شـــركـة نـواة للـطـاقـة
Nawah Energy Company

SEC-PRC-4516

Consolidated Security Operations Center (CSOC) Content Framework

Revision 00

Safety Classification:

Non-Safety Related

Usage Level:

Information Use

SME:	Andrea Amor Castillo
Preparer:	Nathan F. Gibbs
Approval:	Electronically Approved by Salem Al Shamsi
Issued:	28 April 2021

BNPP Non Unit Related

Nawah-DCRM

Digitally signed by Nawah-DCRM
DN: cn=Nawah-DCRM, o=Nawah Energy Company, ou=Nawah-DCRM, email=laarni.olarte@nawahprogram.ae, c=AE
Date: 2021.04.28 10:31:24 +04'00'

REVISION SUMMARY (Previous revision history not listed can be obtained from DCRM)		
Revision Number	**Description**	**Date**
00	Initial issuance.	28 Apr 2021

Table of Contents

1.0 PURPOSE AND SCOPE

1.1 Purpose

1.1.1 The purpose of Content Framework is to describe how the Consolidated Security Operations Center (CSOC) builds Security Information and Event Management (SIEM); Security Orchestration, Automation, and Response (SOAR); and User and Entity Behavior Analytics (UEBA) content to improve its detection (e.g., SIEM use cases, UEBA use cases, SIEM correlation rules, SOAR playbooks). The CSOC Content Framework is the basis of how CSOC will develop better content on a high level.

1.1.2 This procedure provides the guidance needed in terms of methodology and the supporting layout. CSOC will use it to bridge the essential gap between technical issues, business risks, and the regulatory control and compliance requirements related to Continuous Security Monitoring (CSM) of the organization's valuable assets.

1.1.3 The methodology described as part of the Content Framework aims to ensure quality, control, and reliability of SIEM, SOAR, and UEBA content design and implementation. The supporting layout will allow CSOC to formalize all relevant contributions to the use cases by providing a specific naming convention for easier integration with SOAR playbooks and incident categorization.

1.1.4 The framework will support the identification and arrangement of technical, organizational, and business requirements. It will also facilitate definition of the detection rule implementation criteria used by the CSOC to discover any potential threats within the organization and respond to them effectively with procedures/playbooks identified as relevant for the specific scenario under analysis.

1.2 Scope

1.2.1 This procedure covers the following:

A. How CSOC builds content to improve its detection.

B. How CSOC develops and implements better content.

1.2.2 This document describes the well defined content development lifecycle used in creating content.

2.0 APPLICABILITY

2.1 This procedure applies to all CSOC employees of Nawah and BOC Enterprise including consultants, contractors, visitors, and seconded individuals.

3.0 REFERENCES AND REQUIREMENTS

3.1 Implementing

None

3.2 Developmental

3.2.1 SEC-MAN-4501, Consolidated Security Operations Center (CSOC) Use Case Operation Manual

3.2.2 SEC-PRC-4500 (BSI), Consolidated Security Operations Center (CSOC) Analysis and Response

3.2.3 SEC-PRC-4514, Consolidated Security Operations Center (CSOC) Content Development

3.3 Statutory/Regulatory

3.3.1 Dubai Information Security Regulation (ISR)

3.3.2 ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

3.3.3 National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF)

3.3.4 Signals Intelligence Agency (SIA) Standards

3.4 Non-Regulatory

3.4.1 NEI 08-09, Rev. 6, Cyber Security Plan for Nuclear Power Reactors

3.4.2 NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide

4.0 TERMS AND DEFINITIONS

4.1 **Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)** – A framework for describing the actions an adversary may take while operating within an enterprise network. It provides a detailed characterization of adversary behavior in the different stages of a cyber kill chain or a cyber-attack lifecycle.

4.2 **Consolidated Security Operations Center (CSOC)** – An organization unit that monitors, assesses, and defends the organization information systems (websites, applications, databases, data centers, servers, networks, desktops, and other end points) against any information security attacks.

4.3 **Content** – Advanced Security Information and Event Management Tool (SIEM) correlation rules, use cases, scripts, queries, templates, alerts, data repositories, reports, and dashboards to detect well-known and emerging threats.

4.4 **Correlation Rule** – Rule created in the SIEM that scans multiple data sources for defined patterns. When the search finds a pattern, it performs an adaptive response action.

4.5 **Critical Digital Asset (CDA)** – A digital computer, communication system, or network that is:

4.5.1 A component of a Critical Digital System (CDS) including:

A. Assets that perform Safety-Related and Important-to-Safety functions, Security functions, Safeguards functions, and Emergency Preparedness functions, including offsite communications (SSSEP functions).

B. Assets that provide support to, protect, or provide a pathway to CDSs.

4.5.2 A support system asset whose failure or compromise as the result of a cyber-attack would result in an adverse impact to an SSSEP function.

4.5.3 Any digital Structure, System, or Component (SSC) that provides an operator with the only indication they will use to take a plant action that could adversely impact an SSSEP function.

4.6 **Critical Digital System (CDS)** – A system that is associated with or provides SSSEP functions, or support systems and equipment that, if compromised, would adversely impact SSSEP functions.

4.7 **Cyber Kill Chain** – A framework model for identification and prevention of cyber intrusion activity. It has seven steps that enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques, and procedures.

4.8 **Dashboard** – Views that are made up of panels containing modules such as search boxes, fields, charts, tables, and lists. Dashboard panels are usually connected to reports.

4.9 **False Positive** – An alert that incorrectly indicates that malicious activity is occurring.

4.10 **Stakeholders** – Individuals or teams assigned the roles of information system owner, section manager for the system owners, business owner, and users for the information system.

4.11 **Use Case** – A logical, actionable, and reportable component of SIEM. It can be either a rule, report, alert, or dashboard that solves a set of needs or requirements. Use cases offer a way for CSOC to better plan and prioritize the implementation and deployment of the SIEM solution and its related capabilities.

5.0 RESPONSIBILITIES

5.1 SIEM Engineer

5.1.1 Identifies the data source that is relevant for detecting risk.

5.1.2 Checks required data source availability in production environment.

5.1.3 Develops detection content logic.

5.1.4 Deploys content in a test or staging environment.

5.1.5 Completes Attachment 5 – CSOC Content Development ID Card Form, in SEC-PRC-4514, Consolidated Security Operations Center (CSOC) Content Development.

5.1.6 Reviews any engineering processes that the new rule will trigger and sets up alerts.

5.1.7 Updates playbooks and informs personnel involved (SOAR configuration, stakeholder configuration).

5.1.8 Promotes the package of content to production environment and enables rules to run in real time.

5.2 Senior CSOC Analyst (T2)

5.2.1 Tests content deployed in pre-production environment.

5.2.2 Records developed/refined content in change tracking systems.

5.2.3 Completes Attachment 1 – Use Case Template, in SEC-MAN-4501, Consolidated Security Operations Center (CSOC) Use Case Operation Manual.

5.2.4 Trains Analysts and ensures familiarity with handling new SIEM content.

5.2.5 Reviews any analysis processes that the new rule will trigger.

5.3 CSOC Head

5.3.1 Reviews content and documents created and approves content to be promoted in production.

6.0 PROCEDURE

6.1 Detection Approach

6.1.1 Introduction

A. Deficiencies in use cases and SOAR content effectiveness leave organizations with a large amount of data and lack of visibility. Identification of the right content is a critical initial part of the content development process. CSOC identified three approaches in determining the appropriate content to be developed and implemented:

1. Threat-Oriented Approach
2. Compliance-Oriented Approach
3. Data Source Approach

B. These approaches enable building of content for detection and are summarized in Figure 1 – CSOC Approaches to Detection.

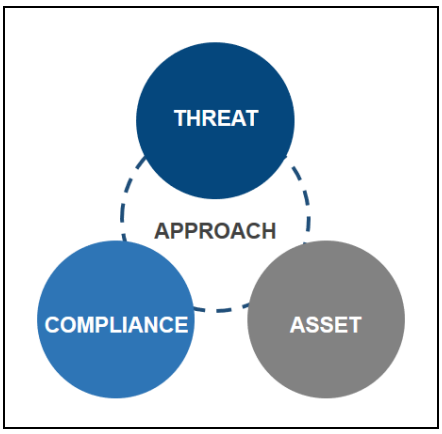

Figure 1 – CSOC Approaches to Detection

6.1.1 (continued)

NOTE

The MITRE ATT&CK® framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks.

C. CSOC will use standards, consider the approaches, and force any new use cases to be mapped to kill chain, MITRE ATT&CK®, naming convention, and alert classification and prioritization.

6.1.2 Threat-Oriented Approach

A. The threat-oriented approach defines the detection of a precise threat, threat actor, or specific malicious activities according to their models and characteristics in terms of tactics, techniques, and procedures (TTPs).

B. CSOC uses a threat process to describe adversary characteristics and typical behaviors with representations of adversary TTPs, a specific technical outline that adversaries might employ during an attack against the organization. CSOC can identify potential weaknesses that act as triggers to create use cases.

C. The benefit from this approach is that it covers behavior exhibited by an adversary through remote access tools, scripts, or interaction at a command-line interface without tying defenses to specific adversary malware and tools that are likely to change over time.

D. CSOC uses the threat-oriented approach as a foundation for the development of specific detection use cases and detectable threat behavior. CSOC will consider the MITRE ATT&CK® framework for its threat approach to enhance detection capability when building use cases to detect threats. This could be achieved by:

1. Relying on the accuracy and effectiveness of detection from other tools within the security stack, which typically depend on rules and signatures.

2. Correlation of known signatures from third-party threat intelligence against the collected log data.

3. Implementation of complex searches created by analysts, who can anticipate certain types of attack or compliance breaches.

6.1.3 Compliance-Oriented Approach

A. Compliance-oriented use cases are those implemented with the intent to monitor and obtain guidance from corporate policies, a framework, or regulatory documents, such as ISO/IEC 27001:2013 and Center for Internet Security (CIS) Critical Security Controls.

6.1.3 (continued)

B. CSOC uses the compliance-oriented approach by identifying compliance controls that are relevant to the organization, either externally mandated (compliance requirements) or selected by internal sources (Internal Audit, Governance and Risk, etc.). This approach starts with identifying the regulations and compliance requirements, as shown in Figure 2 – Compliance-Oriented Approach.

C. CSOC will also consider other cyber security frameworks and standards like ISO/IEC 27001:2013, CIS Critical Security Controls, and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, to enhance its detection capability.

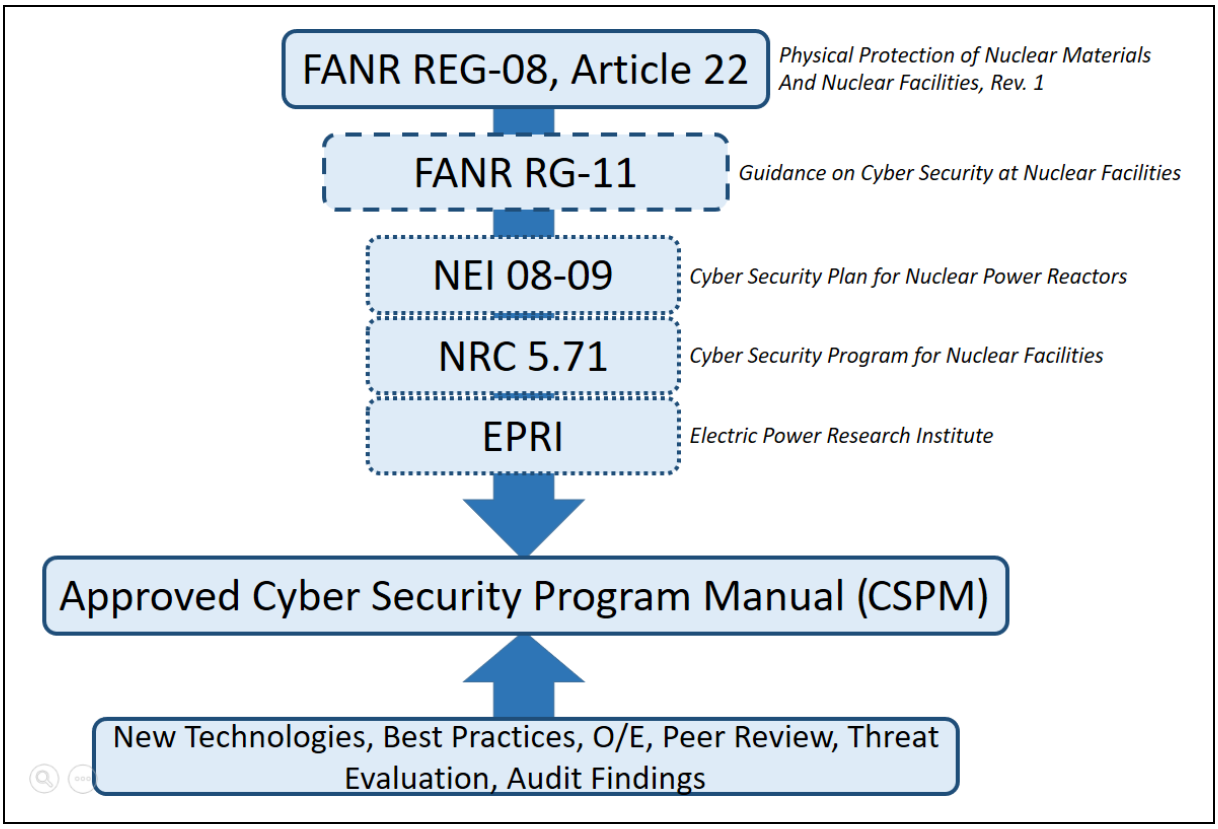

Figure 2 – Compliance-Oriented Approach

6.1.4 Data Source Approach

A. The data source approach involves detection of anomalies or specific activities touching particular data assets, such as payment card data, intellectual property, and personally identifiable information (PII).

B. Use the inventory of sensitive data (or applications) or data classification results to identify the data that should be monitored.

C. CSOC uses the data source approach as follows:

1. Monitor critical applications and infrastructure through logs to provide core services to ENEC/Nawah.

6.1.4C (continued)

2. Identify the servers, components, and locations of the associated assets.
3. Use this information as input for the threat approach [e.g., use case database (UCDB), asset severity].

6.2 Use Case Identification Opportunities

6.2.1 CSOC identifies the activities, exercises, and stakeholders shown in Figure 3 – Identifying Potential Use Cases, that can be leveraged as an opportunity to identify potential new use cases.

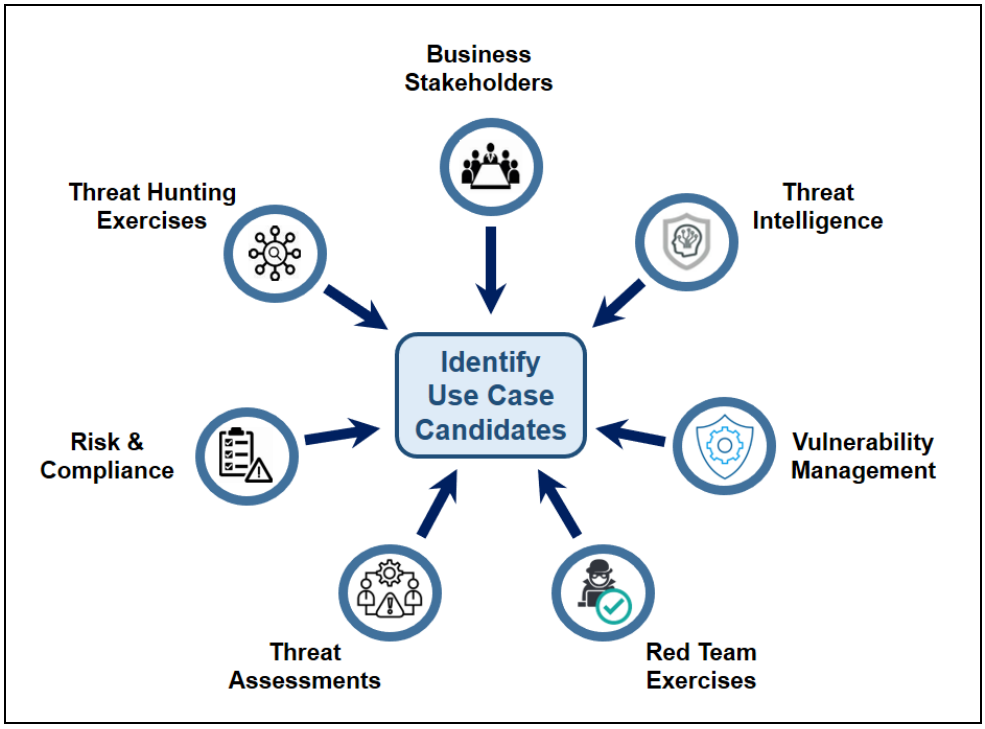

Figure 3 – Identifying Potential Use Cases

6.2.1 (continued)

Source	Description
Business Stakeholders	Business and System Owners may engage CSOC with specific needs to develop and establish security monitoring capabilities customized for their systems or business functions.
Threat Intelligence	Threat Intelligence advisories may provide information about threat actors' tactics, techniques, and procedures (TTPs) that may require the development of a new dedicated use case.
Vulnerability Management	Remediation of vulnerabilities may require time. The time between disclosure of a vulnerability and application of patches can leave the organization exposed to a potential risk. CSOC may develop a new use case to detect vulnerability exploitation attempts for critical vulnerabilities that have not been patched yet.
Red Team Exercises	Red Team exercises may be conducted to test the readiness of the organization's security posture. The outcome of these exercises can be used to improve CSOC detection capabilities.
Threat Assessments	Threat assessment may be performed to assess the behavior and characteristics of a specific threat. The outcome of these exercises can be used to improve CSOC detection capabilities.
Risk and Compliance	Risk and Compliance department may engage CSOC to ensure specific regulation requirements, controls, and constraints are monitored as expected.
Threat Hunting Exercises	Threat hunting exercises may be conducted to verify anomalies and unexpected behaviors within the environments monitored. The outcome of these exercises can be used to improve CSOC detection capabilities.

Table 1 – Opportunities for Use Case Development

6.2.2 These opportunities can help CSOC improve its detection capability and reduce the gap in visibility and severity of threats. CSOC uses the opportunities to improve its overall security monitoring and Nawah's security posture.

6.2.3 Input of these opportunities will be via reports, findings, exercises, or business needs from different stakeholders and will use SEC-PRC-4514, Consolidated Security Operations Center (CSOC) Content Development, to document requirements and design use cases.

6.3 Framework

6.3.1 Introduction

This section describes the supporting layout CSOC uses to document the SIEM, SOAR, and UEBA content during the design and implementation phases. The supporting layout allows CSOC to formalize all the relevant contributions to the content by providing a specific naming convention, alert indication levels, alert classification, and alert mapping for easier integration with SOAR playbooks and incident categorization.

6.3.2 Content Development Lifecycle

NOTE

CSOC uses a well-defined content development lifecycle in creating content. This section explains how CSOC builds content and describes the lifecycle.

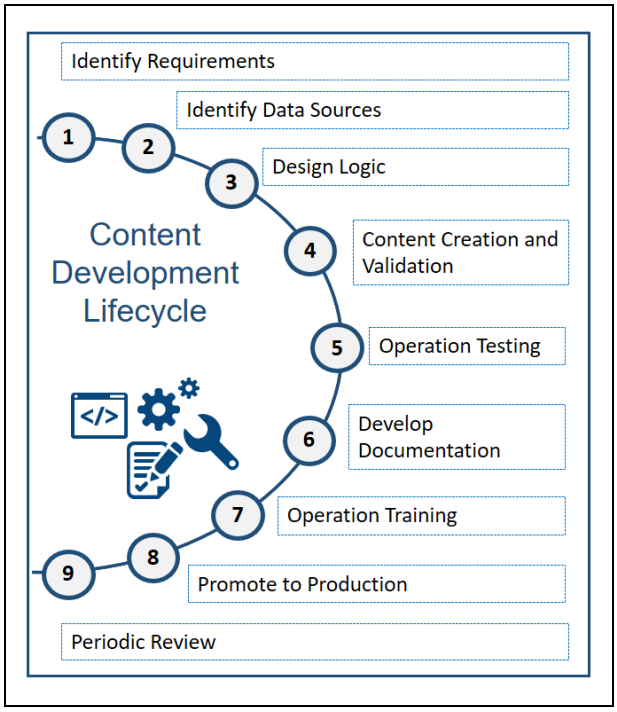

Figure 4 – Content Development Lifecycle

A. Content Development Lifecycle Steps

1. Identify Requirements

a. Once the initial engagement has been received, CSOC SIEM Engineer is responsible for identifying the source of data that is relevant for detecting the risk (i.e., server logs, firewalls, proxy, netflows, user access data, or others).

b. The following should be considered:

1) Availability – Is the detection capability gathering the necessary data?

6.3.2A.1.b (continued)

2) Efficacy – Can the gathered data be processed into meaningful information?

3) Actionability – Is the information provided sufficient to act on?

4) Is there a tool available to address the content?

5) Are the necessary data available?

6) Are the data being collected inside the candidate tool?

7) What will be the performance impact of the volume of required data on the selected tool?

2. Identify Data Sources

   SIEM Engineer checks the availability of the required data sources in the production environment. If the required data sources are not available, then onboard them as required.

3. Design Logic

   a. Once the requirements and the data sources have been identified, SIEM Engineer develops the logic of the detection content. This includes identifying the necessary parameters such as the length of the view or window and the number of events required to trigger the use case.

   b. Based on the logic developed, SIEM Engineer looks for similar existing content in the Live Resource or Threat Intelligence, community platforms, or CSOC's own internal content library, to minimize development efforts and reduce chances of human error.

4. Content Creation and Validation

   a. SIEM Engineer will deploy the content in a test or staging environment by simulating the threat scenario that the content is intended to detect to confirm it is functioning correctly.

   b. The following should be considered in the onboarding, content creation, and data validation phase:

      1) Rollback procedures are included in any change package to ensure prompt recovery of the production environment to the previous functioning state.

      2) People who will be impacted are properly notified about the changes or new content deployed (e.g., CSOC Analyst, business owner, and relevant stakeholders identified during content development).

6.3.2A.4.b (continued)

3) Basic post-implementation checks are performed before considering the change successful and implemented.

4) Apply the change to the use case.

5) Prepare the change package, devise the rollback procedures, and notify CSOC shift members and other operations personnel about new content being deployed.

c. Using a data model is highly recommended to make the rule easier to modify, maintain, and apply to additional log sources.

5. Operational Testing

a. Senior CSOC Analysts must test the content deployed in pre-production to ensure it matches the requirements defined in the earlier stages of the process.

1) Review the output (alerts, scores, and dashboards) to check if the intended conditions are being correctly identified (quality).

2) Test the rule against historical data to determine how often the rule would have operated in the past had it been enabled.

3) Check for cases of false positives and false negatives, and change the created rules accordingly.

b. Once finalized, CSOC Senior Analyst records the content developed/refined in the appropriate change tracking systems.

6. Develop Documentation

a. Once the content has been developed and tested, it needs to be documented. SIEM Engineer will complete the Content Development ID Card Form in SEC-PRC-4514, Consolidated Security Operations Center (CSOC) Content Development, and the Senior CSOC Analyst will complete Attachment 1 – Use Case Template, in SEC-MAN-4501, Consolidated Security Operations Center (CSOC) Use Case Operation Manual. New or modified content is properly documented in a change tracking system per the CSOC change management process.

6.3.2A.6 (continued)

b. Documentation should include all content produced during the initial review phases and findings related to the use case performance during the testing phase, such as detection limitations or conditions in which the use case will not perform effectively.

c. Use case library should be updated with the new use case information.

7. Operation Training

Senior CSOC Analysts should ensure Analysts are familiar with SEC-MAN-4501, Consolidated Security Operations Center (CSOC) Use Case Operation Manual, which contains the operational procedure to handle the new SIEM content.

8. Promote to Production

a. New versions of documents with updated processes and procedures are posted on NCDMS.

1) SIEM Engineer reviews any engineering processes that this rule will trigger, and sets up alerts to go to personnel who know how to triage them.

2) SIEM Engineer also updates playbooks and informs involved people (SOAR configuration, stakeholder notification).

3) Senior CSOC Analysts review any analysis processes that the rule will trigger and update the Use Case Operation Manual if required.

4) CSOC Head reviews both the content and documents created to approve the content to be in production.

b. SIEM Engineer promotes the package of content to the production system, and enables the rule to run in real-time data flow in the production environment.

9. Periodic Review

a. Because the threat landscape evolves constantly, CSOC conducts regular reviews of existing content, and fine-tunes or even retires content if it is no longer relevant, to maintain the overall detection efficiency of the SIEM.

b. CSOC considers the following in removing content:

1) Is tuning capable of keeping false negatives and false positives under an acceptable level?

2) Does the content use too much of monitoring system resources?

6.3.2A.9.b (continued)

3) Are the data required for the content to function no longer available due to changes in data sources?

4) Does the content provide enough value?

5) Are the alerts generated useful for incident response or investigation?

6.3.3 Alert to Asset Mapping

A. CSOC will map each alert to the asset and security control that contributed in the associated use cases for the Analysts to quickly identify what log sources have been considered and if there are other log sources that need to be identified during the investigation. These data will be available for the Analyst in the case management workflow as a reference.

	IDS	DNS	Proxy	DHCP	VPN	Packets	Wi-Fi	Firewall	Email	Windows	Antivirus
Use Case 1	Yes		Yes		Yes			Yes		Yes	
Use Case 2		Yes	Yes	Yes			Yes		Yes	Yes	Yes
Use Case 3				Yes	Yes						
Use Case 4	Yes	Yes	Yes			Yes		Yes		Yes	

Table 2 – Alert to Asset Mapping

6.3.4 Naming Convention

A. CSOC will use its own Use Case Charter and naming convention classification to identify category, method, and asset involved in the detection. The Use Case ID will be defined per the Use Case Charter, referencing different sites and types of detection using its own unique ID. Refer to Figure 5 – Use Case Naming Convention. The following naming convention will be used in operation:

<USE CASE ID> <Incident CATEGORY><USE CASE DETECTION METHOD>-<USE CASE> - On <Asset>

B. Incident Category

Classification per SEC-PRC-4500 (BSI), Consolidated Security Operations Center (CSOC) Analysis and Response.

C. Use Case Detection Method

Description of method of detection used in the use case per the rules and data sources.

D. Use Case

Description of the attack or impact detected.

E. Asset

Description of the asset/user that triggered the use case.

6.3.4 (continued)

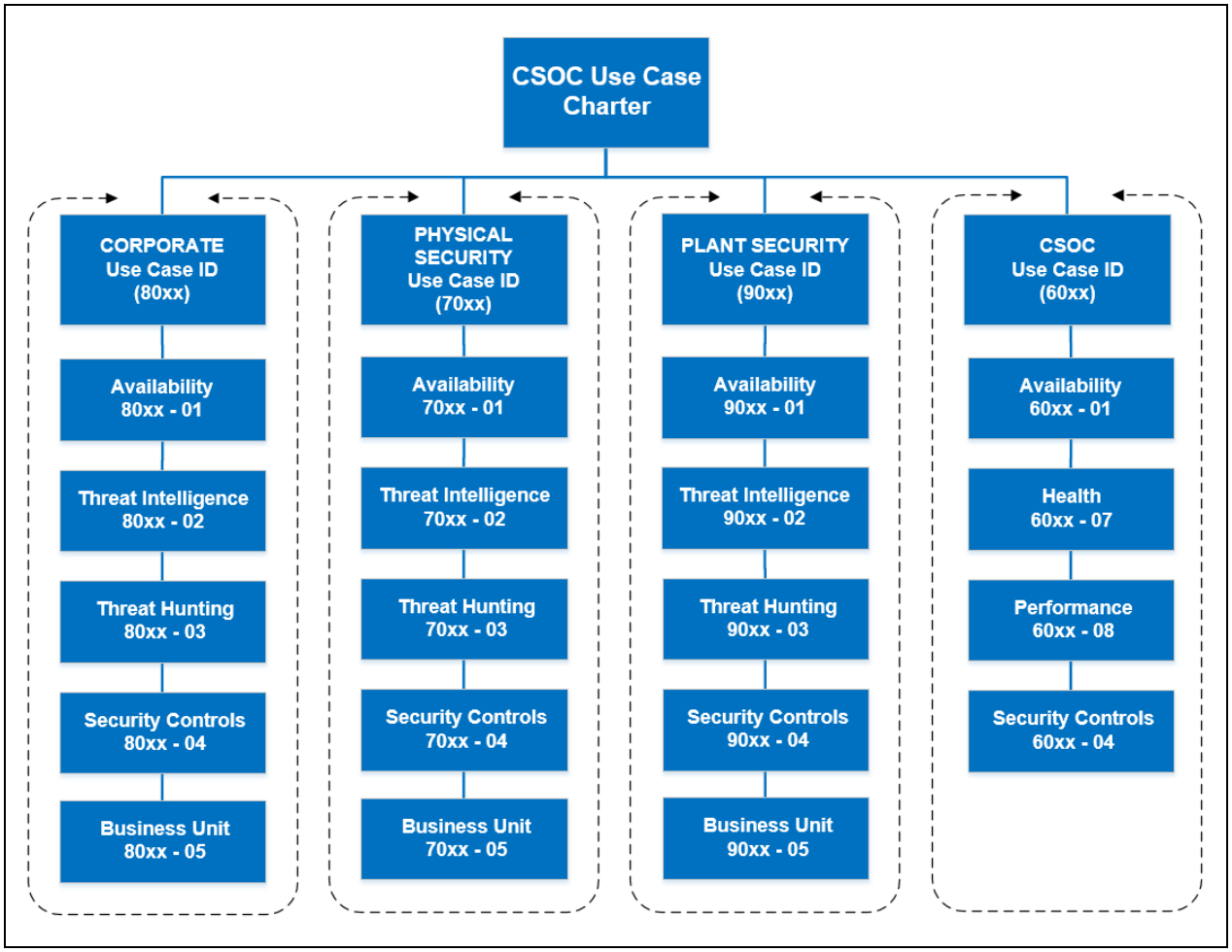

Figure 5 – Use Case Naming Convention

Incident Category	Use Case Detection Method	Use Case	Asset
Brute Force	Behavioral	Remote Desktop Alert	User Normal
Distributed Denial-of-Service (DDoS)	Signature	Unauthorized OPH Login	User SRV Account
Phishing Email	Statistical	Unauthorized SS Login	User Admin
Scans/Probes/Attempted Access	Anomaly		User VIP
Unauthorized Access	Predictive		Critical Server
Malicious Code			Normal Server
Vulnerabilities / Web Application Attacks			
E-Mail Fraud/Phishing/Spoofing			

6.3.5 Cyber Kill Chain Phases

Cyber kill chain is a framework model for identification and prevention of cyber intrusion activity. It has seven steps that enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques, and procedures. These steps are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2C), and Actions on Objectives. CSOC will map each use case to the cyber kill chain framework. Brief descriptions/examples of each step are provided below.

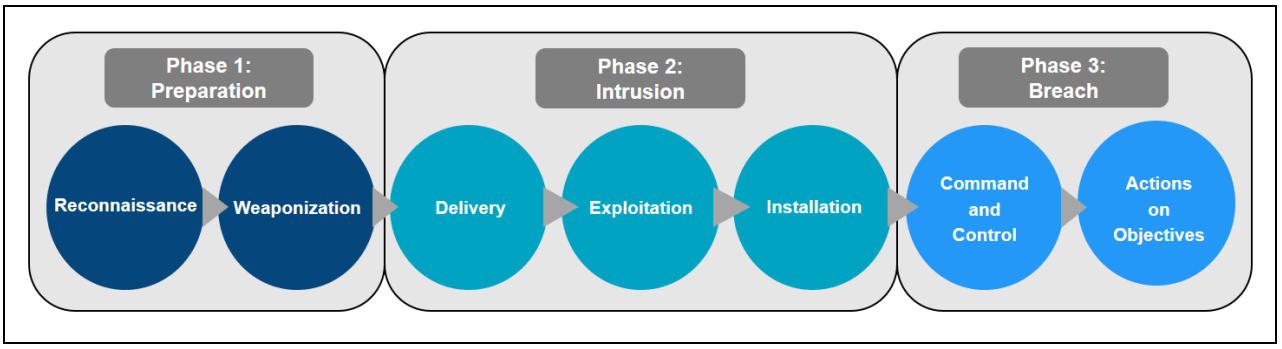

Figure 6 – Cyber Kill Chain Phases

Cyber Kill Chain Step		Description/Example
1	Reconnaissance	Research, identification, and selection of targets by harvesting email addresses, conference information, etc.
2	Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g., Adobe PDF, Microsoft Office files).
3	Delivery	Delivering weaponized bundle into the victim via email attachments, websites, USB drives, etc.
4	Exploitation	Once the delivery of the bundle is successful, then exploitation of a vulnerability will take place to execute code on victim's system.
5	Installation	The weapon will install a malware with a backdoor on a target's system allowing persistent access.
6	Command and Control (C2C)	Command channel/server will communicate with the weapon installed, providing hands-on keyboard access.
7	Actions on Objectives	The attacker will work to achieve objective of the intrusion (e.g., data exfiltration, destruction of data).

6.3.6 MITRE ATT&CK® Framework

A. MITRE ATT&CK® is a framework that has unique ability to provide insights into adversary behaviors, and provides a standardized, easily accessible global language that has led to its growing popularity for organizations that are looking to share threat intelligence and support their security posture. Attachment 2 – MITRE ATT&CK® Framework, shows how MITRE ATT&CK® is structured.

B. The MITRE ATT&CK® framework can help CSOC better classify attacks, understand adversary behavior, and assess the organization's risk. CSOC can also use the framework to gain insight into how adversaries might operate in various scenarios so they can create informed strategies on how to detect and ultimately prevent those behaviors from affecting the security of Nawah. CSOC will map TTPs to MITRE ATT&CK® framework for each use case.

6.3.7 Compliance

CSOC will use NRC Nuclear Compliance (NEI 08-09, Rev. 6, Cyber Security Plan for Nuclear Power Reactors) security controls that are detectable by building use cases related to all BNPP Units when the data are available.

7.0 RECORDS

7.1 The Records section will clearly identify only those records generated as a result of the performance of the procedure that should be retained.

7.2 Quality Assurance Records (QAR) are identified per requirements in DCM-PRC-0013, Records Retention Schedule and Disposition.

7.3 Business Records (BR) are those identified by the owning function to support any business requirements.

Records Generated		
Record Title/Section/Form Number	**Record Class** (BR or QAR)	**Retention Time**
None	N/A	N/A

8.0 ATTACHMENTS

8.1 Attachment 1 – Alert Indication Levels

8.2 Attachment 2 – MITRE ATT&CK® Framework

Attachment 1 – Alert Indication Levels
Page 1 of 3

1. **BLUE or INFO** indicates a low risk. No unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity.
2. **GREEN or LOW** indicates a general risk of increased hacking, virus, or other malicious activity. The potential exists for malicious cyber activities, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.
3. **YELLOW or MEDIUM** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service. At this level, there are known vulnerabilities that are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high.
4. **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure and can cause multiple service outages, cause multiple system compromises, or compromise critical infrastructure. At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.
5. **RED or CRITICAL** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages or significantly destructive compromises to systems with no known remedy, or debilitating one or more critical infrastructure sectors. At this level, vulnerabilities are being exploited with a severe level or widespread level of damage or disruption of Critical Infrastructure Assets.

Alert Level	Examples	Actions	Notifications
Blue – Info	• Normal probing of the network. • Blocked internet probing. • Internal vulnerability scanning. • Internal penetration testing.	• Continue routine security monitoring. • Ensure personnel receive proper training on cyber security policies.	• No notification is warranted if a state is currently at this level.
Green – Low	• A critical vulnerability is discovered but no exploits are reported. • A non-critical vulnerability is being exploited but there has been no significant impact. • A new virus is discovered with no potential to spread quickly. • There are credible warnings of increased probes or scans.	• Continue recommended actions from previous level. • Identify vulnerable systems. • Recommend appropriate countermeasures to protect vulnerable systems. • Create a use case to detect exploit to vulnerable systems if applicable.	• Notification via secure email/ticketing system will be sent to the relevant stakeholders from the communication plan when the state of Alert Level is raised to GREEN or LOW.

Attachment 1 – Alert Indication Levels
Page 2 of 3

Alert Level	Examples	Actions	Notifications
	• An attempt to compromise non-critical system(s) did not result in loss of data.		
Yellow – Medium	• An exploit for a critical vulnerability exists that has the potential to damage. • A critical vulnerability is being exploited and there has been a low impact. • Suspected DDoS attack.	• Continue recommended actions from previous levels. • Identify vulnerable systems. • Increase monitoring of critical systems. • Recommend to implement appropriate countermeasures to protect vulnerable critical systems.	• Notification via secure email/ticketing system will be sent to the relevant stakeholders from the communication plan when the state of Alert Level is raised to YELLOW or Medium.
Orange – High	• An exploit for a critical vulnerability exists that has the potential for significant and moderate damage. • There is a compromise of a secure or critical system(s) containing sensitive information. • There is a compromise of a critical system(s) containing non-sensitive information if appropriate. • A virus is spreading quickly throughout the Internet, causing excessive network traffic. • There is a DDoS attack.	• Continue recommended actions from previous levels. • Closely monitor security mechanisms, including firewalls, web log files, anti-virus gateways, system log files, etc., for unusual activity. • Consider limiting or shutting down less critical connections to external networks such as the Internet. • Consider isolating less mission-critical internal networks to contain or limit the potential of an incident. • Consider the use of alternative methods of communication, such as phone, fax, or radio in lieu of email and other forms of electronic communication.	• Notification to the Cyber Security Incident Response Team (CSIRT) may be required if the case is found to be a confirmed incident. • Notification via secure email email/ticketing system or telephone will be sent to the relevant stakeholders from the communication plan when the state of Alert Level is raised to ORANGE or High.

Attachment 1 – Alert Indication Levels
Page 3 of 3

Alert Level	Examples	Actions	Notifications
Red – Critical	• An exploit for a critical vulnerability exists that has the potential for severe damage. • Loss of visibility. • A critical vulnerability is being exploited and there has been significant impact. • Attackers have gained administrative privileges on compromised systems. • There are multiple damaging or disruptive virus attacks. • There are multiple denial of service attacks against critical infrastructure services. • Complete network failures. • Mission-critical application failures. • Compromise or loss of administrative controls of critical system. • Loss of critical supervisory control and data acquisition (SCADA) systems. • Potential for or actual loss of lives or significant impact on the health or economic security of the state.	• Continue recommended actions from previous levels. • Consider shutting down connections to the Internet and external business partners until appropriate corrective actions are taken when applicable. • Consider isolation of internal networks to contain or limit the damage or disruption when applicable. • Use alternative methods of communication, such as phone, fax, or radio as necessary in lieu of email and other forms of electronic communication.	• Notification to the CSIRT may be required if the case is found to be confirmed incident. • Notification via secure email email/ticketing system and telephone will be sent to the relevant stakeholders from the communication plan when the state of Alert Level is raised to RED or Critical.

Attachment 2 – MITRE ATT&CK® Framework
Page 1 of 1