C|SA™

Certified SOC Analyst

CHAPTER 01

Security Operations and Management

This page is intentionally left blank.

Chapter Objectives

The objective of this chapter is to let you understand how SOC contributes in an organization's security management in its efforts to maintain good security posture of the organization. In this chapter, you will learn:

- Security management in organizations and the security activities involved in security management
- Different aspect of security operations
- Basic concepts of SOC
- Different phases involved in the implementation of SOC
- Challenges of SOC implementation
- SOC Key Performance Indicators (KPI) and Metrics
- Best Practices for running SOC
- Key difference between SOC and NOC

1. Security Management

The security management system is a collection of a systematic, repetitive set of interconnected security activities that help organizations to maintain their security posture at an adequate level. It is an ongoing effort that focuses on both physical safety and digital security of assets. It is a crucial and essential part of every organization. Its main purpose is to protect the organization's assets like information, hardware, and software from malicious activities and reduce the overall risk on the organization. It ensures confidentiality, integrity, and availability of the organization's assets and services. The security management system also develops and implements various documents like policies, standards, procedures, and guidelines. These help the organization in implementing different security practices like risk assessment, training, and security audit.

Security Activities Involved in Security Management

Broadly, security management comprises different security activities:

- **Security Infrastructure**

  It provides security to Perimeter, Network, Endpoint, and Application & Data by implementing adequate preventive, detective, and corrective information security controls.

- **Security Prevention**

  Security prevention services like vulnerability management and penetration testing ensure security in the networks against vulnerabilities and threats. These services not only scan, test, and identify threats across internal or external networks but also remediate or reduce their exposure.

- **Compliance and Validation**

  Various governance risk and compliance programs help the organization to continue its business without any risks. Some of the examples of governance risk and compliance programs involve ISO 27001 Readiness Assessment, Security Baseline policy document for ISMS, and so on.

- **Security Operations**

  These operations are performed by the Security Operation Center (SOC) through real-time security alerting, threat analysis & intelligence, correlation, and preemptive incident reporting, detection, and response.

2. Security Operations

Security operation is the continuous operational practice for maintaining and managing a secure IT environment through the implementation and execution of certain services and processes. Its main purpose is to prevent, detect, prioritize, and respond to security incidents. A well-defined security operation should be specializing in intelligence, incident management, access control, loss control, risk management, and forensics. It involves a predefined set of processes and services that is to be followed during the daily security operation tasks based on the organization's security baselines.

Security operation may consist of various security operation tasks, which include:

- **Security Monitoring**

  It involves collecting and analyzing information to identify abnormal behavior and unusual activities in the network. Also, escalating malicious activities to incident response system for resolution.

- **Security Incident Management**

  It includes detecting, managing, and monitoring security vulnerabilities in real-time with minimal adverse impact.

- **Vulnerability Management**

  It is a cyclical process that includes continuous monitoring, triage, and mitigation of system vulnerabilities. It is an integral part of computer security and network security.

- **Security Device Management**

  It involves maintaining and managing security infrastructure and devices, as well as updating software in the organization. It helps in securing an organization's assets and maintaining a compliance requirement for regulations.

- **Network-flow Monitoring**

  It detects and analyzes inflow and outflow of packets in the network and generates alerts whenever suspicious activities arise.

3. Security Operations Center (SOC)

Security operations are handled and managed with the help of Security Operation Center (SOC). SOC is a centralized unit that continuously monitors, manages, and analyzes ongoing activities on the organization's information systems such as networks, servers, endpoints, databases, applications, and websites. Its end-goal is to maintain the continuity of an organization by determining, preventing, detecting, and responding to intrusion events before they affect the business. It is also sometimes referred to as Security Defense Center (SDC), Security Analytics Center (SAC), Cyber Security Center, Network Security Operations Center (NSOC), Threat Defense Center, and Security Intelligence and Operations Center (SIOC). It provides a single point of view through which the organization's security and assets are monitored, assessed, and defended. It gathers data from logs, IDS/IPS, firewalls, endpoint devices, and network flows and facilitates incident detection, investigation, and response. It evaluates the organization's security posture for any anomalies/organization assets or information systems and facilitates the situational awareness and real-time alerting if any intrusion or attack is detected.

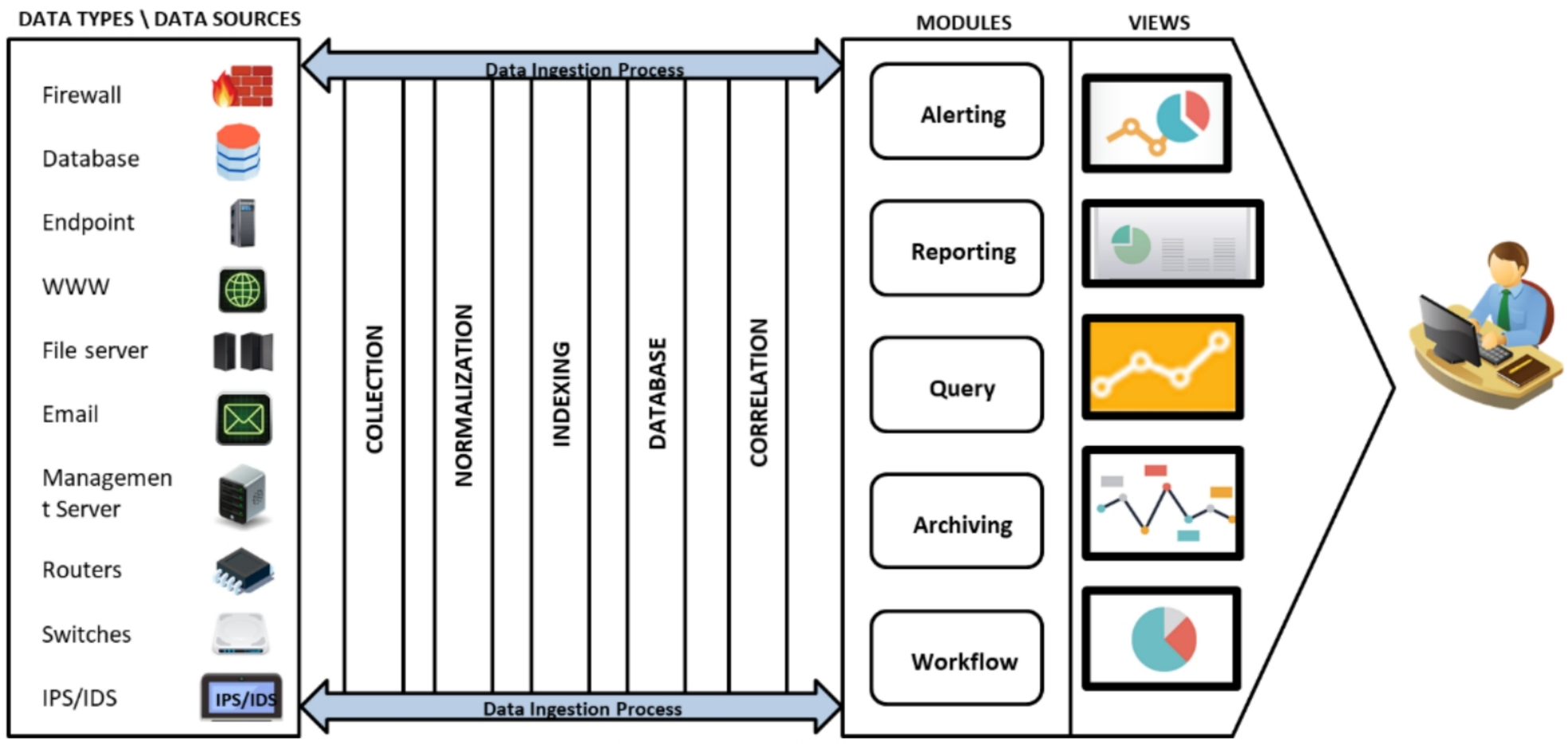

Figure 1. 1: SOC - Single Point View

3.1. Need of SOC

Organizations use various security measures such as intrusion detection/prevention system, firewall, email filtering, URL filtering, and antivirus to protect the organization's network from threats. However, in recent times, these security measures proved insufficient to provide enough security as hackers are inventing new trends and techniques to penetrate the network by evading such security measures. So, the need for such security measures that can keep the security perimeter always updated regarding new and developing threats and vulnerabilities. This is possible through SOC.

SOC is responsible for performing the following types of activities:

- Proactively identifying suspicious activities in the network and system.
- Performing vulnerability management to identify which activities are vulnerable to the network.
- Getting aware of hardware and software assets working in the network.
- Performing log management that facilitates forensics at the time of security breaches.
- Evaluating policies and procedures required for business operations.
- Checking whether the organization has appropriate internal controls and processes to provide proper services to the clients.
- Strengthening the environment of the organization.
- Eradicating internal blinders.
- To manage and handle numerous devices that are no longer managed, unsupported, or legacy.
- To track and secure a large amount of an organization's data and information around the clock.

- To monitor and manage isolated and localized point solutions devices.
- To monitor, mitigate, and manage privileged user abuse.
- To respond faster to cyber threats.
- To minimize business loss.
- To monitor continuously for effective incident detection.
- To implement tools that fit your requirements.
- To have full control over staff resources.
- To customize information security tools.

3.2. SOC Capabilities

The basic capabilities of a SOC include preventing, detecting, responding, and reporting security incidents.

- **Preventive Capability**

  It refers to stopping an attack from getting successful. To prevent the attack, SOC uses fine-tuning and maintenance tools. It also directs the Incident Response Team to perform security monitoring. It also uses the detection rules effectively and considers the Indicators of Compromise (IoC) detected by the incident response team. Thus, SOC detects risks and identify their harmful impact on the organization to design a well-defined and vigilance plan.

- **Detection Capability**

  It refers to monitoring a system or network to identify suspicious activities and security breaches. To fulfill this purpose, SOC collects, analyzes, and correlates security events, as well as triggers alerts when suspicious activity arises. It also informs the client regarding issues through notification and communication.

- **Response Capability**

  It refers to analyzing and handling documented alerts and security incidents instantly with security teams.

- **Reporting Capability**

  SOC offers various reports, which keeps you updated about the various assets and their security events, level of compliance, and alarms generated. SOC uses security dashboard to display service indicators, technical indicators, and trend indicators.

- **Forensics**

  SOC analysts use structured log data to conduct an investigation for identifying the root cause of a particular attack pattern and restrict the attacker's ability to perform attacks against the organization.

- **Audit and compliance support**

  SOC not only collects and stores logs, but also efficiently retrieves them at the time of preparing for an audit.

3.3. SOC Operations

Typical functions of SOC include:

- **Log Collection**

  A SOC collects logs generated from any security system or transactional activities, as it behaves like an aggregator of data. They can be collected either through syslog or writing the logs into the centralized log management system. Without proper log collection, it is not possible to monitor and understand suspicious security events occurring in the organization system.

- **Log Retention and Archival**

  Logs collected by SOC are stored centrally and can be utilized easily whenever required. You can check the logs to perform investigations regarding attacks and identify vulnerabilities. They can also be used for compliance purposes. Moreover, they also contain historical data through which you can specify the patterns of normal systems' behavior. If there is any deviation as per the pattern, then it indicates an ongoing attack on the systems. Thus, log retention and archival help you in risk and downtime reduction, threat control and prevention, administrative overhead reduction, and so on.

- **Log Analysis**

  After collecting, cleaning, and structuring the log data, it gets analyzed to identify abnormal activities. Logs are analyzed through SOC's technology to extract important information like relevant metrics, from the raw data. It enables you to analyze and solve various issues in the organization system and networks. It also facilitates you to understand the behavior of the end-user. Moreover, it allows you to perform investigations and respond effectively to security breaches and incidents.

- **Monitoring of Security Environments for Security Events**

  Information received by log analysis is transferred to the SOC team for monitoring purpose so that it can identify the current security position of an organization.

- **Event Correlation**

  It is an ability to correlate and contextualize events automatically from various sources. This depends upon a set of predefined correlation rules. If the correlation rules are correctly implemented, it reduces the rate of false positives. Event correlation also helps in reducing downtime, threat control, and prevention, minimizing administrative overhead, and so on.

- **Incident Management**

  Incident management is the process of taking action against reported security incidents. It helps in utilizing SOC's resources in an efficient manner so that all the reported incidents can be handled properly. Here, incidents are prioritized as per the predefined rules and objectives. It also helps you in minimizing risk and downtime, as well as in controlling and preventing threats.

- **Threat Identification**

  It is the process of determining threats and vulnerabilities correctly in real-time. It is performed through different methods, like threat intelligence and behavior analytics. It leads to threat control and prevention.

- **Threat Reaction and Response**

  A SOC reacts either reactively or proactively to threats. If the threat reaction is reactive, then immediate action should be applied to remediate it. If the threat reaction is proactive, then try to find out the weakness in infrastructure or processes and remove it before the attack utilizes it. It also leads to threat control and prevention.

- **Reporting**

  SOC generates clients' detailed security reports, including different types of requests ranging from real-time management to audit requirements. It should include malicious system and abnormal network activities, indicators of compromise, unauthorized access or attempts, denial of service attacks, and suspicious emails.

SOC also performs various secondary security operations, like the following:

- **Malware Analysis**

  Malware represents different types of malicious programs such as virus, worm, Trojan horse, rootkit, or backdoor. Malware analysis refers to the process of analyzing and determining the purpose, functionalities, and harmful effect of given malware samples. Based on the collected information, the security analyst creates an appropriate detection technique for malicious codes.

- **Vulnerability Management**

  SOC performs vulnerability management by identifying, classifying, remediating, and mitigating vulnerabilities, using different methodologies like automated testing and manual testing.

- **Security Device Management**

  It means managing and optimizing the security tools and technologies infrastructure.

3.4. SOC Workflow

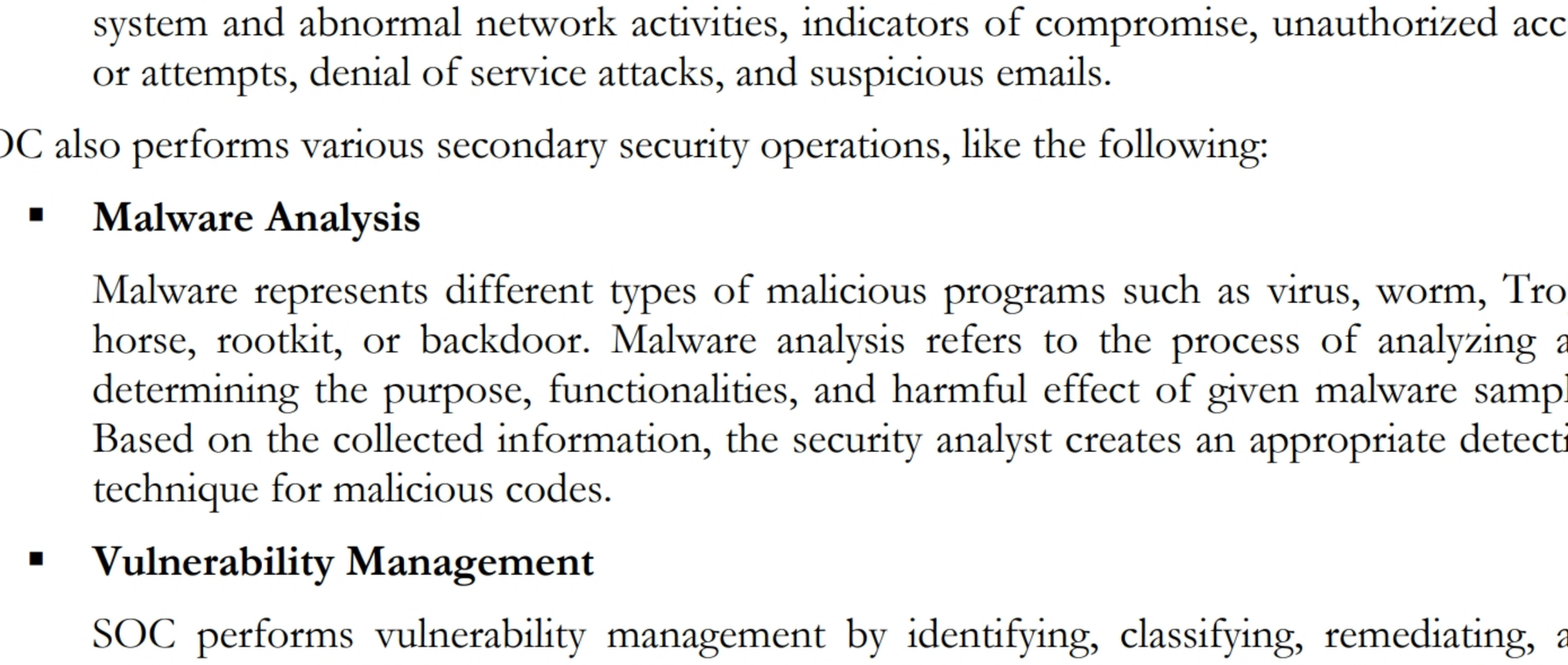

Figure 1. 2: SOC Workflow

Typical SOC workflow includes the following activities:

- **Collection**

  Security logs are collected and forwarded to the SIEM.

- **Ingestion**

  SIEM ingests log data, threat information, indicators of compromise, and asset inventory for machine-based correlation and anomalous activity detection.

- **Validation**

  SOC analysts identify the indicators of compromise, triage alerts, and validate incidents.

- **Reporting**

  Validated incidents are submitted to the incident response teams through a ticketing system.

- **Response**

  SOC team reviews incidents and performs incident response activities.

- **Documentation**

  At last, incidents are documented for business audit purposes.

4. Components of SOC: People, Processes, and Technology

A SOC requires cooperation and communication among people, processes, and technologies to collect, sort, and investigate security events. People are the security talent who are responsible for executing the functions. They may be security operators, analysts, or pen testers, and may be internal or outsourced. Their main objective is to communicate with the security teams and build the vigilance solution to the organization. They are also responsible for responding to the security incidents immediately. Processes should be planned specifically for security monitoring and administration. They should act like a connection between people and technology. Their main motive is to track and identify suspicious incidents as well as provide remediation against them. Technology amplifies the capabilities of SOC by facilitating automatic incident analysis and response, threat detection and prevention, event triage, and so on. Their main objectives are to collect, store, correlate, and report on security incidents.

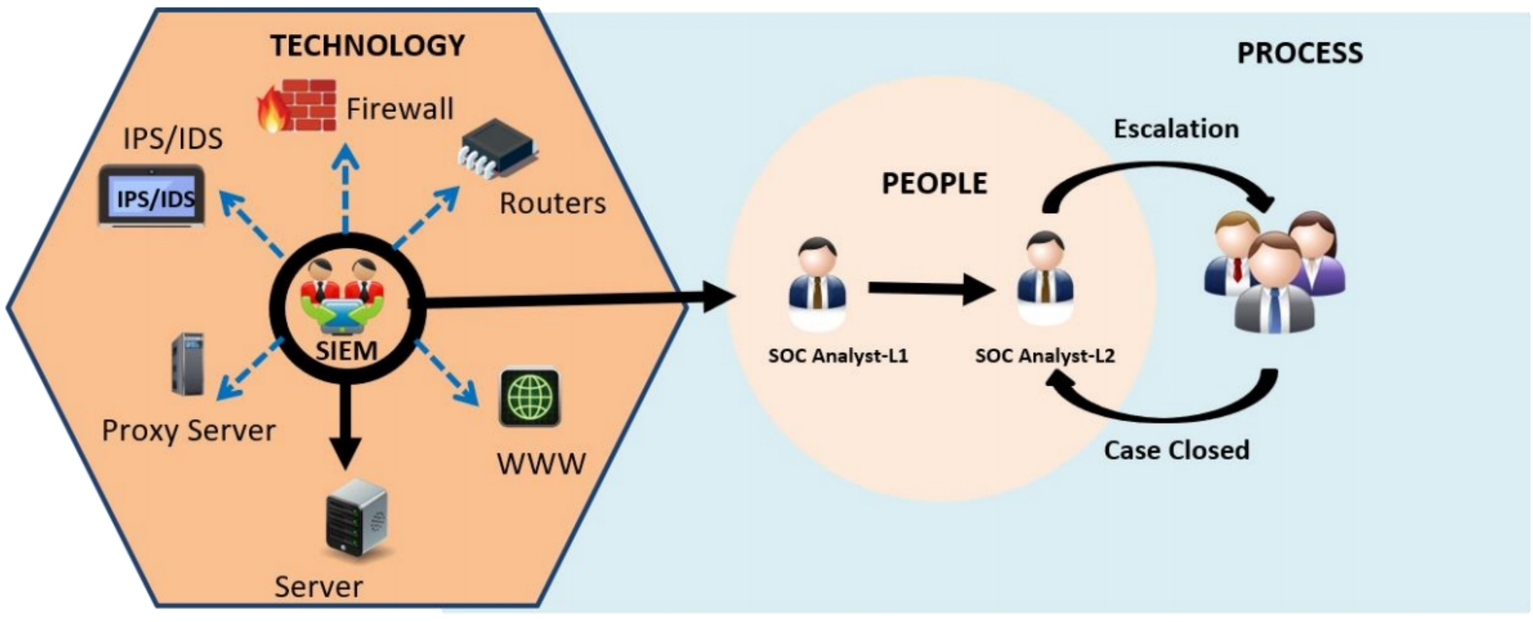

Figure 1. 3: Components of SOC: People, Processes, and Technology

4.1. People

People are specialized individuals working at different levels of SOC. They should have deep technical knowledge, a wide range of capabilities, and a variety of experiences. They should be able to monitor and analyze a large amount of data/information which can be used for further investigations. Each person in the SOC team is responsible for performing several roles. Each role should be clearly defined with the job description, responsibilities, required skills, expected experience, necessary training and certification, chain of command, and career progression paths. The roles and responsibilities of an individual depend upon the size, budget, structure, and objective of an organization. A specific organization may contain numerous SOC analysts with different roles and skills, an incident responder, a subject matter expert/hunter, a SOC manager, and a Chief Information Security Officer (CISO).

Every team in the SOC is different from another, but they have more or less similar roles and responsibilities. They are also facing roughly the same challenges as overstaffed, understaffed, and little support from upper management. It is the responsibility of management to follow best practices and deliver a healthier environment to the SOC teams.

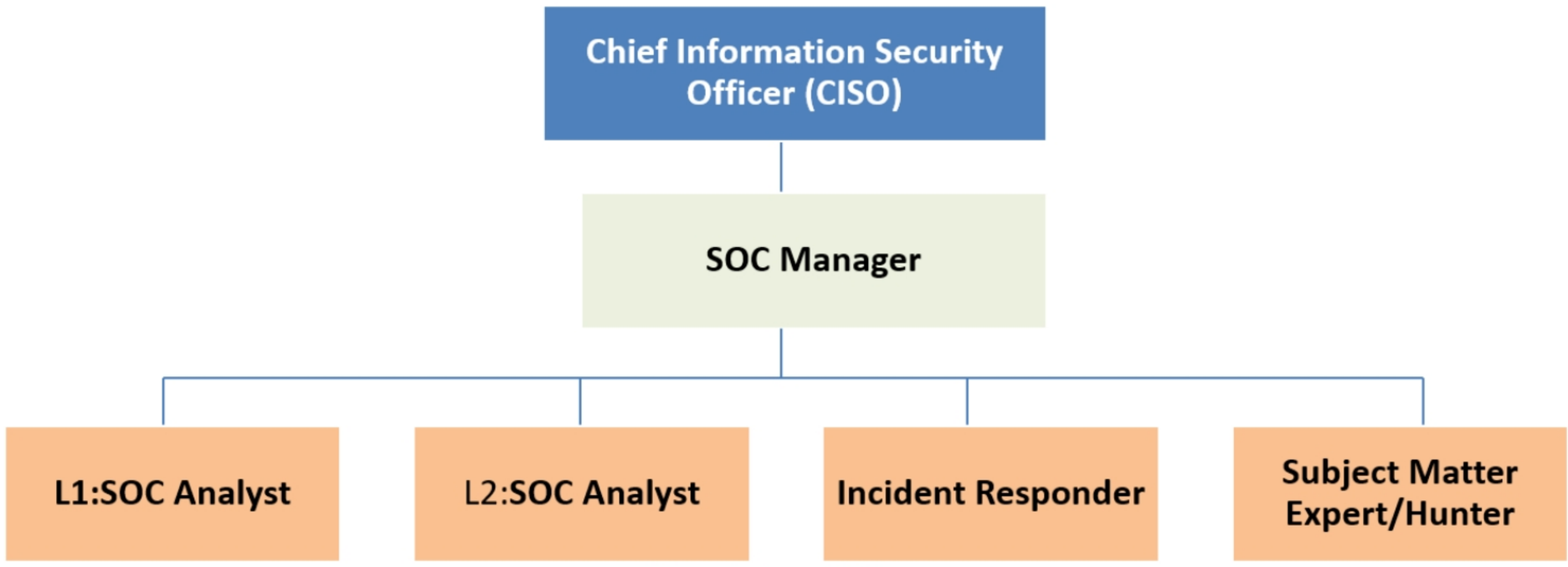

Figure 1. 4: SOC Team

4.1.1. People: SOC Analyst

- **SOC Analyst—Level 1**

  A level-1 security analyst is an individual who is responsible for performing day-to-day security related operations. He/she executes those tasks that are mentioned in processes and subordinate procedures in a repeated manner. He/she also analyzes SOC situational awareness and monitors various automated devices for detecting security incidents.

Responsibilities of SOC Analyst—L1

The security analyst is responsible for performing the following activities:

- Collects and monitors security events from different log sources like firewalls, network devices, web proxies, and antivirus systems.
- Performs initial investigation of security events and escalates them to the next level, if required.

- Maintains email address and distribution lists, answers SOC phone lines, and updates required documentation.
- Performs security research and gathers information about identified threats and vulnerabilities.
- Documents initial investigation results and forwards it to a level-2 analyst for final investigation.
- Monitors security vulnerabilities to detect its root causes.
- Conducts security audits, both internal and external.

- **SOC Analyst—Level 2**

  SOC Analyst-L2 is responsible for monitoring the alert queue in a timely fashion. To do this, he/she is using a wide range of automated tools. He/she collects, and documents data related to suspicious activities, and forwards it to the next level for investigation. When SOC Analyst-L2 identifies that security, issues have occurred he/she will forward them to the incident response team. A SOC Analyst-L2 works like a team member and also communicates with outside stakeholders.

  Responsibilities of SOC Analyst—L2

  An SOC Analyst-L2 is responsible for performing the following activities:

  - Prioritizes security alerts.
  - Keeps track on all alerts and tickets.
  - Examines security sensors and endpoints for alarms.
  - Closes false positives.
  - Monitors open tickets.
  - Performs basic investigation and remediation.

Initially, Level 1 SOC analyst reviews the latest alerts in order to identify which alerts require attention. Once the suspicious alerts are identified, those are escalated to Level 2 security analyst for review purpose. Level 2 SOC analyst performs investigations to determine their relevancy and urgency. Based on the relevancy and urgency, tickets are raised for alerts that indicate an incident and forwarded to Incident Responder. Now, Incident Responder reviews the tickets forwarded by Level 2 security analyst. After reviewing and investigating them, he/she takes the necessary action to remediate and close the issues.

Figure 1. 5: SOC Analyst Responsibilities

4.1.2. People: Other Job Roles in SOC

- **Incident Responder**

  An incident responder or intrusion analyst is a cyber-firefighter who is responsible for in-depth incident analysis by correlating data from different sources. He/she also detects whether the system or data set has been affected; if so, then suggest appropriate countermeasures. The incident responder uses various tools to analyze security incidents and apply suitable action instantly. He/she is also responsible for prioritizing the security incidents and differentiating among actual intrusion attempts and false alarms.

  Responsibilities of Incident Responder

  Incident Responder is responsible for performing the following activities:

  - Analyzes networks and systems for threats.
  - Detects security risks and vulnerabilities and suggest appropriate responses to them.
  - Conducts malware analysis and reverse engineering.
  - Prepares risk assessment reports for management, administrators, and end-users.
  - Communicates with other threat analysis for defining correct security plans.

- **Subject Matter Expert/Threat Hunter**

  Subject Matter Expert/Threat Hunter is a security professional who is responsible for developing, tuning, and implementing threat detection analytics. He/she identifies abnormal behavior before any warning generated by security systems. He/she is using threat intelligence, custom tools as well as threat hunting solutions like Endgame, Infocyte, Sqrrl Data. A subject matter expert should have in-depth knowledge of advanced network forensics, intrusion detection, and cyber incident response.

  Responsibilities of Threat Hunter

  Threat hunter is responsible for performing the following activities:

  - Proactively detects and neutralizes those advanced security incidents that automated security solutions are not able to find.
  - Collects various information about identified potential threats, like their behavior, goals, and methods.
  - Analyzes the collected information and provides appropriate countermeasures.

- **SOC Manager**

  SOC manager is responsible for organizing overall security operations. He/she is also responsible for handling team members and interacting with other security analysts. He/she is also in charge of developing policies and standards for recruiting a skilled team. He/she behaves like a direct boss to all team members.

Responsibilities of SOC Manager

SOC manager is responsible for performing the following activities:

- Tracks security operations.
- Examines policy compliances and regulatory compliances.
- Manages team members and communicates with other departments to minimize risks.
- Documents and defines a security incident response plan.
- Audits security policies and controls regularly.
- Evaluates and implements new tools and technology.
- Keeps track on security tools and technologies.

- **Chief Information Security Officer (CISO)**

CISO is the senior-most executive in the organization. His/her duty is to set the organization's goals, policies, procedures, strategies, and program to keep the information assets and technologies always secured. He/she also directs the security team to implement effective processes across the organization in order to minimize the risks/vulnerabilities.

Responsibilities of CISO

CISO is responsible for performing the following activities:

- Designing and Implementing security policies and procedures to give proper protection to the security system.
- Keeps track on selection testing, deployment, and security hardware and software tools/techniques.
- Communicate with management about security issues.
- Risk management.
- Monitors regulatory compliances.

Identifying skilled and experienced SOC professionals is one of the most difficult jobs in designing SOC. A SOC is nothing without correct people, even if it is implementing the right processes and technologies at the right time. People's ability to detect and investigate new and evolving threats and vulnerabilities play an important role in performing security operations.

4.1.3. Common Soft Skills Required for SOC Professional

- **Team Spirit**

All members of a SOC team should work well in a group, try to understand each other's roles and responsibilities, as well as support one other's functions.

- **Communication**

All the members of the SOC team should be able to communicate effectively with other team members, clients, the public, and executives. Oral communication skill is

not enough; they should also have written communication skills in order to write policies, emails, notices, incidents documents, and so on.

- **Trustworthiness**

  All the members of the SOC team should be able to keep given information secret. They should be capable of maintaining a balance between the information that can be disclosed to the stakeholders and the information that should be preserved.

- **Self-confidence**

  Self-confidence skill is necessary for every member of the SOC team. This skill helps the analyst to make correct decisions, work under pressure, and control and use their emotions properly.

- **Assertiveness**

  All the members of the SOC team should have assertive skill so that they can be able to express their thoughts and feelings in a direct, honest, and proper manner.

- **Empathy**

  Each member of the SOC team should be able to understand the perception of other member of the SOC team.

- **Inquisitiveness and Creativity**

  All the members of the SOC team should be creative in nature so that they can provide innovative solutions to the problems.

4.2. Technology

Organizations should always select that technology which works for people and processes. Technology plays an important role in SOC. Both multidimensional and multilevel technology should participate in an efficient manner to protect the systems, programs, and solutions from unauthorized access for a longer period of time. It may include SIEM solutions, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Firewall, Database Activity Monitoring (DAM), Dashboard, Ticket System, and Automated Assessment tools.

The technology component of SOC comprises technical capabilities for monitoring system logs, detecting security incidents, performing investigations, analyzing network traffic, and monitoring threat intelligence inputs. It supports and increases the capabilities of SOC. So, the technology used in SOC should be collaborated in an efficient manner to secure systems and networks.

SIEM is one of the core technologies that the SOC uses to collect, centralize, aggregate, normalize, and correlate data from various sources like message logs, firewall/IDS output, endpoint devices, OS logs, and network logs.

Security monitoring tools such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Firewall, and Database Activity Monitoring (DAM) are in place to prevent and detect events related to security incidents. For example, IDS monitors all network activity passing through it and generates alerts to SOC administrators whenever inappropriate, incorrect, or malicious activities detected. It uses predefined patterns of malicious behavior and then determines the deviations from expected behavior. It facilitates user behavior monitoring, processes scanning, system file comparisons, and system setting, and configurations monitoring. You can set IDS

strategically either on the network or on each individual system (host). Network intrusion detection system (NIDS) monitors all network traffic where a host-based intrusion system monitors operating system files.

The dashboard is a web-based application that offers a personalized and portable view of critical data to SOC users. It represents data in the form of tables, charts, graphs, and others. Dashboard screen is separated into different blocks, and each block represents different information. These blocks are called widgets. It enables single sign-on, personalization, and integration of data from multiple sources. It takes event log as an input and converts it into informational charts, which allows the SOC team to review event data, determine patterns, and detects threats and vulnerabilities. Dashboard facilitates performance monitoring, decision-making, and trending.

The automated assessment tool is responsible for measuring the performance of SOC under different scenarios. It can perform an investigation to detect the security threat and identifies whether the threat needs any action or not. It is also capable of providing appropriate solutions to remediate the threat and validate whether the threat has been removed. They comprise network security scanners that facilitate risks and vulnerabilities identification. Some of the examples of automated assessment tools are NIKTO, Aircrack, and Nmap.

DAM is a set of tools that monitors and identifies the malicious activities of privileged users or administrators and ensures that integrity and availability of data will not be violated. It will generate alerts in case of policy violations. The tools that monitor database activities are capable of performing multiple activities like vulnerability management, intrusion detection and prevention, integration of identity and access management, discovery and classification, and risk management. These tools also collect database events, database administrator activities, and SQL activities, over different platforms, in real-time.

The ticketing system is an essential part of SOC. It is responsible for streamlining the assessments, automating the responses as well as comprehensive reporting. It provides relevant details about the security incidents such as affected hosts or any previous records. It uses best practice processes to stop and prevent major security incidents from getting worse. It also facilitates proper management of security incidents by capturing and grouping tickets accurately.

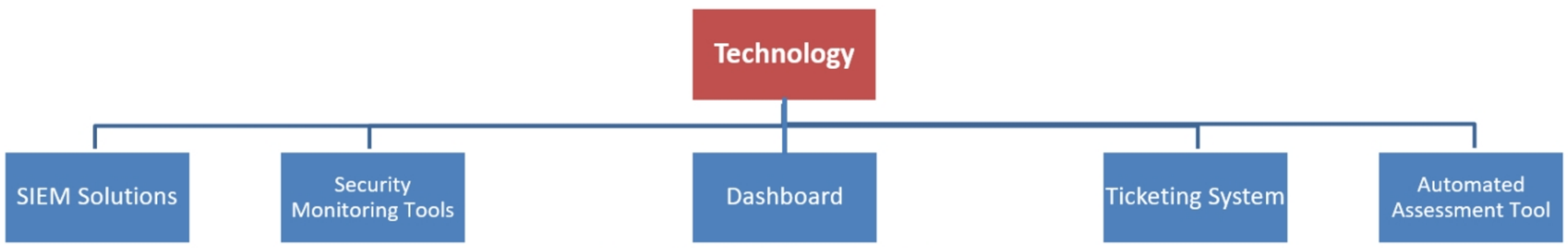

Figure 1. 6: SOC Technologies

4.3. Processes

Processes are the important part of SOC operations. They should not only be present but also be mature. A right team will perform the right tasks through a well-defined process. They are like the interfaces that are used by the different functional parts of SOC to perform seamless and effective operations. A good set of processes helps a SOC to perform in a manageable and quantifiable manner. In the absence of well-defined processes and procedures, SOC has to depend upon the knowledge of individuals. In case the skilled individuals are not available, then it will cripple the SOC capability. Thus, there should be a set of relevant processes that describes a reliable way for the execution of security operations and their expected results. They are designed by considering security monitoring and administration. Their main purpose is to identify available threats and

vulnerabilities, their impact on the organization and responding to them immediately. The processes and procedures for a SOC is planned on the basis of its scope, technologies used, customers supported, and services provided. A well-designed SOC has various processes and procedures.

Typical Processes involved in SOC

- **Business Processes**
  - In these processes, administrative components are defined and documented for the efficient functioning of SOC
  - They position the operations as per the organizational objectives
  - Examples: report preparation, log retention, etc.
- **Technology Processes**
  - In these processes, actions related to IT infrastructure is defined and documented
  - They ensure that IT infrastructure will works at best levels at any particular time
  - Examples: Vulnerability scanning and remediation, Firmware, etc.
- **Operational Processes**
  - These processes describe the different activities that are performed in a SOC
  - Examples: Shift scheduling, Employee training
- **Analytical Processes**
  - Analytical processes explain the way to detect and remediate security issues
  - They include different methods of identifying and understanding surfacing threats
  - Examples: Incident classification, detection and escalation, ticketing, and forensics

5. Types of SOC Models

Organizations are implementing SOC models for managing and monitoring daily business operations. Every organization is different from one another, so their model is also different. The selection of specific type of the SOC model depends upon the requirements, size of the organization, processes, skill set of the personnel, budget, and security incidents occurred in the past, and day-to-day functionalities of an organization. Generally, there are three different types of SOC models:

- **In-House/Internal SOC Model**

  An in-house/internal SOC model is recommended to those organizations that have security issues related to outsourcing. Also, to those organizations that have a budget to invest as internal SOC requires 24/7 efforts. It is also adopted by those organizations to which the integrity of their data is a major concern. It requires a dedicated team which is fully aware of organizational environment, in order to organize human resource for security operation.

Advantages:

- It helps the in-house staff to understand the organization and its environment in a much better manner, as compared to the third-party security service provider.
- It provides a complete picture related to the security posture of an organization.
- It includes a dedicated security team.
- The staff has a better knowledge of the organization environment as compared to the third party
- It saves the logs locally.
- Here, it is easy to customize the solutions.
- It is robust and can handle threats.
- It minimizes the risk of external data transfer as it stores all event logs internally.
- Communication during the attack is performed at a faster rate as it utilizes its personalized means of communication.

Disadvantages:

- This model takes many years to set up infrastructure, threat intelligence, and other capabilities.
- It requires huge advance investment.
- Difficult to identify skilled security analysts.
- The pressure to ROI.
- Lack of Co-ordination among the team may result in missing alerts and important data exchanges.

- **Outsourced SOC Model**

In this model, a Managed Security Service Provider (MSSP) sets up the infrastructure and offers threat intelligence and other capabilities. Its initial start-up cost is low because it spends mainly on the vendor's infrastructure. Here, service providers have multiple connections with different clients through which they are able to develop a sound knowledge base and can repeat the process of detecting and escalating security threats and vulnerabilities. It provides a robust security solution to the organization. It has a dedicated team of trained and experienced security analysts, who can monitor and analyze incidents, respond processes, aggregate technologies, correlate and analyze data, and perform threat research and intelligence on an ongoing basis.

Advantages:

- This model also helps the organization to meet specific compliance requirements.
- It offers cost-effective services as compared to in-house SOC model.
- It takes less time to build this model at an efficient level.
- This type of SOC provides high levels of services.
- Scalability and flexibility.

- A security analyst is an expert in tracking and SIM tools.
- It is unbiased.

Disadvantages:

- It has the risk of external data mishandling.
- It does not provide long-term gain to the company.
- The third party does not have much knowledge about the organizational environment.
- Lack of skilled security team.
- External data mishandling may be possible.
- Customization of solutions is not easy.

- **Hybrid SOC Model**

  It is a combination of both in-house and outsourced SOC model. In this model, the organization is accompanied by MSSP to offer the most secure approach. Its initial start-up cost is the same as internal SOC, but it also includes the cost of vendor staffing at off office hour. It has a semi-dedicated team of security analysts who focus mainly on shift arrangement. If the expertise/skill set of security analysts are not present in-house, then they may be outsourced to the vendor.

  Advantages:

  - They share synergies for technology, processes, expertise, facilities, and personnel to reduce the cost.
  - This model provides the best approach for monitoring and analyzing intrusion incidents, quick detection and response time, and low backlogs.
  - It includes well-skilled internal security team knowledge as well as external team capability and maturity.
  - It uses additional tools and technology for better threat intelligence.

  Disadvantages:

  - It sets up extra hardware, managing data/information by the third party.
  - It is costly as compared to other models.
  - It uses additional hardware for managing data/information.
  - It is handled by both the internal and external organizations so, coordination between both is key for successful operation.

5.1. SOC Maturity Models

Maturity models are IT governance tools that explain the organization's working process as per standardization, results, and measurement of effectiveness. They are used to analyze the effectiveness and capabilities of SOC. They also specify where a SOC succeeds and where it requires improvements.

Few examples of maturity models include Control Objectives for Information Technology (CoBIT) and Software Capability Maturity Model (CMM).

A SOC passes through three levels of maturity before getting integrated with the organization's service management processes:

- **Maturity Level 1: Create the Correlation Rules**

  A correlation rule contains a logical combination of events or conditions and notifies to SOC whether the sequences of events are indicative of attack pattern or not. These correlation rules are designed by security analysts in Regex programming language. While building the rules, security analysts think like an attacker, so that they can design most effective rules for the organization. The correlation rules should be designed in such manner that they trigger only specific attack patterns which affect the organization instead of general rules and signatures such as intrusion detection/prevention systems and antivirus.

- **Maturity Level 2: Automation of Responses**

  Correlation rules give notification about attack patterns, but manually through emails, interruptions, phone calls, and so on. This takes up the majority of SOC analyst's time in determining whether the incident is indicative of attack pattern or false positives. So, it's necessary to make the SOC automated. But it should be done carefully; otherwise, it will negatively affect the organization.

- **Maturity Level 3: Service Management Integration**

  Once the responses are automated, use the enterprise service management tool to integrate the organization's service management processes. The tool helps the security analysts in the monitoring system and application changes, in documenting user service requests, issues, and knowledge.

Types of Maturity Models

1. **SOC-Capability Maturity Model**

   SOC-CMM plays an important role in structuring the SOC. It provides a baseline to identify and evaluate the characteristics of SOCs, like particular technologies or processes used. Moreover, it also allows organizations to make comparison among their capabilities and facilitates administrators to take proper decisions.

   Maturity

   SOC-CMM establishes the maturity levels of SOC. Maturity levels act as a roadmap for building an effective SOC. The SOC-CMM uses the following maturity levels:

   - **Level 0—Non-existent**: At this level, aspects are not managed at all.
   - **Level 1—Initial**: At this level, aspects are disorganized and inconsistent.
   - **Level 2—Defined**: At this level, aspects are documented and analyzed for compliance.
   - **Level 3—Managed**: At this level, aspects are managed and monitored as per the metrics.
   - **Level 4—Quantitatively Managed**: At this level, aspects are measured and managed for quality, quantity, and timeliness of deliverables.

- **Level 5—Optimizing**: At this level, aspects are optimized and improved continuously by following good practices.

The development in SOC-CMM is continuous and is performed on all aspects concurrently and separately. Thus, it can be said that SOC-CMM is a continuous maturity model.

Capability

The SOC-CMM also measures the technical capability of SOC continuously. It comprises four capability levels: Incomplete, Performed, Defined, and Managed. The capabilities are not dependent on maturity levels; hence, it can be enhanced independently.

2. Control Objectives for Information Technology (COBIT)

COBIT is a framework that was developed by ISACA (Information Systems Audit and Control Association) for IT management and IT governance. It was introduced to provide support for the security managers and minimize gap among technical issues, business risks, and control requirements. It can be implemented for any organization to ensure authenticity and standard of information systems. It uses the set of processes to attain the strategic objectives of the organization. Each process is specified with its goals, inputs and outputs, activities, performance metrics, and maturity model.

The following are the important components of COBIT:

- **Framework**: It uses best practices and procedures in processes and domains and helps in attaining the goals of IT governance and management.
- **Process descriptions**: It is a reference model that comprises planning, building, running, and monitoring of processes.
- **Control objectives**: It includes requirements needed for efficient IT business control.
- **Maturity models**: It analyzes the maturity and capability of each process.
- **Management guidelines**: It supports in calculating the performance, assigning roles and responsibilities, and maintaining better interrelationships among the processes.

3. National Institute of Standards and Technology (NIST) Cybersecurity Framework

National Institute of Standards and Technology (NIST) Cybersecurity Framework is a policy framework designed to enhance the critical infrastructure cybersecurity. It includes standards, guidelines, and best practices that help the organization to control cybersecurity-related risk, take risk management decisions, and monitor threats and vulnerabilities. It also helps in identifying those activities that deliver critical operations and service delivery.

Benefits of NIST Framework to Organization

- It supports the organization in identifying, protecting, detecting, responding, and recovering cybersecurity risks and data loss.
- It focuses on contractual and regulatory obligations.
- It enables the organization to determine whether it is a trusted organization that can be able to protect its critical assets.
- It prioritizes investments.

4. Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM is a process-oriented framework that designs secure systems based on Software Engineering Capability Maturity Model. It specifies the important properties of the security engineering process that are needed to maintain security engineering effectively. This model is used as a tool to monitor security engineering practices and standard mechanism for analyzing the capability of the provider's security engineering.

SSE-CMM includes 11 process areas and 5 Capability Maturity Levels. The 11 process areas are Administer Security Controls, Assess Impact, Assess Security Risk, Assess Threat, Assess Vulnerability, Build Assurance Argument, Coordinate Security, Monitor System Security Posture, Provide Security Input, Specify Security Needs, and Verify and Validate Security. Each process area includes its objectives and a set of base processes that are going to assist the process area.

The five capability maturity levels of SSE-CMM are:

- **Level 1—Performed Informally**: At this level, only base processes are executed.
- **Level 2—Planned and Tracked**: At this level, various aspects like project level definition, planning, and performance are focused.
- **Level 3—Well-Defined**: At this level, best practices and standards are defined.
- **Level 4—Quantitatively Controlled**: At this level, measurable quality objectives are set.
- **Level 5—Continuously Improving**: This level focuses on enhancing the capability of organization and efficacy of a process.

5.2. SOC Generations

- **First-generation SOC: 1975–1995**

  The first-generation SOC was developed mainly for the defense organizations and government agencies. It mainly focused on protecting organizations against low-impact malicious code and nuisance programs.

- **Second-generation SOC: 1996–2001**

  In the second-generation era, the attackers keep on improving attack methodologies, so the need for improved SOC arises. The second-generation SOC is capable of intrusion detection. MSSPs started to provide SOC as a service to the organizations. Security Incidents and Event Management (SIEM) technology was developed.

- **Third-generation SOC: 2002–2006**

  In the third-generation era, attackers use bots to steal identity and financial information. The third generation SOC team is capable of handling tasks related to vulnerability management. In addition to this, they can formalize and execute tasks related to incident response. Large-size organizations in specific industries started to adopt in-house SOC.

- **Fourth-generation SOC: 2007–2012**

  Fourth-generation SOC introduces various advanced security services to handle new security threats like hacktivism, intellectual property thefts, and advanced persistent threat.

Big data security analytics, data enrichment, and continuous security monitoring are the different concepts that are added to this generation.

- **Fifth-generation SOC: 2013–till date**

  Fifth-generation SOC uses analytics and big data, intelligence-driven methodology, information sharing, and human adversary approach to handle new security threats. 5G SOC is more efficient than 4G SOC. It automates the tasks performed by 4G security analysts manually.

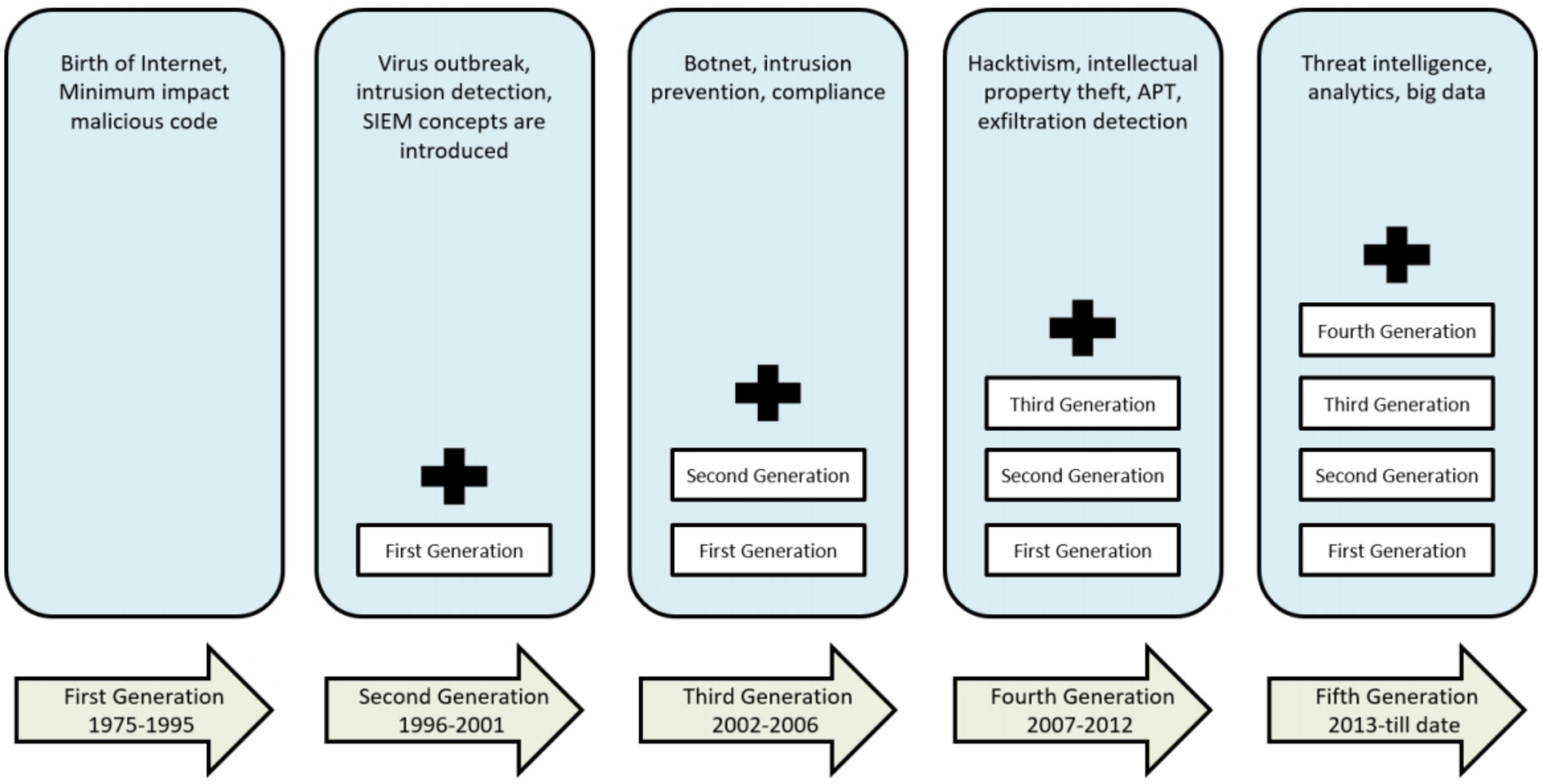

Figure 1. 7: SOC Generations

6. SOC Implementation

There are five different phases involved in the implementation of SOC:

1. **Planning**

   Planning is required for the successful implementation of SOC. Before starting planning, it is important to collect information that is used for setting the organization's goals and objectives, threat environment, budget, and so on. It is also necessary to analyze the existing security capabilities for people, process, and technology. Based on analyzed data, prepare the baseline and compare it with the goals set for the future SOC.

   Use the below steps while applying assessment methodology on data:

   - **Define goals and objectives**: The first idea is to set organization's goals and objectives, as the security management requirements of each organization is different from one another and hence their goals and objectives are also different.
   - **Determine the capabilities that need to be analyzed**: The next step is to determine the capabilities on the basis of decided goals. The capabilities include available people, processes, and technologies.

- **Gather information about people, process, and technology capabilities**: Once the capabilities are identified, gather information regarding them.
- **Analyze and document maturity level**: Set the maturity levels for each identified capability.
- **Discuss and formalize the search**: At last, all parties who are responsible for the implementation of SOC will discuss and formalize the search.

2. Designing and Building the SOC

After planning the SOC, the next step is designing and building SOC. The designing and building phases of SOC are interrelated to each other, and here the important part is to select the best technology to implement efficient SOC. Moreover, the collection of data is also an important point that should be considered here. This task is performed by SIEM, which is the main technical components of SOC. It supports collecting data from various sources like firewalls and intrusion detection/prevention system and in identifying and analyzing the existing security position of an organization.

It's always a best practice to select those security technologies that support layered capabilities, so that if one feature fails to detect suspicious incidents, then another feature should be there to handle it. For example, implementing both an IPS and anti-virus may be beneficial, but both are signature-based technologies and may identify the same type of threats and vulnerabilities. So, the best thing is to implement layered defense/detection capabilities like:

- One content filter knowing about harmful web sources.
- One intrusion prevention system (IPS).
- One breach detection system to identify vulnerabilities that are not detected by IPS.
- One tool for analyzing abnormal incidents.

All areas of the network, such as mobile devices, user desktops, network edge, data center, and branch offices, should have the same level of security. Otherwise, the least protected area will be utilized by the attacker for the attack.

SOC should follow vulnerability management lifecycle for determining and securing the weakest link in a network. Vulnerability management lifecycle uses assessment tools like OpenVAS, Metasploit, and Nessus to detect abnormal incidents and also utilizes multiple methodologies to identify risk associated with the threat. This information helps security analysts in preventing and removing threats. Moreover, the use of the automated inventory-assessment tool is also beneficial as it supports in identifying all the available assets and their current risk to the organization.

3. Operating the SOC

After designing and building the SOC, the next step is to operate the SOC. This phase is also called the "go live" phase. Before moving to operating phase, a new SOC should overcome some important challenges like:

- Validate whether the new SOC still has executive sponsorship.
- Test the new processes.
- Check whether technologies are functioning properly.

- Train the team members who have to use and maintain the SOC.

Moreover, a proper transition plan is required while moving from the building phase to the operating phase. Successful transition plans should be able to have the following factors:

- Clear and well-structured resources.
- Simple checklist specifying how the outputs of each activity or task will be analyzed to achieve the goals.
- Skilled team to perform the desired task.
- Clear and achievable technologies, deliverables, and content.

4. Reviewing and Reporting the SOC

After making the SOC go live, the last stage is to review the SOC to identify the areas of improvement and to check whether it is operating accordingly. Consider the following points while reviewing and preparing a report:

- **Define the scope of the review**: It is always beneficial to limit the scope, only up to specific areas.
- **Identify participants**: Specify the participants who are going to participate in the review based on the scope of review.
- **Built a clear strategy**: Build a clear strategy to perform the review.
- **Identify frequency**: Identify how frequently a review should be done.
- **Prioritize results and action items**: Prioritize areas of improvements and its related action items to make sure that required changes have been done.

6.1. SOC Key Performance Indicators (KPI) and Metrics

Key Performance Indicators (KPIs) are a series of measurements that are used to analyze the performance of an activity. It should be SMART: Specific, Measurable, Actionable, Relevant, Timely. Specific means it should evaluate the attribute of the system directly; it should not depend upon the measurements of other systems as well as the integration of different systems. Measurable means, KPI's should provide accurate and complete information. Actionable means it should provide information which is easy to review on which appropriate action can be taken. Relevant means it should be able to provide relevant data from the collected information. Timely means it should provide information at the requirement. The SOC has the following KPIs:

- **Completion Time**

  Time spent in completing the project as near as possible to 100%. It should be completed on the date demanded by the client.

- **Response Time**

  Time taken to respond to security incidents. It should be given as quickly as possible.

- **Over Time**

  It states, organizing the staffing levels based on the expected volume of calls and service delivery. It should be done in such a manner that it would reduce the unbillable over time and increase the profit as well as the productivity of the system.

- **First-Time Fix Rate**

  It means providing all the necessary information to the staff to monitor and respond to a site effectively. The information given to the client should be accurate enough so that they can take appropriate action against security incidents.

- **Client Satisfaction**

  It means time taken to answer the client's question and satisfy him. It should be done quickly, and for this, your system should be properly automated.

- **Transfer Rate**

  These are incidents that are not handled properly by the first incident responder and are transferred to another incident responder. The transfer rate should be as minimum as possible.

- **Operations Audit**

  It is a scheduled or unannounced deep dive performed by the security team to validate the efficiency and effectiveness of the organization.

- **System Availability and Accessibility**

  It means measuring the up-time reliability of the critical system, subsystem, or process.

Metrics determines how SOC are performing against a defined set of criteria. It helps the security analysts to make decisions and enhance performance and accountability. It provides an overview of levels of regulatory compliance and validates whether the security controls are implemented as per the policy, process, and procedure. It also facilitates in identifying security program effectiveness, people's capabilities to handle issues as well as security trends, both inside and outside the organization's control.

In addition to this, the below metrics can also be used to measure the performance of SOC:

- Number of security events inputted into SOC
- Number of data points gathered and analyzed
- Types of data collected and assessed
- Number of Use Cases
- Outcomes
  - Correlated events
  - Incidents/Cases

6.2. Challenges in Implementation of SOC

SOC has the following challenges that come in between its implementation:

- **Increasing Volume of Security Alerts**

  SOC is receiving a large number of security alerts due to which major amount of SOC analyst time is wasting in triage and validating authenticity of alerts.

- **Management of Numerous Security Tools**

  SOC is using a wider range of security tools which are difficult to monitor and manage individually. So, it would be a good idea to have a central data source and a single platform to collect the data generated from multiple sources. This gives you an overview of your security environment and facilitates you to analyze and manage the security operations properly.

- **Lack of Skilled Analyst**

  This is the most significant issue in the implementation of SOC, and it is increasing day by day. Due to the increase in competition, there is a demand for skilled employees for better handling of security incidents. Moreover, there would be accurate knowledge transfer between analysts for proper detection and remediation of security threats and vulnerabilities.

- **Legal and Regulatory Compliance**

  It is troublesome to meet a number of legal and regulatory compliance such as NIST, PCI GLBA, FISMA, HIPPA as well as industry best practices.

- **Technology Selection and Configuration**

  Selecting the correct technology is very important while implementing SOC. Its proper configuration should also be done; otherwise, it would lead to insufficient monitoring of security incidents.

- **Large Number of Processes and Procedures**

  It is very difficult for security managers to implement SOC processes and procedures. So, it is suggested to use automated processes tool for managing the current processes and designing the new processes.

6.3. Best Practices for Running SOC

Security Operations Centers (SOCs) make use of various security tools and technologies, but security is not only dependent upon the tools and technologies but also requires security team to focus on different other factors like scope of security team and their roles and responsibilities, organization's security budget, security analyst's skills and knowledge, business requirements, detecting and defending perimeter, building incident response system, and right organization infrastructure.

Besides these, there are various other best practices that are required for running SOC:

- Always use real-time security dashboards for receiving notifications
- Use well-defined incident response processes and procedures
- Use critical security alerts to receive notification 24x7
- Develop a risk-aware environment and management system
- Use security intelligence to manage security incidents
- Protect mobile and social workspace

- SOC should receive log and security events from firewalls, routers, netflow, IPS, applications, and operating systems, for monitoring and analyzing
- Protect services by design
- Automate security "hygiene"
- Ensure resilience by controlling access to the network
- Determine the complexity of cloud and virtualization
- Maintain third-party security compliance
- Secure data and protect privacy
- Always understand the working of SOC, and how it monitors the endpoints and networks, detects security threats and vulnerabilities, and handles them appropriately.
- Always use correct tools and technologies, like Firewalls, data monitoring tools, automated application security, asset discovery systems, and endpoint protection system.
- Always use skilled and dedicated security specialists for monitoring and managing alerts, for proposing security actions, and for detecting threats internally.
- Always build an incident response team for giving a response to security incidents effectively.
- Always have a team to collect much information regarding security incidents.

6.4. SOC vs NOC

NOC is a centralized system where administrators manage, control, and monitor the network continuously. It is located within or outside the organization's premises. It can work under pressure to fulfill both technical and business needs. It is used by various managed IT service providers, who want to provide 24/7 uptime services to their clients. It also provides performance monitoring features that help the organization in achieving its network performance objectives and enhancing customer satisfaction. A well-managed NOC should also be able to organize network operations effectively, enhance workforce mobilization, reduce outages, and manage resources in a better way.

NOC technical team always keeps an eye over endpoints for which they are responsible for monitoring and managing. They not only monitor and manage the activities but also correct it and apply preventive measure so that it will not occur in the future. Moreover, they are also responsible for software distribution, router updates, domain name management, performance monitoring, and network coordination.

Beside this, there are wide varieties of NOC applications. Some of them are described below:

- Monitoring and managing intrusion detection/prevention system as well as firewall
- Patch management
- Whitelisting
- Email management services
- Antivirus scanning and threat prevention

- Alarms and log management
- CRM
- Dashboards
- Process management
- Incident management
- Network monitoring
- Threat analysis

NOC is different from SOC. But the marketplace gets confused between their services. NOC is similar to your central nervous system, whereas SOC is like your immune system. Both play an important role in managing security operations but in different ways. NOCs support in managing and monitoring network traffic and keep the network running, whereas SOCs offer a real-time representation of a network's security status.

NOC	SOC
NOC monitors IT infrastructure to ensure **uninterrupted** network service	SOC monitors IT infrastructure to ensure security of the **network**, **web sites**, **applications**, **databases**, **servers**, etc.
NOC is responsible for network fault tolerance, Switch router configuration, sniffing and troubleshooting, system and traffic monitoring, etc.	SOC is responsible for network behavior anomaly detection, intrusion detection, log management, network forensics, vulnerability detection and awareness, management and change policy, etc.
A NOC analyst should be well-skilled in the **network**, **application**, and **systems engineering**	SOC analysts should have **security-engineering** skills
The NOC focuses on **system events** that occurred naturally	The SOC focuses on "**intelligent adversaries**"

Table 1. 1: Difference between NOC and SOC

Chapter Summary

In this chapter, we have discussed security management and its importance in maintaining security in the organization. We have also focused on Security Operations Center and its capabilities and operations to protect security system against security threats. This chapter has also provided an overview of various SOC functions performed by security analysts to gain the actual security posture of an organization. Besides this, we have also discussed SOC components: People, Process, and Technology that play an important role in monitoring and managing different activities of SOC; it's working process to detect and respond to suspicious activities; SOC models; and SOC generations. This chapter ends with an overview of various phases of SOC required for its implementation; SOC KPIs and metrics; and Network Operations Center (NOC).

In the next chapter, we will discuss various types of cyber threats and threat actors, IoCs, and cyber kill chain methodology, including common TTPs used by attackers.