Scientific Research Publishing

Journal of Information Security, 2020, 11, 225-240
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Security Operations Center: A Framework for Automated Triage, Containment and Escalation

Paul Danquah

Council for Scientific and Industrial Research, Institute for Scientific and Technological Information (CSIR-INSTI), Accra, Ghana
Email: pauldanquah@yahoo.com

How to cite this paper: Danquah, P. (2020) Security Operations Center: A Framework for Automated Triage, Containment and Escalation. *Journal of Information Security*, **11**, 225-240.
https://doi.org/10.4236/jis.2020.114015

Received: July 18, 2020
Accepted: September 22, 2020
Published: September 25, 2020

Abstract

There have been a lot of research exertions and studies to improve the safety of critical infrastructures using the Security Operations Center (SOC). As part of efforts, the purpose of this research is to propose a framework to automate the SOC's performance of triage, containment and escalation. The research leveraged on qualitative desk review to collect data for analysis, deduced strengths and weaknesses for the current SOC implementations and used that as a basis for proposing the framework. In view of the constant evolution of SOC operations and capabilities coupled with the huge volumes of data collected for analysis, an efficient framework for SOC operations is proposed. The qualitative analysis is used to deduce strengths and weaknesses for the current SOC implementations as a premise for proposing the framework. It consists of eight interactive stages that further leverage on a proposed algorithm for baselining, remediation and escalation. The result of this research is a proposed framework that serves as a unique contribution to enhancing the SOC's ability to automatically perform triage, containment and escalation. Supplementary to similar and earlier work reviewed, the framework is proposed as the way forward to automatically enable SOC setups with the capacity to efficiently perform triage of security threats, vulnerabilities and incidents, effectively contain identified breaches and appropriately escalate for prompt and accurate solutions.

Keywords

Security Operations Center, Triage, Containment, Escalation, Information Security

1. Introduction

Security Operations Center (SOC)s are central protection groups that focus on security incident management with capabilities such as monitoring, preventing,

responding, and reporting. "They are one of the most critical defense components of a modern organization's defense. Despite their critical importance to organizations, and the high frequency of reported security incidents, only a few research studies focus on problems specific to SOCs" [1]. The growing number and severity of cybersecurity threats, combined with a shortage of skilled security analysts, have led to an increased focus on cybersecurity research and education [2]. These concerns suggest challenges with triage, containment and escalation of security threats. Triage in the information security context refers to the process of determining the priority of addressing incidents based on the severity of the security breach or compromise. Containment in the information security context is the action taken to prevent a security compromise or breach, thus to bring it under control or within limits. Escalation in the information security context refers to the process of involving experts of a higher tier in addressing security incidents, breach or compromise.

Brewer [3] revealed that 77% of respondent organizations in 2018 were compromised during the 12 months ahead of the study. It was further revealed that given a skills shortage and working with tight budgets, security operations centres (SOCs) are struggling with limited resources. The problems faced by SOCs need a solution, and embedded security orchestration, automation and response (SOAR) promises to be just that. This was confirmed by [4] Li and other researchers on the subject matter.

There have therefore been a lot of research efforts and studies to improve the safety of critical infrastructures using the SOC. Notable as part of efforts is the Enhanced Security Control (ESC) model with Blocking Prioritization (BP) process for critical infrastructures to improve daily incidents response activities, this was proposed by [5]. "This ESC model has a BP process with six factors to consider when deciding which IT systems to be blocked from foreign IP ranges: foreign relation, real login, blocking complexity, stop tolerance, outer relation and stop impact. By considering these six factors, the ESC model can make it possible to prioritize Blocking Impact Degree (BID) of IT systems and help make decision to block from unnecessary foreign IP ranges" [5]. The proposed ESC model was intended to reduce security events and make a better condition for concentration on the remaining unblocked and crucial information technology systems. Another proposal for addressing specifically detection of attacks without training, yet improved performance through training was sonification. Proposed by [6], data represented as sound, can be used to turn network attacks and network-security information into audio signals. "This could complement the range of security-monitoring tools currently used in Security Operations Centres (SOCs). Prior work in sonification for network monitoring has not assessed the effectiveness of the technique for enabling users to monitor network-security information". The proposal further investigated the viability of using sonified network datasets to enable humans to detect and identify network attacks. The results showed that "by listening to the sonified network data, participants could detect attacks accurately and efficiently, including combinations of attacks, and

identify the types of attacks" [6]. An interesting outcome was the fact that participants could detect attacks without training, yet improved performance was experienced through training. A description of the design and implementation of an education and research Security Operations Center (SOC) to address SOC issues, these included components such as a lab with honeypots, visualization tools, and a lightweight cloud security dashboard with autonomic orchestration [2].

A structure of a SOC system based on D-S evidence theory was also proposed with a prototype of SOC system developed according to the structure, experimental results indicated that the SOC system based on D-S evidence theory can increase greatly the correctness of detection intrusion and decrease the rate of false positive [7].

As a unique contribution to addressing SOC concerns raised by many researchers and industry professionals such as [1] [2] and [3], this study sets out assess weaknesses of the proposed solutions and propose a unified framework to address limitations observed in delivering optimal SOC solutions with emphasis on automating the process of triage, containment and escalation.

2. Methodology

This research work used a predominantly desk review, qualitative and descriptive approach. Descriptive research design helps provide answers to the questions associated with a particular research problem and can yield rich data that lead to important recommendations in practice [8]. This approach collected a large amount of secondary data for detailed analysis, it is effective to analyze non-quantified topics and issues, the possibility to observe the phenomenon in a completely natural and unchanged natural environment gives the opportunity to integrate the qualitative and quantitative methods of data collection. The methodology is premised on the mindset of a potential cybercriminal operating on the foundations of the criminological theory of Routine Activity Theory which suggests that; all crimes require suitable targets, lack of a suitable guardian and a motivated offender [9]. The research approach therefore uses a predominantly secondary source of data that is qualitatively analyzed to deduce strengths and weaknesses for the current SOC implementations as a premise for proposing the framework.

3. Literature Review

Theoretically, numerous perspectives can be the source of instruction for the automation of SOC operations. It is worth noting that the operationalized definition of information security in this context is ensuring confidentiality, integrity and availability of information at all times. A theory of information security as a number of constructs with relationships to produce resources was proposed by [10]. The constructs are information, controls and threats that interact to produce resources. Relating this to the SOC and the automation of triage, contain-

ment and escalation, information is fundamental to the entire process and its relative exposure to threats is dependent on the efficiency and effectiveness of controls available.

Assessing information security from a criminological perspective**, t**he Routine Activity Theory which is a generic criminological theory that was proposed by [9] suggested that for a crime to be committed, the following must be concurrently present:

"1) A suitable target is available: The suitable target here refers to a person, object or place.

2) There is lack of a suitable guardian to prevent the crime from occurring: The capable or suitable guardian refers to a deterrent like police patrols, security guards, neighborhood watch, door staff, vigilant staff and coworkers, friends, neighbors and CCTV systems.

3) A motivated offender is present: This presupposes that there can be no victim without the intentional actions of another individual."

The theory certainly relates to all forms of cybercrime; a crime would only occur when there is the opportunity for the crime to be committed. Opportunity tends to be root cause of crime, the routine activity theory was tested and confirmed by [11] within the cybercrime context their publication related to on-line activities, guardianship, and malware infection.

The SOC in this context is expected to play the role of a suitable guardian to prevent the crime's occurrence and limit the potential target's suitability.

A theoretical attempt to address crime commission in general was the introduction of the Crime Displacement: [12], this theory focused on crime reduction via opportunity reduction. The theory's suggestion of addressing crime by moving the crime from one locale another tends to its suggestive solution. The locales suggested range from namely:

"Geographical: Moving Crime from one location to the other

Temporal: Moving Crime from one time to the other

Target: Moving Crime from one target to the other

Tactical: Changing the approach to committing the crime from one to the other

Crime type: Changing the type of crime that is to be committed" [13].

These three theories are relatively relevant for theorizing SOC operations from the reason for their existence and essence for optimal operation.

SOC Evolution

The SOC solution components have changed over time due to resources available and expected services. Various professionals and researchers have provided varying stages as the evolution stages in SOC operations. The change over time is as a result of the extent to which information has become so critical and the perceived essence of protecting the information. This well confirmed theoretically by the Protection Motivation Theory by Rogers [14] which suggests that people protect themselves based on four factors being namely:

"1) The perceived severity of a threatening event

2) The perceived probability of the occurrence, or vulnerability
3) The efficacy of the recommended preventive behavior
4) The perceived self-efficacy"

The evolution of SOC is therefore essentially natural as the essence of information is considered critical, furthermore, regulation and directives from supervisory organizations demand formal information security standards, establishment and management of a formal security operations model and review processes in response to the changing the threats landscape. The book on Introduction To Security Operations and Management presents the four incremental generations in the evolution of SOC, this is shown in Figure 1.

HP's business white paper on SOC Generations also outlines the generations shown in Figure 2.

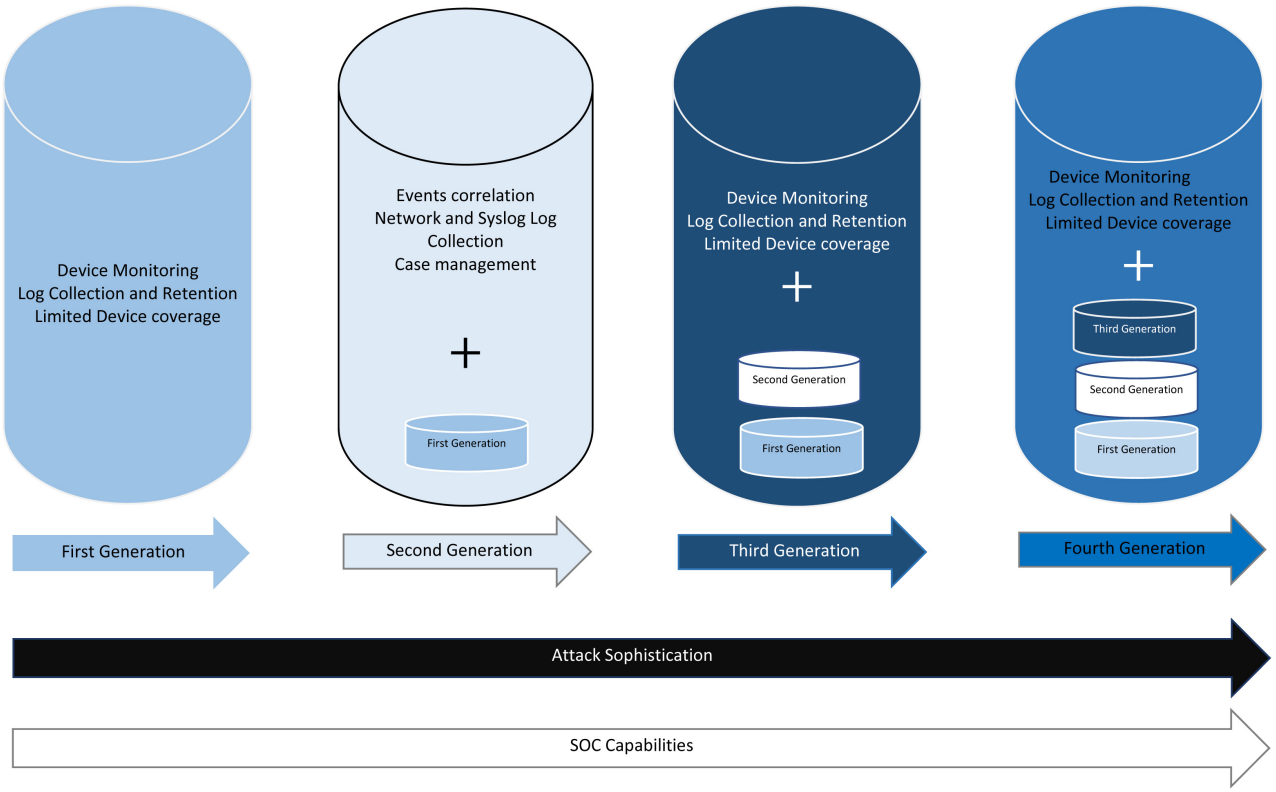

Figure 1. Generations of SOC. Source: [15].

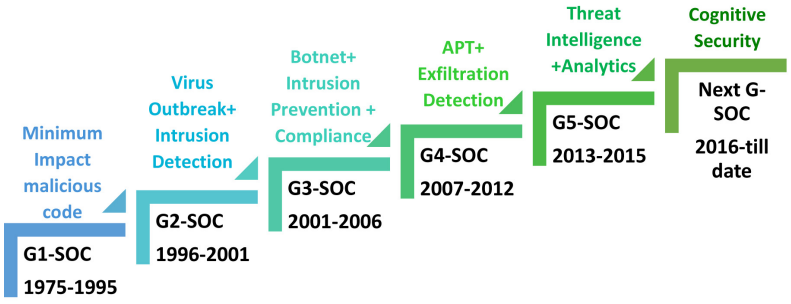

Figure 2. HP's generations of SOC. Source: [16].

Juxtaposing the two evolution generations reveals that the generations depicted SOC capabilities in response to increasingly sophisticated attacks throughout the evolution.

The earliest generation relied on a team not necessarily skilled or trained to handle information security events and incidents. Predominantly troubled by malicious code, security operations were not delivered by the establishment of a formal SOC, but in many cases by IT staff who were not necessarily solely responsible for security. This could be responsibility for device and network health monitoring, managing antivirus security across the organization, and log collection. Log collection for the first-generation SOC was limited in the number of sources and types of devices capable of producing logs, such as firewalls. In many cases, storing logging messages was done locally. In other cases, a central logging facility was provisioned to receive log information, mainly in the form of unencrypted Syslog or Simple Management Network Protocol (SNMP) messages. Unless the system administrator manually accessed and analyzed the logs, events could go unnoticed, overlooking what could potentially be an account compromise and leading to what could be considered a major security incident.

Subsequently, predominantly troubled by botnets, the next generation leveraged on the emergence of tools such as the security information and events management system (SIEM), security threat management (STM) and security event management (SEM), which delivers real-time log analysis for the purpose of threat detection. The typical second generation tool could receive, parse, normalize, and correlate the different events and eventually alert a security analyst of any attempted breach that involved human intervention such as failed login tries.

Beyond this generation was the improvement on the previous generation by including the capability of vulnerability scanning management and by usually executing tasks related to incident response during the vulnerability discovery, confirmation, and tracking phases. This improved functionality of SOCs included the practice in which vulnerabilities are discovered and confirmed, their impact is evaluated, corrective measures are identified and executed, and their status is tracked and reported until closure. Typical examples of tools used for this generation are Qualys27, nCircle28 and Rapid7 Nexpose29.

The most relatively current generation of SOCs extends the limited event correlation seen in previous generations of big data security analytics to perform real-time or offline sophisticated security analytics. The capability of fourth generation SOCs further includes data enrichment through the use of sources such as geo data, Domain Name System (DNS) data, network access control integration, and IP and domain reputation service and visualization.

Superlatively, an organization that uses technologies from the fourth generation, such as big data security analytics, should have assumed most of the SOC services from the previous generations.

Without losing sight of the essence of SOC's generational evolution, there have also been proposals on the measurement SOCs' maturity using bench-

marks. One of such is the SEI Maturity Level shown in Table 1.

The content of Table 1 is predominantly process focused with assessment of readiness, capability and its management. Security involves people, processes and technology. Emphasis from the SEI maturity model is on processes such as incident triage, incident reporting, incident analysis, incident closure, post-incident, vulnerability discovery and vulnerability remediation. The maturity model is relatively silent on the people component which involves structure, training, awareness, SOC knowledge and experience. Furthermore, the technology component of events collection, correlation, analysis, network infrastructure readiness, security monitoring, security control, vulnerability assessment, vulnerability tracking, log management and threat intelligence are equally absent from the model.

Figure 3 shows the security features that became part of the overall IT security of a matured business organization. It provides an insight into how each of the security specific points found their place in the organization. The Logical Security framework presents the defense-in-depth, layered approach to security, these consist of operations, identity and access control, data, hosts and network.

In an attempt to add context to alerts of security incidents, [19] proposed the incorporation of threat intelligence, asset, identity and other context information as another way that an effective enterprise security monitoring solution can aid the SOC analyst's investigative process. It was proposed that in addition to reporting suspicious IP addresses, information such as network flows, network

Table 1. SEI maturity level.

Maturity Level	Process Criteria
0. Nonexistent	No security policy exists.
1. Initial: Process is unpredictable, poorly controlled and reactive	Processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment to support processes. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes.
2. Managed: Process is characterized by projects and is often reactive	The document exists, and has been validated and disseminated, but it is incomplete or does not fit the context of the organization.
3. Defined: Process is characterized as a defined process	The document exists, is complete, has been validated and disseminated, and fits the context of the organization.
4. Quantitatively Managed: Process is measured and controlled	Controls are set up to assess the application of the validated document.
5. Optimized: Focus is on continuous process improvement	A regular review process allows assessing the application of the previously validated document and enables the organization to regularly update it.

Source: [17].

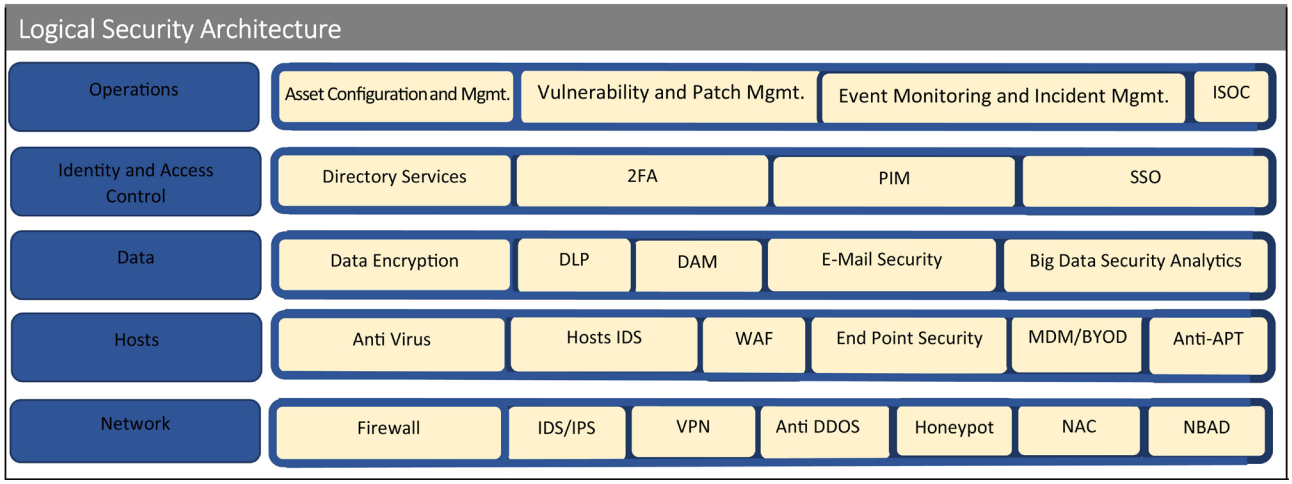

Figure 3. Logical security architecture. Source: [18].

traffic, security events, identity/asset context and endpoint data must be included in alerts and notifications. This is diagrammatically represented in **Figure 4**.

McIntyre, G. & AlFardan [17] were instructive in identifying basis for justifying any form of SOC budget, they explained the essence of responding to essential questions such as how can one detect a compromise, how severe is the compromise, what is the impact of the compromise to the business, who is responsible for detecting and reacting to a compromise, who should be informed or involved and when is the compromise dealt with once detected, how and when should a compromise be communicated internally or externally and is that needed in the first place?

In response to the questions raised, the Observe, Orient, Detect and Adapt (OODA) methodology was proposed as best approach to addressing the issues. The OODA was originally developed for military strategy and was adopted as a proposed basis for justifying SOC budgets. **Figure 5** illustrates the steps diagrammatically and in the cybersecurity context, the steps are elaborated on as follows:

"Observe: Monitor, collect, and store data from various points in your network as the first step in the OODA Loop.

Orient: Analyze collected data in search of suspicious activities. This usually involves the use of tools to process and analyze incoming and stored data.

Decide: Determine an action course based on the results of the analysis phase and the experience you have gained from previous loop iterations.

Act: Execute the action course you determined in the preceding step."

4. Synthesis and Deduction of Related Work

As earlier stated and suggested [3], a security orchestration, automation and response (SOAR) solution to the SOC challenge, Han, Park and Lee [5] proposed Enhanced Security Control (ESC) model with Blocking Prioritization

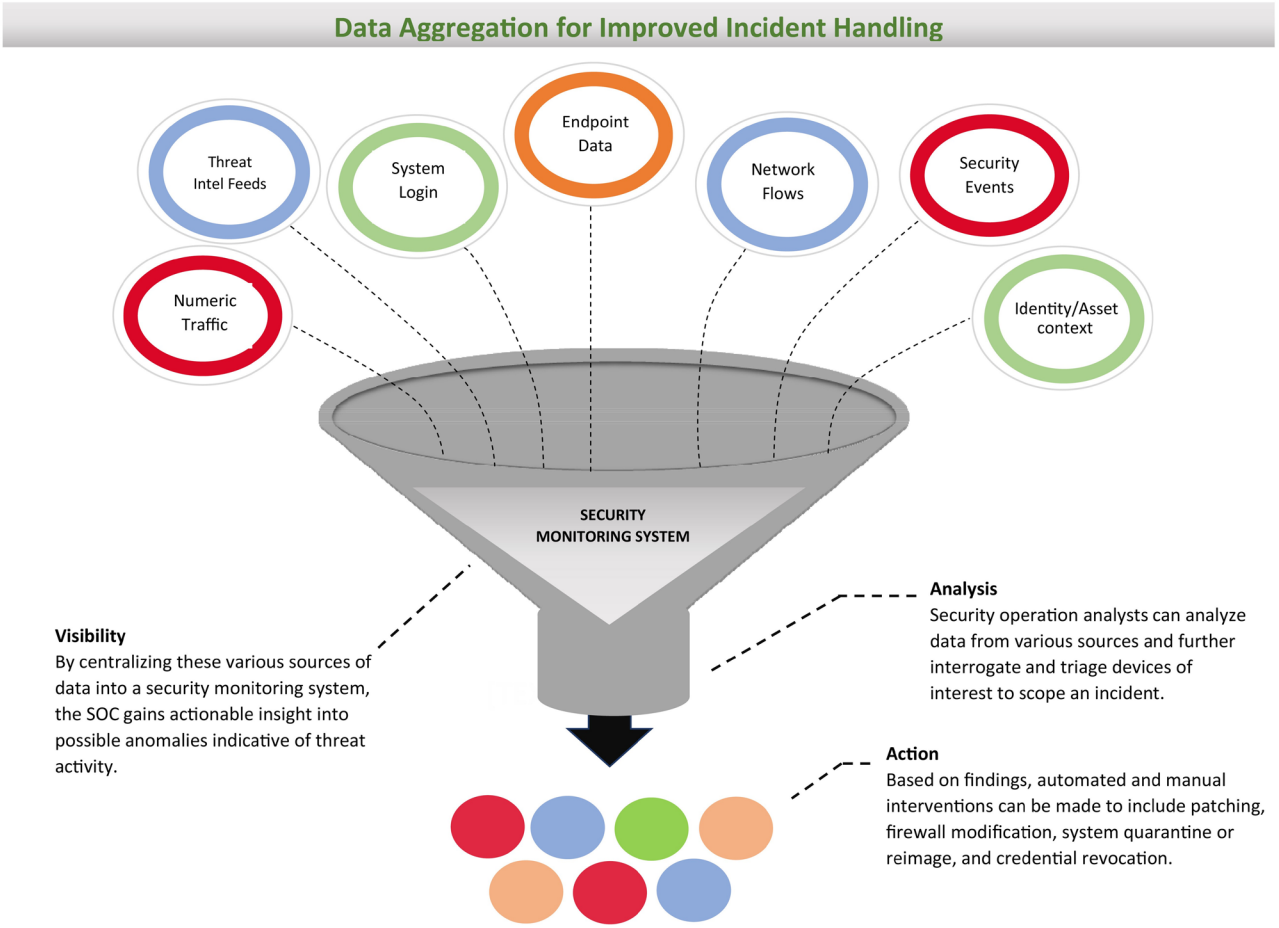

Figure 4. Compatible technologies aid detection. Source: [19].

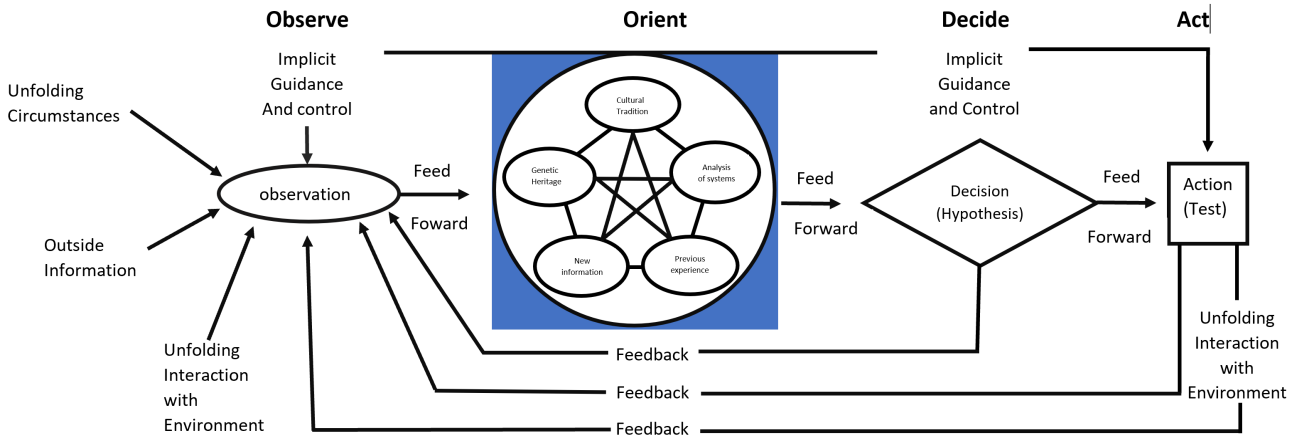

Figure 5. John Boyd's OODA loop. Source: [20].

(BP) process for critical infrastructures to improve daily incidents response activities. A proposal to improve alerts was sonification by [6] where audio signals are used to represent data. Specifically working towards addressing denial of service attack, a proposed defense mechanism consisting of the deep learning algorithm and the Extreme Learning Machine (ELM) algorithm, the Deep au-

to-encoder Extreme Learning Machine (DAELM) algorithm combines the advantages of the fast speed of the extreme learning machine and the advantages of high accuracy of the deep learning were made by [4]. Given the various generations of SOC, the SEI maturity models which serve as a guide for assessing the evolution of SOC solutions, a myriad of proposed solutions have also been reviewed; these include Ramasastri's [18] Logical Security Architecture, Compatible Technologies Aid Detection by Torres [19] and Observe Orient Decide Act (OODA) Loop by Boyd [20].

The deduction from the above mentioned related was aimed at addressing the aspects of the SOC triage, containment and escalation. **Table 2** is a summary of the deduced focus of the related work.

Evidently absent in the reviewed SOC related work is the holistic technology based automation of triage, containment and escalation of threats, vulnerabilities and incidents. This research therefore invariably sets out to attempt a solution for the automation of triage, containment and escalation. This is addressed proposal advanced in subsequent sections of this paper.

5. SOC Architecture

The SOC operations consist of technology, people and processes. In contextualizing this article, the focus is on the technological component and its automation to address the issues of triage, containment and escalation. The technology component of SOC focuses on logs of servers, traffic to and from the servers such as database servers, domain controllers and file servers as well as essential services used such as web, email etc…

Emphasis for this article is on automating the log collection, its analysis and actions to be taken in the form of remediation or containment and escalation. The people component involves various specialists of varying levels referred to as SOC Analysts. These in turn follow through various best practices as processes for logging, remediation if not done automatically, possible further escalation or closing of a ticket.

The SOC log analyzer in **Figure 6** is the most critical system in the automation of triage, containment and escalation in the SOC process. An accurate implementation of the technological solution involves connecting the device(s) to the network at the appropriate location to obtain the essential relevant data. Beyond the connection is the need for a software operating with the appropriate algorithm as shown in **Table 2** to effectively process the collected data to ensure optimal accuracy in the triage, containment and escalation of threats and vulnerabilities.

6. Proposed Framework

Further to similar and earlier work reviewed, the framework below is proposed as the way forward to comprehensively address SOC setups with the capacity to efficiently perform triage of security threats, vulnerabilities and incidents, effectively

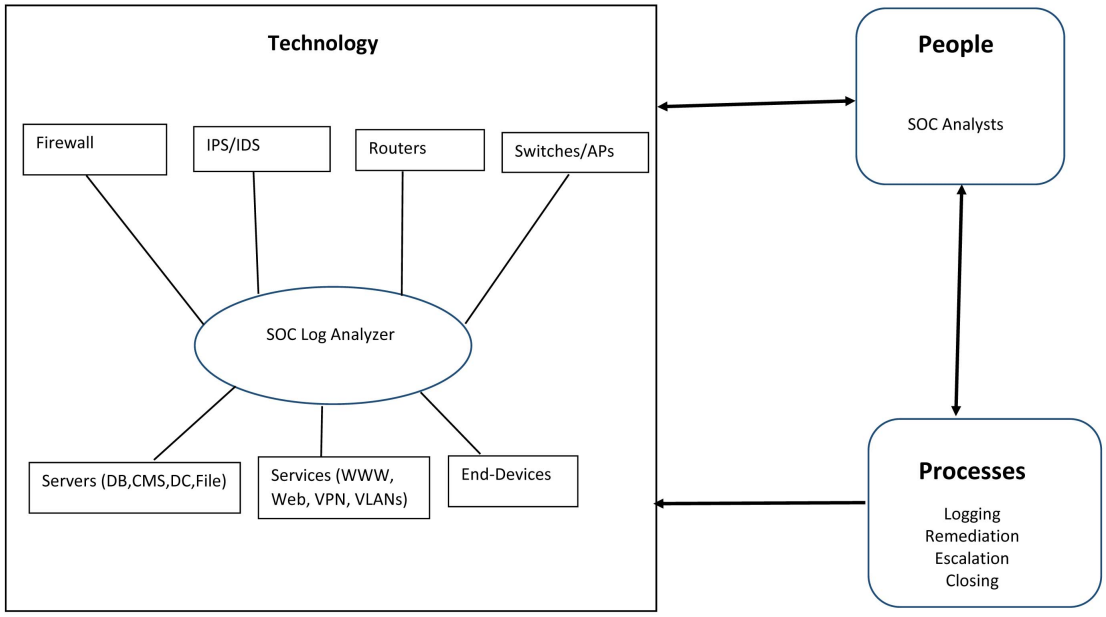

Figure 6. Schematic on SOC architecture. Source: Researcher's Field Work.

Table 2. Summary of literature on SOC triage, containment and escalation.

Researcher	Scope
Kokulu, Shoshitaishvili, Soneji, Zhao, Ahn, Bao and Doupé, 2019	Triage, Containment and Escalation
DeCusatis, Cannistra, Labouseur and Johnson, 2019	Containment
Brewer, 2019	Triage and Containment
Han, Park and Lee, 2019	Triage and Containment
Axon, Happa, Goldsmith and Creese, 2019	Escalation
Li and Zhang, 2019	Triage and Containment
Ramasastri, 2017	Triage and Containment
Ullman, D.G., 2007	Triage, Containment and Escalation

contain identified breaches and appropriately escalate for prompt and accurate solutions. The framework consists of the under listed as required processes:

1) Build Artificial Intelligence (AI) Model to cumulatively develop baseline intelligence into SOC Appliance;

2) Build AI Model to proactively and reactively intervene on identified threats and vulnerabilities;

3) Connect appliance on segments of network to passively listen in on traffic and monitor systems;

4) Events collection log, correlation and analysis;

5) Appliance develops baseline catalogue of systems and network function from learned information;

6) Reference baseline to automatically suggest configuration of thresh holds and alerts or notification;

7) Reference baseline to automatically take action to prevent a security compromise or counter a breach under control or within limits;

8) Communicate alerts or notification to experts where necessary.

1) Build AI Model to cumulatively develop baseline intelligence into SOC Appliance: The collected logs at the various sources of the network are correlated to determine logical sequences, consistent patterns and values with the objective of identifying and defining baselines of the network under investigation. The baselines are achieved by tracking and comparing events across various time periods for consistent sequences of activities. Artificial intelligence will be used to identify and define the usual traffic patterns by comparing events from multiple sources to provide more context and certainty as to patterns on the infrastructure. It can be configured to learn continuously and adapt to new evidence while detecting attacks and threats inside the network before they cause a breach.

2) Build AI Model to proactively and reactively intervene on identified threats and vulnerabilities: This component of the solution leverages on AI algorithms that are self-learning based on the developed baseline of users, devices, systems and network within an organization. It either alerts IT professionals of compliance breaches and potential threats, or proceeds to correct an observed breach where the solution can be automated. Further explanation of algorithm for baselining, remediation and escalation are depicted in Table 2.

3) Connect appliance on segments of network to passively listen in on traffic and monitor systems: The appliance must be plugged onto the network at strategic segments of the network. There must be logging at the core, distribution and access layers of the network, the logging is achieved by passively listening in on traffic to successfully baseline users, devices, and network within an organization.

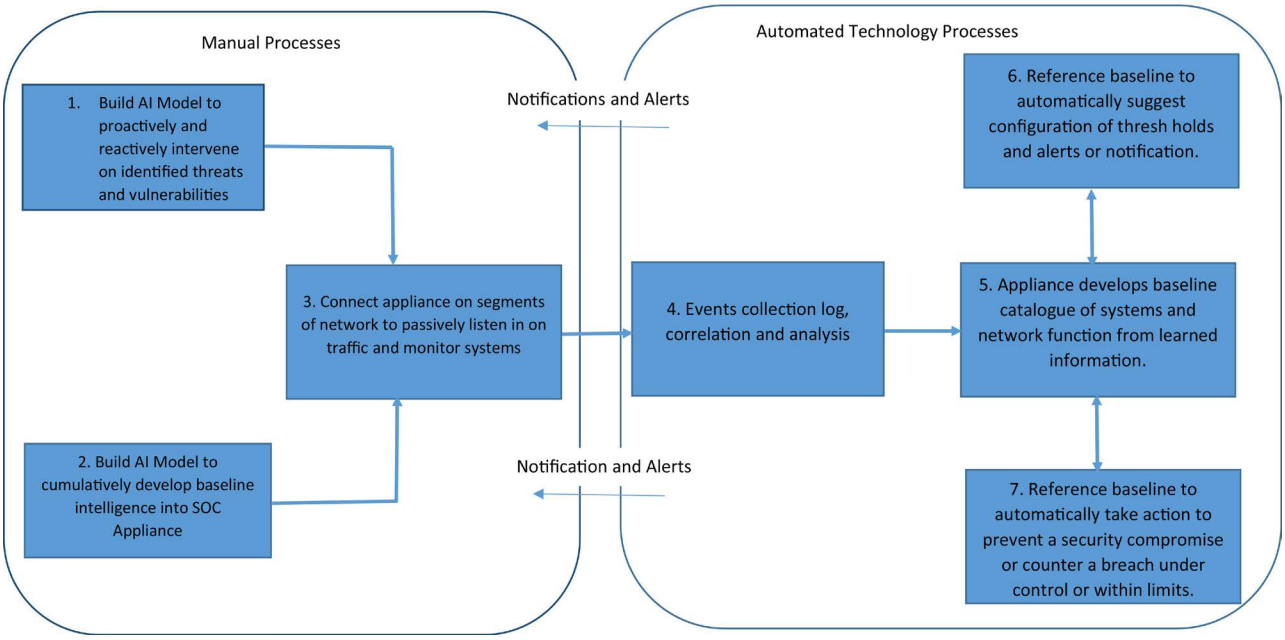

Figure 7. An automated framework for triage, containment and escalation. Source: Researcher.

The connection is done at various sources of the network for the purpose of log correlation to determine logical sequences.

4) Events collection log, correlation and analysis: Fundamental to reliably establishing accurate baselines and determine potential susceptibility to threats and inherent vulnerabilities is the need to correlate collected logs from the various sources of the network. This is automatically done to determine logical sequences, consistent patterns and values with the objective of reliably establishing accurate baselines and eliminating reports of false positive threats and vulnerabilities.

5) Appliance develops baseline catalogue of systems and network function from learned information: The appliance uses collected and correlated logs from the various sources of the network to build a starting point for making comparisons. This point for making comparisons is not static but learns continuously and adapt to new evidence of supposed starting point while detecting attacks and threats inside the network.

6) Reference baseline to automatically suggest configuration of thresh holds and alerts or notification: The established starting point is to be continuously referenced to determine the priority of addressing incidents based on the severity of the security breach or compromise. The thresh holds are automatically suggested based on the Common Vulnerability Scoring System (CVSS) which is an open industry standard for assessing the severity of computer system security vulnerabilities. The suggested thresh holds are made default configuration unless otherwise altered by human intervention.

7) Reference baseline to automatically take action to prevent a security compromise or counter a breach under control or within limits: Further to the suggested thresh holds used as default configuration unless otherwise altered by human intervention, the system could be configured to either alert support or IT professionals of compliance breaches and potential threats, or proceed to correct an observed breach where the solution can be automated.

8) Communicate alerts or notification to experts where necessary: Notifications and alerts to technical support staff are achieved by configuring the prefiltering log events into essential, relevant and meaningful alerts. IT professionals may be notified based on configuration to either address a breach and be notified of a potential breach.

The proposed algorithm focuses on automated baselining for the purposes of triage, remediation for the purposes of containment and escalation. Step 1 in the algorithm focuses on obtaining data from all relevant layers of the network namely the core, distribution and access. Additionally, data is collected from all relevant network devices and services within the scope covered by the SOC. The data is then analyzed to induce regular periodic baselines for all layers, devices and services of the network. This forms the basis for step two of the algorithm, the output determines if the automated remediation will be possible by accessing an in-built remediation capability list. The absence of a remediation capability would then require an escalation the identified threat or vulnerability to a SOC

Table 3. Algorithm for baselining, remediation and escalation.

Algorithm for Baselining, Remediation and Escalation
Step 1.0 Input
1.1 Obtain data from the access, distribution and core layers of the network
1.2 Analyze log data from Firewall, IPS/IDS, Routers, Switches, Access Points, Servers, Services and End-Devices
1.3 Induce regular periodic baseline for all layers, devices and services
Step 2.0 Output Log analysis

2.1 If Analyzed Log is Abnormal
Review In-Built Automatic Remediation Capability List
If Automatic Remediation Possible
Proceed to Remediate
Else
Escalate to SOC Analyst
End if
Else
Log Event
End if

Analyst to manually intervene. Fundamental to all these processes is the optimal operation of the system performing these SOC operations.

7. Discussion on Proposed Framework and Theory

The proposed framework suggests eight steps to efficiently perform triage of security threats, vulnerabilities and incidents, effectively contain identified breaches and appropriately escalate for prompt and accurate solutions. The proposed framework assumes the process of automatically and cumulatively developing baselines and intelligence established. Beyond that, an algorithm is proposed to proactively and reactively intervene on identified threats and vulnerabilities.

In the context of the routine activity theory mentioned earlier, the proposed solution attempts to perform the job of a suitable guardian responsible for preventing the possible commission of a crime. Very little can however be achieved by the SOC in relation to addressing issue of a motivated offender, this is because the SOC has no control over humans' motivation. The suitability of a target is feasible if the SOC is given the privilege to directly protect potential targets, thus addressing inherent weaknesses of potential targets. The proposed framework therefore provides a solution in this context via the containment component once an accurate triage has been affected.

In the context of the crime displacement theory, all actions of containment and escalation from the proposed framework provide a displacement of the crime/breach from one locale to the other. Essentially, all components of the framework are geared towards displacing any potential crime hence its implementation is fundamental to technically displacing the security breach.

8. Conclusion

This research work leveraged on a predominantly qualitative desk review and descriptive approach to collect data for analysis, deduced strengths and weaknesses for the current SOC implementations were used as a premise for proposing the framework. Supplementary to similar and earlier work reviewed, the framework is proposed as the way forward to automatically enable SOC setups with the capacity to efficiently perform triage of security threats, vulnerabilities and incidents, effectively contain identified breaches and appropriately escalate for prompt and accurate solutions. Given the constant evolution of SOC operations and capabilities coupled with the huge volumes of data collected for analysis, an efficient framework for SOC operations is essential, the proposed framework in Figure 7 therefore serves as a unique contribution that is fundamental to enhancing the SOC's ability to automatically perform triage, containment and escalation based on the algorithm in Table 3. It is recommended that further research is carried out to optimize the process of automatically and cumulatively developing baselines and intelligence to further optimize the SOC's process of performing triage, containment and escalation.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Kokulu, F.B., Shoshitaishvili, Y., Soneji, A., Zhao, Z., Ahn, G.J., Bao, T. and Doupé, A. (2019) Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. *Proceedings of the ACM Conference on Computer and Communications Security*, Limasol, Cyprus, April 2019, 1955-1970. https://doi.org/10.1145/3319535.3354239

[2] DeCusatis, C., Cannistra, R., Labouseur, A. and Johnson, M. (2019) Design and Implementation of a Research and Education Cybersecurity Operations Center. In: *Cybersecurity and Secure Information Systems*, Advanced Sciences and Technologies for Security Applications, Springer, Berlin, 287-310. https://doi.org/10.1007/978-3-030-16837-7_13

[3] Brewer, R. (2019) Could SOAR Save Skills-Short SOCs? *Computer Fraud and Security*, **2019**, 8-11. https://doi.org/10.1016/S1361-3723(19)30106-X

[4] Li, Y., Zhang, P. and Ma, L. (2019) Denial of Service Attack and Defense Method on Load Frequency Control System. *Journal of the Franklin Institute*, **356**, 8625-8645. https://doi.org/10.1016/j.jfranklin.2019.08.036

[5] Han, C.H., Park, S.T. and Lee, S.J. (2019) The Enhanced Security Control Model for Critical Infrastructures with the Blocking Prioritization Process to Cyber Threats in Power System. *International Journal of Critical Infrastructure Protection*, **26**, Article ID: 100312. https://doi.org/10.1016/j.ijcip.2019.100312

[6] Axon, L., Happa, J., Goldsmith, M. and Creese, S. (2019) Hearing Attacks in Network Data: An Effectiveness Study. *Computers and Security*, **83**, 367-388. https://doi.org/10.1016/j.cose.2019.03.004

[7] Hu, Z. and Xie, C. (2006) Security Operation Center Design Based on D-S Evidence Theory. 2006 *International Conference on Mechatronics and Automation*, Luoyang, 25-28 June 2006, 2302-2306. https://doi.org/10.1109/ICMA.2006.257690

[8] Dudovskiy, J. (2018) The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance.

[9] Cohen, L.E. and Felson, M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, **44**, 588-608. https://doi.org/10.2307/2094589

[10] Horne, C.A., Ahmad, A. and Maynard, S.B. (2016) A Theory on Information Security. *Australasian Conference on Information Systems*, Wollongong, 2016, 1-12.

[11] Bossler, A. and Holt, T. (2009) Online Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, **3**, 400-420.

[12] Cox-Johnson, R. (2009) Routine Activity Theory and Internet Crime. In: Schmalleger, F. and Pittaro, M., Eds., *Crimes of the Internet*, Pearson-Prentice Hall, Upper Saddle River, 302-316.

[13] Felson, M. and Clarke, R.V. (1998) Opportunity Makes the Thief: Practical Theory for Crime Prevention (Police Research Series Paper No. 98). Research, Development and Statistics Directorate, London. https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

[14] Rogers, R.W. (1975) A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, **91**, 93-114. https://doi.org/10.1080/00223980.1975.9915803

[15] Ortmeier, P.J. (2012) Introduction to Security: Operations and Management. 4th Edition, Pearson, London.

[16] Business White Paper 5G/SOC: SOC Generations HP ESP Security Intelligence and Operations Consulting Services (2013). http://www.cnmeonline.com/myresources/hpe/docs/HP_ArcSight_WhitePapers_5GSOC_SOC_Generations.pdf

[17] McIntyre, G. and AlFardan, N. (2015) Security Operations Center: Building, Operating, and Maintaining Your SOC. Cisco Press, Indianapolis.

[18] Ramasastri, A.S. (2017) Handbook on Information Security Operations Center, Institute for Development and Research in Banking Technology (Established by Reserve Bank of India).

[19] Torres, A. (2015) Maturing and Specializing: Incident Response Capabilities Needed. SANS™ Institute, London. http://www.cnmeonline.com/myresources/hpe/docs/Report_SANS_Incident_Response_Capabilities_Needed.pdf

[20] Ullman, D.G. (2007) "OO-OO-OO!" The Sound of a Broken OODA Loop. Robust Decisions. https://www.researchgate.net/profile/David_Ullman4/publication/268415631_OO-OO-OO_The_sound_of_a_broken_OODA_loop/links/575ea54108ae9a9c955f6091/OO-OO-OO-The-sound-of-a-broken-OODA-loop.pdf