# Security Operations Center in a Box:

## *A How-To Guide for Building Your Own SOC*

Careers Preparation National Center


NUARI

NORWICH UNIVERSITY APPLIED RESEARCH INSTITUTES

Norwich University Applied Research Institutes

February 7, 2023

This product developed under the 2020 NCAE-C grant H98230-20-1-0380 (Evidencing Competency) and 2022 NCAE-C grant H98230-22-1-0329 (Careers Preparation National Center)

# Contents

# Version History

| Version | Date | Changes Made |
|---|---|---|
| v0.5 | April 2022 | Original documentation |
| v1.0 | January 2023 | Expansion of Operational and Technical sections to be more inclusive of various SOC implementations; Identification of strategy added to Academic section; Administrative section supplemented with relevant data to building partnerships and obtaining contracts. |
| V2.0 | June 2023 | Cover page: logo change and grant information |

# Errata

This table contains changes incorporated into the SOC-in-a-Box documentation after v1.0. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either editorial or substantive in nature.

| Date | Type | Change | Page |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Introduction

This outlines professional considerations to provide strategic and technical guidance and virtual/remote support resources for CAE-C institutions interested in implementing a Security Operations Center (SOC) at their home institution, for future execution of services and enhanced academic and workforce development experience. Furthermore, this set of guides can be directly utilized to build, staff, and operate a scalable SOC with professional cybersecurity personnel and student interns. This center can supplement a client's existing cyber security team, while educating students through experiential learning by exposure to actual organizations' infrastructures and teaching reputable, industry-standard frameworks. Within the cybersecurity industry, there are multiple groups (civilian, government, and military) who each take their own approach to building a SOC or its equivalent. This work utilizes a neutral but strategic approach to encompass all aspects and similarities between the various foundational frameworks, while also incorporating knowledge gained from prior experiences creating and implementing internal processes and collaborating with clients. The provided SOC-in-a-Box documentation aims to provide a foundational structure to any person or organization who has identified the necessity for creating a group that monitors for malicious cyber activity as it affects that group and/or its client(s).

This project contains four main chapters of foundational elements that address the distinct aspects of initialization and maintenance needed to host a functional SOC – administrative, academic, operational, and technical. The Administrative chapter explores the business functions and structures necessary to promote a successful SOC implementation, ranging from organizational departments to obtaining new contracts. The Academic chapter focuses on course curricula, program learning objectives, and other pedagogical matters, to ensure a baseline of knowledge, skills, and abilities through standardized training for SOC staff, whether short-term, like interns, or long-term employees. The Operational chapter identifies the processes, necessities, and procedures that allow the SOC to conduct missions while standardizing common operations. The Technical chapter outlines the types of tools/applications required to ingest and process logs and intelligence data, report on threats, and train staff.

## Evidencing Competencies in Students

This project seeks to identify and foster programs within CAE-C institutions that provide students with foundational, real-world experience in accordance with NIST NICE work roles, while providing simultaneous experiential learning for the civilian role of SOC Analyst. The ideology of "evidencing competency" roots itself in bridging the knowledge and maturity gap between being a student in university and a professional entering the workforce. The *Academic* chapter has more specificity regarding implementation and maintenance of this program at the institutional level.

## How to Use this Guide

Utilize this guide as a supporting framework to building a SOC or apply supplementally to an existing SOC. Each section includes foundational structures that must be in place, so utilizing this document as a checklist will help ensure cohesion throughout the SOC. This document is meant to be thought-provoking regarding often overlooked elements of SOC creation, implementation, and maintenance, and not

intended as a dictated step-by-step guide. Every SOC will have their own necessities, expectations, and use cases. More specific questions related to this document's contents or how it may apply to your situation may be brought to NUARI for consultation and assistance.

## What is a Security Operations Center?

The SANS Institute[1], defines a security operations center (SOC) as "*A combination of people, processes and technology protecting the information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects.*"[2] NUARI expands this definition to also include analysis and reporting, outside of just monitoring and detection.

## Tools, Brands, and Systems

This SOC-in-a-Box guide establishes and teaches a framework for the tools and applications necessary for creating a SOC, but the final decision for brands and entering vendor contracts must be managed by each organization following the applicable rules of acquisition. This document can be utilized to aid an organization in outlining their use case(s) and requirements as assorted options/vendors are researched and/or pursued. By remaining tool agnostic, this guide provides a stronger focus on processes, procedures, and policies.

## Terminology

Unless otherwise stated, the terminology utilized in this document comes from the National Institute of Science and Technology, or NIST, a commonly accepted framework in both the civilian and government space. Working with a common vocabulary within day-to-day SOC operations, with organizational executives, and with clients will reduce confusion and help to quickly identify mutual expectations and situations. Additionally, all abbreviations are defined within the text at first use and can also be found at the end of this document in the *Glossary*.

# NUARI

The Norwich University Applied Research Institutes (NUARI) is a 501(c)(3) non-profit that serves the national public interest through the interdisciplinary study of critical national security issues with a focus on strengthening and protecting critical infrastructure.

# Norwich University

Norwich University, a Senior Military College located in Northfield, Vermont, is the oldest private college in the United States. Established in 1819 as the American Literary, Scientific and Military Academy, Norwich is recognized as the Birthplace of the Reserve Officers' Training Corps (ROTC).

---

[1] https://www.sans.org/about/

[2] https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf

# Administrative

When building and maintaining a SOC, administrative support is necessary when it comes to bidding for, obtaining, and maintaining contracts with clients, as well as supporting the internal relationship between the SOC and the rest of the company.

## Outreach

Each organization should have an outreach representative or team that aids in translating the SOC's capabilities to a marketable framework. This could involve an internal partnership between the SOC and outreach (sometimes referred to as business development) to guarantee that proper utilization and application of terminology in potential pitches / bids, as well as ensure that the SOC's services line up with expectations of the industry. This may also include drafting a template response to Requests for Information (RFIs) or Requests for Proposal (RFPs).

### Requests for Proposal

Within the cybersecurity industry, when a company identifies the necessity of outsourcing services, they may release an RFP. These RFPs may be on the company's website, uploaded to a centralized RFP repository, or found via other methods. These documents include an outline of the needed services, highlighting key elements such as expected hours, company-specific requirements, and a brief overview of expectations. These RFPs have a hard deadline for submitted responses, or bids, but may have a preliminary deadline for questions. Outreach should work with the SOC to determine any elements of the RFP that may need clarification. The finalized, submitted bid should outline how your SOC will fulfill the requirements listed in the RFP, as well as a quote for these services. Determination of the quoted cost will be led by administration / executives within the company, but should include details such as:

- The estimated hours needed to meet expectations,
- The number of staff needed to maintain the requested schedule, if applicable,
- The number of staff needed to fulfill the daily objectives listed in the RFP,
- The cost of any tools/applications,
- Any related onboarding costs,
- And if services such as Incident Response will cost more than the standard daily cost.

### Contracts

A contract is an outlined legal document that specifies the responsibilities and expectations of all parties contained within. Within the realm of SOC Services or SOC-as-a-Service (SOCaaS) solutions, contracts identify the services expected, any potential timelines associated therein, any relevant financial information, and the start and end dates of said contract. A common component of modern service contracts, Service Level Agreements (SLAs) are a commitment between a service provider and a customer, and they ensure a documented record of metrics, responsibilities, and expectations for both parties. Should a contract-related question (such as if a specific service is within scope) arise after all parties have signed the contract, the SOC has a responsibility to internally promote to the appropriate

organizational authorities, who will determine proper response. Depending on the organization's internally outlined policies, the organization may also pursue legal consultation.

## Human Resources

Every organization will have different necessities to match internal requirements and workflows to the people conducting those processes. Human Resources (HR) helps bridge communication gaps, processes required forms for employees, ensure employment benefits, and function as an intermediary. HR also fulfills the role of a necessary authority when hiring, promoting, and dismissing employees.

## Decisionmakers

Whether at the executive level, the SOC level, or somewhere in-between, decisionmakers are critical to guiding the direction of a SOC. Business strategies such as five-year plans, company projects, and overall future vision are a necessity to continue growing a SOC from an original concept to a unique service for clients. Decisionmakers may also work with outreach and SOC management to tailor the SOC and its marketed services to identified industry trends.

# Academic

This chapter describes the academic foundations and additional training required for staff and students to become SOC Analysts, or the organizational equivalent role. The academic element of a SOC consists of two parts: academic curriculum and training. If linked to a hosting institution, they should provide courses that educate students on cybersecurity and other technological concepts. The SOC's training builds the tactical knowledge, skills, and abilities (KSA) the students will need to positively contribute to the objectives and projects within the SOC, while also providing a scalable foundation for professional capabilities.

## Workforce Development

The SOC directly supports workforce development through evidencing competency in students, outlined through one or more competency statements. These statements address key takeaways that the SOC and/or supporting institutions want to instill. The following ABCDE template outlines the five elements of a competency statement:

> *An actor (A) performs a behavior (B) within a context (C) to an acceptable degree (D) according to the normative expectations of an employer (E).*[3]

This standardization of syntax ensures that all relevant parties comprehend the purpose of the SOC's contribution to individuals looking to bridge the gap between obtaining knowledge in an educational environment and applying that knowledge to a new career.

### Internships

If linked to a hosting institution, they may identify prerequisite criteria for students to become SOC interns. Potential criteria may include prerequisite courses, meeting/maintaining a specified GPA, and/or being a specific class year (e.g., must be a Junior to pursue an internship). The SOC may set additional criteria for students pursuing an internship, but necessary institutional requirements must be met first.

The work that interns do in the SOC may award academic credit for any linked institutions. The amount of credit and the process for documenting and awarding credit will vary for each institution, so identification of these details and stipulations is encouraged, if not required, by the SOC and/or organizational leadership prior to hiring students as interns. The amount of credit earned connects directly to the number of hours spent as a SOC intern, and these definitions of credit hours per time spent must be agreed upon between the SOC and educational institution(s).

## Training

The SOC's training course will identify the role that the intern or new hire will fill, and work backwards to identify the knowledge, skills, and abilities the trainee should have to work effectively within that role. If utilizing a NIST NICE work description, the KSA are listed accordingly. If utilizing the SOC Tiers as

[3] https://www.caecommunity.org/sites/default/files/blogfiles/Evidencing%20Competency%20pilot_0.pdf

guidance for the roles and responsibilities, multiple resources also identify the KSA associated. Training should identify resources, projects, and assignments that will aid in a new person developing the knowledge to appropriately apply the necessary skills and abilities to their work. Competency statements may aid in outlining necessary training elements. Additionally, this course should include references to necessary SOC policies and procedures, allowing trainees a balance between learning the industry standards of the role, and how those standards apply to this specific SOC.

## Staff Positions

There are multiple services a SOC offers to their clients through managed SOC services or SOC-as-a-Service (SOCaaS) offerings. Fulfillment of this services may be divided between the various roles within the SOC, such as by type (research vs. analysis), by skill tier (responding to SIEM Alerts vs. Threat Hunting), or by genre of service (policy consultation vs. threat analysis). With a large team, everyone may have their own dedicated assigned field or service. However, with smaller teams, individuals may be expected to adapt to multiple responsibilities. Ensure consistent communication for maintaining workload balance for all staff.

One method of building the staffing structure at the SOC includes two roles, and associated responsibilities, that any SOC staff could be assigned: Analyst and Researcher. The analyst responsibility maps directly to the cyber defense analyst (work role PR-CDA-001) in the NIST NICE framework[4] and uses data (e.g., network traffic logs, process logs, security application events) collected from a variety of cyber defense tools to analyze events and promote incidents that occur within cyber environments. The researcher responsibility of a SOC Analyst combines the threat analyst and all source analyst roles (work roles AN-TWA-001[5] and AN-ASA-001[6]) and reviews open-source intelligence (OSINT) and information received from external partners to build intelligence reports within the SOC's Threat Intelligence Platform (if applicable), complementing / supplementing the Analyst role.

The use of crew positions in the SOC allows interns and full-time staff to focus their efforts during a mission and creates a repeatable framework and foundational expectations, which could be filled by any trained staff.

## Training Course Expectations

A SOC should utilize a structured learning environment, such as an LMS, to provide intern training and staff onboarding. The course materials should include sample assignments that utilize the same skills as the role they are in training for. By introducing complex concepts through bite-size assignments, students can become more comfortable with the knowledge, skills, and associated processes, before expected to accomplish objectives at the same tier as the SOC's full-time staff. Other onboarding assignments could be outsourced to another vendor that specializes in onboarding/training or could involve pairing a trainee with a full-time SOC staff member to shadow that person's current objective.

---

[4] https://niccs.cisa.gov/workforce-development/nice-framework/work-roles/cyber-defense-analyst
[5] https://niccs.cisa.gov/workforce-development/nice-framework/work-roles/threatwarning-analyst
[6] https://niccs.cisa.gov/workforce-development/nice-framework/work-roles/all-source-analyst

Additionally, the SOC staff coordinating the training could have a trainee shadow them, where the person learning a new skill pairs with someone conducting an objective that highlights that skill. Encourage the trainee to ask questions related to analysis, tool usage, or other elements of the mission, but they should show proficiency and professionalism in the fundamentals of working in a SOC.

Once seen as proficient with the assigned objectives, the trainee may be shifted to day-to-day operations on their own, with consistent support from the SOC team, just as the SOC team provides support for each other.

## Failure to Meet Expectations

Should a trainee show difficulty in understanding specific concepts of the training or the SOC's day-to-day taskings, supplemental instruction should come from individualized instruction to better ensure retention and understanding. Consistent difficulty may need promotion up the SOC's hierarchy to determine the best path forward for helping the trainee understand the concepts being taught.

Should the trainee make an egregious mistake, which may need to be defined on a case-by-case basis, SOC management must be notified, and proper correction provided for provided for the trainee, highlighting the importance why the SOC does not conduct certain actions. If the action directly breaches a policy, contract, or other documented agreement, SOC management may consult appropriate department(s) to identify proper course of action, which may include dismissal of the trainee from the SOC.

# Operational

To coordinate expectations within the SOC and with the SOC's clients, a standardized set of directives must be documented to ensure efficient communication and proper prioritization of processes. Additionally, the SOC's operations and configuration should allow the SOC team to operate in a professional setting, using the common practices and vocabulary of a large cybersecurity organization, allowing for scalability as the environment and daily expectations expands to meet new clients, new funding, and new opportunities. Lastly, if there are any processes or policies the SOC is expected to implement or support on behalf of the company or clients, these should be documented and communicated with the SOC.

## Organizational Policies and the SOC

Every organization must have supplemental policies and procedures; a standardized list can be found online and applied, where necessary. For policies that involve technology, there may be an expectation for the SOC to supplement the organization's ability to track compliance. There should be proper communication between the SOC and the organization's administration, to ensure that any applicable expectations are within scope of the SOC's capabilities and do not detract from SOC services provided to clients. For example, if the organization has an Incident Response Plan, the SOC could supplement with daily monitoring and analysis, as if for a client. Additionally, policies like an Acceptable Use Policy often outline the rules of utilizing organizational equipment, applications, and/or tools – a SOC could create alerts to identify activity that may be breaching this policy and promote this activity up the pre-defined hierarchy.

## Standard Operating Procedures

All SOCs should have a document that explicitly details daily operations, employment, and standard operating procedures (SOP) for missions executed in or on behalf of the SOC team. The purpose of this document is to 1) Provide a focused and standardized results-oriented workflow to identify, research, track, hunt, monitor, and report known threats in cyberspace to the SOC and its clients, 2) Ensure client requests for information (RFI) are tracked and serviced in an efficient and standardized manner, 3) Communicate effectively with crewmembers and clients while accomplishing the mission, 4) Measure effectiveness and performance of the mission plan and team, and 5) Continuous Process Improvement.

The SOP should include the following sections:

- Daily expectations of the SOC and staff
- Expectations of use of the physical SOC space (if applicable)
- Outlines of commonly repeated process
- Identification of the main services the SOC provides to its clients with a brief description of each, including measures for Quality Assurance (QA) and/or Quality Control (QC)
- Organization of the SOC roles and responsibilities, with an included hierarchy for promotion of incidents

Suggested processes outlined within the SOP include:

- Training/Onboarding,
- Reporting,
- Running a mission,
- Responding to client requests,
- Communications plans, or comm calls,
- Incident Response, if applicable and not already covered in an Incident Response Plan (IRP),
- Expectations or policies related to remote work,
- Expectations of visitors, and
- Expectations of personal electronic devices.

An SOP should be updated whenever there is a major change to ensure that it remains relevant and referenceable by all current and future staff. Encourage feedback on the document to allow for continuous process improvements (CPI).

*Sample SOP sections are listed below for adoption or reference for a SOC.*

### Standard Contingencies

The SOP should also contain processes for handling standard or anticipated problems. There is no need to include these within day-to-day planning, but employees should be aware of the contingencies and the proper process to follow for each. These contingencies may include:

- Loss of Power (on site)
- Loss of Power (remote)
- Loss of local network/infrastructure
- Loss of necessary applications
- Loss of client-provided logs/tools

## Sample SOP Sections

The following sections are derived from the NUARI Security Situation Center's SOP. They demonstrate how NUARI operationalized the SOC concept to support their cyber workforce development mission, alongside an ongoing military training role with the Vermont Air National Guard (VTANG). NUARI customized design and training methods around the Air Force's implementation of Cyber Protection Teams to support the particular career paths and operational tasks of their intern population.

NUARI's SOC design matched the customers served, the intern demographics, and Department of Defense grant requirements. Your organization will determine the SOC design and architecture that meets your needs based on similar analysis.

### Sample: Intern Scheduling

Given the scheduling of full-time SOC Analysts, the SOC currently has the capability of training up to twelve interns. Interns assigned to the SOC should be able to fulfill the role of a Tier 2 SOC Analyst or Cyber Defense Analyst upon internship completion. To ensure the SOC grants interns the requisite time

for training, experiential learning, and pursuing internship-based projects, the following guidelines have been identified:

- When an intern is offered a position with the SOC, they will be fit into the schedule that meets the needs of the SOC and its clients.
- Interns will communicate their availability at the beginning of their employment. Any changes to this availability should be communicated by the intern to the SOC's Intern Coordinator.
- No more than four interns will be on shift at any given time.
- Interns will not be assigned more than 15 hours per week while classes are in session.
- Interns will not work more than 4 days in a calendar week.

## Sample: Crew Organization

The SOC's staff may have a crew commander, mission developer, and one or more Analysts and Researchers, to conduct daily mission operations. Should circumstances limit the number of staff working for a particular shift, it is possible that one individual may have to function as both the Analyst and Researcher. If deemed necessary, individuals may work collaboratively in Hunt Teams, which consist of one analyst and one researcher. There is only ever one crew commander on a mission unless exigent circumstances require otherwise.

Should there be a Mission with no Crew Commander and a current situation dictates the necessity for one (e.g., a non-info Report ready to send to client, client reaches out for Incident Response), the Mission Developer is responsible for initiating contact with one or more of the Crew Commanders. Should none of the Crew Commanders be reachable, the Mission Developer is responsible for promoting the incident up the chain of command. Please note, responsibilities that fall on the Crew Commander that do not require immediate action (such as promotion of a threat intelligence entry) can remain pending until the next shift's Crew Commander arrives on station at the beginning of their shift. It is up to each crewmember to make the appropriate judgement in determining the criticality of the current situation.

### Crew Commander

The crew commander (CC) is a full-time SOC staff member. They have the responsibility of making executive-level decisions on behalf of the SOC Director, supporting the Director in ensuring SOPs are followed, reviewing reports for applicable elements and criteria, and submitting completed paperwork to clients. See *Reporting Procedures* section below.

### Mission Developer

The mission developer (MD) is an additional role filled by Crew Commander, Analyst or Researcher. This person will develop the mission plan for the next Mission and lead the pre-mission brief and post-mission debrief. The Mission Developer is also expected to make the appropriate timing comm calls (see *Appendix A*) for Mission Begin, Home Stretch, and End Mission, as well as respond to SIEM alerts, if the original alert owner is not on station.

### Analyst

The analyst crew position refers to individuals who execute tasks related to SIEMs, XDR tools, and/or other threat hunting. Analysts generate reports to clients in response to findings from Threat Hunting, Security Response, or other Analyst roles. They may work with one or more Researchers to aid in connecting OSINT data to client-provided logs. This could include searching for IoCs (e.g., hashes, IP addresses) or working to create hunts to track behavioral activity. Further definition for this role as it relates to various SOC processes should be in the documentation for those processes.

### Researcher

The researcher crew position refers to individuals who execute tasks related to open-source research (also referred to as OSINT), review of client requests, and generating reports based off OSINT findings. Further definition for this role as it relates to various SOC processes should be in the documentation for those processes.

### SysAdmin

System Administrators have elevated permissions for multiple assets on a domain. SysAdmin work consists of administrative-level maintenance of multiple internal assets that could impact the SOC's capabilities. This does not include crewmembers working on individually assigned systems, such as the SIEM SME performing administrative functions/maintenance on a SIEM tool.

## Sample: Threat Hunting Services

Threat Hunting within the SOC references David J. Bianco's Pyramid of Pain model[7], which places IoCs (hash values, IP addresses, and domain names) at the bottom, due to their high likelihood of changing when a cyber threat changes or updates their procedures. At the top of the Pyramid of Pain are TTPs, or Tactics, Techniques, and Procedures. These are not concrete indicators, but behavioral identifiers of malicious activity, that aid Threat Hunters and Cybersecurity Incident Responders in identifying, tracking, and attributing activity to known threats, even when the IoCs involved are unknown.

The SOC should work under the notion of an assumed breach and utilize an industry-recognized threat hunting foundation (e.g., Lockheed Martin Kill-Chain, MITRE ATT&CK) to build queries or "hunts" that return specified behavioral activity that allow the SOC to surveil client terrain for suspicious/malicious events. These foundations are broken down into Tactics utilized by potential cyber threats; it is the SOC's responsibility to define the rotational hunt schedule needed to meet client expectations. Between A Mission and B Mission, it is expected that the requisite Tactics will be assigned and covered by the SOC, unless a conscientious decision is made by SOC leadership to postpone the hunts for a later Mission.

### Security Monitoring

Where possible, automate Threat Hunting using the SOC's SIEM(s). Rather than manually working through potentially hundreds of queries per client, convert queries known to return zero results and/or few false positives to an automatic query or rule, set to alert to the SOC when results occur outside of a

[7] https://www.sans.org/tools/the-pyramid-of-pain/

pre-defined threshold. This automation allows for increased scalability for the SOC, as well as potentially faster identification of malicious activity, therefore reducing the mean time to detect (MTTD) of the SOC.

## Sample: Missions

A Mission is a designated timeframe with associated assignments for each person. To break down the workday into manageable sections, the SOC has identified the hours of 0700 to 1230 as Mission A and the hours of 1300 to 1730 as Mission B, with the unassigned time from 1230 to 1300 utilized to conduct a debrief. Missions allow for a designated and communicated focus on objectives for the specified period, while balancing daily operations and expectations with longer term projects for the SOC and its clients.

### Mission Planning Process

The mission planning process' design produces a specific mission plan for each Mission. Each mission is named based on the date (yyyy-mm-dd) and a letter (A or B) to identify when the mission took place (A for morning, B for afternoon.) The first objective of a morning shift is mission planning. The afternoon shift works on their Mission Objectives as assigned when they arrive On Station. When Home Stretch is called for Mission A, the Mission Developer for Mission B will start the process of developing the next mission, pending carry-over objectives and new Rolling Objectives. The following steps are executed during mission planning:

- Review of previous shift's Mission Report (MisRep) (or the posted carry-over objectives if developing for B Mission),
- Review any requests for information from client(s),
- Determine the next set of MITRE ATT&CK Tactics to Threat Hunt (based off the rotation),
- Set and review current mission objectives,
- Review environment status and consider the latest intelligence,
- Assign crewmembers to objectives, and
- Include Rolling Objectives from shared OSINT data, ensuring that the data is either relevant to the SOC or its clients.

At the end of the planning the Mission Developer (MD) will document the plan into the SOC operations order format and save this document to the appropriate shared location.

### MISSION OBJECTIVES

The mission objectives will be set during mission planning. The objectives take two forms: specific and implied objectives. Specific objectives support fulfilling required contract deliverables and/or SOC Continuous Process Improvement (CPI). Implied objectives are commonly those outcomes that contribute to success. Perennial implied objectives could include knowledge and application of the Incident Response Plan, as necessary, and reporting of suspicious/malicious data to the appropriate client. Standard specific objectives will be developed and assigned during mission planning; typical objectives include:

- Surveil client terrain for TTPs

- Discover data related to client Requests for Information

### ONGOING PROJECTS

Projects can be assigned through SOC administration or a higher position within the organization. A client could also introduce projects, but these should go through administration and/or management before assigned to the SOC directly. The Mission lists these projects to aid with communication within the Team. A SOC could have multiple types of projects including short-term and long-term projects. Projects that will always exist within the SOC could include query development for Threat Hunting. A centralized project board or tool may aid with project management.

### ROLLING OBJECTIVES

Rolling objectives are a list of OSINT analyses or articles that can "roll" from one Mission to the next. These resources help provide the SOC situational awareness of the cyber landscape while balancing Threat Hunting and Project Work. If an individual has completed their assigned taskings for the day and has no Project Work, then one could self-assign one of the rolling objectives or other OSINT research, specify the resource chosen for analysis in the mission log, and begin their research. This research can lead to supplementary Threat Hunting, development of new Threat Hunting queries, and/or an entry to the utilized threat intelligence platform(s).

## Final Mission Plan

Once the Mission begins, the mission plan is seen as finalized. The mission runs using the plan produced during the mission planning meeting. Exigent circumstances take precedence over this MP, in which case, the team will follow the instructions of the MD, CC and/or Director.

## Mission Execution

When the Mission starts, analysts use SOC systems to execute the tasks and communicate in accordance with the mission plan. Encourage analysts to take individual notes while they are on mission to help with the debrief process. The mission plan cannot be changed while the mission is taking place. However, a "Hold Short" can be issued to a crewmember or to the entire team, which puts the assigned Mission objectives on pause. For more details, see *Appendix A*. Identify a centralized mission log for communication and tracking objectives.

### MISSION LOG

A centralized mission log could utilize any of the popular group chat programs such as IRC, Slack, or Microsoft Teams. As with the adoption of any tool / application, the SOC should identify use cases beforehand and ensure that any compliance standards or other expectations are met. Use one specific channel for mission-based communications, and create other channels for helping new crew members, social interactions, and other relevant activities. The only text on your mission channel should be appropriate mission communications, to maintain focus and decrease confusion. Appendix A contains a sample of comm calls, for reference.

### Post-Mission Debrief Process

Once the mission has finished, the mission developer will lead a debrief with the team to determine if the mission was successful, if the mission plan covered the needs of the mission and quantifying the performance and efficiency of crewmembers during the mission. The MD will review the mission report with the team, and each crewmember on shift will take turns speaking in an "around the room" format, discussing the following:

- Objectives assigned and completed
- Any findings of interest
- Objectives left to complete
- Any issues identified/encountered, with fixes

### COMPLETING THE MISSION REPORT

Each SOC should identify a MisRep template to help standardize the process of a post-mission debriefing. There should also be a centralized location (e.g., SharePoint) where the mission developer can upload the MisRep upon completion of the debrief.

## Sample: Reporting Procedures

All SOC staff are expected to follow a standardized set of processes and procedures when escalating incidents to clients. Incidents added to the SOC's case management system should follow all associated documentation and standards. While Incident Reporting should have an internally utilized template to follow, each client may request a different level of specificity in their received reports. It is the SOC's responsibility to internally document these expectations and to do internal quality assurance / quality control before submission of a report.

### Incident Detection

When an analyst identifies Indicators of Compromise (IoC) or suspects/verifies a threat to the network, they should create a new incident case or ticketing event, depending on the software application utilized. When adding this new ticket/case, a unique ID number or identifier should be assigned automatically. If the affected client utilizes a method of report promotion that is not within the same tool (such as the use of email as opposed to a shared ticketing system), this number will become the report number. As the investigation progresses, information related to the event will be added to the appropriate case management tool. This can include spreadsheets containing traffic and/or process data and the final report as sent to the SOC client, if conclusive and not dismissed as a false positive.

### Incident Reports

Unless advised otherwise by a client, write all investigated incidents in a defined standard word processing software (e.g., Microsoft Word) to ensure compatibility within the SOC and with clients. Any information that is placed into the report must be timely, relevant, accurate, specific, and actionable.

Suggested Report sections:

- Title: Each report title will include the assigned report number with the report category and priority ranking. The table below articulates the distinct categories for reporting.

- Summary: What is happening? Why is it important? Why is it being promoted? Data in this section should include hostname, username, and malicious file / command line, as well as malicious hashes.
- Log Source(s)
- Details: More in-depth than the Summary. Break down the events that led to the malicious activity in a step-by-step manner and link back to MITRE ATT&CK, providing evidence from the logs.
- Times (detection time, start time, stop time/on-going)
- Category of Report (see chart below)
- References: Links to OSINT or other supporting data. Could include VirusTotal for hashes, Malware Analysis articles for the malware family, or Microsoft/Linux documentation for how certain executables/arguments work.

| Category | Description |
|---|---|
| **Information** | Shared for situational awareness – no action is necessary. |
| **Suspicious Activity** | Something is acting in an unexpected way, but the SOC cannot confirm malice. |
| **Vulnerability** | There is a known exploit in the wild for an asset/service you utilize. |
| **Risk Activity** | Confirmed activity that weakens the overall Confidentiality, Integrity, and/or Availability of your infrastructure. |
| **Breach** | A threat compromised your infrastructure, and/or exfiltrated data. Incident Response falls under this category, unless confirmed as a false positive. |

Cite information included in the report to the original source(s). If, while drafting the report, the author makes an assertion based on the facts presented, a discrepancy must be made between this statement and prior statements of fact. This could be identified with the text [ASSERTION] directly after the asserted statement or stating that the SOC "speculates" about a particular event. See the example below for usage of the [ASSERTION] tag. Document as much information as reasonable.

## SUBMISSION OF REPORTS TO CLIENTS

Once written, upload the report to the SOC's case management application following the documented process. To notify the Crew Commander that a report is ready for review, post to the mission channel, tagging the CC with "Happy Birthday" with the assigned report number, and include a hyperlink to the case in the application. The Crew Commander will then review the report for clarity, completeness, and proper application of the relevant framework, and ensure the associated case includes all relevant tags and data.

Once approved, the CC will forward the report to the client for investigation and remediation. Upload the official report for the incident to the case management system. After sending the report to the client, the Crew Commander will annotate the event as sent. The Crew Commander will announce “Happy Trails” with the associated report number within the mission log.

## TASK CLOSURE

Crew Commanders will mark cases in the case management application Closed once the associated client communicates to the SOC that the incident is closed or after 14 days without supplemental communication related to the incident.

# Technical

When setting up a SOC, consider the necessary tools and potential hardware for conducting SOC functions. In the Operations chapter, there were references to tools such as SIEMs, a communications tool, and physical workstations. This chapter will help build the framework necessary for ingesting and processing logs from a client's environment, using Open-Source Intelligence to enrich processed logs, and ensure the proper applications are in place to aid with the analysis and tracking of potentially malicious activity within those logs. If applicable to the SOC's use case, the infrastructure may be divided into a production environment and a test environment, depending on the tools utilized and their levels of testing.

This document is written to be tool agnostic, so while specific brands or tools may be mentioned as examples, this should not be interpreted as an endorsement or suggestion that one tool may fit needs better than others – each SOC will need to identify their own requirements, use case(s), and budget, before determining which tools work best for them.

Required Tools:

- SIEM
- Case Management
- Learning Management System
- Ticketing System
- Server(s) to host tools
- An application bundle that includes a word processor and spreadsheet program
- Individual workstations

Suggested Tools:

- Syslog Server
- Threat Intelligence Platform
- Project Management System
- Change Management System

# Required Tools

## SIEM

A Security Information and Event Management (SIEM) application will process all logs generated for analysis (including clients' logs and internal SOC logs). There are multiple well-known industry standards including the Elastic Stack and Splunk, both of which have free options if hosted locally and ingesting under a vendor-specified threshold of data. The SIEM will be utilized by Analysts daily to fulfill responsibilities like Threat Hunting, responding to Alerts, and other processes put in place by the SOC.

### Log Ingestion

After choosing and acquiring a SIEM, the SOC will need to understand how to ingest logs. Many SIEM solutions will have their own brands of agents, which are applications placed on an endpoint to pull

specific data. For example, the Elastic Stack utilizes a family of agents called “Beats,” which are pre-programmed to pull specific data upon installation, while Splunk utilizes a Universal Forwarder. Each SIEM and their agents have their own pros and cons.

## Case Management

The SOC needs a method of tracking suspicious and malicious activity, once identified by a SOC Analyst. The Case Management application allows for a centralized resource to hold Analyst findings, while applying a level of cross-referencing or OSINT data to enrich the data entered. For example, if an Analyst adds a malicious hash value to the Case Management System, it may connect that case with other cases in the organization with the same hash and/or apply OSINT resources to determine its reputation. Some Case Management Systems also provide the option to designate tasks and assign those tasks to other users, should a particular incident’s analysis require compartmentalized taskings. Examples include StrangeBee’s TheHive and Atlassian’s Jira.

## Learning Management System

A new SOC may be able to train through shadowing and one-on-one instruction. However, a larger SOC can benefit from a learning management system, or LMS, to aid in efficiency and standardization of onboarding and training for staff and interns. This section will not dive into the training process directly, but the chosen LMS should have the capability to support training without hindering a trainee’s potential through technological restrictions.

## Ticketing System

A ticketing system (e.g., Remedy, ServiceNow) is a critical component of the SOC infrastructure. This tool enables the SOC to track status of open issues, communicate, and ensure the tracking of client needs to completion. Workflow generation ensures that required actions are completed by individuals or departments in a timely manner or are escalated per SOP.

Evaluate various products to match your organizational need. Some products are considerably basic, and others – such as ServiceNow – are far greater in capability. The ticketing system may be configured to accept direct input from clients, which can streamline communications, or it may be reserved to the SOC organization. A ticketing system optimized for several external clients may not work as well for a SOC that wishes to communicate with the internal information technology operations team.

Ticketing systems may integrate with Case Management systems, or incorporate the function, depending on the product or modules purchased.

## Servers

As the SOC obtains the necessary applications for building the foundation of the day-to-day processes, one must also identify where these applications are hosted. Should the SOC pursue a Software-as-a-Service (SaaS) offering from a vendor, the vendor may provide the hosting platform themselves, in their own cloud or through a reputable cloud service such as AWS or Azure. If the Software-as-a-Service option is not offered or otherwise obtained by the SOC, a separate storage solution must be identified. Going through a cloud service (such as AWS or Azure, listed above) to host the data is an option, as well as

hosting locally, should the SOC have the physical equipment and storage available. A hybrid option between cloud and on-premises is also equally viable.

### Office Applications

Daily SOC operations include writing reports, sorting through spreadsheets, or working to present data in an understandable format. To support those objectives, an office bundle should be obtained if not already. Necessary applications within this office bundle should include a word processor, a spreadsheet program, and a presentation software, if within scope of the SOC. Examples include Microsoft Office, LibreOffice, and OpenOffice.

### Individual Workstations

Some level of physical computer should be provided for staff and interns. Specific operating systems, pre-installed applications and other organization-specific data will not be included here, but the system should allow anyone working on SOC tasks to accomplish their work without being slowed down or otherwise inconvenienced by the technology. If there are specific applications necessary for completing SOC work, install and pre-configure those applications. Additionally, consider the necessity of obtaining logs from these workstations – install and configure the necessary endpoint agents for centralized logging in the chosen SIEM prior to distribution.

## Recommended Tools

### Syslog Server

A syslog server, sometimes abbreviated as SLS, is a centralized host that holds logs, but does not process that data. Many SOCs will utilize the syslog server as a central location for clients to send their logs, so that the SOC can then parse the logs to the appropriate SIEM(s) in a scalable solution without having to collaborate with each client for custom configurations. This is a recommended but not required tool, as there is the option of sending client logs straight to the SIEM without a syslog server in place.

### Threat Intelligence Platform

As a supplementary tool to manual OSINT research, a SOC could utilize a threat intelligence platform, or TIP, to help aggregate, correlate, and analyze threat data from multiple sources in real time to support defensive actions. Many SIEMs can ingest Threat Intelligence data from a TIP to supplement or enrich the logs being ingested from clients. Setting up an alert for any relations between the threat intelligence data and the ingested logs will allow for faster response time and increased efficiency from the SOC team, rather than manually querying for indicators of compromise.

### Project Management

Project management is critical to identifying, pacing, and communicating medium to long-term projects for the SOC. However, this is listed under recommended, as utilizing a project management specific program is not required to maintain projects, so long as there is a centralized resource with a defined/documented expectation of communication and a team-wide understanding of who is responsible, accountable, consulted, or otherwise informed.

## Change Management

Mirroring project management above, change management is a concept that should be in place for a SOC, not a requisite tool or application. The main purposes are for communication and being able to track how changes to one application or process may affect others within the SOC and/or organization. Each SOC should implement the process in the method most beneficial to their team or organization.

# Conclusion

This guide explores the four areas required to build a functional SOC: administrative, academic, operational, and technical. Administrative details involve ensuring that the people and departments are in place to support the ideology and intent of a SOC and the staff within; Human Resources, a budgeting group, legal consult (where necessary), and a marketing and/or outreach team are crucial to ensuring overall success of the SOC's foundations as well as its marketability. Academic elements of maintaining a SOC focus on prior knowledge and the onboarding process of staff and interns, ensuring that all staff are aware of the skills and abilities they must have for carrying our SOC processes, either internally or for clients, without the presumption that specific skills are inherent to the field. Operational elements focus on the internal documentation that should be in place to support the SOC from the inside, allowing for the standardization of skills, tools, and processes across the board. Lastly, the technical chapter can be used as a referenceable checklist for the types of applications and tools necessary for implementing a SOC with standard services.

# Appendix A: Sample Communication Codes

The following table explains the brevity codes and common phrases used in the mission channel. It is imperative that mission analysts utilize the phrases agreed upon by the SOC to reduce confusion and to enhance clarity and focus.

| Criteria | Auth | Comms | Action |
|---|---|---|---|
| The crewmember has arrived for their shift. | All | On station [COMPUTER NAME] / [location] | Sit down at the system ready to start. Computer Name is optional in this call. |
| Leaving mission | All | Off station | Leave the ops position for the shift, or for an unknown extended period |
| Need to visit rest room, get water, away for <8 minutes | All | Station break | Leave ops position for no longer than 8 minutes |
| Taking a lunch break | All | Station Break – Lunch | Take lunch and respond with "On Station" once returned. |
| Request to leave the mission for longer than a short break | All | Request Exit | Wait for confirmation from CC/MD then call off station |
| Allow a crewmember to leave for a long break | CC | Exit granted NAME | |
| Start of mission execution | MD | Begin mission | All crew start executing the Mission plan |
| Begin end of mission actions, normally 30 min prior to end of Mission | MD | Home stretch | All crew start executing end of mission activities |
| End of the mission execution | MD | End mission | All crew finish last task and begin debrief prep |
| Taking over a crew position from another crewmember during IR | Inbound crew person | Tapping in for NAME | Assume tasks of person NAME |
| Acknowledging as relieved by another crewmember during IR | Outbound crew person | Tapped out by NAME | Leave the ops position allowing NAME to sit down/assume tasks |
| Emergency evacuation of work environment | Any | Evac | A crewmember calling evac indicates that their working conditions are unsafe, and they will be off station while |

| | | | |
|---|---|---|---|
| | | | responding to the environmental change. |
| Reviewing topic/IOC /TTP | Any | Tracking RELEVANT DATA | Begin research, add entry in TIP (if necessary), and begin hunting for IoCs, TTPs, etc. Write report, if necessary. |
| A new report has been written and is ready for the CC to review and send to the client. | Any | @CC Happy Birthday [Report Name] | Post |
| A new case has been entered to be referenced later [e.g., Plaintext Credentials] | Any | @CC Happy Birthday Case #xxx | Post |
| Sent report to client | CC | Happy Trails [Report Name] | The report has been sent to the client and further investigation is no longer required. |
| Promoted Case has been approved by the CC and is ready for long-term storage / later reference. | CC | Case #xxx Reviewed | The CC has reviewed the case entry, added the appropriate marking of review / approval, and has completed their portion of the Case. |
| The previously mentioned DATA is not relevant to clients, previously identified as something unimportant, or is otherwise not a risk. | All | Splash DATA | This data is left alone and not acted upon. Crews move on to other tasks |
| Mistake in previous message | All | CORRECTION: [DATA] | The previous post from this crewmember is erroneous |
| Notify the team of something related to the Mission, a client, or otherwise important data. | All | @Mission FYSA: INFORMATION/TOPIC | The SOC should review info to enhance other tasks |
| The client has requested we look for specific info mid-mission | CC | BOLO: INFORMATION or new data to BOLO | The SOC should review info to enhance other tasks |

| | | | |
|---|---|---|---|
| Asset indicated is unreachable. | All | SICK: [asset] | Mission Support starts troubleshooting and prepares to start contingency plan |
| Asset indicated is inoperative. | All | BENT: [asset] | |
| The malfunctioning asset returns to functioning status. | All | SWEET: [asset] | |
| Crewmember is ready to accomplish tasks but is not actively working | All | NAME Standing by | |
| Crew commander needs team or crewmember to wait for further instructions | CC or Director | Hold short | |
| Ask if crew are functioning and working effectively | CC | @Mission Report in | All analysts report status (Standing by, Current Tasking) |
| Ask if a specific crewmember is functional/effective | CC | @NAME Report in | NAME reports status (Standing by, Current Tasking) |
| Tag Mission Support and request current asset health for a particular asset. | Any | @Support Asset Status for [ASSET] | The SysAdmin for the Asset determines |
| The crew commander is flying solo and finishing the mission off site | Any | Change of Venue | Commander leaves the SOC and will report back in via On Station call |

# Glossary of Terms

| | |
|---|---|
| **CC** | Crew Commander; the lead SOC employee on shift |
| **CPI** | Continuous Process Improvement |
| **IoC** | Indicator of Compromise; often used to refer to IP addresses, hashes, domains, etc. |
| **IR** | Incident Response; the actions conducted to address a potential compromise |
| **IRP** | Incident Response Plan; the outlined process for handling a potential compromise |
| **KSA(s)** | Knowledge, Skills, and Abilities |
| **LMS** | Learning Management System |
| **MD** | Mission Developer; the lead SOC strategist for the Mission's objectives |
| **MTTD** | Mean Time to Detect; often associated with an organization's IRP |
| **NIST** | National Institute of Science and Technology; responsible for creating multiple foundational frameworks, esp. for cyber security |
| **OSINT** | Open-Source Intelligence |
| **QA** | Quality Assurance |
| **QC** | Quality Control |
| **RFI** | Request(s) for Information |
| **RFP** | Request(s) for Proposal(s) |
| **SaaS** | Software-as-a-Service; the application vendor oversees configuration/management, rather than the SOC |
| **SIEM** | Security Information and Event Management |
| **SLA** | Service Level Agreement |
| **SLS** | Syslog Server |
| **SME** | Subject Matter Expert; the topmost authority and/or go-to person for a particular tool or KSA |
| **SOC** | Security Operations Center |
| **SOCaaS** | SOC-as-a-Service; an outsourced SOC that performs functions as though an internal SOC for a client company |

| | |
|---|---|
| **SOP** | Standard Operating Procedures |
| **TIP** | Threat Intelligence Platform |