System Information Event Management (SIEM) Solutions in the Navy Continuous Training Environment (NCTE): Implementation, Authorization, and Implications

Ritz Carr

Navy Surface Warfare Center Corona

August 4th, 2023

TABLE OF CONTENTS

LIST OF ACRONYMS

ATO – Authorized To Operate

CCI – Control Correlation Identifier

CONMON – Continuous Monitoring

COTS – Commercial Off The Shelf

CS – Cybersecurity

CSS – Cybersecurity Strategies

CTH – Cyber Threat Hunting

CUI – Controlled Unclassified Information

DAR – Data At Rest

DISA – Defense Information Systems Agency

DOD – Department of Defense

DON – Department of the Navy

EL – Event Logging

ES – Enterprise Security

EU – European Union

GDPR – General Data Protection Regulation

ISO – Information System Owner

IT – Information Technology

NAVSEA – Naval Sea Systems Command

NCTE – Navy Continuous Training Environment

NETTN – Navy Enterprise Tactical Training Network

NSWC - Naval Surface Warfare Center

OMB – Office of Management and Budget

RMF – Risk Management Framework

RMP – Risk Management Process

RMFKS – RMF Knowledge Service

RMFKSSCE – RMFKS Security Controls Explorer

SDLC – Software Development Life Cycle

SIEM – System Information and Event Management

SEM – System Event Management

SIM – System Information Management

SOAR – Security Orchestration, Automation, and Response

STIG – Security Technical Implementation Guide

TTP – Tactics, Techniques, and Procedures

UBA – User Behavioral Analytics

WWW – World Wide Web

INTRODUCTION

According to the InfoSec Institute, there are two approaches to strengthening cybersecurity posture: proactive and reactive. Cyber Threat Hunting (CTH) is an example of the proactive approach for network defense. The reactive approach is associated with detection as the trigger is the catalyst for defense. This is accomplishable by a System Information Event Management (SIEM), which alleviates the difficulty monitoring entire network for irregularities. The DOD's process for implementing new tools, systems, and concepts is rigorous and abundant, requiring an Authorization To Operate (ATO) and continuous compliance with DOD policy. With this, the system will have permission to operate on the network. SIEMs are difficult systems to integrate due to implications such as reliance on human factors such as advanced threat intelligence and correlation rules (Cinque et al., 2018). Both proactive and reactive approaches can be used in concert to make a resilient network.

The goal of this proposal is to understand the importance of evaluating what our network requires for a SIEM to be implemented and consistently compliant with DOD policy. The policy helps with making the SIEM an effective network defense and monitoring tool. In the Navy Enterprise Tactical Training Network (NETTN), how can a SIEM be implemented while abiding by DOD policy to make it an effective network defense tool?

PURPOSE

LogRhythm is the current SIEM used by the NETTN. Over the past few years, NETTN has shifted to an enterprise scale that has increased the volume of data ingestion. The current configuration of LogRhythm cannot support this increase nor data storage requirements and Data At Rest (DAR). It is no longer DOD-compliant, requiring NCTE to search for another SIEM solution increasingly scalable. Without LogRhythm being DOD-compliant, network defense fails to be optimal.

Despite selecting a new SIEM, the implementation process is different from when LogRhythm was acquired. This is due to a multitude of factors including those that outdate LogRhythm for our network. To achieve an ATO, SIEM capabilities and implications must be understood in addition to organizational policies.

SCOPE

The SIEMs solution needs to be adaptive to the NETTN environment, not possible with the current solution, LogRhythm. It is unable to meet all organizational and DOD requirements given the new configuration of NETTN.

The scope of this study is limited to Naval Surface Warfare Center (NSWC) Corona Controlled Unclassified Information (CUI), the World Wide Web (WWW), and the professional testimony of personnel in the Range System Engineering Division of NSWC Corona. Due to the rapid evolution of the cybersecurity field, sources besides policies are limited to, at most, five years before this document.

INTENDED AUDIENCE

This research is intended for those with knowledge of federal cybersecurity compliance and SIEM solutions apart of Navy Continuous Training Environment (NCTE)'s NETTN and other Federal institutions to consider possible implications in implementing a SIEM such as Splunk Enterprise Security (ES) following DOD policy.

DEFINITIONS

CYBER THREAT HUNTING (CTH)

Cyber Threat Hunting (CTH) is the proactive searching for cyber threats such as adversary Techniques, Tactics, and Procedures (TTPs) in a network. As cyber threats evolve, so must our methods at detecting, eradicating, and preventing them. CTH is a process that should be a continuous process with the assumption that an adversary is always present in the network (Taschler, 2023).

EVENT LOGGING MATURITY LEVELS (ELs)

Outlined in the Office of Management and Budget (OMB) Memorandum M-21-31 are the Event Logging (EL) Maturity levels in four tiers, 0 to 3:

Table 1: Summary of Event Logging Tiers

Event Logging Tiers	Rating	Description
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met
EL1	Basic	Only logging requirements of highest criticality are met
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met
EL3	Advanced	Logging requirements at all criticality levels are met

These tiers were created to "accelerate incident response efforts and to enable more effective defense" of all DOD Information Technology (IT) systems and their information. Within each tier are requirements to achieve the EL rating for that tier and the previous tier requirements (Young, 2021).

NAVY CONTINIUOUS TRAINING ENVIRONMENT (NCTE)

NCTE is the organization that contains the NETTN used by the Navy for Live Virtual Constructive (LVC) exercises that train their sailors in warfighting capabilities and readiness. LVC is an effort to combine real system operators like ranges (L) with operating simulators and or simulated systems (V) using computer-generated forces that augment both environments (C). NSWC Corona maintains and operates the network, owned by its Information System Owner (ISO), the Fleet Forces Command (NSWC Corona – What we do, 2023) (NSWC Corona – CITO Brief, 2023).

SECURITY CONTROLS

NIST defines security controls as: "A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements." (NIST – Information Technology Library). Controls can be administrative, physical, and technical and are selected to fulfill cybersecurity requirements set by the organization (NIST, 2013) (RMFKS, 2016).

SYSTEM INFORMATION EVENT MANAGEMENT (SIEM)

In 2005 the SIEM, a combination of both System Event Management (SEM) and System Information Management (SIM), was born (Fortra). The SIEM is a single aggregated location of

collected, stored, and correlated event data from various sensors connected to it. The system's capabilities consist of the following: "real-time behavioral anomaly detection, faster incident management, and intelligent visualization of the network and all its interconnected nodes" (Diaz et al., 2021). SIEMs also analyze security events and prioritize threats, possible with the following features: risk analysis, reaction and reporting, correlation rules, and security (Fortra).

REFERENCES

Cinque, Marcello; Cotroneo, Domenico; Pecchia, Antonio. Oct, 2018. "Challenges and Directions in Security Information and Event Management (SIEM)." *IEEE.* *https://ieeexplore.ieee.org/abstract/document/8539170*.

Diaz, Rodrigo; Gonzalez-Granadillo, Gustavo; Gonzalez-Zarzosa, Susana. Jul. 12, 2021. "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures." *Sensors (Basel)*.

Fortra. n.d. "What Is Siem?" What Is SIEM? Meaning, Function, and Benefits | Core Security, www.coresecurity.com/siem.

NIST. Apr. 2013. *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST SP 800-53r4.

NIST. n.d. "Security Control - Glossary: CSRC." NIST - Information Technology Library. csrc.nist.gov/glossary/term/security_control.

NSWC Corona. 2023. "Corona Division Departments". *NAVSEA.* https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Corona/What-We-Do/

RMFKS. Jun 14, 2016. "Introduction to Security Controls." RMF Knowledge Service (RMFKS). www.nist80037rmf.com/rmf-knowledge-service-rmfks/.

Taschler, Scott. Apr. 27, 2023. "What Is Cyber Threat Hunting? [Proactive Guide] - Crowdstrike." Crowdstrike.Com. www.crowdstrike.com/cybersecurity-101/threat-hunting/.

Young, Shalanda. Aug. 27, 2021. “Memorandum For The Heads of Executive Departments and Agencies: Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents.” OMB M-21-31.