Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 2, May 2026, pp. 518~530
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i2.pp518-530

A structured process model to optimize detection capabilities in security operations centers (SOCs)

Adi Nugroho, Charles Lim, Heru Purnomo Ipung
Department of Information Technology, Faculty of Engineering Swiss German University, Tangerang, Indonesia

Article Info

Article history:

Received Dec 13, 2025
Revised Mar 4, 2026
Accepted May 26, 2026

Keywords:

Cyber threat detection
MITRE ATT&CK
Security operations center
SOC
SOC detection capability

ABSTRACT

The security operations center (SOC) is essential for protecting organizational assets and maintaining operational continuity against rapidly changing cyber threats. Despite its significance, numerous SOCs establish detection capabilities lacking of a systematic framework, frequently culminating in inefficiencies and constrained efficacy. This paper presents a process model aimed at improving SOC detection capabilities by aligning them with business objectives, pertinent risks, and the evolving character of contemporary threats. The study includes an evaluation of current detection methodologies, utilizing the MITRE ATT&CK architecture and threat intelligence data to pinpoint relevant risks and detection deficiencies. A case study was performed at the XYZ Organization to evaluate current detection capabilities and implement the recommended process model. The model was validated through interviews with experts in the SOC field, verifying the findings' credibility. The findings demonstrate that the model efficiently helps SOC in synchronizing detection methods with organizational objectives, prioritizing pertinent threats, and promoting the enhancement of more targeted and adaptable detection capabilities. This research provides theoretical insights into SOC detection modeling and practical assistance for enterprises aiming to enhance their cybersecurity operations.

Corresponding Author:

Adi Nugroho
Departement of Information Technology, Faculty of Engineering
Swiss German University
15143 Tangerang, Indonesia
Email: adi.nugroho@student.sgu.ac.id

1. INTRODUCTION

The swift advancement of information technology has established a borderless cyberspace that propels global social, economic, and technological development. This rise has been followed by more sophisticated cyber threats that provide significant risks to organizations aiming to protect key assets and ensure operational continuity. Verizon's 2023 data breach report reveals that 74% of breaches were attributable to human reasons, including negligence, misuse of access, stolen credentials, and social engineering [1]. Consequently, firms encounter increasing pressure to enhance their capacity for rapid detection and response to possible crises to avert financial losses and operational interruptions.

A security operations center (SOC) serves as a centralized entity that oversees an organization's assets to detect, identify, and respond to security threats and incidents [2]. According to [3], the SOC's primary role is to maintain constant surveillance of potential attacks and suspicious activities in order to safeguard organizational infrastructure. However, SOC teams often face operational challenges, including the problem of alert fatigue caused by an overwhelming number of alerts with varying levels of importance [4]. This burden can lead to low morale and difficulty in distinguishing genuine threats from false alarms, thereby

weakening the SOC's mission to detect adversarial activities [5]. To address these issues, SOCs must continuously improve detection quality by updating detection methods and adapting them to evolving threats and organizational needs [6].

Detection capability is a core determinant of SOC effectiveness, directly affecting the speed and accuracy of incident identification and response. Frameworks such as MITRE ATT&CK support the development of detection use cases aligned with adversary tactics, techniques, and procedures (TTPs) [7]; however, detecting all possible TTPs is neither feasible nor necessary for effective defense [8]. Consequently, detection strategies must be developed selectively, considering organizational risk, resource constraints, and operational priorities. Prior research has proposed threat-centric models [9], maturity-based assessments [10], and ATT&CK-based gap analyses [8], [11] to support detection engineering; however, these approaches primarily emphasize detection coverage assessment and capability evaluation rather than guiding the systematic execution of detection improvement activities. Moreover, several studies have highlighted that ATT&CK-based detection approaches often lack explicit mechanisms for organizational risk alignment and prioritization, limiting their practical applicability in complex SOC environments [12], [13]. The limited incorporation of business context and feedback-driven improvement mechanisms continues to hinder practical and sustainable detection optimization in real-world SOC environments [14].

Beyond traditional enterprise IT environments, SOC implementations are increasingly extended to industrial control systems (ICS) and operational technology (OT) domains. In these environments, centralized platforms correlate alerts and logs from diverse monitoring devices to provide real-time threat detection and situational awareness [15], [16]. Unlike conventional IT SOCs, OT SOCs must accommodate legacy systems and critical operational constraints that differ from standard IT practices [17]. Shared ICS SOC models have also been proposed to reduce security staffing burdens across multiple organizations [18]. Furthermore, ICS SOCs support functions such as incident response, vulnerability management, asset inventory, network monitoring, and compliance with standards like IEC 62443 [16].

Despite the availability of threat-centric frameworks, maturity models, and MITRE ATT&CK-based gap analyses, existing research lacks a structured process model that systematically optimizes SOC detection capabilities by integrating organizational risk, detection prioritization, and continuous validation. Addressing this gap, this study proposes a structured process model for optimizing detection capabilities in SOCs. The study adopts the design science research (DSR) methodology to design, develop, and evaluate an artifact that addresses both practical SOC challenges and theoretical shortcomings in existing detection engineering literature. The proposed model integrates business context, risk identification, detection gap analysis, prioritization, and continuous improvement through validation and feedback.

To the best of our knowledge, this study is among the first to propose a structured detection optimization process model that bridges SOC operational practices and detection engineering, rather than focusing solely on compliance, threat taxonomy, or tool-specific detection coverage. The main contributions of this research are as follows:

- The design of a structured, process-oriented model for SOC detection optimization that integrates business context, risk-based prioritization, and continuous improvement.
- The alignment of the proposed model with SOC operational workflows and detection engineering practices.
- An empirical evaluation of the model through its application within a government-operated SOC environment, supported by expert validation.

The remainder of the paper is structured as follows. Section 2 describes the research method, explaining the application of the DSR approach used to develop the proposed process model. Section 3 presents the results and discussion, outlining the common challenges faced by SOCs, reviewing existing detection models and approaches, introducing the proposed process model, and describing its implementation in XYZ Organization along with expert validation. Section 4 concludes the study by encapsulating main contributions, delineating limits, and proposing directions for future research.

2. METHOD

2.1. Research methodology

This study employs the DSR methodology, which is well-suited for research aimed at creating and evaluating artifacts that solve practical problems while contributing to scientific knowledge. According to [19], DSR is comprised of six iterative phases: problem identification and motivation, objectives definition, design and development, demonstration, evaluation, and communication. Each of these phases provides a structured pathway to ensure that the artifact developed in this case, a process model for enhancing detection capabilities in SOC is both scientifically rigorous and practically relevant. Figure 1 shows the DSR cycle used in this study to develop the proposed SOC detection model.

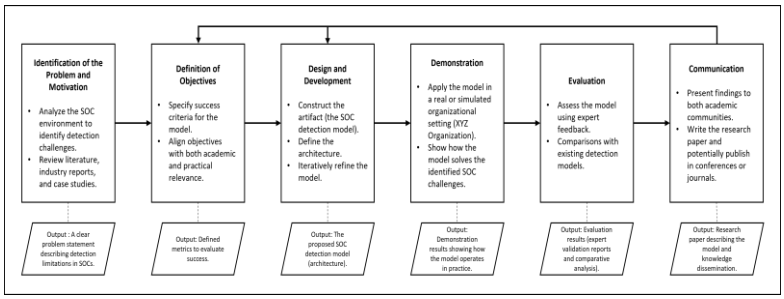

Figure 1. DSR cycle for developing the proposed process model

2.2. Design and development

The design and development phase focuses on constructing a structured process model for optimizing detection capabilities in SOCs. The model was informed by existing SOC detection literature and frameworks as well as common operational challenges faced by SOCs. These inputs ensured that the model addresses both theoretical considerations and practical constraints encountered in real-world SOC environments. Based on these inputs, the proposed model was structured into a sequence of interrelated phases: (1) understanding the business context, (2) scope definition, (3) risk identification, (4) gap analysis, (5) development of prioritization and detection strategies, (6) implementation and refinement of detection strategies, and (7) testing. The design process followed an iterative approach, allowing refinements as new insights emerged during development and supporting continuous improvement rather than a linear, one-time design. The outcome of this phase is a structured, process-oriented detection optimization model intended to guide SOCs in planning, implementing, validating, and refining detection capabilities in a consistent and repeatable manner.

2.3. Demonstration environment

The proposed process model was demonstrated in a controlled test environment designed to reflect typical SOC operational conditions at XYZ Organization, a government agency operating an internally managed SOC. The environment incorporated centralized security monitoring components and standard enterprise log sources to evaluate detection workflows rather than introduce new security technologies. Adversarial behavior was emulated using the Atomic Red Team framework, which maps test scenarios to MITRE ATT&CK techniques to systematically simulate attacker tactics, techniques, and procedures. The test environment used virtualized Linux and Windows Server systems to represent key organizational assets, while detection performance was evaluated based on alerts generated by the monitoring platform and perimeter controls. The setup included standard SOC components such as a centralized SIEM, firewall, Active Directory, and Windows and Linux hosts, as shown in Figure 2. Although detailed configurations cannot be disclosed due to confidentiality constraints, the architecture reflects a typical enterprise SOC environment and supports replication in similar operational contexts.

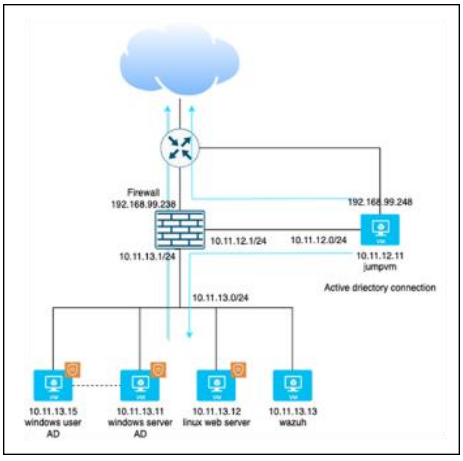

Figure 2. Network architecture of the demonstration environment

2.4. Evaluation strategy

The proposed process model was evaluated using a mixed-method evaluation approach, combining process-level quantitative assessment with expert-based qualitative validation. The quantitative component focused on comparing detection coverage between existing SOC detection practices (baseline) and detection activities structured using the proposed model. Detection coverage was assessed by examining the extent to which relevant threat techniques were systematically identified and addressed through the model-guided detection process, providing an empirical basis for evaluation within the SOC environment.

The qualitative component of the evaluation was supported by expert validation involving three SOC professionals, representing roles in SOC operations and detection engineering. The background, roles, and professional experience of the participating experts are summarized in Table 1, highlighting their extensive involvement in SOC operations and detection engineering. Experts reviewed the structure, phases, and applicability of the proposed process model through structured walkthroughs and discussions. Feedback obtained from this validation was used to iteratively refine and improve the model, ensuring that the proposed process aligns with practical SOC workflows and operational constraints.

Table 1. Expert profiles involved in the validation phase

Criteria	Expert		
	1	2	3
# year of work experience in SOC	5 – 10 years	> 10 years	> 10 years
Current position	Cybersecurity consultant	SOC Manager	SOC Lead
Previous experience in SOC	- SOC Analyst - SOC Team Lead - SOC Consultant - MSSP SOC	- SOC Consultant - SOC Security Engineer	- SOC Analyst - SOC Team Lead - SOC Consultant - SOC Manager - MSSP SOC

3. RESULTS AND DISCUSSION

This section presents the main findings of this study based on the application of the DSR approach. The discussion begins with an overview of the challenges that limit SOC detection performance, followed by a review of existing models and approaches. The proposed process model is then described, outlining its structure and intended improvements. The section continues with the implementation of the model in XYZ organization and concludes with the results of expert validation and performance assessment.

3.1. Common challenges faced by SOC

SOCs encounter numerous challenges that hinder their overall performance and operational efficacy. To increase threat detection and response as well as SOC performance, it is important to address the complexity underlying these challenges. Despite the importance of these issues, the body of academic research on SOC challenges remains limited, making this a relatively underexplored domain [20]. Based on a synthesis of recent literature, the challenges can be grouped into three key dimensions: people, process, and technology.

In the human resource aspect, the lack of structured training programs for SOC analysts is a widely reported concern. Without continuous competency development and simulated exercises, analysts are often ill-prepared to handle complex or evolving threats [20], [21]. This gap leads to blind spots in detection and increases the workload on experienced analysts. Additionally, the demanding nature of SOC roles contributes to what has been described as "SOC analyst pain." Analysts are expected to remain alert and operational around the clock, which, combined with repetitive tasks and limited visibility, results in high levels of fatigue and burnout [22]. Communication breakdowns between analysts and managers also exacerbate response delays and reduce collaboration efficiency [20].

From a process standpoint, business alignment remains a critical weakness for many SOCs. Surveys in [22] and [23] reveal that misalignment with organizational objectives often results in resource limitations, understaffing, and poor executive support. Another issue is the ineffective use of metrics. While metrics are crucial for performance evaluation, many SOCs either lack relevant ones or fail to tie them to strategic goals, which diminishes their value and impact [20]. In addition, SOC personnel frequently lack a sufficient understanding of business operations, such as service hours, business priorities, and third-party risks, making it difficult to assess the true impact of security incidents [24], [25]. These issues become worse by the lack of standardized playbooks, which leaves analysts without defined protocols for dealing with various incident categories.

In the field of technology, SOCs often operate with restricted visibility throughout infrastructure, which makes it challenging to identify and address threats instantly. This lack of visibility increases stress among analysts and leaves gaps in monitoring coverage [20] [23]. Another persistent challenge is the high

volume of false positives generated by detection systems. Excessive alerts contribute to alert fatigue and reduce the ability of analysts to focus on genuine threats, increasing the risk of missing real attacks [24], [26]. Many SOCs also suffer from ineffective or poorly integrated tools that limit operational efficiency. According to [20], tool fragmentation and the absence of backup mechanisms further expose organizations to risk during system failures. Additionally, maintaining optimal performance of critical systems such as SIEM platforms, firewalls, and endpoint solutions is essential, yet many SOCs face constraints in hardware and software capabilities.

Developing effective detection strategies requires an understanding of the difficulties present in SOC environment. To improve threat detection, people, processes, and technology must be managed in concert. Organizations can improve overall security operations and deploy resources more efficiently when these elements are clearly understood.

3.2. Existing detection models and approaches

Various models and approaches have been proposed to evaluate and enhance the detection capabilities of SOCs. Each approach provides distinct perspectives, from maturity-based evaluations to threat-centric methodologies, addressing different aspect of SOC detection strategies. This subsection reviews representative approaches to highlight their contributions and limitations in relation to structured detection optimization.

The threat-driven model in [9] emphasizes structured threat modeling using frameworks such as STRIDE-LM and IDDIL/ATC to identify and prioritize threats, arguing that compliance-based strategies are insufficient for dynamic threat environments. In contrast, [10] evaluates detection capability through a maturity model covering people, process, technology, and detection domains, providing a high-level view of detection program development. While both approaches offer valuable insights, they either focus on control design or provide broad capability assessment without detailed guidance for systematic detection improvement. Other studies concentrate on ATT&CK-based evaluation. The work in [8] assesses detection coverage for ransomware using the MITRE ATT&CK framework and recommends defining clear detection scope and understanding attacker intent, yet it lacks practical guidance for risk-based detection prioritization. Similarly, [11] analyzes gaps between tool capabilities and ATT&CK mapping to measure detection readiness but does not incorporate organizational risk alignment or prioritization mechanisms. Overall, existing approaches contribute to detection assessment but do not provide an integrated, process-oriented model for systematic and risk-aligned detection optimization.

Table 2 presents a summary of the primary features of each model, encompassing objectives, detection capabilities, employed methodologies, and acknowledged limitations. Overall, although existing approaches have contributed significantly to threat detection research, many continue to encounter difficulties in practical implementation, alignment with business risks, and strategic prioritization. There continues to be a requirement for an integrated process model that links technical capability with contextual risk awareness to improve the overall effectiveness of SOC detection in a more comprehensive manner.

Table 2. Comparison of existing SOC detection strategy

	[26]	[9]	[8]	[10]
Objectives	Threat-driven security control design	SOC detection maturity assessment	MITRE ATT&CK-based detection gap analysis	Evaluation of MITRE ATT&CK-mapped detection implementation
Detection capability aspect	STRIDE-LM + IDDIL/ATC threat modeling	People, Process, Technology, Detection domains	Mapping security product coverage to MITRE ATT&CK	Identifying gaps between MITRE ATT&CK–mapped tool capabilities and their actual implementation
Measurement methodology	No specifc measurement, not using MITRE ATT&CK Framework	Measure capability level based on defined criteria	Measure security product detection capability based on gap analysis	Assess log source coverage against ATT&CK techniques
Stages	IDDIL/ATC combine with STRIDE-LM	No specific stages	Assessment of the coverage of MITRE ATT&CK security technologies	Analysis of existing infrastructure, log source mapping to MITRE ATT&CK
Threat Intelligence requrement	Require threat intelligence information	No specific threat intelligence requirement	No specific threat intelligence requirement	No specific threat intelligence requirement
Detection validation	No specific process to validate detection	No specific process to validate detection	Hands-off	Hands-off
Weakness	Focuses on control design, not detection optimization	High-level maturity view, lacks implementation guidance	Tool-specific, limited risk alignment	Lacks organizational risk prioritization

3.3. Proposed process model

As seen in Figure 3, the proposed model uses an iterative and sequential framework to align detection activities to organizational goals and emerging threats. Business alignment and scope definition are the first steps in the process, which then moves on to risk assessment and gap analysis before strategy creation, implementation, testing, and ongoing improvement. The model combines organizational and technological aspects to provide a systematic framework that SOCs may use to assess current capabilities, identify weaknesses, and direct targeted enhancements.

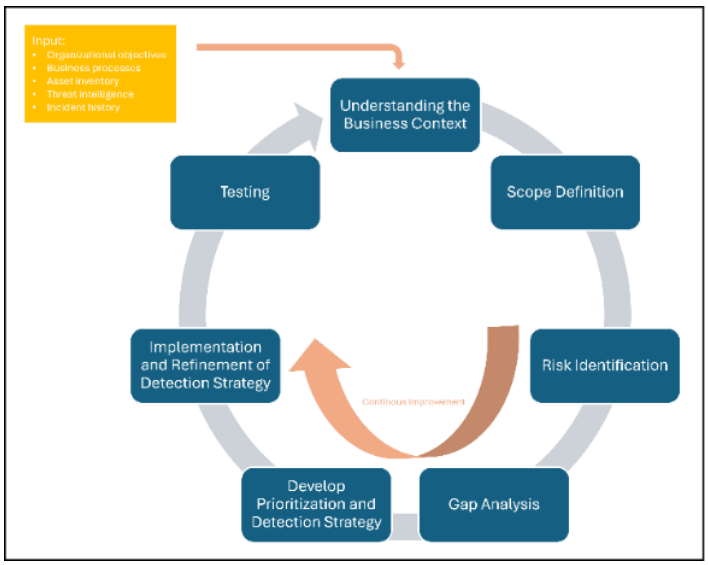

Figure 3. Proposed model for SOC detection improvement

3.3.1. Understanding the business context

The foundation of a successful SOC detection strategy is an understanding of the business context. Before defining technical controls, the organization must understand its operational objectives, critical assets, and business priorities to ensure that detection activities align with organizational goals. Without this alignment, security efforts may lead to inefficient resource use and overlooked risks. This phase involves structured discussions with key stakeholders, including representatives from business units, IT, compliance, security teams, and executive management, to identify critical assets and clarify security priorities. To formalize this alignment, the COBIT 5 goal cascading method is applied, translating stakeholder needs into enterprise goals and subsequently into IT and security objectives, ensuring that governance and management activities consistently support business outcomes.

3.3.2. Scope definition

Defining the scope ensures that SOC detection activities focus on the most critical parts of the organization. Based on the established business context, key systems, data, infrastructure, and services that directly support strategic objectives are identified and prioritized, particularly those whose compromise would result in significant operational, financial, or reputational impact. A risk impact assessment is conducted to evaluate potential consequences such as data breaches, service disruptions, regulatory exposure, and loss of customer trust, enabling the SOC to focus detection efforts where they provide the greatest value. Inputs to this process include the aligned business objectives, enterprise risk register, defined risk appetite, and mapped business processes and assets. The outcome is a prioritized list of mission-critical assets and their associated risks, documented in Table 3, which guides a focused and risk-aligned detection scope.

Table 3. Scope definition of improving SOC detection

Business context	Relevant business process	Relevant aset/application	Relevant enterprise risk	Probability	Impact	Risk value
(1)	(2)	(3)	(4)	(5)	(6)	(7)

3.3.3. Risk identification

The main objective of this stage is to prioritize the assets and business processes identified in the previous phase and to define the focus for developing detection capabilities. This phase identifies relevant threats and attack methods through structured threat modeling. The resulting TTPs form the foundation for the subsequent gap analysis and the improvement of SOC detection strategies.

The process begins with asset and application decomposition. Key assets and applications are broken down into their components, services, and connections. This step enables detailed mapping of potential threats and vulnerabilities at the component level. It also supports analysis of the telemetry produced by each asset. This analysis helps determine whether configuration changes are required to improve visibility and detection. The decomposition process is documented in Table 4.

Table 4. Assest/application decomposition process

Business context	Relevant business process	Relevant enterprise risk	Relevant aset or application	Application component	Desc
(1)	(2)	(3)	(4)	(5)	(6)

As part of threat modeling, the STRIDE-LM methodology is applied. A flow diagram represents interactions between asset components. Potential threats are identified using STRIDE-LM categories, including spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege, locking, and misuse. These threats are then developed into realistic scenarios, which summarized in Table 5.

Table 5. Threat model identification form

Scenario name	Point of entry	Threat actor	Sequence of attack	Threat events
(1)	(2)	(3)	(4)	(5)

The organization then identifies threats that are relevant to its environment by reviewing internal incident history and external threat intelligence. Several factors guide this assessment. These include geographic relevance, sector relevance, organizational similarity, and asset relevance. This step ensures that the selected threats reflect the actual risk exposure of the organization. The results of this analysis are summarized in Table 6.

Table 6. Relevant threat/incident to organization

Threat	Relevant factor				Probability	Impact	Risk
	CR	SS	OR	AR			
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)

From this analysis, specific cybersecurity risks are identified for the prioritized assets and business processes. Each risk is linked directly to an asset or component within scope. This targeted approach directs SOC resources toward areas with the highest potential impact. The mapping between assets, vulnerabilities, threats, and associated risks is presented in Table 7.

Table 7. Identification risk relevant to the organization assets

Business context ID	Relevant business process ID	Application	Application component	Vulnerability	Threat ID	Probability	Impact	Risk
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)

In the final step, organization maps identified threats to the MITRE ATT&CK framework and to the MITRE ATT&CK Top 10 techniques. This mapping aligns organizational risks with known adversary behaviors. It supports the prioritization of detection use cases based on relevance and likelihood. The detailed relationship between asset components and relevant MITRE ATT&CK techniques is shown in Table 8.

Table 8. Mapping organization asset component to MITRE ATT&CK top 10 relevant threat

Business context ID	Relevant business process ID	Application	Application component	Relevant MITRE ATT&CK
(1)	(2)	(3)	(4)	(5)

3.3.4. Gap analysis

This stage follows risk identification and focuses on assessing current SOC detection capabilities against identified threats mapped to the MITRE ATT&CK framework. The objective is to identify critical detection gaps using two complementary approaches. First, existing security technologies and in-scope assets are evaluated against relevant threats to determine areas of insufficient or missing detection coverage, with the results documented in Table 9. Second, threat emulation is conducted using realistic, organization-specific attack scenarios to validate these findings in practice and reveal operational weaknesses not visible through static analysis. The outcomes provide a clear view of SOC readiness and identify specific capabilities that require improvement to strengthen detection coverage.

Table 9. Gap assessment based on existing technology capability

Business context ID	Relevant business process ID	Application	Threat	MITRE ATT&CK	Possible source detection	Existing condition	Gap
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)

3.3.5. Develop prioritization and detection strategy

The prioritization and detection strategy phase aligns detection efforts with the highest-risk assets and business processes identified in the defined scope. Prioritization focuses on threats with both high likelihood and significant potential impact, ensuring that detection resources are directed toward the most critical risks. Particular attention is given to frequently observed techniques, including those highlighted in the MITRE ATT&CK Top 10, as well as to the availability and quality of relevant telemetry required for reliable detection. The strategy also considers the organization's technological capabilities to collect, store, and analyze security data effectively. Emphasis is placed on detecting early-stage attack techniques, such as command execution and defense evasion, to prevent escalation into persistence, lateral movement, or credential abuse.

3.3.6. Implementation and refinement of detection strategy

The implementation and refinement phase focuses on operationalizing the detection strategy derived from the gap analysis. This involves configuring monitoring rules, alert logic, and telemetry collection across prioritized assets and business processes to translate the strategy into active SOC controls. Following deployment, continuous validation and testing are conducted to identify misconfigurations, detection gaps, and false positives. Based on these findings, adjustments are made to improve accuracy, relevance, and effectiveness. This iterative approach ensures that detection capabilities remain aligned with evolving threats and organizational priorities.

3.3.7. Testing

The testing phase is essential for confirming the efficacy of the enhancements implemented in the detection strategy. This method involves re-emulating the identified threats and attack techniques to assess whether the updated detection mechanisms can reliably and speedily identify them. The results from this testing determine whether the previously reported deficiencies have been effectively remedied and confirm that the SOC's detection capabilities correspond with organizational security goals. Continuous testing enables iterative improvements, which encourages a stronger security posture.

3.4. Demonstration in XYZ organization

In XYZ Organization, the demonstration focused on assets supporting the Information Dissemination and Public Service process, particularly the Service and Information Portal, including its web application and database servers. Threat modeling using STRIDE-LM identified multiple exposure points across application, infrastructure, and security layers, including risks related to spoofing, tampering, privilege escalation, credential abuse, and lateral movement. Historical incidents such as brain cipher ransomware and mustang panda activity confirmed the relevance of these threat scenarios within the organizational context. As summarized in Table 10, the database and web application servers were assessed as high-risk due to weaknesses such as insufficient user activity control and outdated software versions.

Table 10. Risk identification of asset component

Relevant business process	Asset	Asset component	Vulnerability	Threat ID (MITRE)	Probability	Impact	Risk
Information dissemination & public service	Service & information portal	Db server & Web app server	Lack of user activity control	T1078.003, T1078.001	3	4	17 (High)
Information dissemination & public service	Service & information portal	Db server & Web app server	Outdate application version	T1068	2	5	21 (Very High)

Following the identification of relevant threats and risks, a gap analysis was conducted to assess current SOC detection capability in XYZ Organization. This stage used a documentation-based review of deployed security technologies and a controlled threat emulation activity. The goal was to measure coverage, identify blind spots, and determine which parts of the attack surface remain weak or unmonitored.

The documentation-based review examined four security technologies: web application firewall, firewall, network detection and response (NDR), and endpoint detection and response (EDR). Each technology was mapped to the identified threat scenarios and the MITRE ATT&CK Top 10 techniques. As shown in Table 11, detection coverage varied significantly across technologies. EDR provided the highest coverage, followed by NDR, while the web application firewall and traditional firewall showed limited capability, particularly against techniques associated with brain cipher and mustang panda. These results indicate detection gaps at the perimeter layer and limited visibility at critical entry points.

Table 11. Detection coverage summary based on documentation-based review

Security technology component	Detection coverage		
	Brain cipher	Mustang panda	MITRE ATT&CK Top 10
Web application firewall	3/25	5/48	6/21
Firewall	8/25	5/48	6/21
NDR	17/25	35/48	20/21
EDR	25/25	45/48	21/21
Overall coverage	25/25	46/48	21/21

To validate these findings in practice, threat emulation was conducted using high priority scenarios connected to brain cipher and mustang panda. The emulation environment reflected the operational setup of XYZ, including Linux based web systems and Windows server for directory services. The activity confirmed that several techniques were recorded in logs but not elevated to alerts. Table 12 presents the quantitative results of this evaluation. For brain cipher, 20 out of 35 emulated techniques generated alert-level detections (57%), while the remaining 15 techniques were recorded only at the logging level. For mustang panda, 36 out of 48 techniques resulted in alerts (75%), with 12 techniques producing logging-only visibility. These results indicate that while a portion of the emulated techniques generated alerts, a substantial number were recorded only at the logging level, revealing gaps in detection capability.

Table 12. Detection coverage summary based on threat emulation

Threat actor	Techniques	Detection status		Detection rate
		Logging-only	Detected with alert	
Brain ciper	35	15	20	57%
Mustang panda	48	12	36	75%

After identifying several detection gaps through adversary emulation, the next step focused on developing a structured strategy to address these gaps. Technique selection was based on risk level, feasibility, and available resources. Priority was given to threats that posed the highest impact, techniques included in the MITRE ATT&CK Top 10, and those with accessible data sources. Particular emphasis was placed on early-stage attack techniques, such as command execution and defense evasion, to disrupt adversary activity at an early phase. Techniques associated with the mustang panda threat group were selected due to their relevance to the organization's threat landscape. Among these, technique T1218.005 (execution of remote HTML applications via mshta) is presented as a representative example of the refinement process.

To support detection of T1218.005, relevant data sources were identified and enabled. These include process creation, command execution, file creation, and network connection data. A detection rule was created to identify suspicious mshta activity, including execution of external scripts and unusual command-line behavior, as shown in Figure 4. It should be noted that developing and maintaining effective detection rules requires skilled and experienced human resources, which may present challenges for organizations with limited detection engineering expertise.

```
(SrcProcName = "mshta.exe" and EventType = "Open Remote Process
Handle") OR (SrcProcName = "mshta.exe" AND SrcProcCmdLine RegExp
"https?:\/\/(www\.)?[-a-zA-Z0-9@:%._\+~#=]{1,256}\.[a-zA-Z0-
9()]{1,6}\b([-a-zA-Z0-9()@:%_\+.~#?&//=]*)")
```

Figure 4. Detection rule for T1218.005 based on mshta command line and process behavior

The logging configuration on the Windows Server was updated to collect the required telemetry using Sysmon, and the generated logs were forwarded to the centralized monitoring platform for analysis. This configuration provided enhanced visibility into mshta process execution and related command-line activities without disrupting existing logging mechanisms. The developed detection rule for technique T1218.005 was then validated through multiple simulation rounds reflecting misuse of remote HTML application execution. During testing, the monitoring system successfully generated alerts for the emulated scenarios, confirming that the refined telemetry collection and detection logic effectively transformed previously logging-only events into actionable alerts.

Table 13 presents the comparison of detection performance before and after optimization. Prior to refinement, several techniques were recorded only at the logging level and did not generate actionable alerts. Following structured rule development and telemetry enrichment, all previously logging-only techniques were consistently detected at the alert level during repeated simulations. This measurable improvement demonstrates how the proposed process model systematically transforms detection gaps into validated detection capabilities through risk-based prioritization and iterative refinement.

Table 13. Comparison of detection coverage for mustang panda using the proposed process model

Stages	Techniques emulated	Baseline SOC		Optimized SOC	
		Detected with alert	Detection rate	Detected with alert	Detection rate
Initial access	3	3	100%	3	100%
Execution	5	4	80%	5	100%
Persistence	3	1	33,33%	3	100%
Privilege escalation	1	0	0%	1	100%
Defense evasion	7	4	57,14%	7	100%
Credential access	1	0	0%	1	100%
Discovery	8	4	50%	8	100%
Collection	4	4	100%	4	100%
Command and control	3	2	66,67%	3	100%

3.5. Discussion and practical implications

The expert evaluation indicates that the proposed process model aligns well with real-world SOC operations and addresses common operational constraints such as limited analyst capacity, competing priorities, and scalability challenges. Rather than introducing isolated detection techniques, the model's structured and sequential nature supports consistent execution of detection engineering activities within existing SOC workflows. These findings suggest that the model's effectiveness stems from its ability to formalize detection improvement as a repeatable operational process, while still allowing flexibility based on organizational context and data availability.

From an operational perspective, the early phases of the model (business context understanding, scope definition, and risk identification) play a critical role in mitigating alert fatigue and detection overload. Aligning detection activities with business goals enables SOCs to prioritize threats based on organizational impact rather than alert volume alone, shifting the SOC toward a value-driven function. Precise scope definition further constrains detection efforts to relevant assets and attack paths, while risk identification informed by internal incident history and external threat intelligence ensures that detection development remains focused on realistic and high-impact adversary behavior. The use of MITRE ATT&CK as a

supporting framework reinforces consistency in threat mapping and prioritization without dictating rigid coverage requirements.

The later phases of the model (gap analysis, prioritization, implementation, and testing) explain the observed improvements in detection effectiveness reported in Section 3.4. Systematic gap analysis, supported by adversary emulation, exposes discrepancies between available telemetry and alert generation, providing a concrete basis for targeted detection refinement. Risk-based prioritization balances detection impact against available resources, preventing overextension of SOC teams, while iterative implementation and feedback ensure continued alignment with evolving threats. Mandatory testing before deployment reduces false positives and missed detections, contributing to more reliable alerts and minimizing operational disruption. Collectively, these mechanisms illustrate how the proposed model bridges SOC operations and detection engineering through structured feedback and continuous refinement.

4. CONCLUSION

This paper presents a structured process model for optimizing detection capabilities in SOCs by systematically aligning detection activities with business context, risk prioritization, and iterative validation. The empirical evaluation conducted in XYZ Organization indicates measurable improvements in detection coverage following structured refinement, demonstrating the practical applicability of the model within the evaluated environment. Beyond operational benefits, the study contributes to the body of knowledge in SOC and detection engineering by formalizing detection optimization as a repeatable, risk-driven process that bridges SOC operations and structured detection engineering practices. However, the validation was conducted within a single organizational context and limited threat scenarios, and the effectiveness of the model may vary depending on organizational structure, technological infrastructure, and resource constraints.

Future research should extend validation across multiple industries and organizational contexts to assess broader applicability and performance consistency. Further work may explore formal integration of the process model into SIEM and SOAR platforms to automate prioritization, feedback loops, and validation workflows. AI-driven techniques can be investigated to enhance risk scoring, detection prioritization, and adaptive rule refinement within the model. Additional research may also develop quantitative metrics for measuring detection optimization progress and examine cross-SOC collaboration mechanisms for shared detection improvement strategies. These directions provide a roadmap for evolving the proposed process model into a scalable and empirically validated framework for detection optimization.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Adi Nugroho	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	
Charles Lim		✓		✓			✓			✓		✓		
Heru Purnomo Ipung		✓		✓			✓			✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available on request from the corresponding author, AN. The data, which contain information that could compromise the privacy of research participants, are not publicly available due to certain restrictions.

REFERENCES

[1] P. Langlois, A. Pinto, D. Hylender, and S. Widup, *2023 data breach investigations report (DBIR)*. Verizon, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

[2] C. Onwubiko, "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy," in *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015*, IEEE, Jun. 2015, pp. 1–10. doi: 10.1109/CyberSA.2015.7166125.

[3] S. Schinagl, K. Schoon, and R. Paans, "A framework for designing a security operations centre (SOC)," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, IEEE, Jan. 2015, pp. 2253–2262. doi: 10.1109/HICSS.2015.270.

[4] J. Lemon, "Building a new cybersecurity alert priority matrix." Uptycs.com. Accessed: Sep. 1, 2024 [Online]. Available: https://www.uptycs.com/blog/cybersecurity-alert-priority-matrix

[5] Palantir, "Alerting and detection strategy framework." Blog.palantir.com. Accessed: Sep. 01, 2024. [Online]. Available: https://blog.palantir.com/alerting-and-detection-strategy-framework-52dc33722df2

[6] Gartner, "Modern Security Operations Center (SOC) Strategies." gartner.com. Accessed: Sep. 2, 2025. [Online]. Available: https://www.gartner.com/peer-community/

[7] MITRE ATT&CK®, "Get Started | MITRE ATT&CK®." Accessed: Sep. 02, 2025. [Online]. Available: https://attack.mitre.org/resources/

[8] J. Kinnunen, "Threat detection gap analysis using MITRE ATT&CK Framework," M.S. thesis, JAMK Univ. Appl. Sci., Jyväskylä, Finland, 2022.

[9] M. Muckin and S. C. Fitch, *A threat-driven approach to cyber security: methodologies, practices and tools to enable a functionally integrated cyber security organization*. Bethesda, MD : Lockheed Martin Corporation, 2015.

[10] K. Bailey, "Detection engineering maturity matrix," DetectionEngineering.io, 2021. Accessed: Sep. 01, 2024. [Online]. Available: https://detectionengineering.io/

[11] S. A. Chamkar, Y. Maleh, and N. Gherabi, "Security operations centers: use case best practices, coverage, and gap analysis based on MITRE adversarial tactics, techniques, and common knowledge," *Journal of Cybersecurity and Privacy*, vol. 4, no. 4, pp. 777–793, 2024, doi: 10.3390/jcp4040036.

[12] H. Dost, "Detection development lifecycle." medium.com. Accessed: Sep. 01, 2024. [Online]. Available: https://medium.com/snowflake/detection-development-lifecycle-af166fffb3bc

[13] D. Oktavianto, "Evaluating organisation's cyber defense capability with MITRE Top 10 ATT&CK technique." medium.com. Accessed: Sep. 01, 2024. [Online]. Available: https://medium.com/mii-cybersec/evaluating-organisations-cyber-defense-capability-with-mitre-top-10-att-ck-technique-58764390eccf

[14] ADEO Cyber Security, "The importance of developing a detection framework for cyber attacks." Adeosecurity.com. Accessed: Sep. 01, 2024. [Online]. Available: https://www.adeosecurity.com/the-importance-of-developing-a-detection-framework-for-cyber-attacks

[15] G. B. Gaggero, R. Caviglia, P. Girdinio, and M. Marchese, "Toward a security operation center for operational technology in industrial networks," in *2024 IEEE International Workshop on Technologies for Defense and Security, TechDefense 2024 - Proceedings*, 2024, pp. 160–164. doi: 10.1109/TechDefense63521.2024.10863654.

[16] R. Caviglia, D. Aliaskharov, A. Aceti, M. D. Preda, P. Girdinio, and G. B. Gaggero, "A security operation and event management (SOEM) platform for critical infrastructures protection," *Computers, Materials and Continua*, vol. 85, no. 3, pp. 5327–5340, 2025, doi: 10.32604/cmc.2025.068509.

[17] M. Jbair, "Security monitoring strategies for your OT infrastructure," *Cyber Security: A Peer-Reviewed Journal*, vol. 3, no. 3, p. 265, 2019, doi: 10.69554/zwfl5253.

[18] W. Dimitrov and S. Syarova, "Analysis of the functionalities of a shared ICS security operations center," in *2019 Big Data, Knowledge and Control Systems Engineering, BdKCSE 2019*, 2019. doi: 10.1109/BdKCSE48644.2019.9010607.

[19] K. Peffers *et al.*, "The design science research process: a model for producing and presenting information systems research," in *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006)*, Claremont, CA, USA, 2006, pp. 83–106.

[20] F. B. Kokulu *et al.*, "Matched and mismatched SOCs: A qualitative study on security operations center issues," in *Proceedings of the ACM Conference on Computer and Communications Security*, New York, NY, USA: ACM, Nov. 2019, pp. 1955–1970. doi: 10.1145/3319535.3354239.

[21] F. D. Janos and N. H. P. Dai, "Security concerns towards security operations centers," in *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, IEEE, May 2018, pp. 273–278. doi: 10.1109/SACI.2018.8440963.

[22] Devo Technology, "2021 Devo SOC performance report: SOC leaders and staff are not aligned." devo.com. Accessed: Dec. 18, 2024. [Online]. Available: https://www.devo.com/blog/2021-devo-soc-performance-report-soc-leaders-and-staff-are-not-aligned/

[23] Ponemon Institute, "Improving the effectiveness of the security operations center," no. June. pp. 1–40, 2019. [Online]. Available: https://www.devo.com/wp-content/uploads/2019/07/2019-Devo-Ponemon-Study-Final.pdf

[24] B. A. Alahmadi, L. Axon, and I. Martinovic, "99% false positives: a qualitative study of SOC analysts' perspectives on security alarms," in *Proceedings of the 31st USENIX Security Symposium, Security 2022*, 2022, pp. 2783–2800.

[25] S. A. Chamkar, Y. Maleh, and N. Gherabi, "The human factor capabilities in security operation center (SOC)," *Lecture Notes in Networks and Systems*, vol. 357 LNNS, pp. 579–590, 2022, doi: 10.1007/978-3-030-91738-8_53.

[26] D. Crémilleux, C. Bidan, F. Majorczyk, and N. Prigent, "Enhancing collaboration between security analysts in security operations centers," in *Risks and Security of Internet and Systems*, Lecture Notes in Computer Science, vol. 11498, Cham, Switzerland: Springer, 2019, pp. 136–142.

BIOGRAPHIES OF AUTHORS

Adi Nugroho earned a bachelor's degree in applied science in cryptography from the National Cyber and Crypto Polytechnic in 2006 and a bachelor's degree in computer science at the University of Indonesia in 2010. Currently, he is a master's student in information technology at the information technology department of Swiss German University. His research interests include security operations centers, cyber incident response, cryptography, and information security governance. He can be contacted at email: adi.nugroho@student.sgu.ac.id.

Charles Lim is a distinguished cyber security expert with extensive academic and professional achievements. He holds a Doctorate in Electrical Engineering from the University of Indonesia, a master's in electrical engineering from the University of Hawaii-Manoa, and a bachelor's in electrical engineering from the University of Wisconsin-Madison. As a researcher and lecturer at Swiss German University, he is actively involved in developing robust digital security systems and defending against cyber crime. His work includes collaborations with national agencies and industry leaders, such as BSSN and Bank Indonesia, focusing on cyber security regulations, threat intelligence, and malware analysis. He has received multiple awards for his contributions, including the ECCouncil Circle of Excellence Instructor Award and various teaching accolades. His research interests include cyber security threat sharing and malware analysis, supported by grants from the Information Society Innovation Fund. He can be contacted at email: charles.lim@sgu.ac.id.

Heru Purnomo Ipung received Doctorate in Computer Science from Institut Teknologi Sepuluh Nopember Surabaya (ITS), a Master of Engineering in Information Technology from Royal Melbourne Institute of Technology (RMIT), and a Bachelor of Engineering in Computer Engineering from ITS. Dr. Heru Purnomo Ipung is a distinguished experts in the fields of Enterprise Architecture and Information Systems, with a robust portfolio of academic and professional accomplishments. He has been an integral part of Swiss German University since 2010, serving as a researcher and lecturer in Information Technology. His leadership roles at the university include serving as the Head of the Research Center of Technology and Innovation from 2014 to 2020, and as the Head of Information System Services from 2010 to 2015. Dr. Ipung's professional experience extends to independent IT consulting and advisory roles, which he has held since 2010. Prior to his tenure at Swiss German University, he was a prominent Enterprise Architecture Lead and consultant at Accenture Indonesia from 1995 to 2009. Dr. Ipung's expertise encompasses Enterprise Architecture, IT Valuation, Digital Transformation, and IoT and Sensor technologies. His research spans advanced topics such as Artificial Intelligence and Sensor Fusion, Simulation and Modeling, Multispectral Imaging, and Computer Vision. He can be contacted at email: heru.ipung@sgu.ac.id.