MSP1

Whitepaper: Creating and Maintaining a SOC

Introduction

Security is becoming more and more established in the corporate structure—it is no longer acceptable for security to be a secondary function of an IT department. To address this challenge, organizations are investing in the development of security operations centers (SOCs) to provide increased security and rapid response to events throughout their networks. Building a SOC can be a monumental task. Although the finer points of SOC deployment are very much network-specific, there are several major components that every organization must include: people, process, and technology. The three exist in all elements of security and should be considered equally critical components. This paper explains how strong people and well-defined processes can result in an operationally effective SOC.

Proper planning is critical in the development and implementation phases. As with many security programs an iterative process is most effective in developing a refined set of procedures. This approach will allow an organization to more quickly recognize benefits from their investment, positioning them to take advantage of knowledge gained and lessons learned through the actual operation of the SOC. It is important to set appropriate expectations and timelines for the deployment of the SOC so the initial operational period is viewed as a period for refinement.

The primary components of a SOC reviewed in this paper are:

- Define the security operations center—Establish the mission, responsibility, and scope of the SOC
- Determine the processes—Identify and clearly document key templates, procedures, and processes required to support the SOC
- Understand the environment—Determine the technical domain to be monitored, the "use cases," and the type of data that is received by the SOC
- Identify the customer—Determine the classes of customers and their interaction with the SOC
- Staff the SOC—Define the operational hours and the required staff per shift
- Manage the events—Categorize, assign, and prioritize events received by the SOC
- Leveraging ITIL—Understand the core ITIL components to continually run an effective SOC

Define the Security Operations Center

The first and most important component when implementing a SOC is to define the mission, charter, objectives, and responsibilities. Defining these core items will ensure its longevity and help avoid conflict with other companywide functions. To begin, create a SOC manual that formally documents each of the following items:

- Mission
- Charter
- Objectives
- Responsibilities
- Operational Hours

This manual will continually be used as a reference for the SOC staff and management. The definition statement should be clear and provide specific detail as described in the below example statement:

"The SOC is responsible for monitoring, detecting, and isolating incidents and the management of the organization's security products, network devices, end-user devices, and systems. This function is performed seven days a week, 24 hours per day. The SOC is the primary location of the staff and the systems dedicated for this function."

The above example may not be comprehensive for some organizations and should be expanded upon with more specific details based on your organization's mission and objectives. Once the responsibility definition has been documented, a list of service functions for the SOC must be defined. These may include:

Service functions	

▪ Status Monitoring and Incident Detection
  o SIEM Console
  o AV Console
  o IPS Console
  o DLP Console
▪ Initial Diagnostics and Incident Isolation
▪ Problem Correction
▪ Security Systems and Software
  o Update and test DAT definitions
  o Apply corrective IDS/IPS and Firewall Rules
  o Apply other corrective software as instructed or required
	▪ Computing Equipment and Endpoint Devices
	  o Remote administration
	  o Update antivirus
	  o Tune HIPS alerts
	  o Configure whitelisting
	▪ Work with Third-Party Vendors
	▪ Escalation to Next Tier Level
	▪ Closure of Incidents
	  o Coordination with tier levels
	  o Coordination with end users and system administrators
	▪ Persistent Threat Investigation

The service functions, once defined, will guide the daily processes and procedures for the SOC staff. Once each service is defined, each tier within the SOC can be assigned a series of responsibilities based on each individual's expertise within the tier level. For example, monitoring the antivirus (AV) and security information and event management (SIEM) console may be a service function of every tier; however, working with third-party vendors may be a service function only reserved for tier 2 or tier 3 SOC staff. Once each service function is defined, a series of documents must be developed to ensure the appropriate information is gathered during an event or incident and to ensure consistency across all SOC staff.

Determine the Processes

The number of processes and procedures for a SOC is determined by its scope, how many services are offered, the number of customers supported, and the number of different technologies in use. An established global SOC environment may have tens or even hundreds of procedures. At a minimum, the basic procedures that are required for maintaining the SOC are:

- Monitoring procedure
- Notification procedure (email, mobile, home, chat, etc.)
- Notification and escalation processes
- Transition of daily SOC services
- Shift logging procedures
- Incident logging procedures
- Compliance monitoring procedure
- Report development procedure
- Dashboard creation procedure
- Incident investigation procedures (malware, etc.)

Required templates

A series of baseline templates should be created to help maintain documentation consistency by establishing the same format and basic information sets across policy and procedure documents. For example, templates for proper data input into ticketing systems and the GRC system will need to be developed to help ensure the appropriate technical information is gathered.
A few key templates required are:

- Shift log templates for each use case
- Templates for each incident trouble ticket category

Reporting process

As a primary function, regular reports will need to be generated and provided to different audiences within the organization. Usually a weekly report is prepared for incidents, detailing the activity within the SOC. These reports can be delivered to management and other members on the core escalation contact list.

The SOC manager should review all incident records regularly to ensure they were resolved within the parameters of the defined severity levels. The manager should also audit incident records that have exceeded standard resolution times to validate that the incident records were handled appropriately. The SOC processes and procedures should be reviewed regularly and updated based on the report data reviews and audits. In addition, many other reports can be created depending on the type of data received or requested by management.

For a very detailed list of reports, refer to the "Operationalizing Information Security Putting the Top 10 SIEM Best Practices to Work" by Scott Gordon in the references section. Among these items are other key reports to measure staff on, including:

- Shift log metrics
- Trouble Ticket metrics

Understand the Environment

Without an understanding of the technical environment, it will be difficult to investigate and to understand if an actual attack has occurred. For this reason, the staff within the SOC must have the appropriate tools, diagrams, and knowledge of the network to perform their daily job. It is important to have both an electronic and a hard copy of the key network and application architecture diagrams.

For any new SOC staff, navigating and understanding the environment should be included as part of their required basic training. This will also help meet SLAs and overall customer service within the SOC.

As a part of the SOC's service functions the security architecture will be defined and the SOC staff will have access to the different components and tools within that architecture. These may include, but are not limited to:

- SIEM monitoring and correlation
- Antivirus monitoring and logging
- Network and host IDS/IPS monitoring and logging
- Network and host DLP monitoring and logging
- Centralized logging platforms (syslog, etc.)
- Email and spam gateway and filtering
- Web gateway and filtering
- Threat monitoring and intelligence
- Firewall monitoring and management
- Application whitelisting or file integrity monitoring
- Vulnerability assessment and monitoring

Developing Use Cases

To ensure the SOC is effective, a series of Use Cases must be defined. The term "Use Cases" may be a little misleading—think of them as events that require SOC intervention and/or monitoring. For instance, a repeat attack from a single source is a Use Case. It's an actionable component of the SIEM in which the SOC was notified of, through the network's primary monitoring tool. A Use Case may include the involvement of a Rule, Alarm, or even a Dashboard to meet the organization's requirements. Before defining Use Cases, it is important to have a firm grasp on the company policy, its assets, and the technical environment. A good way to develop Use Cases is by viewing the network from an attacker's perspective; think of a disruption to the environment. Another option is to look at the regulations the organization is subject to and evaluate the items that could become non-compliant. Below is a list of some important Use Cases to consider when initially setting up the SOC.

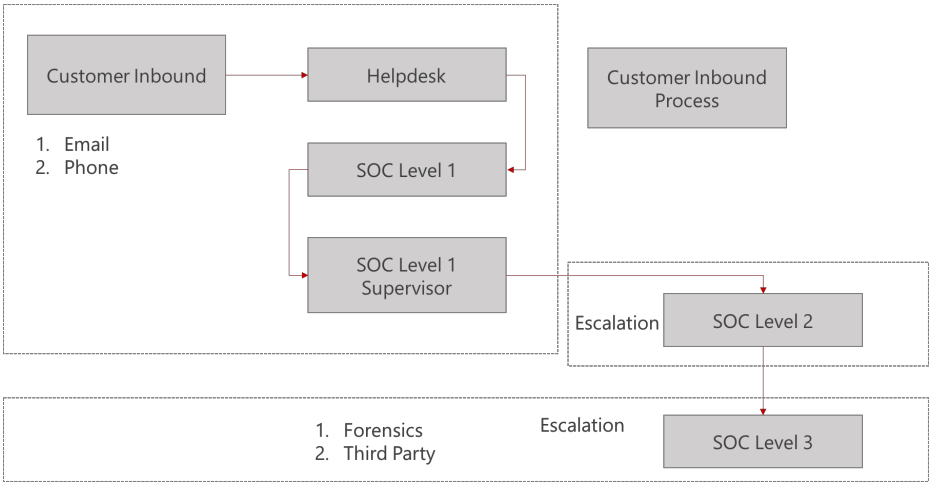
Use cases	
▪ Repeat attack from a single source	▪ Anomaly in DoS baselines
▪ Repeat attack on a single ID	▪ Anomaly in recon baselines
▪ SMTP traffic from an unauthorized host	▪ Anomaly in malware baselines
▪ Antivirus failed to clean	▪ Anomaly in suspicious activity baselines
▪ Excessive SMTP traffic outbound	▪ Anomaly in user access and authentication baselines
▪ Excessive web or email traffic outbound	
▪ Excessive traffic inbound (streaming, web, etc.)	▪ Anomaly in exploit baselines
▪ Excessive access to a malicious website from a single internal source	▪ Anomaly in network baselines
	▪ Anomaly in application baselines
▪ Excessive connections to multiple hosts from a single host	▪ Multiple logins from different locations
	▪ Multiple changes from administrative accounts

- Excessive exploit traffic from a single source
- Excessive exploit traffic to a single destination
- Excessive port blocking attempts from antivirus or other monitoring systems
- Excessive scan timeouts from antivirus
- Accessing a malicious website from multiple internal sources
- Service account access to the Internet
- Service account access to an unauthorized device
- Scanning or probing by an unauthorized host
- Scanning or probing during an unauthorized time window
- Multiple infected hosts detected on a subnet
- Unauthorized user access to confidential data
- Unauthorized subnet access to confidential data
- Unauthorized user on the network
- Unauthorized device on the network
- Unauthorized server connection to the Internet
- Suspicious traffic to known vulnerable host
- Logging source stopped logging
- Logs deleted from source
- Device out of compliance (antivirus, patching, etc.)

Use Case development is a critical component within a SOC and it must be understood. Below are two good write-ups that can be used to help understand the process for creating Use Cases as well as additional reporting that can be defined for the SOC environment.

Identify the Customer

In some cases, the customer may define which services are provided by a SOC. The entire organization may be a customer, or the SOC may be setup to support multiple client (customer) environments. For each of these customers, the SOC will provide a series of services and will need to determine the inbound communication process. The first step in defining the SOC's customer inbound process is to determine which services are provided to each customer. Is the SOC going to allow end users to call or will the SOC be facilitating calls and emails from the help desk and internal administrators only? Once the customer base, service functions, and tier levels have been defined,
the SOC inbound process should be diagrammed. An example is shown below.



Staff the SOC

Staffing a SOC can be more difficult than expected. Two questions that executives ask are:

- How many employees do I need?
- What skill sets are required?

The number of employees is dependent on the operating hours of the SOC. If the operations are maintained 24 hours a day, seven days a week, not only do shifts need to be considered, but you will also need to consider time off, sick days, and holidays. A standard 24-hour SOC must be maintained by at least seven staff members. If not, procedures should be put in place for off-hours monitoring.

This enables the staff to have a one-hour overlap for shift transfer and a floater to cover any holidays or time off when needed. This is discussed in more detail in the Staffing Schedule section below.

Finding the right skills and hiring staff is a difficult task at the current time because there are a limited number of security professionals in the market. The security staff within the SOC must have a solid background in many different aspects of computer technology usually focusing on networks, applications, and in some cases, reverse engineering. In addition, a good manager or director is required to ensure documentation, optimization, and reporting are maintained appropriately. Typical roles within a SOC may include:

- Security Analyst
- Security Specialists
- Forensics or Threat Investigators
- Manager or Director

Staffing schedule

When setting up a SOC, ensuring you have appropriate coverage is critical. Some SOC operations will support 24/7 operations, and others will have limited remote support after certain hours. The following tables are a partial representation of the staffing hours for an eight-week period. Each SOC engineer is assigned per the shift schedule for the eight-week period. These engineers are identified by A which reflects the morning shift in the SOC and the afterhours shift Monday through Friday. The B represents the afternoon shift in the NOC center and the pager shift over the weekends.

SOC schedule		**Week**							
Staff	Level	1	2	3	4	5	6	7	8
Manager	M								
SOC engineer	SE	A	A	A	A	A	A	A	A
SOC engineer	SE	B	B	B	B	B	B	B	B

Time slot	**Monday**	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Saturday**	**Sunday**
00:00-00:30	A	A	A	A	A	B	B
----------	A	A	A	A	A	B	B
06:00-06:30	A	A	A	A	A	B	B
06:30–07:00	A	A	A	A	A	B	B
07:00–07:30	AB	AB	AB	AB	AB	B	B
07:30–08:00	B	B	B	B	B	B	B
----------	B	B	B	B	B	B	B

Holiday coverage

One item typically overlooked is holiday coverage. In most cases, holidays should be treated as normal business days. There should be dedicated staff in the SOC for the given shift as described in the organization's staffing schedule. All responsibilities regarding standard shift schedules should also be in effect.

Shift logs, incident logs, and turnover

Shift logs must be maintained for audit and to ensure continuity of the SOC operations. SOC shift logs should be maintained daily for every shift. Shift logs can also be maintained in a database or GRC system and used regularly to help identify past issues and the resolution of those issues. Any significant event or incident should be recorded in the shift logs. This includes all high-priority incidents, incident records, escalation actions, and any procedural problem that has or could have a security impact.

Some very specific shift log procedures that are typically overlooked are:

- Entries on the shift log are mandatory for each shift; a "blank" entry is not acceptable

- If there is no activity or no open problems to turn over, put an entry in the log that says "No incidents to turn over"

Shift log entries should use a defined format that includes the following:
- Details of the event
- Impact of the threat to the organization or asset
- Description of the items found during the investigation while researching the event
- Recommendations for the next analyst that might be taking over the incident

If possible, shift logs should be maintained in a secure role access controlled system such as a GRC.
A typical example of a shift log is below.

> Details:
> The SOC has detected traffic from <source IP / hostname> to <destination IPs> over <ports>. Information gathered would indicate the asset is infected with malware. Traffic activity is being reported by <device detecting traffic>.
>
> Impact:
> Malware is performing a remote call back, possibly leaking data or expanding its presence in the network.
>
> Description:
> <Detailed observations of the pattern and activity>.
>
> Recommendations:
> Find the source IP asset. Contain the device. If no signs of malware are found, determine the cause for the detected event and remediate. If signs of malware are found, perform the required antivirus updates and/or forensics on the machine. Remediate or clean the system prior to connecting it back on the network.

In addition to shift logs, incident log entries should also be kept. Although incidents should be maintained in a ticketing system, daily log entries should be used to transfer incidents. This log should follow a defined format that includes the following information: time stamp, staff initials, the incident record number, and a brief description of the incident or event. An example of a typical incident log entry is below.

Time	Incident Record #	Staff Name	Description of Event
07:30	No incidents to turn over	SOC engineer name	N/A

Event Management

The core function and technology within a SOC are based on events from hundreds or even thousands of different systems. Essentially the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon. The management of events must include a list of instructions that apply on a 24x7 basis. This does not necessarily have to be the Incident Response Program Guide or Handbook. An event is any element that comes into the SOC and is monitored; while an incident is an event that must be acted upon.

As a part of event management, the SOC provides telephone and email assistance to its customers covering some of the following areas:
- Malware outbreak
- Phishing attacks
- Social engineering calls
- Access to the organization's security portal
- Data leak/loss incidents
- Customer account lockout
- Customer inquiries

Also defining the guidelines for the level-one SOC support is important. These may include:
- Open an incident ticket for any problems noticed and reported
- Serve as the initial point of contact for customers on the organization's network
- Maintain daily shift logs

- Perform rudimentary testing and diagnosis
- Validate that the incident is not a user error
- Formally assign the incident to the SOC

Incident assignment, update, and escalation

Before assigning incidents and defining the escalation process, the organization will need to agree on the technical solution used to maintain the incident records. Depending on the requirements, the organization may leverage an existing trouble ticket system or may implement a separate solution.

The main aspect is to ensure the system allows for the assignment of the ticket and handoff if the incident continues past the SOC operator's normal work shift. This system must also provide a level of security to ensure that tickets with sensitive information are only viewed by those with approved access. To ensure quick attention to incidents, the priority level and timeline of the response must be defined as an incident is assigned. Below is an example of the different assignment levels that may be used.

Priority	Impact Description	Response Time
Priority 1	Multiple systems and devices affected/compromised or possible data breach.	Within 10 minutes
Priority 2	Multiple devices or users affected/compromised.	Within 1 hour
Priority 3	Multiple devices or users affected/compromised.	Within 1 hour
Priority 4	No impact, logging response.	No response

Priority should not be confused with severity. Severity will be explained below. Priority is the level of response time identified when the incident ticket is created or updated based on the extent of the impact.

Security severity

Providing clear and adequate details on severity levels is required for all levels of the SOC and its customers. Typically, four or five severity levels are used. Organizations will want to be very specific in defining the different levels. Below is an example.

Severity	Explanation
Severity 1	Critical Compromise. Major service disruption or publicly displayed attack.
Severity 2	Serious Impact or Compromise. Attack affects multiple customers.
Severity 3	Intermittent incidents or alerts, but not critical.
Severity 4	Informational, no security impact.

In addition, each severity must be expanded upon. For example, Severity Level 1 may be described as:

SEVERITY 1: HIGH

- System component complete compromise and possible full data-privacy breach
- Critical impact to the organization (reputational)
- Attack possibly still in progress
- Multiple systems, groups, and users affected
- Resolution Goal: 1 hour to immediate
- Immediate manager notification when incident record is created

Severity level 2 (Medium), level 3 (Low), etc. should also be defined in a similar manner.

Incident and event categorization

There are very good standards available to categorize events and incidents. These categories can be defined in the organization's Governance Risk and Compliance System and metrics can be tracked accordingly for each category. The ten categories defined in the Chairman of the Joint Chief of Staff Manual 6510.01B with detailed explanations of their use should be leveraged within the SOC.

These are:

- Training and Exercises
- Root Level Intrusion (Incident)
- User Level Intrusion (Incident)
- Denial of Service (Incident)
- Malicious Logic (Incident)
- Unsuccessful Activity Attempt (Event)
- Non-Compliance Activity (Event)
- Reconnaissance (Event)
- Investigating (Event)
- Explained Anomaly (Event)

Incident resolution and escalation procedures

Resolution of incidents in the SOC may tie into an existing incident response practice, but it must be included in the incident ticket record escalation process, which documents the steps required by the SOC staff. For resolutions of incidents many tasks will need to be completed, including:

- Documenting incident description and resolution
- Referencing any other trouble ticket or incident record IDs
- Closing the incident record and the communication methods used to notify the end user or tier level contacts
- Documenting the underlying root cause of the problem
- On high-priority incidents, the SOC should have a defined distribution list that is used for sending the problem resolution and assigned incident record ID

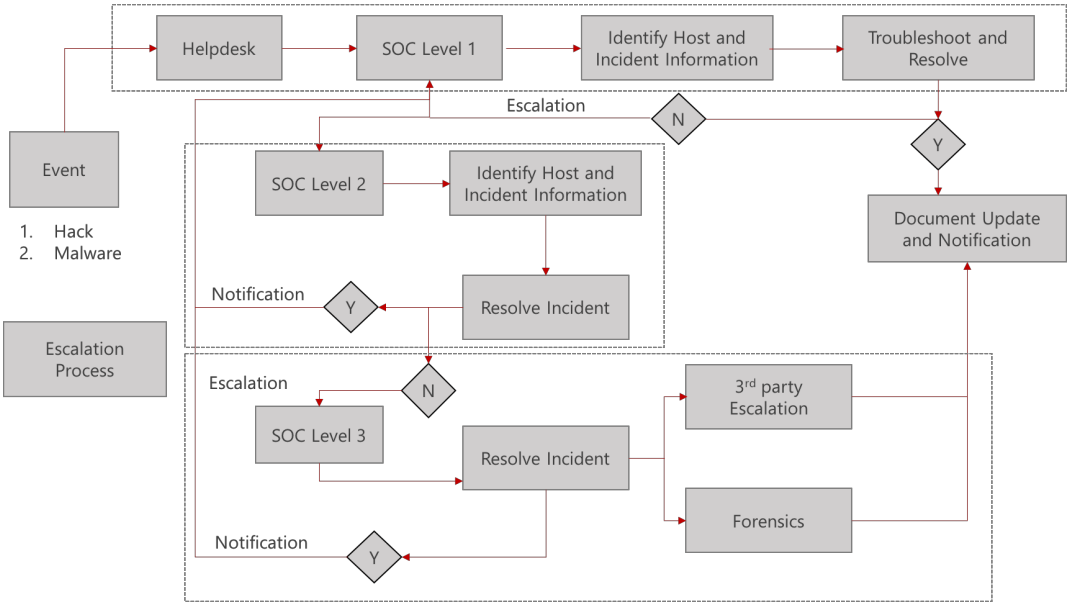
If an issue is not resolved at the first tier, then an escalation to the next tier is required and the SOC must have documented procedures in place to address the escalations. For example, if an issue is escalated to tier 2 the procedure in place may dictate something like the following:

> As initial Incident Record Owner, the Level 1 SOC engineer evaluates the problem and determines if he/she has the ability to resolve the issue.
> If the Level 1 SOC engineer has the ability to resolve the Incident Record, he/she:
>
> - Defines the incident in specific terms.
> - Gathers additional facts necessary for troubleshooting and resolving the issue(s).
> - Considers possible causes or options and creates an action plan.
> - Implements the action plan and observes results.
> - Iterate steps until issue is resolved or it needs Level 2 SOC assistance.
>
> If the Level 1 SOC engineer does not have the ability to resolve the Incident Record, the Level1 SOC professional determines if another Level 1 SOC professional or Level 2 SOC assistance is required.
>
> If field security support is required, the SOC professional uses the escalation process and then refers to the documented escalation procedures to dispatch an on-site security analyst.
>
> If Level 2 assistance is required, the SOC technician assigns the Incident Record to the Level 2 group responsible for resolving the problem, and then refers to escalation procedures to notify the appropriate Level 2 security professional.

There must also be additional escalation procedures in place. The SOC must have clearly defined procedures for the escalation tier that address, at a minimum:

- Resources to assist with resolution of incidents
- Review of open incident records
- Status updates
- No response from customer (again customer is defined as part of the SOC services and in many cases may be the end user or system administrator)
- Adding notes to the incident record
- Additional escalations
- Incident record closure
- High priority / high severity handling
- Lack of resolution

In addition, a detailed step-by-step process needs to be documented for each level in the SOC for the analyst to know exactly what information is required, who to contact, and how to deliver the known information quickly and accurately. Below is an example of this escalation process:



Third-party resolution and escalation procedures

In some cases, there will be a need to involve third parties in the escalation process. This may include when a software patch or antivirus update needs to be developed quickly. This may also include engagement of a third party to perform a more detailed forensics investigation and analysis. The SOC must have defined procedures in place for escalating these instances and the appropriate contact information to support that escalation process.

Incident escalation contact list

As a good practice, the SOC should maintain a complete and detailed escalation contact list. This should include all internal contacts, third-party contacts, distribution lists, and phone numbers as shown below.

Contact	Role	Phone	Mobile	Email	Escalation
SOC OP1	Level 1 SOC	###-###-####	###-###-####	SOCOP1@soc.com	SOC#OP2

Escalation guidelines

The process of correcting incidents requires that detection, isolation, circumvention, and resolution disciplines be established and practiced by all levels of the SOC. This process can and should be mapped to the phases in the incident response plan, where applicable. A structured progression of recommended actions that directs individuals to perform the appropriate meaningful analysis and actions while troubleshooting is required. The SOC staff must also have guidelines for referring incidents to the proper specialists when they cannot be resolved. These can be organized in a simple table format as shown in the high-level example below.

	Detect	Isolate	Circumvent	Resolve
Level 1	Notice of incident	Host status	Modify host	Primary configuration
	Validation of incident and host	Query alerts and events	Modify host	Confirm restoration
	Review logs	Perform analysis	Document errors and outcome	Close incident
	Open incident record and document issue	Update record with analysis results		Notify customer
Level 2	Review logs	Review incident record	Modify host	Develop, test, and deploy fix
		Run malware analysis		

Notice the phases of the incident resolution process evolve from left to right and from Level 1 to Level 2. When activities at one skill level have been exhausted on an incident, the incident should be escalated to the next skill level for further action.

Tier functional responsibilities

Functional responsibilities are important for each operator. Documenting the SOC functions and assigning these responsibilities to each level is necessary to ensure tasks are escalated and handled properly. Below is a sample of the functional responsibilities.

SOC Function	Level 1	Level 2	Level 3
Takes inbound request	▪		
Creates shift logs	▪	▪	▪
Logs incidents and requests	▪	▪	
Creates trouble tickets	▪	▪	
Isolates and validates incidents	▪	▪	▪
Monitors events and alarms		▪	▪
Plans and implements change		▪	▪
Performs forensics investigation			▪

Leveraging the IT Infrastructure Library (ITIL) Service Management Lifecycle

Because ITIL has such a focus on service management, the SOC management team should use it as a guideline to ensure consistent performance and management over time. Many organizations will assess or audit a SOC based on the ITIL methodology, especially if they do not understand the underlying technology or the effectiveness of its monitoring. As a manager, it is important to be prepared for these audits. This can be achieved by implementing ITIL processes throughout the SOC.

A few key items that must be in place are outlined in the following sections.
Service Vision and Strategy– The mission statement, charter, or group objectives.
Service Design– During this stage of the ITIL framework, it is important that the SOC has analysed and documented all the business requirements. This enables the SOC to provide value to the business and align the SOC's strategies and business objectives with the organization. This also enables the SOC to define key performance indicators (KPI) that can be leveraged to design services in accordance with the business requirements.

As we defined earlier, the service catalogue or "Service Functions" must be defined. For each of the SOC core functions, service level agreements (SLA) will need to be clearly defined with management. Typically, the business should drive the SLAs. Other key considerations that should be addressed are personnel management of the SOC and the continuity of the operations.

Service Transition– The important items to consider within this section are changes to the infrastructure. The SOC must be made aware of changes implemented across the enterprise. Otherwise, if monitoring systems are setup correctly, alarms will go off and unnecessary work will occur. Also, the SOC may perform specific services where they are responsible for change. As a result, tight integration between the SOC and change management is required.

Service Operations– The service operations were defined earlier. This is mostly how event and incident management is conducted for the business. Several items must be in place for service operations, including:

- Trend analysis
- Tracking of remediation items
- Reporting to the organization on SOC activities
- Classification of issues
- Software license compliance
- Tracking and inventory of assets

Continuous Service Improvement– Continuous Service Improvement identifies and structures an improvement process to enhance the SOC over time. This includes:

- Determining what to measure, such as use cases, alerts, shift logs, etc
- Defining what you can measure

- Gathering the data, in the SIEM, a Governance Risk and Compliance (GRC) system, or manually
- Processing and analyzing the data
- Reporting or sorting through the data to help understand and identify improvements
- Implementing the corrective controls and actions

Conclusion

Security becomes integrated into an organization's processes and every day it becomes more mature and over time, many organizations will choose to implement some type of security operations center.

A SOC can provide significant value as long as the proper planning occurs and sound processes have been created. Hopefully this document has provided insight for those either embarking on a new SOC or looking for improvements to their current operations.

With a solid managed operation and well trained employees an organization can rest easy knowing its customer base is happy with quality service and feels confident in the response to security events.

Contact Sales

+1 (408) 769 5030
+91 9769757668

www.MSP1services.com
info@msp1services.com

MSP1 helps businesses fight cybercrime, protect data and reduce security risk. We are a leading provider of cybersecurity solutions and services. Through our global SOC and delivery center we monitor detect, contain and remediate IT threats.

With integrated technologies and our team of security experts we enable businesses to transform the way they manage their information security and compliance programs. Our services are customized, tailored and white labeled that fit your budget.