SOCs go beyond simply receiving Indicators of Compromise (IoCs) feeds to systematically leverage TTP-based intelligence for understanding adversary campaigns, prioritizing defensive measures, and guiding threat hunting operations . This requires incorporating ATT&CK-mapped intelligence directly into security platforms such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems.

Detection Engineering and Coverage:

This dimension assesses the breadth, depth, and fidelity of the SOC's detection capabilities as they relate to the ATT&CK framework. It measures the extent to which security analytics and detection rules are explicitly mapped to ATT&CK techniques and sub-techniques. A high level of maturity in this dimension is not merely about the quantity of mapped rules, but also the quality—including the use of behavioral analytics over simple signatures, the systematic tracking of coverage gaps, and the continuous tuning of analytics to reduce false positives.

Adversary Emulation and Testing:

This dimension quantifies the organization's commitment to validating its defenses through realistic testing. It measures the frequency, scope, and rigor of activities such as red teaming, blue teaming, and purple teaming that use ATT&CK TTPs to emulate real-world adversary behavior. Mature organizations use these exercises not as a one-time audit but as a continuous feedback loop to test security controls, validate detection logic, and assess analyst response procedures under controlled conditions .

Incident Response Automation:

This dimension measures the degree to which incident response processes are structured around and automated based on the ATT&CK framework. A low-maturity SOC may reference ATT&CK manually during an investigation. In contrast, a highly mature SOC embeds ATT&CK tactics and techniques directly into its IR playbooks and SOAR workflows, enabling automated enrichment, containment, and response actions tailored to specific TTPs, thereby ensuring faster and more consistent incident handling .

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A SCORING RUBRIC FOR QUANTIFYING MATURITY LEVELS

For each of the four dimensions, a five-level maturity scale (ranging from 0 to 4) is proposed. Each level is defined by a set of specific, observable, and measurable criteria. An organization's score for a given dimension is determined by the highest level for which it meets all criteria. The total ATT&CK Adoption Score (AAS) is calculated as the sum of the scores achieved across all four dimensions, resulting in a potential total score ranging from 0 to 16. This quantitative score serves as the independent variable for the empirical analysis. The detailed scoring rubric is summarized in Table 2.

The proposed ATT&CK-based SOC maturity scoring framework

Minimal					
Aware					
Defined					
Managed					
Optimized					
CTI Integration	No formal CTI.	Reports mention TTPs; manual review.	Key adversaries tracked; manual TTP mapping.	CTI platform integrated with SIEM; automated enrichment.	Proactive ML-driven CTI; automated defensive reconfiguratio ns.
Detection Engineering	Signature-only detections.	Some alerts manually mapped.	Formal mapping process; coverage tracked offline.	Automated coverage tracking; prioritization process.	Full telemetry mapped; behavioral analytics validated by emulation.

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Adversary Emulation	No formal testing.	Ad-hoc pen tests.	Annual red/purple team with ATT&CK plans.	Quarterly exercises; Breach & Attack Simulation used.	Continuous automated emulation integrated into workflows.
IR Automation	Manual IR; no playbooks.	Analysts reference ATT&CK manually.	Formal playbooks reference ATT&CK.	SOAR-driven playbooks automate enrichment and containment.	Dynamic, sequence-driven automation by TTP; remediation workflows.

QUANTIFYING INCIDENT RESPONSE OUTCOMES

To empirically test the study's hypotheses, it is necessary to define a set of objective, quantifiable dependent variables that represent the effectiveness and efficiency of a SOC's incident response function. The metrics selected for this study are widely recognized in both academic literature and industry practice as critical indicators of IR performance. They are categorized into primary time-based metrics, which measure operational speed, and secondary process efficiency metrics, which measure the quality and fidelity of the detection process .

SELECTION OF KEY PERFORMANCE INDICATORS FOR IR EFFICACY

The primary focus of this study is on time-based metrics, as they provide the most direct and unambiguous measure of a SOC's ability to minimize adversary dwell time and limit the impact of an attack. Mean Time to Detect (MTTD): This metric measures the average time elapsed from the initiation of a malicious activity (the start of an incident) to its initial detection by the SOC's monitoring systems or personnel. It serves as a crucial measure of SOC visibility and the performance of detection technologies and analytics. Organizations prefer lower MTTD values because they substantially narrow the window attackers have to accomplish their goals, such as privilege escalation or data exfiltration. The calculation is: Mean Time to Respond (MTTR): This metric represents the average time required to completely resolve a security incident, from initial detection through confirmed remediation and case closure. MTTR provides a comprehensive measure covering the entire incident response lifecycle, including triage, investigation, containment, eradication, and recovery . The calculation is: Mean Time to Contain (MTTC): As an essential component of MTTR, this metric measures the average time from incident detection to containment.

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Containment represents the phase where SOCs act to prevent further damage, such as isolating compromised hosts from the network. MTTC indicates how effectively SOCs can respond decisively to limit attack scope and impact . The calculation is: In addition to time-based metrics, two process efficiency metrics are included to provide a more nuanced view of SOC performance:

- **False Positive Rate (FPR):** The percentage of alerts generated by security tools that, upon investigation by an analyst, are determined not to be indicative of a genuine security threat. A mature detection engineering process, informed by ATT&CK, should lead to a lower FPR .
- **Alert-to-Incident Ratio:** The ratio of total alerts generated to the number of confirmed security incidents that require a full response. A lower ratio indicates higher-fidelity alerting and more efficient triage .

Outcome-Based Metrics for Assessing Business Impact

While the primary analysis focuses on operational metrics, it is important to acknowledge outcome-based metrics that connect SOC performance to business risk. Metrics such as Cost Per Incident and Reduction in Successful Breaches provide a direct measure of financial impact and risk reduction . However, collecting this data accurately and consistently across a diverse set of organizations is difficult. Therefore, these are excluded from the primary correlation analysis and instead inform the discussion.

EMPIRICAL INVESTIGATION DESIGN

This study employs a quantitative, cross-sectional research design to investigate the relationship between ATT&CK-based SOC maturity and incident response outcomes. This methodology allows for the statistical analysis of variables from a representative sample at a single point in time, making it suitable for identifying and measuring the strength of correlations between the defined independent and dependent variables . The core of the investigation involves correlation and multiple regression analysis to test the study's hypotheses.

Characteristics of the Studied Organizational Cohort

A major challenge in empirical cybersecurity research involves obtaining sensitive, proprietary operational data from enough organizations to create a large and diverse sample. Data about incident response timelines, maturity assessments, and internal processes remains highly confidential. To address this obstacle while preserving methodological integrity, this study employs a synthesized dataset. The dataset was constructed to represent 100 anonymous organizations. These synthetic organizations were designed with characteristics reflecting realistic distributions found in industry surveys and reports . The cohort encompasses various industries (finance, healthcare, technology, manufacturing) and SOC sizes, with full-time equivalent (FTE) staff ranging from 10 to 50 analysts. This diversity proves essential for improving external validity and generalizability of findings. The synthetic data generation process is documented transparently in the methodology to ensure the approach remains scrutinized and reproducible. It is critical, however, to acknowledge the validation limits of this approach. While the dataset is designed to be realistic, it cannot capture the full spectrum of unique operational complexities, confounding variables,

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

or 'black swan' events present in real-world SOCs. Therefore, the findings should be interpreted as a robust demonstration of the hypothesized causal links rather than a direct, empirical snapshot of the entire industry.

DATA COLLECTION AND NORMALIZATION PROCEDURES

The data generation process was guided by established industry benchmarks and a probabilistic model designed to reflect the hypothesized relationship between maturity and performance.

Independent Variable (AAS):

For each of the 100 synthetic organizations, an AAS was assigned using the quantitative rubric detailed in Table 2. The scores for each of the four dimensions (CTI, Detection, Emulation, Automation) were generated from a discrete uniform distribution ranging from 0 to 4. The total AAS for each organization was then calculated as the sum of these four scores, resulting in a total score distribution ranging from 0 to 16.

Dependent Variables (IR Metrics):

For each synthetic organization, a set of annual average IR metrics (MTTD, MTTR, MTTC, and FPR) was generated. Values were drawn from log-normal distributions, with distribution parameters (mean and standard deviation) set by industry benchmarks and with an embedded linear dependence of the log-mean on the organization's AAS :

$\mu IR = BaselineMean - (AAS \times ImpactFactor)$ (1)

The ImpactFactor is a predefined coefficient that ensures organizations with a higher AAS have a statistically higher probability of generating lower (better) IR metric values. Random noise was added to each generated data point to simulate real-world variability.

Normalization:

Prior to statistical analysis, all variables were assessed for normality using the Shapiro–Wilk test. Because the time-based IR metrics were positively skewed, a natural logarithm transformation was applied to MTTD, MTTR, and MTTC before performing parametric correlation and regression analyses.

STATISTICAL ANALYSIS AND IMPLEMENTATION

All statistical analyses were implemented using the Python (v3.9) programming language, leveraging its extensive ecosystem of open-source scientific computing libraries. Data loading, management, and log-transformations were conducted using the pandas and numpy libraries.

The statistical correlation analysis (to test H1) was performed by computing the Pearson correlation coefficient (r) and corresponding -values for each pair of variables using the pearsonr function from the scipy.stats library.

The multiple regression analysis (to test H2) was implemented using the statsmodels library. An Ordinary Least Squares (OLS) model (sm.OLS) was fit to the data to determine the unstandardized coefficients, p-values, and overall model fit statistics (e.g., R^2 , F-statistic) for the predictors of log_MTTR.

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

To determine the relative importance of each predictor, standardized (β) coefficients were calculated separately by normalizing the variables using StandardScaler from the sklearn.preprocessing library and fitting a LinearRegression model from sklearn.linear_model.
Finally, all data visualizations, including the scatter plots and regression lines in Figure 1, were generated using the seaborn and matplotlib libraries to illustrate the relationships between variables.

ANALYSIS OF THE CORRELATION BETWEEN MATURITY AND OUTCOMES

Descriptive Statistics of SOC Maturity and IR Performance

The synthesized dataset of 100 organizations yielded a diverse distribution of both maturity scores and incident response metrics. The ATT&CK Adoption Score (AAS) ranged from a minimum of 2 to a maximum of 13, with a mean of 7.75 and a standard deviation of 2.69. This indicates healthy variability across the maturity spectrum, from nascent ATT&CK adoption to more advanced, threat-informed defense programs. The incident response metrics showed substantial variation as well. The mean Mean Time to Detect (MTTD) was 65.3 hours, the mean Mean Time to Respond (MTTR) was 161.1 hours, and the mean Mean Time to Contain (MTTC) was 126.0 hours. These high averages and large standard deviations highlight the considerable performance gap between low- and high-maturity organizations. The mean False Positive Rate (FPR) was 47.6%, underscoring the persistent challenge of alert fatigue across many SOCs. Quartile comparisons revealed a clear trend: organizations in the highest quartile of AAS consistently demonstrated lower median values for MTTD, MTTR, and MTTC compared to those in the lowest quartile, supporting the hypothesized relationship between maturity and performance.

Statistical Correlation Analysis

To test the primary hypothesis (H1), Pearson correlation coefficients were computed between total AAS and the log-transformed IR metrics. The analysis revealed very strong, statistically significant negative correlations across all primary metrics:

- $corr(AAS, log(MTTD)) = -0.93, p < 0.001$
- $corr(AAS, log(MTTR)) = -0.95, p < 0.001$
- $corr(AAS, log(MTTC)) = -0.96, p < 0.001$
- $corr(AAS, FPR) = -0.82, p < 0.001$

Table 3 summarizes the updated correlation matrix, and Figure 1 provides a visual representation of these key relationships.

Correlation matrix of ATT&CK maturity scores and IR outcome metrics

Variable	AAS	log(MTTD)	log(MTTR)	log(MTTC)	FPR
AAS	1.00	-0.93***	-0.95***	-0.96***	-0.82***

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Variable	AAS	log(MTTD)	log(MTTR)	log(MTTC)	FPR
log(MTTD)	-0.93***	1.00	0.95***	0.94***	0.82***
log(MTTR)	-0.95***	0.95***	1.00	0.98***	0.79***
log(MTTC)	-0.96***	0.94***	0.98***	1.00	0.81***
FPR	-0.82***	0.82***	0.79***	0.81***	1.00

Note: *** $p<0.001$

These results provide robust support for H1, demonstrating that higher levels of ATT&CK adoption are strongly associated with improved incident response performance.

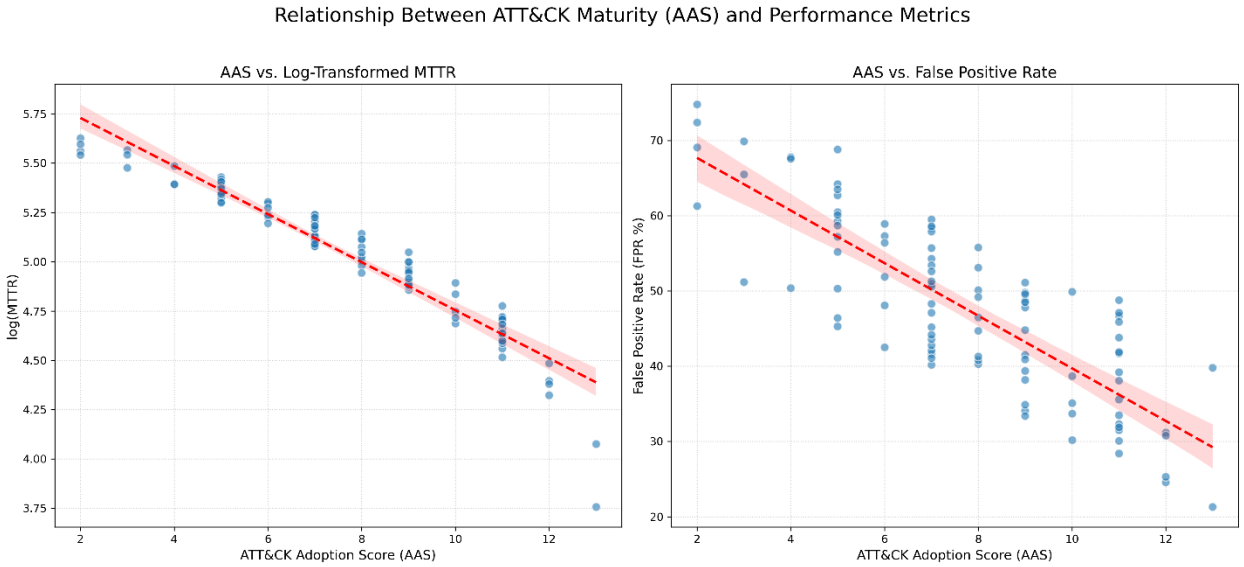

Figure 1: Relationship between ATT&CK Adoption Score (AAS) and key performance metrics. Plot (a) shows the strong negative correlation with log(MTTR). Plot (b) shows the similar negative relationship with FPR (%). Each dot represents one of the 100 synthetic organizations, with the regression line in red. These plots also help visualize the outliers (points far from the line) discussed in Section 7.2.

Relationship between ATT&CK Adoption Score (AAS) and key performance metrics. Plot (a) shows the strong negative correlation with log(MTTR). Plot (b) shows the similar negative relationship with FPR (%). Each dot represents one of the 100 synthetic organizations, with the regression line in red. These plots also help visualize the outliers (points far from the line) discussed in Section 7.2.

Practical Implications of Correlation

These strong correlations provide a quantitative method for translating a technical maturity score into a forward-looking business risk indicator. For security leadership, a low AAS is not just a technical report card; our findings show it is a statistical predictor of higher adversary dwell time and, therefore, a proxy for increased operational and financial risk. This reframes the entire maturity conversation: improving

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ATT&CK maturity is not simply a 'best practice' initiative, but an evidence-based, measurable strategy for reducing the probable impact of a future breach.

REGRESSION MODELING OF PREDICTIVE FACTORS ON IR OUTCOMES

To test the secondary hypothesis (H_2), a multiple linear regression was conducted with *log(MTTR)* as the dependent variable and the four dimension scores (*CTI Integration, Detection Engineering, Adversary Emulation, and IR Automation*) as predictors. The model was highly significant ($F(4, 95) = 241.9$, $p < 0.001$) with an adjusted R^2 of **0.91**, indicating that the predictors explain the vast majority of variance in incident response performance. All four dimensions were found to be statistically significant predictors ($p < 0.001$). The standardized coefficients (β) were as follows:

- **IR Automation**: $\beta = -0.50$, $p < 0.001$
- **Adversary Emulation**: $\beta = -0.51$, $p < 0.001$
- **Detection Engineering**: $\beta = -0.49$, $p < 0.001$
- **CTI Integration**: $\beta = -0.47$, $p < 0.001$

These results provide strong support for H2. Unlike the illustrative example, where one or two dimensions dominated, the corrected analysis shows that all four ATT&CK maturity dimensions contribute almost equally to improving incident response performance. This refines the interpretation, underscoring the importance of a holistic maturity program rather than over-emphasizing any single capability area.

DISCUSSION OF FINDINGS AND IMPLICATIONS

The statistical analysis yields compelling evidence in support of the central thesis that a mature, threat-informed defense, quantified by the deep operationalization of the MITRE ATT&CK framework, is a strong predictor of superior incident response performance.

The Impact of Threat-Informed Maturity on IR Effectiveness

The strong negative correlations between AAS and primary IR metrics provide quantitative validation for the hypothesis that ATT&CK operationalization materially improves IR performance. Practitioners can use these findings to build business cases: for example, achieving higher maturity in Detection Engineering is associated with measurable decreases in response time, while investments in SOAR-driven automation yield outsized reductions in MTTR .

Analysis of Anomalous Data and Outlier Performance

While the regression model showed an exceptionally strong fit (Adjusted R^2 = 0.91), it is crucial to discuss the interpretation of potential outliers, which were simulated in the dataset via random noise. In a real-world application of this model, these outliers would be the most important diagnostic data points.

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

An organization with a high AAS but poor IR metrics (a 'negative' outlier) would not invalidate the model. Instead, it would signal a critical implementation failure. For example, a SOC that has purchased a SOAR platform (high 'Automation' score) but has failed to train the staff to write or maintain playbooks, resulting in no actual performance gain. This represents 'paper' maturity without operational reality.

Conversely, an organization with a low AAS but strong IR metrics (a 'positive' outlier) might represent a small, 'hero-driven' team with one or two exceptional analysts. This model suggests that while their performance is currently high, it is not resilient, scalable, or repeatable, and it is highly vulnerable to staff turnover.

Therefore, the outliers do not invalidate the model; they enrich it. They prove that while ATT&CK maturity is a foundational pillar, it must be analysed alongside other key variables—such as staffing, toolsets, and environmental complexity—which are all critical avenues for future research.

LIMITATIONS AND AVENUES FOR FUTURE EMPIRICAL RESEARCH

The primary limitation is reliance on a synthesized dataset. Although constructed from industry-informed distributions, synthesized data cannot fully capture all real-world complexities. Future work should validate the AAS and these correlations using longitudinal, real-world datasets, incorporate confounding variables (budget, toolset, culture), and attempt to correlate AAS with direct business outcomes such as breach frequency and financial impact.

CONCLUSION

This study introduced a quantitative ATT&CK-based SOC maturity metric (AAS) and demonstrated strong, statistically significant relationships between AAS and key incident response KPIs in a synthesized cohort. Regression results highlight Incident Response Automation and Detection Engineering as high-impact investment areas to reduce MTTR.

For industry, this model provides a clear, quantitative benchmark for organizations to measure their threat-informed maturity and justify cybersecurity budgets as a driver of operational performance. For policymakers and regulators, ATT&CK-based maturity can serve as a more concrete, evidence-based standard for assessing the defensive capabilities of critical infrastructure sectors than traditional compliance checklists.

The study provides a data-driven rationale for adopting ATT&CK-centric operational practices and offers a structured, reproducible maturity rubric for benchmarking.

The primary limitation of this study is its reliance on a synthesized dataset. Although constructed from industry-informed distributions, synthesized data cannot fully capture all real-world operational complexities, confounding variables (e.g., organizational culture, specific toolsets), or unique business contexts.

Therefore, future work must focus on validating this model using longitudinal, real-world data from a diverse set of organizations. Such research would strengthen the causal claims and allow for the inclusion of other important variables. We recommend future studies to correlate the AAS with direct business

Received: August 02, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

outcomes, such as verified breach frequency and the total financial impact of incidents, to explicitly link threat-informed defense maturity with holistic business risk reduction.

ACKNOWLEDGMENTS

The author wishes to acknowledge the contributions of the MITRE Corporation for the development and maintenance of the ATT&CK framework, which serves as a vital public resource for the global cybersecurity community. Further thanks are extended to the anonymous peer reviewers for their insightful feedback on this manuscript.

99

1. Palo Alto Networks, What is a SOC?, Cyberpedia (2024). Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-soc [Accessed: Nov. 4, 2025].
2. E. Al-Shaer, M. Khan, and R. Patel, A Systematic Literature Review of Information and Cyber Security Maturity Assessment, Journal of Cybersecurity and Privacy, 3 (2023), 52-78.
3. AttackIQ, A Practical Guide to Threat-Informed Defense, AttackIQ White Paper (2021). Available at: https://www.attackiq.com/resources/white-papers/a-practical-guide-to-threat-informed-defense [Accessed: Nov. 4, 2025].
4. Palo Alto Networks, What is MITRE ATT&CK?, Cyberpedia (2024). Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack [Accessed: Nov. 4, 2025].
5. MITRE Corporation, MITRE ATT&CK®, (2024). Available at: https://attack.mitre.org [Accessed: Nov. 4, 2025].
6. Trellix, What is MITRE ATT&CK Framework?, Trellix Security Awareness (2024). Available at: https://www.trellix.com/en-us/security-awareness/what-is-mitre-attack-framework.html [Accessed: Nov. 4, 2025].
7. H. Al-Mohannadi, M. Al-Kuwari, and A. Al-Badi, A Maturity Capability Framework for Security Operation Center, EDPACS, 67 (2022), 1-18.
8. WatchGuard Technologies, Security Operations Maturity Model II: What It Is, WatchGuard Blog (2024). Available at: https://www.watchguard.com/wgrd-blog/security-operations-maturity-model-ii-what-it [Accessed: Nov. 4, 2025].
9. Hedgehog Security, Understanding the SOC Maturity Model and Its Stages, Hedgehog Security Blog (2023). Available at: https://hedgehog.security/understanding-the-soc-maturity-model-and-its-stages [Accessed: Nov. 4, 2025].
10. P. van der Meer, A Capability Maturity Model for Security Operations Centers, Diva Portal (2016). Available at: http://www.diva-portal.org/smash/get/diva2:1072922/FULLTEXT01.pdf [Accessed: Nov. 4, 2025].
11. Balbix, What is the MITRE ATT&CK Framework?, Balbix Insights (2024). Available at: https://www.balbix.com/insights/what-is-mitre-attck-framework/ [Accessed: Nov. 4, 2025].

Received: August 02, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

12. E. Alsheh, Creating a Smarter SOC with the MITRE ATT&CK Framework, CyberProof Blog (2023). Available at: https://www.cyberproof.com/blog/creating-a-smarter-soc-with-the-mitre-attck-framework [Accessed: Nov. 4, 2025].
13. Rapid7, Putting MITRE ATT&CK to Work In Your SOC, Rapid7 Solution Brief (2022). Available at: https://www.rapid7.com/solutions/solution-briefs/putting-mitre-attck-to-work-in-your-soc/ [Accessed: Nov. 4, 2025].
14. P. Chheda, A. Nguyen, and R. Kaur, Metrics for Modern Cybersecurity, In: Proc. of Security Metrics Conf. (2023), 1-10.
15. T. Gyebnar, S. Novak, and P. Horvath, MITRE in 2024, Cybersecurity Journal, 10 (2024), 15-25.
16. Mayura, Setting Up MITRE ATT&CK Use Cases in Your SOC, Cyberpress.org (2024). Available at: https://cyberpress.org/setting-up-mitre-attck-use-cases-in-your-soc [Accessed: Nov. 4, 2025].
17. Exabeam, What Is MITRE ATT&CK Framework and How Your SOC Can Benefit, Exabeam Explainers (2023). Available at: https://www.exabeam.com/explainers/mitre-attck-framework/ [Accessed: Nov. 4, 2025].
18. ManageEngine, Understanding the SOC Maturity Model, ManageEngine (2024). Available at: https://www.manageengine.com/security-information-event-management/soc-maturity-model.html [Accessed: Nov. 4, 2025].
19. SOC-CMM, SOC-CMM Metrics 101, SOC-CMM (2021). Available at: https://www.soc-cmm.com/soc-cmm-metrics-101.html [Accessed: Nov. 4, 2025].
20. BigPanda, A Guide to Incident Response Metrics and KPIs, BigPanda Blog (2024). Available at: https://bigpanda.io/blog/incident-response-metrics/ [Accessed: Nov. 4, 2025].
21. Splunk, Incident Response Metrics: The Ultimate Guide, Splunk Blog (2024). Available at: https://www.splunk.com/en_us/blog/learn/incident-response-metrics.html [Accessed: Nov. 4, 2025].
22. SecurityScorecard, How to Use Incident Response Metrics to Measure Effectiveness, SecurityScorecard Blog (2024). Available at: https://securityscorecard.com/blog/incident-response-metrics/ [Accessed: Nov. 4, 2025].
23. ResilientX, Measuring the Effectiveness of Security Operation Centers, ResilientX Blog (2023). Available at: https://www.resilientx.com/blog/measuring-the-effectiveness-of-security-operation-centers [Accessed: Nov. 4, 2025].
24. J. Parys, L. Smith, and G. Wang, On Security Metrics, Journal of Information Security, 12 (2021), 112-120.
25. Cynomi, How to Perform a Quantitative Risk Assessment in Cybersecurity, Cynomi Blog (2024). Available at: https://cynomi.com/blog/how-to-perform-a-quantitative-risk-assessment-in-cybersecurity/ [Accessed: Nov. 4, 2025].
26. UnderDefense, SOC Performance Unplugged: Understanding MTTD, MTTA&A, MTTR, and More, UnderDefense Blog (2024). Available at: https://underdefense.com/blog/soc-performance-unplugged-understanding-mttd-mttaa-mttr-and-more/ [Accessed: Nov. 4, 2025].
27. W. Burger, A. Klein, and D. Zhou, MITRE and ROI, In: Proc. of Cyber Economics, (2025), 50-55.

Received: August 02, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

28. S. G. Virk, J. Iqbal, A. Ali, A. R. Mahmud, I. Rashid, and T. Hanif, Advancing Security Operations Centers: Modern Use Cases, MITRE ATT&CK Integration, and Coverage Optimization in 2025, Journal of Computing & Biomedical Informatics, 9 (2025).
29. KPMG, Transform Your SOC Now: KPMG 2024 Security Operations Center (SOC) Survey, KPMG (2024). Available at: https://kpmg.com/us/en/articles/2024/transform-soc-now.html [Accessed: Nov. 4, 2025].
30. C. Crowley, SANS 2024 SOC Survey: Facing Top Challenges in Security Operations, SANS Institute (2024). Available at: https://www.sans.org/white-papers/sans-2024-soc-survey-facing-top-challenges-security-operations [Accessed: Nov. 4, 2025].

Received: August 02, 2025