2022

Cybersecurity Logging & Monitoring Security Program

Thai H. Nguyễn
Sacred Heart University, tvhn.433@gmail.com

Recommended Citation

Nguyễn, T. H. (2022). Cybersecurity Logging & Monitoring Security Program [Unpublished manuscript]. School of Computer Science & Engineering, Sacred Heart University.

Cybersecurity Logging & Monitoring Security Program

Thai H. Nguyen
Department of Cybersecurity
School of Computer Science & Engineering
Sacred Heart University
Fairfield, USA
nguyent62509@mail.sacredheart.edu

***Abstract*—With ubiquitous computing becoming pervasive in every aspect of societies around the world and the exponential rise in cyber-based attacks, cybersecurity teams within global organizations are spending a massive amount of human and financial capital on their logging and monitoring security programs. As a critical part of global organizational security risk management processes, it is important that log information is aggregated in a timely, accurate, and relevant manner. It is also important that global organizational security operations centers are properly monitoring and investigating the security use-case alerting based on their log data. In this paper, the author proposes a model for security logging and monitoring which details the inception, implementation, and operations of the program. This entails providing an overview of the logging and monitoring program, its purpose, and structure.**

Keywords—Cybersecurity, Logging, Machine Data, Monitoring, NIST, Security Data, Syslog, Risk Management, Security Operations Center (SOC)

I. Introduction

Global governments and economies are voyaging into a future of exponential reliance on technologies to enhance their technical and non-technical operations and processes. These reliances are spurred on by modernization of old technologies and competition with global governments and markets. In a recent 2022 Tech Trends report from Deloitte, they outline six (6) technologies that will enable incredible enhancements to organizations and their employees. Deloitte states the trends are the following [1]:

1) *Data-sharing made easy:*

> *"A host of new technologies promise to simply the mechanics of data-sharing across and between organizations while preserving the veil of privacy. As part of a growing trend, organizations are unlocking more value from their own sensitive data while leveraging enormous volumes of externally sourced data that has traditionally been off limits…" (pp.7)*

2) *Cloud goes vertical*

> *"The center of gravity around digital transformation has shifted from meeting the IT needs of an industry-agnostic organization to meeting operational needs of each sector and even subsector…" (pp.7)*

3) *Blockchain: Ready for business*

> *"Trendy cryptocurrencies and nonfungible tokens (NFTs) capture media headlines and the public imagination, but these and other blockchain and distributed ledger technologies (DLTs) are also making waves in the enterprise…" (pp.7)*

4) *IT, disrupt thyself: Automating at scale*

> *"Faced with creeping technological complexity and higher expectations of stability and availability, some CIOs are radically reengineering their IT organizations…" (pp.8)*

5) *Cyber AI: Real defense*

> *"Security teams may soon be overwhelmed by the sheer volume, sophistication, and difficulty of detecting cyberattacks. Enterprise attack surfaces are expanding exponentially…" (pp.8)*

6) *The tech stack goes physical*

> *"With the explosion of "smart devices" and the increased automation of physical tasks, IT's remit is growing again, extending beyond laptops, and phones. CIOs must now consider how to onboard, manage, and secure such business-critical physical assets as smart factory equipment, automated cooking*

robots, inspection drones, health monitors, and countless others…" (pp.8)

As organizations move to integrate and adopt these trends at breakneck speeds, it provides an increased threat surface from which cyber-attackers such as organized crime and Advance Persistent Threat (APT) groups can attack. It has been reported year-over-year cyber-attacks have been increasing at a steady pace which leverage vulnerabilities in old and new technologies. In a recent statistical report released by cybersecurity consulting company PurpleSec, some of the notable findings state the following [2]:

1) *IoT attacks were up 600% in 2017.*

2) *60% of small businesses say that attacks are becoming more severe and more sophisticated.*

3) *79% of financial CISOs said threat actors are deploying more sophisticated attacks.*

4) *69% of financial institution CISOs are planning to increase cyber security spending by 10% or more in 2019.*

5) *52% of healthcare business associates say their top vulnerability is tied to employee negligence in handling patient information.*

6) *The education industry is ranked last in cyber security preparedness out of 17 major industries.*

Technology and Cybersecurity go hand-in-hand with each other across every aspect of global societies. While there are a wide range of security management programs to protect organizations from cyber threats such as asset, control, configuration and change, vulnerability, incident management, the author of this paper is concentrating on cybersecurity risk management, primarily focused on the cybersecurity logging and monitoring functions. In this research paper, the author is proposing a cybersecurity logging and monitoring model which will utilize the syslog protocol.

The rest of this paper is organized as follows: Section 2 (Background & Related Work) provides an overview of the National Institute of Standards and Technology (NIST) Frameworks which outline industry standards for risk management, logging and monitoring, and the syslog protocol. Section 3 (Logging & Monitoring Overview) provides a detailed breakdown of the author's proposed security logging & monitoring model which entail a description of the model, the purpose of the model, and structure of the model. Section 4 (Proposed Work) provides a detailed breakdown of the management of the author's proposed logging & monitoring program, from its inception, to implementation, and finally to its operation. Finally, Section 5 (Conclusion) concludes with closing remarks on the author's security logging & monitoring program and model.

II. Background & Related work

In the following sub-sections of the Background & Related Work, the author provides an overview of the NIST Frameworks and Special Publications which have relevance to risk management and logging & monitoring [11 – 18]. In addition, the syslog protocol and its applications will be highlighted in this section [3 – 10].

A. *The National Institute of Standards and Technology (NIST)*

The author chose NIST and its work in the development and special publications of cybersecurity related standards because their work is widely accepted by all industries including public, private, and governmental organizations. There are three (3) distinct cybersecurity concepts which are relevant to the author's proposed security logging & monitoring program; they pertain to cybersecurity risk management, log management and continuous monitoring through enterprise security operation centers.

In the following the author outlines important guidance and knowledge from risk management related content proposed by NIST:

1) ***NIST Special Publication 800-37, Revision 2: Risk Management Framework for Information Systems and Organizations*** *[7]*

a) Prepare: To execute the Risk Management Framework from an organization-and a system-level perspective by establishing a content and priorities for managing security and privacy risks.

b) Categorize: The system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.

c) Select: An initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.

d) Implement: The controls and describe how the controls are employed within the system and its environment of operation.

e) Assess: The controls to determine if the controls are implemented correctly, as operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.

f) Authorize: The system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.

g) Monitor: The system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analysis, and reporting the security and privacy posture of the system.

2) ***NIST Special Publication 800-39: Managing Information Security Risk*** *[5]*

a) Framing Risk: Establishes the context and provides a common perspective on how organizations manage risk. Risk framing, as its principle output, produces a risk management strategy that addresses how organizations intent to assess risk, respond to risk, and monitor risk.

b) Assessing Risk: Risk assessment identifies, prioritizes, and estimates risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, *individuals, other organizations, and the Nation, resulting from the operation and use of information systems. Risk assessments use the results of threat and vulnerability assessments to identify and evaluate risk in terms of likelihood of occurrence and potential adverse impact (i.e., magnitude of harm) to organizations, assets, and individuals.*

c) Responding to Risk: Risk response identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.

d) Risk Monitoring: Risk monitoring provides organizations with the means to: (i) verify compliance; (ii) determine the ongoing effectiveness of risk response measures; and (iii) identify risk-impacting changes to organizational information systems and environments of operation. Analyzing monitoring results gives organizations the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed.

3) ***NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)*** *[9]*

ERM Playbook:

a) Identify the Context: Context is the environment in which the enterprise operates and is influenced by the risks invovled.

b) Identify the Risks: This means identifying the comprehensive set of positive and negative risks --- determining which events could enhance or impede objectives, including the risks of failing to pursue an opportunity.

c) Analyze the Risks: This involves estimating the likelihood that each identified risk event will occur, and the potential impact of the consequences described.

d) Prioritize the Risks: The exposure is calculated for each risk, based on likelihood and potential impact, and the risks are then prioritized based on their exposure.

e) Plan and Execute Response Strategies: The appropriate response is determined for each risk, with the decisions informed by risk guidance from leadership.

f) Monitor, Evaluate, and Adjust: Continual monitoring ensures that enterprise risk conditions remain within the defined risk appetite levels as cybersecurity risks change.

4) ***Framework for Improving Critical Infrastructure Cybersecurity*** *[6]*

The Five (5) Framework Core Functions:

a) Identify --- Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

b) Protect --- Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

c) Detect --- Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

d) Respond --- Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

e) Recover --- Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

5) ***NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations*** *[10]*

PM-9 Risk Management Strategy

Control:

a) Develops a comprehensive strategy to manage:

1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b) Implement the risk management strategy consistently across the organization; and

c) Review and update the risk management startegy or as required, to address organizational changes.

6) ***NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*** *[8]*

The five (5) Privacy Framework Functions:

a) Identify-P: Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

b) Govern-P: Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

c) Control-P: Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

d) Communicate-P: Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.

e) Protect-P: Develop and implement appropriate data processing safeguards.

The author recognizes the vast breath and depth of research and development undertaken by NIST to provide a substantial knowledgebase to approaching cybersecurity risk management. While this paper only highlighted the important knowledge sections of each framework and special publications; this is due to sheer volume of information in each content. This work provided the author with organizational best practices to conduct cybersecurity risk management. An important aspect of the cybersecurity risk management functions that stood out to the author encompass detection and monitoring. This leads into the next critical concept which influenced the author’s proposed logging & monitoring program; this is the concept of detection which is achieved through log management. NIST provides incredible guidance and knowledge to approach this cybersecurity process in a structured and methodical manner.

In the following the author provides a summary of each critical aspect in managing security logs.

7) NIST Special Publication 800-92: Guide to Computer Security Log Management [4]

a) Log Management Infrastrucutre

A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data. Log management infrastructures typically perform several functions that support the analysis of events, such as filtering, aggregation, normalization, and correlation. The infrastructures also provide assistance in making log data accessible and maintaining it through functions such as log parsing, viewing, analysis, rotation, and archival, as well as log file integrity checking [pp.3-11].

b) Log Management Planning

To establish and maintain successful log management infrastructures, an organization should perform significant planning and other preparatory actions for performing log management. This is important for creating consistent, reliable, and efficient log management practices that meet the organization's needs and requirements and also provide additional value for the organization [pp.4-10].

c) Log Management Operational Processes

System-level and infrastructure administrators should follow standard processes for managing the logs for which they are responsible. The major operational processes for log management are configuring log sources, performing log analysis, initiating responses to identified events, and managing long-term data storage [pp.5-11].

The guidance and knowledge outlined by NIST SP 800-92 provides critical mile-markers for organizations seeking to architect, implement, and operate their own log management on-premises or solutions organizations providing log management as a service business model. The author recognizes the in-depth detail and best practices outlined by NIST SP 800-92, which provided the inspiration for the author's inception and implementation for their logging & monitoring program. To achieve the critical function of continuous monitoring; global organization's security operation centers (SOCs) are at the tip of the spear.

In the following the author provides an overview of security operation center services and functions.

B. *Security Operations Center (SOC) [14 – 17]*

Security operation centers were formed by organizations or outsourced from 3rd party security services to tackle increased threats, growing regulatory, and compliance requirements to enterprise technology assets [14 – 17]. SOCs provide critical enterprise cybersecurity services, which Jacobs et al. outline comprehensively in the following [17]:

1) *Log Collection;*
2) *Log Retention and Archival;*
3) *Log Analysis;*
4) *Monitoring of Security Environment for Security Events;*
5) *Diversity of devices integrated;*
6) *Event Correlation and Workflow;*
7) *Incident Management;*
8) *Reaction to threats;*
9) *Threat Identification; and*
10) *Reporting*

While these are some of the many services SOCs provide to organizations that they belong to, they do not convey the entire picture of mature SOC operations as new demands and services are required of them from emerging threats. The author's work focuses on the primary services of log collection, retention and archival, analysis, and monitoring of security environment for security events. These functions can be organized into three (3) components which are collection, analysis, and monitoring [15].

In the following the author provides a highlight of the syslog protocol which facilitates cybersecurity logging & monitoring.

C. *Syslog (Current: RFC 5424, Prior: RFC 3164)*

System Logging Protocol, commonly known as syslog, was originally proposed by C. Lonvick from Cisco Systems in 2001 under RFC 3164, which has been superseded by RFC 5424 under R. Gerhards from Adiscon Gmbh in 2009 [3]. This protocol outlines the standards used to transmit system log or event messages to a syslog server. As outlined in the previous sections, syslog is the primary protocol used to collect, analyze, and monitor for security operation centers. A few of the most important concept of the syslog protocol are outlined in the following [3]:

1) *Syslog Transmission*
   - *User Datagram Protocol: Port 514*
   - *Transmission Control Protocol: Port 1468*
2) *Syslog Message Format*

   Parts:
   - *PRI (priority value)*
   - *Header (identification information)*
   - *Message (message content)*
3) *Message Length*
   - *1024 bytes*

It is important to mention that a security consideration in implementing a logging & monitoring program using syslog data is the inherent lack of security of the syslog protocol. The protocol does not have authentication baked in to ensure the log data is originating its intended system. The log data is also travelling across the wire in plaintext, which allows attackers to implement attacks such as playback attacks which allows the attackers the ability to generate illegitimate log data. This can cause log poisoning and can have detrimental outcomes for SOC functions.

The author has outlined the work proposed by NIST to achieve successful cybersecurity risk and log management, as well as the importance of having a security operations center to monitor cybersecurity risks and logs. In addition, the author provided a brief overview of the syslog protocol which facilitates these important cybersecurity functions. In the next section, the author outlines the security logging & monitoring program.

III. Logging & Monitoring Model Overview

In the following sub-sections of the Logging & Monitoring Overview, the author provides a detailed description of the author's logging & monitoring program, its purpose, and its structure. Using the inspirations provided to the author by NIST, the author outlines the following:

A. Description

With the explosion of ubiquitous computing in global societies, the amount of log data from these new sources will become a monumental task for global organizations to collect, analyze, and monitor for security threats. This requires security operation center teams to be equipped with the necessary processes, technologies, and tools to be able to successfully research, investigate, and mitigate security threats. To achieve success, a mature log management and continuous monitoring which leverages specialized use-case alerting is required.

B. Purpose

The purpose of a mature log management and continuous monitoring which leverages specialized use-case alerting is required because it will enhance:

1) Industry Specific Regulartory & Compliance

- *Federal Information Security Management Act of 2002 (FISMA)*
- *Gramm-Leach-Bliley Act (GLBA)*
- *Health Insurance Portability and Accountability Act of 1996 (HIPPA)*
- *Sarbanes-Oxley Act (SOX) of 2002*
- *Payment Card Industry Data Security Standard (PCI DSS)*

2) Threat Specifics

- *Advanced Persistent Threats (APT)*
- *Hacktivists*
- *Insider*
- *Script-kiddies*
- *Malware Strains*

The author recognizes the complexity when approaching logging & monitoring for a wide range of industries, organizations, and governments. It is acknowledged that there are some regulatory, compliance, and threat crossovers between organizations. There will be increased separation as IoT and other smart devices become saturated, for example, mobile device enable systems and satellite-based systems. These systems will carry additional threats and risks from which organizations must perform risk management processes and mitigate for.

C. Structure

Based on the work of NIST SP 800-92 [4], the structure of the logging & monitoring program will be outlined as follows:

1) Logging

a) Types of Log(s)

- *Security Logs: Contain security related data which are generating from a multitude of sources including but not limited to antimalware, IDS, IPS, vpn, proxy, vulnerability assessment and management, authentication servers, router, firewalls, and bastion networks.*
- *Operating System Logs: Contain general system level event data, including a multitude of system wide usage I/O operations, but usually all system events will generate with a timestamp, status code, and error codes.*
- *Application Logs: Contains operation and usage events of the application such as client and server create, read, update, and delete (CRUD) operations. These logs can also include security events such as successful and failed authentication attempts, brute-force attacks, and escalation of privilege attacks.*

b) Log Generation & Storage

Logs will be expected to generate from the following:

- *Windows, Mac, Linux, and Unix based systems.*
- *Server, Desktop, Laptop, Tablet, Ultrabook, Mobile, Smart Devices*

Logs will be stored in the following architecture:

- *On-premises Configuration*
- *Multiple log concentrators (collection server)*
- *Logs will be replicated with a ratio of 1 primary to 3 backup servers.*

c) Security Information & Event Management (SIEM)

In this paper the author will be utilizing a fictious SIEM system called Odin Sight. This SIEM system was developed by the author for the purpose of this research, which replicate existing industry SIEM systems [11 – 13].

Odin Sight is a next generation Security Information and Event Management (SIEM) system that will provide clients a set of security tools and services to holistically view and manage their organization's cyber infrastructure. Odin Sight achieves advantages over the competition by providing on-premises and cloud implementation of our next generation data collection, policy enforcement, data consolidation and correlation, and security event notifications. To achieve the advantages listed, Odin Sight collects and analyzes log data from enterprise cyber information systems on-premises and cloud integration, including network devices, operating systems, applications, and user activities. Log data are collected and analyzed in real-time, enabling clients to quickly identify malicious threats and automatically stop malicious attacks on the cyber infrastructure. Odin Sight is able to integrate industry intelligence feeds into the platform to provide the client enhanced capabilities in the increasingly dynamic realm of information security. Odin Sight provides the client with convenient and secure access to the SIEM platform via our dedicated application software or web browser interface.

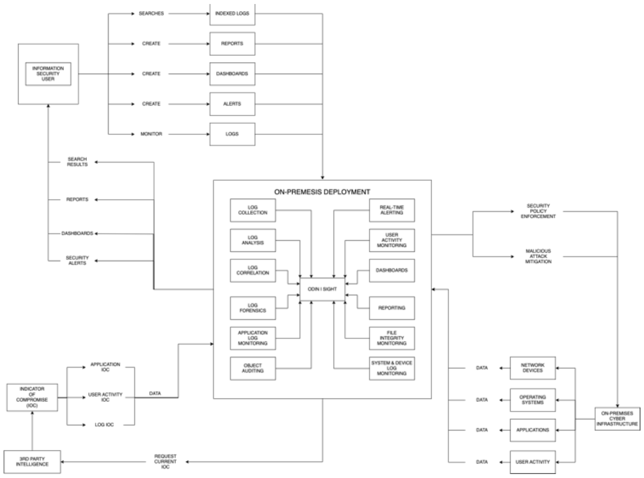

Figure 1: Odin Sight, Dataflow

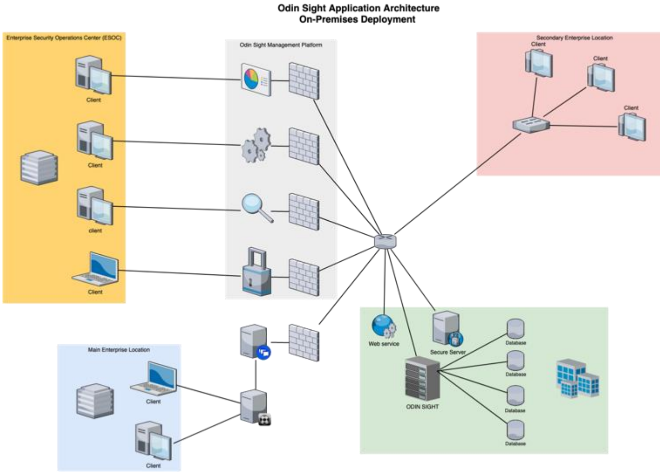

Figure 2: Odin Sight, Application Architecture

2) *Monitoring*

a) User-case Developers

Use-case developers are cybersecurity engineers which understand security and non-security log data, Odin Sight platform, and cybersecurity researching capabilities. They utilize cybersecurity threat intelligence from all open and closed sources to develop threat alerting. They will use log data to replicate threat signatures and alert to the security operation center for further investigation and potential mitigation.

b) Security Operation Center

Security Operation Center teams and analysts will monitor use-case developed by the use-case developing team. They will use a feedback loop to provide any suggestions, improvements, and deprecations of use-cases based on the evolving risk tolerance of enterprise assets.

In the next section, the author outlines their proposed work for the inception, implementation, and operations of their security logging & monitoring program.

IV. Proposed Work

The author's proposed security logging & monitoring model is developed under the assumption an organization is implementing an on-premises logging & monitoring program. This entails architecting, designing, and operating their own log collection and storage.

The author's logging & monitoring program will entail three (3) phases:

A. *Inception*

Inception phase begins with senior management conducting a comprehensive cybersecurity risk assessment of the organization. In this proposed work, the author will be utilizing NISTIR 8286, please refer to Background & Related Work part 3 for the steps outlined. Once the risk assessment has been completed with senior management approval, the next step is outlining the strategies, policies, and requirements for an organization-wide security logging & monitoring program. Once this step is completed, the organization will move into the implementation stage of the security logging & monitoring program.

B. *Implementation*

Implementation phase will primarily involve the design, architecting, and engineering the organization's log management infrastructure. In this function some considerations must be taken, they are the following [4]:

1) Log Generation: In this process, hosts from a number of sources are inventoried that will be sending logs to log collectors. Log data is also defined in a specific format to normalize the data traveling across the wire.

2) Log Analysis and Storage: In this process, log collectors or aggregators will receive and replicate log data. Log data will also be analyzed by initial metadata either by real-time or near-real-time transference.

3) Log Monitoring: In this process, raw log data is monitored and reviewed by log engineers to ensure proper data normalization and intgrity is maintained across the wire.

4) Log Security: In this process, syslog security implementations are evaluated and deployed. The security implemenations include reliable log delivery via TCP and backup routes, transmission confidentiality protection via TLS, and transmission integrity protection and authentication via SHA-1 or stronger.

Once the organization's logging architecture has moved from development to staging, and is about 80% progress towards production, this phase will begin to pull security operations center senior management and engineers to begin formulating and developing strategies, playbooks, and organize teams to create use-case alerting and monitor these alerts.

C. *Operation*

Operation phase begins to steadily mature the organization's security logging & monitoring program through continuous cross-functional communications between security teams, such as vulnerability assessment and management, threat intelligence, red team, blue team, purple team, security partners, and open-source intelligence community.

In this phase, use-case developers will utilize a structured development lifecycle such as agile to create security use-case alerting for the organizations. This will involve steps of research, development, testing, and peer-review as the use-case moves from development to production. These cybersecurity engineering teams will also handle enterprise specific threat alerting, internal organization requests for alerting such as web application teams. The maturity of the use-case alerts will be continuously evaluated based on evolving cyber risks and organizational risk tolerance. As new log sources continue to aggregate into Odin Sight, this will provide cybersecurity engineers new sources of enrichment to existing and new use-case alerts.

As use-case alerts move into production to be monitored by the security operations center teams, there is a continuous assessment and evaluation of the use-case alerts by cybersecurity engineers. This can be because of multiple factors including but not limited to, threats have increased or increased on the specific asset and threat investigations have revealed additional data points which require alert adjustments. There is a symbiotic relationship between the use-case developers and the security operations center which continuous feedback loops of improvements and collaboration.

In the next section, the author concludes with a review of the proposed security logging & monitoring model.

V. Conclusion

In conclusion, the author provided an overview of the frameworks and special publications from the National Institute of Standards and Technology that pertain to cybersecurity risk and log management, as well as a brief history of the syslog protocol which facilitates a vast majority of the enterprise logs and the security operations center team which monitors security threats using logs. These concepts were used as an inspiration for the author's work in developing their security logging & monitoring program. The author provided an overview of their proposed security logging & monitoring model which included a description, purpose, and structure of the model. This finally led to the author's detailed proposed work which outlined the inception of the security logging & monitoring program, how the program would be implemented, and lastly, the continuous operations of the security logging & monitoring program with a collaborative effort between use-case developers and security operation center teams.

References

[1] Deloitte, "Deloitte Insights: Tech Trends 2022", Accessed: Feb 2022. https://www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf

[2] PurpleSec, "2021 Cyber Security Statistics: The Ultimate Lists of Stas, Data & Trends", Accessed: Feb 2022. https://purplesec.us/resources/cyber-security-statistics/

[3] R. Gerhards, "The Syslog Protocol", Network Working Group, RFC: 5424, Adiscon Gmbh, Mar. 2009.

[4] K. Kent and M. Souppaya, "Guide to Computer Security Log Management", NIST Special Publication 800-92, Recommendations of the National Institute of Standards and Technology. Sep. 2006

[5] J. T. Force and T. Initiative, "Managing Information Security Risk: Organization, Mission, and Informaiton System View", NIST Special Publication 800-39, Mar. 2011.

[6] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", Feb. 12, 2014.

[7] J. T. Force, "Risk Mangement Framework for Information Systems and Organizations", NIST Special Publication 800-37, Rev. 2, Dec. 2018. https://doi.org/10.6028/NIST.SP.800-37r2

[8] National Institue of Standards and Technology, "NIST Privacy Framework", Jan. 16, 2020. https://doi.org/10.6028/NIST.CSWP.01162020

[9] K. Stine, S. Quinn, G. Witte and R. K. Gardner, "Integrating Cybersecurity and Enterprise Risk Mangement (ERM)", NIST, Oct. 2020. https://doi.org/10.6028/NIST.IR.8286

[10] J. T. Force, "Security and Privacy Controls for Information Systems and Organizations", NIST Special Publication 800-53, Rev. 5, Sep. 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[11] Y. Taguchi, A. Kanai and S. Tanimo, "A Distributed Log Management Method using a Blockchain Scheme", 2020 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2020.

[12] N. Sukma, W. Srisawat, P. Sa-nga-ngam and A. Leelasantitham, "An Analysis of Log Management Practices to Reduce IT Operational Costs Using Big Data Analytics", The 2019 Technology Innovation Management and Engineering Science International Conference (TIMES-iCON2019), IEEE, 2019.

[13] F. Rivera-Ortiz and L. Pasquale, "Automated Modelling of Security Incidents to Represent Logging Requirements in Software Systems", ARES 2020, ACM, 2020.

[14] A. K. Jain, A. Bhargava and A. Rajput, "Role of Log Management in Information Security Compliances", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 4, April 2016.

[15] C. Onwubiko, "Cyber Security Operations Centre: Security Monitoring for protecting Business and supporting Cyber Defense Strategy", IEEE Xplore, Accessed: 2022.

[16] A. Madani, S. Rezayi and H. Gharaee, "Log Management comprehensive architecture in Security operation Center (SOC)", IEEE, 2011.

[17] P. Jacobs, A. Arnab and B. Irwin, "Classification of Security Operation Centers", IEEE Xplore, 2013