SECURITY OPERATIONS CENTRE

THE PLAIN ENGLISH, STEP-BY-STEP HANDBOOK FOR SECURITY PRACTITIONERS

THE DEFINITIVE GUIDE TO BUILDING A WORLD CLASS

KENNETH HO

The Definitive Guide to Building A World Class Security Operations Center

Table of Contents

The Definitive Guide to Building A World Class Security Operations Center

INTRODUCTION

There is no shortage of threats to data security for the home computer user as well as for business and corporate owners. Private identities, accounts, files, and records data are under threat of compromise 24/7. Threats may

- Be internal or external,
- Impact the network and/or system, or
- Cause personal and sensitive data and systems losses.

Once information is compromised, it is hard to replace. Hurricanes, fires, and floods can destroy systems and massive amounts of stored data. However, hackers and infectious malware embedded in your system and network have farther reaching consequences, often for a much longer time and disastrous results. Information and data security ensures data is stored safely from corruption and its access may be controlled. A – centrally located operations unit provides greater control over a broader spectrum.

Malicious activity has become Web-based. Social networking sites are especially attractive to those who would exploit the end users instead of computers. Cyber attackers adapt and escalate activity as rapidly as patches, anti-viruses, and firewalls are created and updated.

Securing Data

Data security ensures privacy. In the rapidly expanding age of Cloud storage and sharing, securing data from unauthorized disclosure or modification / alteration and destruction are paramount. Security of multiple user data sharing must be in a central data location and require PINs, authentications, and other rights to access.

Utilizing a Security Operations Center (SOC)

Firewall, anti-virus, OS logs and intrusion detection systems (IDS) such as encryption, and physical password protection are not enough to ensure security today. A centralized security operations center (SOC) which handles security issues on an organizational and technical level is necessary in today's rapidly evolving, remote, and mobile technology environment.

- Firewalls do not protect users (only data).
- Anti-virus detection is slow to catch *new* threats and do not match traffic patterns.
- Intrusion detection systems (IDS) do not alert provide system, proxy, or DNS log information.

Definitively, a security operations center (SOC) is a centralized unit in an organization that deals with security issues, on an organizational and technical level. The SOC is usually centrally located within a building. It has an IT staff that monitors the site using data processing technology. The SOC typically monitors and has access and control to lighting and alarms, vehicle access and entry, and emergency systems as well as networked personal computers and shared peripherals.

Barriers to Adopting In-House Security Operations

Managed Security Services Providers (MSSPs) are often used to perform and manage most of security monitoring and testing. Advocates in favor of IT operations outsourcing contend that managing information/data security internally requires:

- a higher initial set up cost for the company,
- 24/7 monitoring,
- more capital to run and maintain operations upgrades,
- more accountability for network and systems changes, and
- long-term IT security professionals (high attrition rates can threaten a company's intellectual properties).

What MSSPs do and do not do:

- MSSPs do not know the organization's policies, procedures, or it's general IT environment.
- MSSPs do not have dedicated staff for smaller customers (larger organizations spending more will receive "dedicated support").
- MSSP security services are standardized (to gain economies of scale, no customized services, processes, or procedures are generally offered).
- MSSPs transmit and store organizations' security data at the MSSP premises, which may or may not be in the same country as the organization.

Advantages of In-House Security Operations

Cost and special business requirements may influence the decision to develop an in-house Security Operations Center (SOC). The advantages of an in-house SOC include:

- Having a central point for all information and Internet security operations,
- An innate familiarity with the environment than a third party,
- Close by real time monitoring of multiple security-related systems, and

- Threat prevention, early detection and quick response, and protection.

This Ebook intends to provide a guide and understanding on how to determine if an in-house SOC is appropriate for a particular organization, planning and staffing considerations, consideration of the customer and IT environment and best practices for maintaining a functional security operation center (SOC).

It takes into account the need for establishing a strong project and operations foundation while effectively and efficiency maximizing capital and utilizing available resources.

PART 1 – Building the SOC

Chapter 1 – The Security Operations Center (SOC): Mission, Scope, and Goals

The Decision to Build / The Mission

To determine if building an in-house SOC is the right decision, the organization should collectively ask:

1. How will an SOC benefit the organization overall?
2. What specific tasks will the SOC perform? (i.e.: detection, monitoring, incident response, forensic analysis, vulnerability assessments, etc.)
3. Who are the SOC customers? What SOC requirements and needs do they have?
4. Who will sponsor the SOC project ("sell it" to the rest of the organization)? What SOC requirements and needs do they have?
5. What "use-case" security events will be "fed into" the SOC for monitoring?

The Business Plan / Scope / Charter

Building, developing, and implementing an SOC requires a significant commitment of capital. The organization will want to know how and how long it will take for the SOC will return their investment. A plan outlining the necessary SOC components as well as a justification of expenditure should be prepared:.

Necessary initial and ongoing SOC components:

- **Building / Area** including furnishings, equipment, access security, power, telephony
- **Labor:** Analysts, Experts, Leads, SOC Manager(s)
- **Labor Support** techs for the network, system, database, telephony, security
- **Training** classes, continuing education, seminars and conferences
- **I T subscriptions** that provide real time threat information

- **Service Technologies** for implementation, monitoring, response, and change management (hardware / software, storage, email, knowledge sharing).

Cost Justification

Overall, building the SOC is proactive; it increases efficiency; costs may be shared; and services may be offered to customers for a fee. Additionally,

- Remaining vulnerable to attacks and unprepared to respond is more costly than building the SOC.

- The SOC can automate a number of the organization's current processes and technologies using a new data feed, reducing the cost of manual effort.

- Outside groups / agencies tasked with threat prevention, monitoring, and incident response may be willing to outsource these responsibilities to the SOC, which would help minimize cost impacts to both parties.

- There is the prospect to leverage SOC services to customers, especially internal customers, to recover initial costs as well as operational expenses.

Goals / Objectives / Responsibilities

After the mission and charter (scope) are defined, teams (labor and support groups) and their responsibilities, process and procedures, and technology must be determined. Typical team member roles within an SOC include:

- Security Analysts
- Security Specialists / Technicians
- Forensics / Threat Investigators
- SOC Manager(s)

Security events, or breaches, may be stolen, lost, compromised, altered, or destroyed data, network, and / or system. Firewalls, anti-virus (AV), and intrusion detection systems (IDS) prevent and provide alerts on events. These are not fully effective without continued, monitoring, suspicious event reporting, timely mitigation, and prioritized remediation by IT staff.

Initial data security involves

- developing an overall security strategy and
- risk assessment.

Identified risks provide warning to mitigate those risks as well as usable information when security analysts and experts encounter events that compromise, lose, or destroy valuable data, by theft, malware, or system crash.

Internal threats include:

- Human error (information processing error, unintended data input or delete)
- Malicious corporate activities / espionage

External threats include:

- Power outage, fire, theft
- Malicious corporate activities / espionage
- Universal attacks (viruses, embedded malware, code)

Identify areas of vulnerability. Strategies for securing data and information may include:

- Restricting data access,
- Restricting Internet and system email accesses (authentication required),
- Supervised use and maintenance of passwords,
- Relevant firewalls and anti-malware solutions, and
- Trained IT data security staff.

Prioritizing Information

Security Analysts perform IT forensics as the incident happens. They evaluate and prioritize specific data and determine what additional security measures are necessary. Having and maintaining a *Business Continuity Plan* is necessary so the security staff may continue working when systems fail. An organization's risks and security measures should be reviewed periodically and updated to keep pace with the growth of the organization and other changes.

Reporting / Reports

It is the responsibility of security operations Experts to mitigate the reported incident when phishing, data loss, stolen email, or other incidents are reported.

Regular reports must be generated and periodically provided to organization management and directors. Weekly reports are commonly prepared citing in detail, incidents, responses, and other activity within the SOC. These reports are typically provided to management and other members on the core escalation contact list (ref.: Chapter 8, Event Management).

It is the SOC Manager's responsibility to review all incident records to ensure events and incidents are resolved within the parameters of the defined severity levels. The Manager must also audit incident records, particularly those which have exceeded standard resolution times.

SOC processes and procedures should also be reviewed regularly and periodically updated as data reviews and audits require.

Other required report templates, such as *Shift Logs* and *Trouble Tickets,* may be created for data received or requested. Templates such as these are necessary to ensure the appropriate technical information is collected, recorded, and responded to in a timely manner.

The SOC Manual

At the onset, an SOC Manual should be created which includes the defined mission, charter, goals and objectives, and additional core items. This helps ensure the SOC's longevity and reduces conflict with other organizational functions. The following items must be included and periodically updates as the organization grows and changes.

- Mission
- Charter
- Goals and Objectives
- Staff and Responsibilities
- Hours of Operation

The *SOC Manual* should be made available in a central location which is easily accessible by all employees with the intent it is to be a reference guide for the SOC staff and management. It must clearly define, in detail, the main articles above.

Chapter 2 – SOC Staff: Hiring & Training

Security implementation includes more than the technology, firewall protection and virus scanning. It requires hiring competent, responsible, and reliable staff. It also requires on the part of management, to keep the employees IT skills and knowledge current through ongoing training, seminars, conferences, and visits from experts in the field.

"Organizations lacking sufficient internal skills, knowledge and resources to develop and maintain security architecture are at the greatest risk." However, outsourcing IT functions can be more costly in the long term, and comes with its own security-based drawbacks.

Hiring Qualified SOC Staff

A frequent mistake in-house SOC managers make is attracting people lacking the necessary skills required to detect, analyze, mitigate, respond, investigate, and protect the organization's data, network(s), and system.

The SOC Analyst is the daily mainstay of the SOC. Organizations must realize the importance of this front line position and require the candidate have a respectably high-level skill set. General qualifications should include:

- An understanding of the attention and thoroughness required during continued monitoring for malicious events which are typically masked by "nuisance events."
- Troubleshooting patience and the ability to research problems.
- The ability to calmly communicate during stressful times with intense customers.

A good decision may be to hire from within the organization. A help-desk technician familiar with the IT environment, process, and procedures may be an effective SOC Analyst.

A Systems Administrator, or Desktop Support or Network Operation staff having a troubleshooting background and experienced in network, server, and desktop support may more quickly adapt to tasks involving TCP/IP protocol suite and intrusion detection signatures.

SOC Analysts must undergo appropriate training that combines formal standard information security skills training as well as on-the-job training (OJT). To maximize the SOC Analysts' effectiveness, organized refresher mini-courses on new products, new

threats, mitigation techniques, and other skills upgrades should be included in the SOC Manager's training program.

Formal Training

The industry standard for formal Analyst training includes:

- The SANS (System Administration and Network Security) "Intrusion Detection in Depth" training module,
- The GCIA (GIAC Certified Intrusion Analyst) certification, and
- Fundamentals of TCP/IP, TCP/IP monitoring tools, and skills associated with advanced intrusion analysis.

These formal training pre-requisite qualifications are necessary for organizations having a standardized Security Information and Event Management (SIEM) program with ArcSight. The desirable candidate will be ACSA (ArcSight Certified Security Analyst) certified. ACSA training uses the ESM product to instruct analysts in properly identifying, correlating, and filtering critical security events.

On-The-Job Training

SOC Analyst on-the-job training programs should:

- Provide an overview of information security concepts,
- Instruct the analyst in how to use available intrusion detection tools,
- Brief the analyst on analytical processes and procedures, and
- Teach effective communication skills and combative communication techniques.

Communication is key to an analyst's success with stakeholders. The SOC Analyst should be aware they will be required to effectively communicate and brief all levels of senior management and engineers in stressful situations under less than idea circumstances. Learning how to manage combative communication is extremely important.

Communication training should also include the hierarchy of communication methods, which instructs the analyst when to call, email, or assign an incident ticket. Additionally, the analyst must learn how to effectively communicate in writing, such as in emails, memos, papers, and other correspondence.

Expansively, SOC managers should be encouraged to create programs that encourage analysts to express their experiences and finding in written analytical papers and presentations to peers and professional groups.

It behooves the SOC Manager to encourage team as well as individual professional development. As the team matures, more skilled assignments may be accepted, services expanded, and IT growth within the organization. It promotes good team morale as well as reduces the organization's daily IT risks from outside.

Chapter 3 – SOC Staffing Plans

Staffing a SOC raises initial questions:

1. How many employees are needed? and
2. What skill sets are required?

The number of employees depends on the SOC's hours of operation. Shifts and staff to man the SOC are typical for 24/7 SOC operations. Holiday, vacation, and sick leave must also be factored into the 24/7 shift schedule.

Unless off hour monitoring measures are in place, a standard 24-hour SOC is manned by a minimum of seven staffers. This provides a a one-hour overlap for shift change and "a floater" employee to cover holidays or time off. Additionally, all staffing activities must be consistently and properly documented, optimized, and reported by the SOC Manager.

Staffing Plans / Models

Staffing plans evolve directly out of the SOC's mission needs. The SOC scope, structure, and character are the basis for the SOC staffing model.

- What is the SOC and what does it do? A virtual entity where events are collected, analyzed, alerted, and reported?

- Is it necessary to have 24/7 monitoring, analysis, alerts, and reporting?

All staffing models, regardless of specific design, follow similar guidelines::

- For safety as well as performance reasons, no single SOC Analyst should ever be manning a SOC shift alone.

- Each SOC shift and SOC staffer should have a clearly defined role, known responsibilities, and be clear on expected deliverables.

- Each analyst must be thoroughly briefed on their role and what is expected from them at any given time during their SOC shift.

- A formal *Shift Log* documenting events and issues needing additional or continued attention must be kept and regularly updated by each shift. There must

be no ambiguity between shifts regarding what must be done and who needs to do it.

- Night shift staff must be apprised of SOC activities beyond what is logged. The SOC Manager must maintain constant communication with the night shift staff. When there is no designated SOC Night Shift Manager, the SOC Manager should schedule time to work with the night shift staff.

- **The 24/7, 365 days/year Shift:** Ten SOC Analysts are required to efficiently staff a SOC that operates on this model. The preferred shift schedule for this staffing model is four, 12-hour shifts per week:

    Each Analyst works three days with 4 days off, followed by 4 days on, and three days off for a total of 84 hours every two weeks.

    Additionally, two of the more experienced (Level -2) Analysts work an 8/5 shift and are available to cover shifts for planned and unplanned absences**.**

The Shift Log

Shift logs ensure SOC continuity of operations and must kept daily for every shift and be made available for audit. Shift logs do not necessarily need to be manually-kept records. They may be maintained in a database or GRC system. Shift logs are intended to be used frequently and help identify past issues and resolution of those issues. Significant events and incidents should be recorded in the shift logs, including:

- all high-priority incidents,
- incident records,
- escalation actions, and
- procedural issues that have had or may impose a security impact.

Frequently overlooked shift log procedures include “blank” entries. All required shift log entry lines are mandatory and should be acknowledged, never left blank. “No incidents to turn over” should be written when there has been no shift activity or open problems to turn over.

Shift log entries should use a defined format which details of the event, the impact the threat is to the organization, a description of findings during the event investigation, and recommendations to the next-shift analyst charged with taking up the incident.

Scheduling

Ensuring the SOC has the appropriate coverage is critical. Some SOC operations will support 24/7 operations schedules (as shown below), while others will have limited remote after hours support (Fig. 1).

DAILY SCHEDULE (8AM TO 8AM)				
Level 1 Analysts	Night Shift	Day Shifts 1 & 2 10AM to 10PM	Night Shifts 3 & 4 10PM to 10AM	
Level 2 Analysts	Day Shift 8AM to 5PM		Night Shift 5PM to 2AM	On-call Rotation
Security Engineers	Day Shift 8AM to 5PM		On-call Rotation	
SOC Management	Day Shift 8AM to 5PM		On-call Rotation	

Fig. 1 A Standard 24/7, 365 Day/Year Schedule

Chapter 4 – SOC Processes and Procedures

A process defines who is responsible for doing which tasks.

A procedure describes in detail how to accomplish the task.

A SOC's number of processes and procedures is determined by:

- Its size and scope,
- How many services it offers,
- How many customers it supports, and
- How many different technologies it has in use.

For example, a well-established global SOC environment may feasibly have hundreds of procedures.

Compiled and sometimes call the SOP (*Standard Operating Procedures*), SOC processes and procedures provide a guide for new Analysts when seasoned staff and management do not have the time to orient the new employee. Processes and procedures inform about current SOC routines and activities, sometimes giving information about how they came into being, SOC enhancements, and gaps in the process and how to overcome them manually to accomplish required tasks.

SOC processes and procedures must be mature. The process must have been adopted through continued repetition. It matures as it is continuously used and improved upon. *The Carnegie Mellon® Software Engineering Institute (SEI) Capability Maturity Model® Integration (CMMI)* provides Managers an eminent approach to continuous process improvement.

Capability Maturity Model® Integration (CMMI)

CMMI provides organizations a foundation to help get organized, and maintain and continually improve its vast numbers of processes and procedures. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.

CMMI Level 3 is considered a sufficient process and procedures maturity level for most organizations. Any Analyst on any shift executes a procedure exactly the same. if an

error is found or a change is necessary, the Analyst may make an immediate correction. All Analysts that follow will immediately benefit from the improvement. (This type of process and procedure maintenance is best achieved using the constant documentation update collaboration environment (e.g., Twiki or MediaWiki).

Process Hierarchy / Flow

There are typically fourteen primary processes, and about 36 subordinate procedures, as shown below (Fig. 2). Each process, with accompanying procedures, relies on the processes below them. So, metrics support process improvement; technology design and event management support intrusion analysis; and so on.

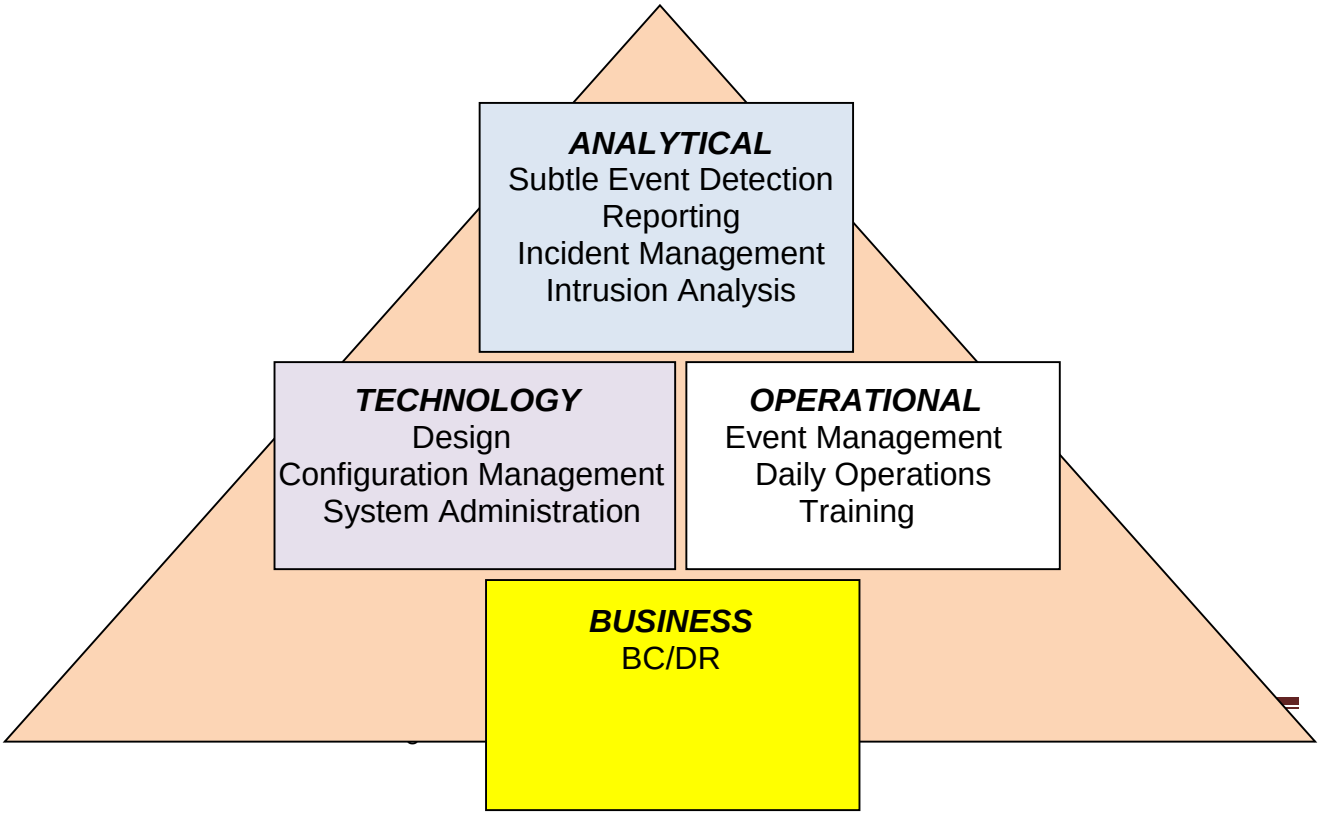
SOC processes may be put into the four main categories:

1. **Business Processes:** Document ALL administrative and management components required to effectively operate a SOC.

2. **Technology Processes:** Maintain all system administration, configuration management, and conceptual design information.

3. **Operational Processes:** Document daily operations such as shift schedules and turn-over procedures.

4. **Analytical Processes:** Include all activities that detect and understand malicious events.



Process Improvement
Compliance
Metrics

Fig. 2 Process Hierarchy

Organizational / Internal and External Relationships

The SOC must also maintain many internal team relationships (i.e.: Incident Response, Security Management, Security Engineering, Legal, HR, PR, and Lines of Business), as well as external teams (i.e.: CERT/CC, Information Sharing and Analysis Centers (ISAC), Law Enforcement, supporting product vendors, etc.). ALL points of contact (POCs) should be documented including their role and when the SOC should contact and include them in a developing (event) situation.

Detection and Analysis

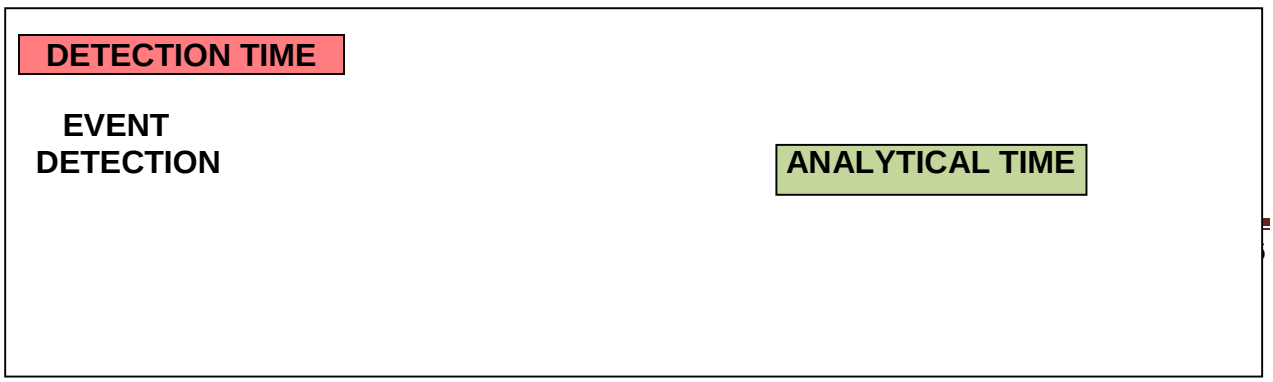
A distinction must be made between processes and procedures when developing them for the SOC (Fig. 3).

Detection time is the period from when an event is identified within the SOC, to when the analyst makes a decision as to how to act on it.

1. The analyst detects an attack.
2. The analyst conducts and initial research using intelligence about the various threats (Is it a true attack?).
3. The analyst determines the priority of the event and reports the event.

Analytical time begins when the operational time is over and continues up to 90 days.

1. Senior staff continues researching the events, using visual data mining and other analytical tools.
2. Necessary constituents a
3. re notified.
4. The event is reported.
5. A forensic analysis is performed (as necessary).



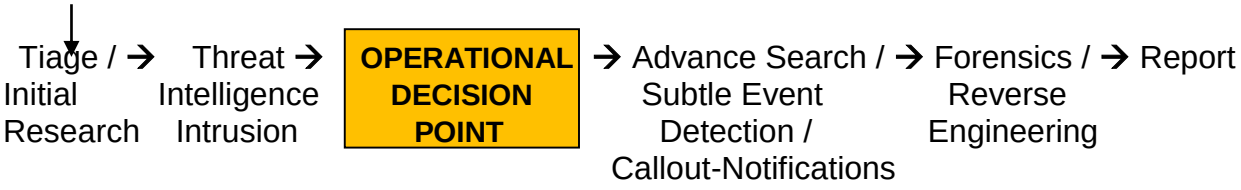


Fig. 3 Event Detection and Analysis

Procedures / Procedure Flow

Minimal procedures required for maintaining the SOC include:

- Monitoring; Compliance monitoring
- Notification (email, mobile, etc.)
- Notification and escalation processes / procedure
- Daily SOC services transitions
- Shift logging
- Incident logging
- Report development
- Dashboard creation
- Incident investigation

Each primary SOC process area has its own procedures. Below are examples from each area (Fig. 4).

Process Category	SOC Process	Procedure	Procedure Description
BUSINESS	Metrics Reporting	KPI Reporting	Outlines steps involved in reporting key SOC performance indicators (KPIs).
TECHNOLOGY	System Administration	User Access Management	Details necessary steps to request, approve, and grant access to the SOC tools.
OPERATIONAL	Daily Operations	Shift Turnover	Outlines content of shared shift log to ensure no information gaps occur at shift change.
ANALYTICAL	Intrusion Analysis	Threat Intelligence	Lists the steps the Level-2 Analysts use to collect current cyber intelligence information,

			analyze it for relevance, and produce a daily report analysts will use in their monitoring.

Fig. 4 Procedure Outline By Category

Service Functions

Service functions include monitoring, detection, incident resolution, etc. Once defined, they help guide the daily SOC staff processes and procedures. Service functions are associated with various SOC components:

1. Real-time monitoring / management:
    - Aggregate logs and data
    - Coordination of response and remediation
2. Status monitoring and incident detection
    - SIEM Console
    - AV Console
    - IPS Console
    - DLP Console
3. Initial diagnostics and incident isolation
4. Problem correction
5. Security systems and software
    - Update / test DAT definitions
    - Apply corrective IDS/IPS and Firewall Rules
    - Apply other corrective software as instructed or required
6. Computing Equipment and Endpoint Devices
    - Remote administration
    - Update antivirus
    - Tune HIPS alerts
    - Configure whitelisting
7. Work with third-party vendors
8. Escalation to next tier level
9. Close incidents

- Coordination with tier levels
- Coordination with end users and system administrators

10. Continue threat investigation

Each tier within the SOC can be assigned responsibilities based on each analyst's level of expertise within the tier level (Ref. Chapter 8 - Event Management).

Procedures must be continually revised as technologies advance and experience increases. The *"SOC Runbook"* must be kept current and controlled.

What Constitutes a Security Event?

Trying to determine what constitutes a security incident can be difficult. Traffic that does not appear threatening at first may be extremely malicious when compared with other security information. Developing consistent and rapid process repetition is effective but may be burdensome to smaller organizations when there is a small margin of error.

Develop Test / Use Cases

"Use Cases" are repeated attacks from a single source. They require SOC intervention and/or monitoring. Use Case development is a necessary and critical exercise within a SOC.

To ensure the SOC is effective, series of Use Cases must be defined. The Use Case may be an actionable component of the SIEM which notifies the SOC through the network's primary monitoring tool which may involve triggering a Rule, Alarm, or Dashboard when it fails to meet the organization's requirements.

Use Cases are typically developed by viewing the organization's network from the attacker's perspective. The organization's policy, its assets, and the technical environment must be well known prior to defining a Use Case since the intent of the test is to significantly disrupt or do damage to the organization's IT environment responsible for the organization's infrastructure and base. Another option is to look at the regulations the organization is subject to and evaluate the items that could become non-compliant. Below are some, not all, useful Use Cases (listed by McAfee) to implement upon initial SOC set up.

Use Cases - Initial SOC Set Up

- Repeat attack from a single source
- Repeat attack on a single ID
- SMTP traffic from an unauthorized host
- Antivirus failed to clean

- 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
- 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
- Anomaly in DoS baselines
- Anomaly in Recon baselines
- Anomaly in Malware baselines
- Anomaly in suspicious activity baselines
- Anomaly in user access and authentication baselines
- Anomaly in exploit baselines
- Anomaly in network baselines
- Anomaly in application baselines
- Multiple logins from different locations
- Multiple changes from administrative accounts
- 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.)

Chapter 5 – Technology

Technology challenges for SOC include:

- Identification of significant events among a large number of other minor events all of which is filtered through an assorted array of security devices and systems,
- correlating the event feeds, and
- reducing the overall volume and event level to something that is manageable by the analysts.

Analysts often have to log in to a number of management consoles to investigate events. The volume of events (e.g., firewall logs) prevents a comprehensive analysis. To automate event collection and correlation, SOCs must deploy a Security Information and Event Management (SIEM) solution. The SIEM core technology acts as an information repository that may also be accessed virtually.

The SIEM solution is a premier emerging technology solution for monitoring, investigating, and responding to malicious events. It goes beyond storage and alerts the analyst to manage a higher level of risk by providing

- real-time monitoring and correlation,
- historical analysis, and
- automated response.

Selecting the SIEM Tool

When the SOC becomes overwhelmed with data, a good SIEM tool consolidates data, analyzes it intelligently, and provides visualization into the environment. SIEM and configuring it is key. Define requirements and choose the SIEM that proves to be the most flexible and agile as well as provides:

- Priority determination,
- Real-time correlation,
- Cross-device correlation,
- Audit and compliance capabilities, and

- Tracking and escalating in accordance with the threat level.

Data Correlation

A successful SIEM technology capably controls, categorizes, and links data across many technologies. It technically ensures data is collected and centralized. Specifically, to be effective, a SIEM must be able to accomplish eight designated tasks:

- **Normalization** - To normalize data across many different devices, the SIEM must provide enough data fields so all necessary information from these devices may be correlated against them. It is necessary for a SIEM to possess this data capability for it to add or integrate with multiple devices within the organization, such as network devices, servers, security systems, applications, video analytic systems, physical access, and environmental controls.

- **Categorization** - The SIEM should provide a categorized table which describes events in a simplified format. Events should be categorized according to established vendor-independent rules. New devices should be able to be easily integrated.

- **Simple Event Correlation** - Event aggregation and investigation of multiple events for detection of underlying issues which would otherwise be overlooked is characteristic of any efficient SIEM. This is a very basic functionality is which allows several events to be correlated. The outcome produced may be compared with other events in the flow (i.e.: Six attempts to login to a system within one minute using the same user account may indicate a “brute force login attempt”).

- **Multi-Stage Event Correlation** - The SIEM should be able to analyze information from a variety of different events. There may be as many as three or more which need studied to determine if they are all part of the same incident. For example, the SIEM should detect the relationship between the firewall accepting the attack and the attacked system responding to the intruder. This relationship must be detected among hundreds of events that pass through the correlation engine.

- **Prioritization** - The SIEM should successfully identify the (business) relevance of the target as it relates to the organization’s business requirements. Revenue-generating systems or those containing classified data are considered the highest priority as opposed to a little used system in a lab.

- **Statistical Analysis –** The SEIM should detect significant events through the identification of mathematical deviations which appear as irregularities from normal traffic. Indicators may appear as sudden increases in activity on a specific port, protocol, or event type.

- **Historical Analysis** - The SIEM should provide forensic or historical information that aids the SOC in determining what is missing. SIEM solutions not having advanced correlation engines capable of reassessing past data which may have gone undetected are of little use. Be aware the attacker might be doing "organizational reconnaissance" (mapping the network in preparation to launch a major attack in the future). The SOC must be able to detect and monitor unusual activity over long periods prior to a major attack being launched.

- **Physical and Logical Analysis/Location Correlation** - The SIEM should perform physical correlations as well as logical correlations. The SOC must be able to correlate between physical access systems and logical operating system logs and VPN data security devices. Physical correlations enable the SOC to detect incidents resembling account sharing / VPN access violation, a geographic access violation, or suspicious after-hours activity.

ArcSight ESM Data Aggregation

ArcSight ESM is a brand claiming to collect thousands of events per second, storing them in a relational database for analyst to analyze, display, investigate, and report. Data may be collected and aggregated "agentlessly" through the ArcSight Manager. Various devices and concentrators may be deployed throughout the network using ArcSight SmartConnectors. The benefits result in:

- Easier manipulation of the existing infrastructure without needing to install additional hardware,

- Installation that does not require re-architecting existing devices and protocols,

- Distributed data collection that operates from a central platform and utilizes a variety of protocols (e.g., Checkpoint, Cisco SecureIDS, SNMPs, and any syslog),

- Communications transmitted securely over existing IP or IPsec protocols and through firewalls conforming to standard security policies, and

- The ability to scale and handle progressively wider deployments that bring additional information into the system without requiring additional installation and maintenance.

The ArcSight ESM data aggregation strategy completely captures firewall and intrusion detection system status, alarms and alerts. Other relevant and monitored sources are also captured regardless of what combination of agents and centralized collectors is

used. As a result, every field from every event may be accessed for real-time correlation, display, investigation, and reporting. In combination with other supporting products, WArcSight SmartConnectors may make it possible to effectively:

- Control every alarm and alert through a central security schema,
- Filter out unwanted traffic,
- Determine event severity in accordance with standard classification criteria, and
- Minimize network traffic by managing the bandwidth.

Other Security Technology

Intrusion Detection System (IDS) **s**oftware includes: Snort, Barnyard2, Pulled Pork, and stunnel .

Management System software includes: BASE, Snorby, OCCIM, Splunk, and Nagios.

*Network monitoring and analytical tools***,** which assist the analyst in network and computer forensics, and enhance incident investigations include NAV (Network Analysis and Visibility) tools.

Chapter 6 – Understanding the Security Environment

Understanding the environment is essentially determining the technical domain that must be monitored and the types of data the SOC receives. “Use Cases” test for potential attacks and help develop attack protection, early detection, mitigation, and resolutions.

Without an understanding of the technical environment, it is difficult to investigate and determine if an actual attack has happened. It is imperative the SOC staff has the correct tools, diagrams, and knowledge of the network to fully execute their duties. New SOC staff should have electronic as well as a hard copy of the key network and application architecture diagrams. New SOC staff training should include instruction on navigating and gaining a thorough understanding the technical environment they will be working with. This information also helps meet SLAs and indirectly enhances overall SOC customer service.

The Security Architecture and Tools

As previously discussed, included in the SOC’s service functions is the security architecture. The SOC staff has access to the security architecture components, and tools within that architecture, so it becomes necessary each analyst becomes familiar with that environment that includes, but is not limited to:

- SIEM monitoring and correlation
- Network and host IDS/IPS and DLP monitoring and logging
- Antivirus and threat monitoring, intelligence, and logging
- Centralized logging platforms (i.e.: syslog)
- Email, spam, and web gateway and filtering
- Firewall monitoring and management
- Application whitelisting
- File integrity monitoring
- Vulnerability assessments and monitoring.

Security threats are no longer gigantic and massively broadcasted events. Today’s landscape experiences understated, at least at first look, targeted attacks which have

many tentacles and multiple exploitation methods. These low-profile, targeted, attacks typically evolve from, what appears to be on the surface as, “trusted sites.” There is no shortage of cyber criminals searching for new ways to steal information for their own profit.

The attacks are slower to spread which allows them to slip by undetected and increase the chance of successful compromise. The game is to infect the system or steal the data before security measures can be put in place. The Internet environment, and social networking sites in particular, are most attractive to fraudsters and hackers. Personal information is routinely traded on underground economy servers for financial gain. Bank account and credit card information, online auctions, chat rooms, Craigslist, and Facebook … if the information is out there, it is exposed and vulnerable, as are the individuals it belongs to.

Site-specific exposures and vulnerabilities are the clearest indication cybercrime has gone low-key. These vulnerabilities affect site specific custom and proprietary Web-application code. Site-specific cross-site scripting vulnerabilities have been on the rise since 2007. Attackers routinely compromise specific Web sites that are easy to launch subsequent attacks. This springboard strategy has proven effective time and time again against unsuspecting users. Thousands of multistage attacks that exploit clientside vulnerabilities occur daily.

The most effective system of security against vulnerabilities, misuse, and theft is a combined protection defense which uses technical measures, physical security, and well educated SOC staff. Clearly defined policies should be included in the organization’s infrastructure and reviewed with the management and personnel.

- Monitor and alarm offices and data centers
- Remove computers, operations, and associated components from public view
- Implement and enforce restrictions, authorizations, and authentications on Internet access
- Keep anti-malware solutions up to date
- Keep operating system is up to date
- Maintain an effective and efficient SOC or responsible and reliable Third-Party security to protect, detect, mitigate, respond, analyze, and report attacks
- Maintain backup energy sources and utilize a protected power supply.

Chapter 7 – Identifying the Customer

Who the customer is will determine the focus and extent of SOC support and interaction required. The customer may be the organization, or the customer may be a multiple-client environment. A series of services provided to the customer will be customized based on the customer's inbound communication process.

First, determine which services will be provided to each customer. Ask, for instance, if the SOC will permit end-users to call or will emails and calls be facilitated only by the Help Desk and internal administrator?

Diagramming the inbound process is necessary once the customer base, service functions, and tier levels have been defined. Below is an example (Fig. 5):

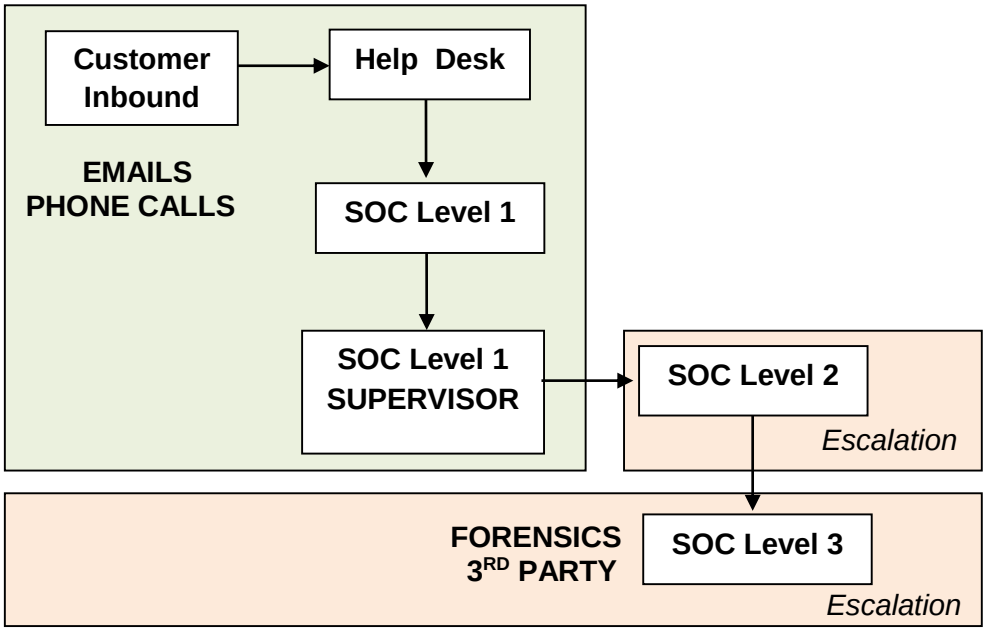


Fig 5 Customer Inbound Process

PART 2 – Best Practices

Chapter 8 - Event Management

"The SOC is the correlation point for every monitored event logged within the organization." The SOC decides how each event is managed and responded to.

An event is any element that comes into the SOC and is monitored.

An incident is an event that must be acted upon.

Management of Events / Contact List

Event management essentially categorizes, assign, and prioritizes each event received by the SOC. Applicable event management instructions should be posted and readily accessible 24/7, although it is not necessary to include this information as part of the *Incident Response Program Handbook*.

The SOC should also provide email and telephone assistance to its customers and answer questions such as those related to:

- Malware outbreak
- Phishing attacks
- Social Engineering calls
- Data Leak/Loss incidents
- Customer account lockout

Incident and Event Categories

There are US Standards for categorizing security events and incidents. Compliance and metrics may be defined accordingly for each category (Fig. 6).

The following help categorize events and incidents and should be leveraged within the SOC.

Incidents

- Training and Exercises
- Root Level Intrusion

- User Level Intrusion
- Denial of Service
- Malicious Logic

Events

Unsuccessful Activity Attempt

Non-Compliance Activity

Reconnaissance

Investigating

Explained Anomaly

Security events and incidents are further classified according to US-CERT recommendations:

CATEGORY	FUNCTION
CAT^0	Exercise / Network defense testing
CAT^1	Successful unauthorized access
CAT^2	Denial of service
CAT^3	Successful installation or post-install beaconing of malicious code
CAT^4	Improper usage
CAT^5	Scans/probes/Attempted Access
CAT^6	Investigation

Fig. 6 US-CERT Severity of Security Events Categories

Security Evaluation / Security Severity

Clear and adequate descriptions and details regarding specific incident and event severity levels is required for all levels of the SOC and its customers. (Typically four or five severity levels are used).

- Severity 1 (HIGH) - Critical Compromise – Causes a major service disruption or publicly-displayed attack.
- Severity 2 - Serious Impact or Compromise – Affecting multiple customers.
- Severity 3 - Intermittent incidents or alerts (not critical)
- Severity 4 (LOW) - Informational (no security impact)

Every severity level must be further clarified to provide more detail regarding the critical nature of the attack. McAfee Example (Fig. 7)

SEVERITY 1: HIGH IMPACT

- 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

Fig. 7 Incident: Severity 1 Detailed

Incident Resolution Procedure

SOC incident resolutions should be handled according to established procedure, which includes following an incident ticket record escalation process. The incident ticket opens the response process and documents the required procedural steps are taken by the SOC staff. Incident resolution tasks must be completed and include:

- Documenting the incident (description and resolution)
- Referencing any other open trouble-ticket or incident record
- Closing the incident record
- Documenting the communication used to notify the end-user or tier level contact
- Documenting the root cause of the problem.

High-priority incidents require the SOC maintain and use a defined distribution list to whom notification of the problem, resolution, and assigned incident record ID will be sent.

Incident Assignment, Resolution Procedure Guidelines

Not all incidents can be resolved at the first tier level. There must be documented procedures in place to address escalations. When an issue is not resolved at the first tier level, the escalation to the next tier is required in accordance with the SOC documented procedures.

Guidelines for the Level 1 SOC support are important and should include

- Opening an incident ticket
- Being the initial point of contact for customers within the organization's network
- Maintaining the daily shift log
- Performing rudimentary testing and diagnosis
- Validating the incident is not a user error
- Formally assigning the incident to the SOC

Incident Assignment

What technical solution is there for maintaining incident records? The "trouble-" or "incident ticket" system is the most common solution organizations use, although not everyone does. The primary intent 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.

Regardless of how the incident is assigned, the system must also provide a level of security. Incident tickets containing sensitive information may only be viewed and handled by those with prior approved access. The incident priority level and prescribed timeline of the response must be defined as an incident is assigned to ensure timely attention to incidents. Priority assignment levels are not to be confused with incident and event severity. Priority assignments are task driven assignments to analysts for review and action and interaction with the customer. "Priority" is the level of response time identified when the incident ticket is created. It may be updated based on the discovered extent of the impact.

Priority 1 - Multiple systems / devices are affected or compromised; a possible data breach has occurred: Respond within 10 minutes

Priority 2 - Multiple devices / users are affected or compromised: Respond within 1 hour

Priority 3 – A single device / user is affected or has been compromised: Respond within 8 hours

Priority 4 - No impact; logging response: No response

Escalation Guidelines

Resolving incidents requires all levels of the SOC practice established procedures for detection, isolation, circumvention, and resolution. When applicable, this process should be mapped to the phases in the Incident Response Plan.

Table 1 below shows the generally accepted structured progression of recommended actions Level 1 and Level 2 SOC individuals use when performing the appropriate incident troubleshooting and analysis. When incidents cannot be resolved by one level of SOC staff escalation guidelines provides instructions for moving incidents on to the proper specialists who may be better equipped to resolve them.

	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		

Table 1 Incident Resolution Process - Escalation Actions

The incident resolution process moves from left to right and from Level 1 to Level 2. When activities at Level 1 are exhausted, the incident should be escalated to the next skill level for further action.

The Escalation Tier

The SOC must be adequately staffed with trained professionals that can handle incident escalations. There needs to be clearly defined procedures for the escalation tier, which minimally address:

- Resources assigned to assist with the resolution of incidents

- Resources assigned to review open incident records
- Incident and ticket status updates
- Customer non-response
- Additional notes to the incident record
- Additional escalations
- Incident record closure
- High priority and/or high severity incident handling
- Lack of resolution

Escalation Procedure Example

The following illustrates the escalation of an issue, in accordance with the SOC procedure, when it has escalated to tier 2:

The incident ticket is open and the Level 1 SOC engineer becomes the initial Incident Record Owner. The Level 1 SOC engineer evaluates the problem and determines if they have the ability to resolve the issue.

Level 1 SOC engineer may be able to resolve the Incident Record after they have

1. Specifically defined the incident
2. Collected additional information needed to troubleshoot and resolve the issue
3. Determined possible causes or options
4. Created and implemented an action plan
5. Observed the results and repeated the steps until the issue is resolved or
6. Determined they need other Level 1 professional assistance or Level 2 SOC assistance

Field Support

When field security support is needed, the SOC engineer follows 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.

Third Party Resolution / Procedures

Sometimes it becomes necessary to involve third parties in the escalation process. A software patch or antivirus update may need to be developed quickly. Or a third party may be asked to assist with or perform more detailed forensics investigation and analyses. The SOC is responsible for having defined third party participation procedures in place for escalating in these kinds of instances. Appropriate contact information must also be available to support that escalation process.

Tier Functional Responsibilities

Each tier within the SOC may be assigned responsibilities based on each staff member's level of expertise within their tier level (Fig. 8).

For example, AV and SIEM console monitoring may be a service function of every tier but working with third-party vendors may be a service function only reserved for tier 2 or tier 3 staff.

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			•

Fig. 8- SOC Tier Responsibilities

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.

Business Continuity Plan (BCP)

A Business Continuity Plan (BCP) should be in place so staff is still able to work effectively if the systems happen to fail.

Chapter 9 - Critical Success Factors

An in-house SOC provides a centralized monitoring and management system of network security over a diverse IT environment. It is critical to thoroughly know the business' technical requirements, infrastructure, security needs, and policies.

However, there are five very basic elements to consider in determining if a company should undertake forming its own security operations center and if it will generally be successful:

- Is knowledgeable and trained IT staff available or are there capital and resources to hire and train IT professionals?
- Is good management and IT supervision in place?
- Is there adequate budget to plan, implement, and maintain SOC operations and resources?
- Is there knowledge of IT security best practices and good processes in place?
- What is the integration into incident response?

The success of the SOC depends on the quality of its staff. The success of the SOC staff success ultimately depends on the quality of the SOC-manager.

Mitigation and Response

Security breaches and risk may be reduced by:

- Implementing User education,
- Reducing User-access to controls,
- Restricting administrative access,
- Regularly updating proxy servers and firewalls,
- Denying access to known "bad" sites,
- Denying certain downloads, and by
- Blocking posting to known "bad IP's."

Service Management

The long term goal of SOC managers is to continually run an effective SOC. It is important to establish guidelines to ensure performance is consistent and the SOC management team will be ready should the organization decide to assess or audit the SOC. Not everyone in the organization understands the underlying technology or the effectiveness of SOC monitoring, so periodic SOC assessments and audits are necessary.

It is important to prepare for these service audits. Key items that must be in place include:

- *The Service Vision and Strategy* -The mission statement, charter, and objectives.

- *The Service Design* – A full SOC analysis and documentation of all of the business requirements which enables the SOC to provide value to the organization and support the SOC's strategies and business objectives with the organization's. The Service Design also enables the SOC to define their KPI (key performance indicators) that may be used to keep the SOC's design services in accordance with the business requirements.

- *The Service Functions* – A service level agreement (SLA) is required for each SOC core function. This must be clearly defined with management. The business typically drives the SLAs.

- *Service Transition* – SOC personnel management is another key consideration when maintaining the continuity of SOC operations. The SOC must address changes which are implemented throughout the organization.

  Changes to the infrastructure impact SOC monitoring systems and how they are setup, as well as how the alarms are cued to go off, and changes in relevance of various work tasks.

  Close integration between the SOC and change management is often required.

- *Service Operations*— Several items must be in place for service operations to run effectively and efficiently:

  Trend analysis,

  Remediation items tracking,

  SOC activities reports presented periodically to the organization,

  Accurate classification of issues,

  Software license compliance, and

  Asset tracking and inventory.

- *Continuous Service Improvement*— This is ongoing, intended to provide an improvement process to increase robust development of the SOC over time. To assist in accomplishing this goal, the SOC should continue:

  Measuring progress (Use Cases, alerts, shift logs, etc.),

  Gathering the data (In the SIEM, manually, or in the GRC (Governance Risk and Compliance) system,

  Processing and analyzing data,

  Reporting or sorting data to understand and identify improvements made, and

  Implementing corrective actions and controls.

CONCLUSION
The Next Gen SOC

Security operations and established SOCs are in their fifth generation. The first generation SOC began in 1975. Until 1995 the SOC programs utilizes emerging technologies but were generally often ad hoc in nature and routinely understaffed. It was the emergence of the Internet that woke organizations up to data exploitation and abuse. Early detections were countered and resolved through creative thinking and problem solving. However, efforts were neither organized nor repeatable.

The first security tools (antivirus software and firewalls) were developed once Hollywood, books, and Congress acknowledged cyber threats in the mid-eighties. Proxies and network intrusion detection systems followed.

The first Security Operations was typically one person with a networking background that responded to detected threats for their organization. By the mid-nineties, SOCs began to appear in military and government entities.

Second-Generation SOC (1996-2001)

Enters the “era of the malware.” Malware outbreaks were rampant as were viruses and worms all but destroying government networks. Although narrowly focused and built on a foundation of defense, SOCs began formalizing processes and procedures around intrusion response and vulnerability tracking.

- Intrusion detection systems played an important part
- Vulnerability tracking
- Formalized system patching
- The emergence of the Managed Security Service Provider model
- Security event analysis was performed through scripts and IDS consoles
- SIEM was introduced (as a technology to correlate disparate security events into a single system).

Third-generation SOC (2002-2006)

The third gen saw the rapid growth of organized cybercrime and Bots used to steal identities and financial information. SQL Slammer malware and Blaster terrorized the Internet. The US-CERT was formed in 2003 to categorize the events. By the end of the generation, malware matured from worms to targeted attacks. The formal SOC was

developed – first in government, military, and managed service provider (MSSP) organizations, and then to the larger corporations in the private sector.

- The PCI council began regulating and standardizing payment card security
- Cyber exploitation capabilities of China and other nation-states gained recognition
- Security programs in the private sector increase
- Major data breaches began being detected and publicly reported due to new breach notification laws.

Fourth-generation SOC (2007-2012)

As security develops, so does the size and sophistication of the attacks. Government's and mainstream media's attention was finally piqued due to attack vectors targeting Individuals. Publicity of a politically motivated cyber threat landscape resulted in a greater push for security controls and a new generation of security operations.

Nation-states were now attacking one another, intent on sabotage and theft of intellectual property or sabotage. The first publicly known cyber-attacks in the context of an armed conflict changed the concept of war forever.

- Successful attacks against individuals as well as organizations
- Social media tools provide easy access and coordination and information dissemination.
- Intrusions will happen regardless of preventative security technologies in place
- The focus shifts from detection and prevention to exfiltration detection and containment.
- SOCs purpose is detection, escalation, and remediation of security events.

New Horizons – Next Gen SOCs

Cyber-attacks are still growing exponentially. Organizations race to find technologies to mitigate their risk and reduce impacts from a breach.

Security operations have moved from reactive to proactive. Fifth-generation SOCs are combining solutions; high visibility security devices and SIEM combined with big data analysis. The SO capability to detect previously unknown attack vectors and indicators of long-undetected compromise is rapidly expanding. Advance SOCs are everywhere around the world, in government, private enterprises, and SMEs. Anyone connected to the Internet has some means of security embedded in their operations.

Security Operations and the SOC continue to evolve as the cyber threat landscape continues to expand at an unprecedented rate. Historically threats are driven by human enemies. Until now, most security products on the market have only provided point solutions for signatures, faults, viruses, and worms.

The next gen SOCs recognize the changes in threat environment and are making changes of their own in the area or human resources. In an effort to gain a proactive edge on the attackers, SOC analyst training now includes lessons in security counter-intelligence, surveillance, criminal psychology, and analytical thinking.

Standards and compliance efforts have improved and SOCs are more efficient than ever before. Fourth-gen SOC analysts manually performed incident containment and response. Today, SOC human cycles are applied to advanced analytics and subtle event detection.

SOCs are analysis-focused. They are storing enormous amounts of structured and unstructured data from inside and outside of their organization and using advanced analytical tools to derive intelligence and make predictions based on newly discovered patterns.

5G/SOC's merge business intelligence and security intelligence tools to create contextual understanding of enterprise and its risks.

5G/SOC analysts include mathematicians, statisticians, theorists and big data scientists to achieve their goals.

A New Perspective

The 5G/SOC has the same goal to reduce the organization's risk by proactively detecting threats before they do damage. The idea of willing collaboration with others (at least as well as attackers are collaborating) has taken root.

No single organization possesses all the data needed to detect all threats. "Threat Intelligence" services have narrow focuses. Formal consortiums are still guarded.

5G/SOC leaders are becoming more adaptive and collaborative:

- Forming active information sharing groups
- Forming direct relationships within their industry to leverage communal expertise in match wits with the attackers
- Leveraging and investing in the expertise of people
- Consulting seasoned information security professionals to provide effective threat detection.

Pushing Back

Organizations are creatively and logically pushing back. They are:

- exploring applicable counter attack capabilities,
- significantly investing in intelligence gathering teams,
- formalizing teams to track malicious groups and individuals (both inside and outside)
- continually testing using Red Team / Blue Team, attack and defend exercises

Intelligence teams are increasingly collaborating and sharing details about attackers' methods, techniques, and tools with various organizations.

Hunt teams are moving away from the routines of their "triage of alerts" and are utilizing big data stores to aid in searching for previously unknown, unseen, and unforeseen attacks. As a result, these "data analytics driven hunt teams" are able to broaden their searches. From historical data stores, they are able to search farther back into the past than they have been able to previously. They will be able to determine how long a threat has been active in the environment once its presence is detected.

Fifth generation SOCs can advantageously learn from and build on the history of previous generations of SOC capabilities. It is no different today that in past generations and SOCs must still cover perimeter security, vulnerability tracking, malware detection, and incident response.

The 5G/SOCs must detect insider threats as well as advanced persistent threats from the outside. SOCs must monitor user activity for data exfiltration. They must effectively utilize threat intelligence and "big data" tools to discover previously unknown attacks.

- New tactics and techniques must be utilized.
- New technologies must be implemented.
- Existing processes must be automated.
- Staff must become highly trained and motivated to reduce risk.
- Staff must collaborate to reduce the risk.

The SOC is expected to do more than just secure the infrastructure.

References

BUILDING A SUCCESSFUL SECURITY OPERATIONS CENTER HP Enterprise Security Business Whitepaper, August 2011, HP.

Business white paper | HP ESP Security Intelligence and Operations Consulting Services, May 2013, HP.

Creating and Maintaining an SOC: The details behind successful Security Operations Centers, 2013, McAfee® Foundstone® Professional Services, http://www.mcafee.com/us/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf

SIEM Use Cases—What you need to know by msonomer; *http://infosecnirvana.com/siem-use-cases*

Kelley, Diana and Moritz, Ron. *Best Practices for Building a Security Operations Center. Operations Security.* http://www.infosectoday.com