Chapter 21
An Introduction to Security Operations

Gurdip Kaur and Arash Habibi Lashkari

21.1 Introduction to Security Operations

Security attacks have become complex and sophisticated over the past decade. In the recent years, cyberattacks such as WannaCry (2017) have come into limelight by major losses to worldwide organizations by locking the sensitive information files on victim computers. According to a report by Kaspersky, around 230,000 computers in over 150 countries were infected by this ransomware [1]. The intensity and impact of such attacks raise concern for imparting security to crucial informational assets. What if financial losses are also involved? The risk associated with such attacks can also result in significant monetary losses, the loss of the firm's reputation, and business. Addressing the potentially composite and advanced attacks not only includes modern technology but also the development of intelligent monitoring and incident response systems. Consider that a maliciously fabricated Internet Protocol (IP) packet destined for a specific host on a victim network is successful in crashing the target host. The sequence of events (incident) needs investigation to identify the root cause and perform remediation. In such a scenario, security operations generate the vital information that drives the investigation process to understand what happened, how the attack was executed, which vulnerability was exploited, how much risk is associated with the compromised system, and how to mitigate the situation.

Security operations (SOs) aim to monitor the organizational assets, investigate and respond to security events and incidents, identify indicators of compromise (IOC), manage risk, scan vulnerabilities, perform data forensics, and patching

G. Kaur (✉) · A. H. Lashkari
Faculty of Computer Science, Canadian Institute for Cybersecurity (CIC),
University of New Brunswick, Fredericton, NB, Canada
e-mail: Gurdip.Kaur@unb.ca; A.Habibi.L@unb.ca

K. Daimi, C. Peoples (eds.), *Advances in Cybersecurity Management*,
https://doi.org/10.1007/978-3-030-71381-2_21

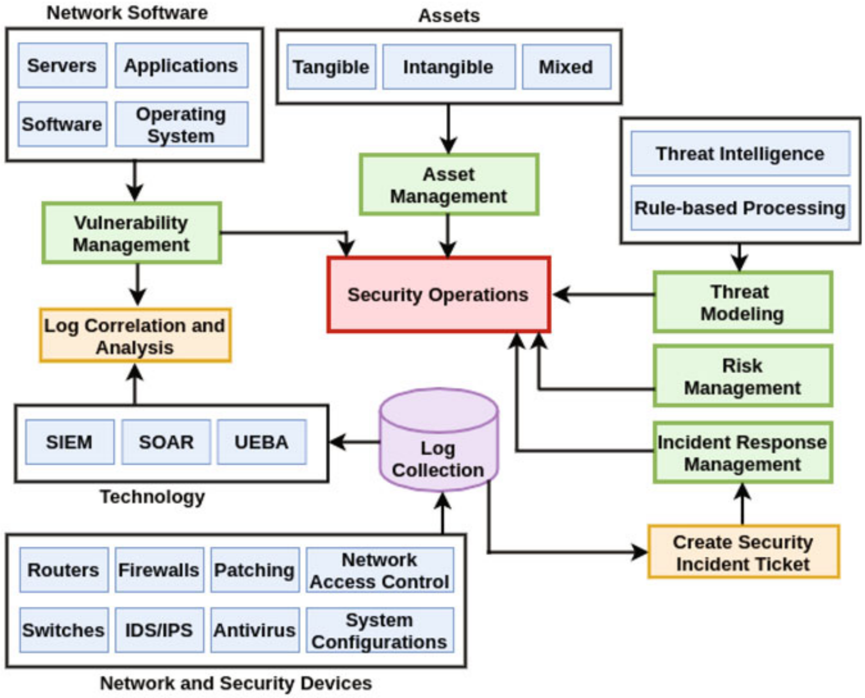


Fig. 21.1 Components of security operations

[2]. All these tasks are performed by a designated security operations team that addresses the following basic security questions:

- What are the assets and vulnerabilities that can exploit those assets?
- How can a compromise be detected? What are the indicators of compromise?
- What is the severity of compromise? How does that compromise impact the business processes?
- What immediate action is required?

To answer these questions, the security operations perform continuous monitoring of endpoint devices, servers, networks, applications, databases, and security solutions to collect and analyze security events to reduce the attack surface. Apparently, it needs sophisticated technology such as Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), and Security Orchestration, Automation and Response (SOAR) to aggregate security events and generates alerts. Figure 21.1 presents the core components of security operations, which will be discussed in the forthcoming sections.

The primary objectives of this chapter include a comprehensive introduction to the concept of security operations and major components associated with it in a clear and simple manner. The chapter sheds light on the evolution of generations of security operations and explains five main components of security operations architecture. In addition, several special issues and challenges in security operations are highlighted. It also brings into light the importance of qualitative and quantitative performance measures that add value to resolving some of the challenges. Finally, the chapter outlines the emerging trends and technologies in security operations.

The remainder of the chapter is organized as follows: Sect. 21.2 summarizes the evolution of five generations of security operations emphasizing the technologies developed in each generation. Section 21.3 introduces various assets and functions performed by asset management. Section 21.4 briefs the types of vulnerabilities that may be exploited and procedure to detect them. A step-by-step threat modeling process is explained in Sect. 21.5 and is followed by risk management in Sect. 21.6. Section 21.7 provides insights into incident response management, and Sect. 21.8 puts forward special issues and challenges faced by security operations. Section 21.9 introduces emerging technologies that aim to improve security operations that is followed by chapter summary.

21.2 Generation of SO

Security operations have evolved over four decades. Starting as early as 1975, security operations' capabilities can be grouped into five generations. Figure 21.2 presents the evolution of these generations from 1975 to 2020. It highlights the sophistication of attacks and the development of advanced tools to detect those attacks in every generation.

First generation: 1975–1995 First generation of security operations mainly focused on low-impact malicious code for government and defense organizations. Early security operations utilized emerging technologies such as antivirus and firewall [3]. Security operations were handled by a single person. Log collection was limited to this generation, with firewalls being the main source. In some cases, logs were stored centrally using unencrypted Syslog servers and Simple Network Management Protocol (SNMP) messages [4]. However, in most cases, logs were stored locally. This led to some events not being detected.

Second generation: 1996–2001 The second generation began around 1996 to detect viruses using proxies, vulnerability scanners, and intrusion detection systems in addition to firewalls and antiviruses. There was an improvement over the first generation, but most attention was paid to reactive security [3]. Security operations began emerging in the commercial sector, and some government and military sectors started using SNORT and *tcpdump*. Although the tools deployed to collect logs were performing to the best of its abilities, what to do with this collection was the question before security professionals. Thereby, they started performing event analyses using scripts, intrusion detection systems, and other in-house developed tools. Since the attackers developed sophisticated attack methodologies to use bots in denial-of-service attacks, this generation also developed intrusion prevention systems. Threats

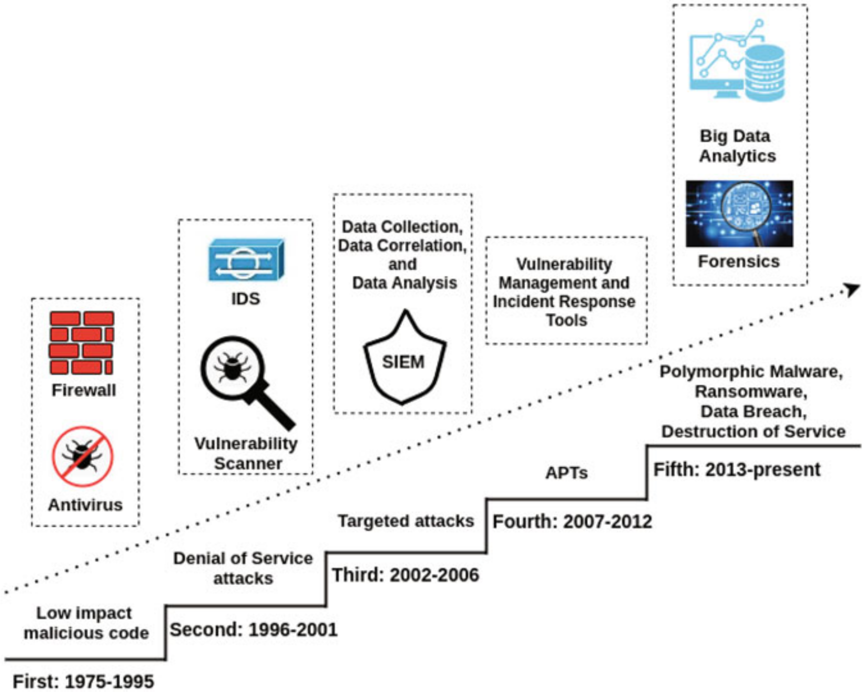

Big Data Analytics
Forensics
Data Collection, Data Correlation, and Data Analysis
SIEM
Vulnerability Management and Incident Response Tools
IDS
Vulnerability Scanner
Firewall
Antivirus
Polymorphic Malware, Ransomware, Data Breach, Destruction of Service
Fifth: 2013-present
APTs
Fourth: 2007-2012
Targeted attacks
Third: 2002-2006
Denial of Service attacks
Second: 1996-2001
Low impact malicious code
First: 1975-1995

Fig. 21.2 Generations of security operations

and vulnerabilities were escalating so fast that the MITRE corporation created Common Vulnerabilities and Exposures (CVE) repository to keep track of it.

Third generation: 2002–2006 By the mid-2000s, malware such as SQL Slammer and Blaster worm created havoc. Bots were being used to steal financial information. With the growth of the third generation, disruptive cyber threats were transformed into targeted attacks. Several mainstream events such as the formation of Payment Card Industry (PCI), BitTorrent, operation Titan Rain, The Honeynet Project, and US-CERT took place. Finally, SIEM was coined in 2005, which marked the beginning of a new era for event data collection, correlation, and analysis.

Fourth generation: 2007–2012 This generation was marked by the beginning of cyberwar among politically acclaimed countries that attacked one another for stealing intellectual property using advanced persistent threats (APTs). Cybersecurity professionals realized the inability of intrusion detection and prevention systems to detect such attacks, and their focus was shifted to detecting data exfiltration and containment strategies.

Fifth generation: 2013–present With big data analytic capabilities, fifth-generation security operations focus on the analysis of enormous amounts of structured and unstructured data, threat modeling, and advanced SIEM to explore the counterattack tactics. Fifth generation also incorporates data enrichment with geo-location data, Domain Name System (DNS) data, network access control, and IP data. New forensic technologies are also being used to detect breaches [3]. It uses defense in depth by utilizing layered security, expanded threat landscape, continuous monitoring to gather intelligence, and automated reporting tools to reduce response time to incidents. The governing bodies have introduced several policies for process improvement and scheduled reviews to effectively manage the business processes.

In summary, the fifth generation is still evolving, but there is a need to integrate SIEM, SOAR, and threat modeling to cover a larger threat landscape that caters for diverse cyberattacks and risks associated with them.

It is apparent that all the generations include the tools and technologies used in previous generations and add advanced techniques to combat sophisticatedly growing cyberattacks. Next generation of security operations is deemed to include big data analytics, threat modeling, SIEM functionality and security orchestration, automation, and response in a single large framework to mitigate the next generation of cyberattacks.

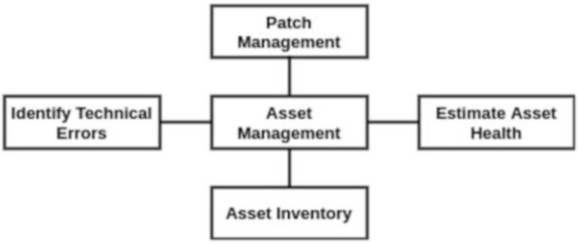
21.3 Asset Management

The first component of security operations architecture is asset management. Asset management deals with managing and provisioning resources. The security operations team continuously monitors the organizational assets owing to the vulnerabilities that can be exploited to compromise the critical services. The primary goal of asset management in security operations is to gain an imperative understanding of patching level, health, vulnerabilities, and policy gaps in the organization so that risks associated with the exploited vulnerabilities can be assessed in advance.

Security operations are primarily concerned with tangible assets, but sometimes intangible and mixed assets are also considered. These assets are generally classified as physical resources (hardware), digital resources (software and data), and human resources (employees and contractors). Figure 21.3 summarizes the four main functions performed by asset management: identify technical errors, maintain asset inventory, estimate asset health, and patch management. Identifying technical errors and estimating asset health are grouped together as asset monitoring functions.

Asset monitoring Monitoring the infrastructure as part of a security operations team provides twofold functionality [5]: (1) It estimates the health of organizational assets, critical infrastructure, and applications (2). It identifies and understands the technical errors to provide an insight into the proper training, workload, and cognitive health [5]. Technical errors may be committed by operators (faults and issues), a programmer (buffer overflow), or system administrator (inappropriate privileges and misconfigurations).

Fig. 21.3 Functions performed by asset management



Asset inventory Asset management takes note of any attempts to compromise assets and detects them. Consider the situation where a security operations analyst is trying to investigate a recent attack that targeted several computers on the network that he manages. To start the incident response, the security analyst needs essential information such as IP addresses, location, configuration, and applications running on compromised systems which are readily available in asset inventory maintained by every organization. A typical asset inventory list contains the following essential details [6]:

- System type and version
- Host name
- Operating system installed and version
- Applications/Software installed and version
- Service pack and patch level
- Network devices (switch, router, firewall, and IDS/IPS)
- Hardware details
- Purchase date
- Physical and logical addresses
- System settings

Patch Management Asset management systems also keep track of the patch management status of the systems. However, they are not comprehensive in patch management compared to vulnerability management. In the current era, asset management is one of the key concepts in security operations that abets keeping the devices up to date and allows the security team to retire the obsolete devices and software once it reaches end of life (EOL). This process helps to avoid vulnerabilities that are no longer patched by the vendor. Asset inventory information is supplemented with additional information to determine critical and noncritical systems. It further helps guide decisions to perform vulnerability scans, scan frequency, and priority to remediate identified vulnerabilities. The relation between asset and vulnerability management is discussed in the next section.

Protecting assets is also one of the elements of security operations. Physical assets can be protected by using physical controls such as barricades, closed-circuit television (CCTV) cameras, fences, bollards, etc. Software assets such as operating systems and applications can be protected using endpoint security devices, such as antivirus, firewalls, intrusion detection, and prevention systems. Apart from physical and software assets, virtual assets also need protection. Virtual assets not only include servers but also virtual machines, virtual desktops, virtual storage, and software-defined networks. In addition to all these assets, managing cloud-based assets also falls under asset management [7].

21.4 Vulnerability Management

After successfully listing the assets in the organization, the next step for the security operations team is to identify the vulnerabilities those assets are exposed to. This is the second component of security operations architecture. A successful vulnerability management program seeks to identify, prioritize, and remediate the vulnerabilities before the attacker does so. There are two common elements of the vulnerability management process: vulnerability scan and vulnerability assessment. Vulnerability scans are performed routinely, while vulnerability assessments are periodic in nature. A vulnerability scan is used to detect weaknesses in a system or network. Vulnerabilities may include unpatched software, or weak passwords. Scanners are used by attackers as well as administrators to identify potential vulnerabilities that can be exploited. The purpose of scans varies. Administrators use the scanners to identify and later fix the vulnerabilities before the attackers can exploit them.

There are certain requirements that the security operations team needs to consider before planning a vulnerability scan:

- *Scan frequency* determines the scan schedule that meets business needs, resources, and compliance to organization policy.
- *Scope* addresses systems and targets to be included in a vulnerability scan.
- *Scan sensitivity* considers the configuration settings to minimize the service disruption in the target network.
- *Scan perspective* considers the location from which the scan is scheduled such as from within the network to capture insider threats or external that would foresee the potential vulnerabilities from the viewpoint of internet.

Vulnerability assessment analyzes all the vulnerability scans to determine how the organization is addressing vulnerabilities. It is often performed as a part of the risk assessment or risk analysis process that is discussed in Sect. 21.6. With a plethora of vulnerabilities disclosed every year, it is extremely difficult and tedious for security teams to patch everything. So, their role is to perform decision-based vulnerability management. The crucial point to consider while making decisions is that although thousands of vulnerabilities listed by Common Vulnerabilities and Exposures (CVE) every year, only a small percent of them are exploited [2].

As a security operations team member, the primary responsibility is to determine the challenges associated with addressing vulnerabilities such as prioritizing known vulnerabilities based on severity rating by Common Vulnerability Scoring System (CVSS), mitigating vulnerabilities that cannot be patched within stipulated time,

Table 21.1 Types of vulnerabilities

Type	Examples
Infrastructure	Channel, equipment
Platform	Hardware, platforms, and operating systems
Software	Client and server software, applications, database management systems, and business software
Service delivery	Service application software
Operations	Service management and operational processes
Management	Management and protection tools, services to the infrastructure, platform, and software layers
Personnel	Malicious users

and following Common Platform Enumeration (CPE) naming scheme for software applications.

Vulnerability scan reports provide critical information and aid to analyze the overall trends in vulnerabilities, including the number of new vulnerabilities arising over time, time required to remediate these vulnerabilities, and age of already existing vulnerabilities. Types of vulnerabilities classified by security operations are presented in Table 21.1 [8].

The common workflow followed in vulnerability management is to repeatedly detect, remediate, and test the vulnerabilities. As an exception to severity ratings provided by CVSS, it is imperative to fix a lower external vulnerability before a higher internal one depending upon the damage it may cause to the critical assets of the organization. Moreover, the security operations team must be familiar with common servers and endpoint vulnerabilities, such as outdated or unpatched software to prioritize severe vulnerabilities.

21.5 Threat Modeling

Threat modeling is the third component of security operations architecture. It is the process of identifying potential threats and risks from internal or external actors, evaluating gaps, and developing a strategy to bridge those gaps. Security operations follow a structured approach to identify and model threats. Threat modeling approaches focus on assets, attackers, or software [7]. Asset-based threat modeling uses asset valuation results to identify threats. Attacker-based threat modeling focuses on potential attackers and its objectives to breach the network. The motive for breach is of interest in security operations. Identified threats are then prioritized based on the objectives of the attacker. Software-based threat modeling gives importance to threats against applications and software developed by the organization.

STRIDE and PASTA are the famous threat models used by organizations to identify threats. STRIDE is developed by Microsoft and is primarily used to assess

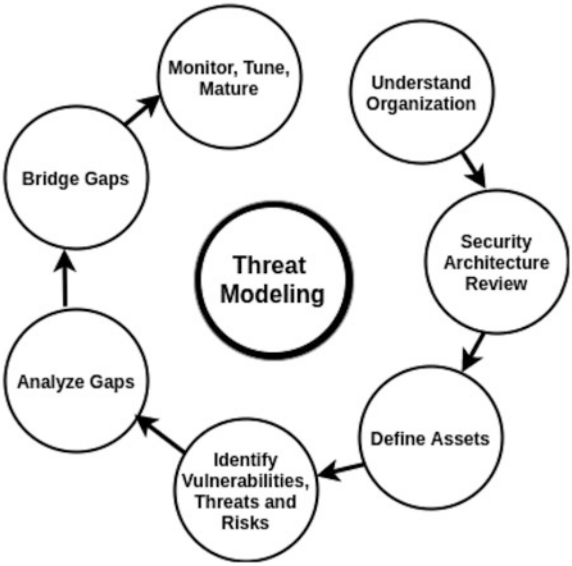


Fig. 21.4 Threat modeling in security operations [9]

applications and software. However, it can also be used for modeling networks and host threats. It is based on six functions: **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege. Process for Attack Simulation and Threat Analysis (PASTA) is a seven-step model that primarily uses a risk-centric approach to analyze threats, vulnerabilities, and risks. Detailed discussion on both models is beyond the scope of this chapter.

Figure 21.4 showcases the standard step-by-step threat modeling process followed in security operations.

Understand the organization The first step in the threat modeling process is to identify the threats that an organization is exposed to. Every organization has different threats and risks involved. For example, threats to the financial sector are totally different from the health sector. Therefore, understanding the nature of threats is highly important to recognize threat actors and attack motives.

Review security architecture Reviewing the high-level design of an organization covers segregating the organizational assets such as physical, logical, and network assets and intellectual property to different security domains. Physical assets include office branches, building, and hardware devices, while logical assets comprise software packages running on hardware devices. Network assets are physical or logical network connections within the devices used by the organization. Finally, intellectual property covers any source code or proprietary code and secret document developed by the organization. After reviewing the high-level design, it is pertinent to categorize the design into different security domains to prioritize threat handling events.

Define assets Security operations team creates an inventory of all the assets owned by the organization. It includes physical, logical, or network assets as explained in the previous step.

Identify vulnerabilities, threats, and risks This is a complex step in threat modeling, where all the threats, vulnerabilities, and risks associated are carefully assessed to compute a risk score. This step considers all the stakeholders in the organization, such as cybersecurity team, application developers, testers, code reviewers, network and operations team, and even the security personnel. Sometimes, penetration testers are involved to reveal the vulnerabilities and hidden threats in the network. Apart from that, some organizations follow game theory exercise to protect their premises by creating red, white, and blue teams. The red team attempts to attack the target systems, and the blue team tries to defend against the attacks launched by the red team while the white team acts as a referee to monitor the activities of the red and blue team and ensures fair play.

Analyze gaps Each risk identified in the previous step is reviewed, and countermeasures are applied to mitigate it. A simple example of a countermeasure includes placing bollards to restrict the entry of cars on organization premises. The amount of risk that cannot be mitigated at this stage is called a gap and needs new countermeasures to mitigate it, which is a time-consuming and costly process.

Bridge gaps Risk mitigation strategies are adopted to bridge the gap so that risks can be accepted, avoided, transferred, or mitigated. SIEM, as a security operations tool, is integrated with threat modeling to collect, correlate, analyze, and visualize threat data for automated response and action to mitigate risks. However, installing new countermeasures to fill the gap may involve huge expenditure which is beyond the reach of a small- or medium-scale organization.

Monitor, tune, and mature For SIEM to be effective, continuous monitoring and tuning are needed so that new gaps are identified in time. In addition, the security model is expected to be mature enough to mitigate those gaps by integrating all assets into SIEM, defining and simulating threats, and building a correlation plan to collect and configure rules in SIEM.

In recent research, a Bug Bar technique is proposed to classify and model threats [10]. The technique computes the severity of threats and then prioritizes the order of threats. It achieves high accuracy in predicting the rating and severity of threats with machine learning models. This technique is assumed to complement the threat modeling approaches used by commercial systems.

21.6 Risk Assessment, Analysis, and Mitigation in SO

Risk is commonly defined as the probability of occurrence of a threat that exploits a vulnerability and impacts the organizational business after successful exploitation. Based on the risk management framework proposed by ISO/IEC 31000:2009, risk

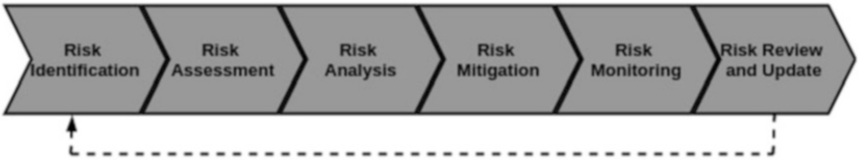


Fig. 21.5 Risk management cycle

management is a continuous process in which the security operations team assesses risks associated with assets, analyzes the severity of compromise, and proposes actions needed to mitigate it [2].

Risk management is the fourth component of security operations architecture. It can be classified as a two-step procedure that (1) provides critical insights into real risks faced by the organization and (2) streamlines available resources to mitigate risks. Figure 21.5 presents the risk management cycle including risk identification; assessing, analyzing, mitigating, and monitoring risks; and reviewing and updating risks. All these phases of the risk management cycle are elaborated subsequently.

21.6.1 Risk Identification

The risk management process begins by identifying risks in an organization as shown in Fig. 21.5. To do so, the security operations team performs asset valuation to estimate the importance of assets and identify the risks associated with important assets that may influence business processes. Although it is highly recommended to identify risks at various levels, it is frequently ignored [4]. Risk identification addresses the following questions:

- What information is collected?
- How is it stored?
- Who has access to that information?

Apart from that, the risk identification phase also finds internal (malicious insiders) and external (perpetrators) threats.

21.6.2 Risk Assessment

Most of the time, the security operations team considers tangible assets, but sometimes intangible and mixed assets are also considered to incorporate them into the risk assessment process. Risk assessment can be qualitative or quantitative depending upon the type of assets included in determining the threats and vulnerabilities related to those assets. For example, if tangible assets (direct costs) are counted by the security team, risk assessment is quantified. In the case of intangible and mixed assets (indirect costs), qualitative risk assessment is performed.

According to NIST definition, risk assessments are used to identify, estimate, and prioritize risk to organizational operations. Risk assessment attempts to find the level of risk that an organization is comfortable taking. In other words, risk assessment estimates the risk appetite of an organization. It lists cyberattacks or security incidents that could impact business. The security operations team makes use of these assessments to reduce long-term costs, avoid data breaches and regulatory issues, reduce application downtime in case of severe risk, and facilitate future assessments.

21.6.3 Risk Analysis

The assessor puts together information on assets, threats, and vulnerabilities to compute the probability of the occurrence of risk and its impact on business. Risk analysis is performed qualitatively and quantitatively. Quantitative risk analysis begins with asset valuation and proceeds with computing the frequency of risk and its exposure to the system. The following parameters are used to compute the risk:

- **Asset value (AV): AV** computes the valuation of assets.
- **Exposure factor (EF):** EF estimates the percentage of loss to the organization if an asset becomes unavailable or lost due to risk.
- **Single loss expectancy (SLE):** SLE is the cost associated with a single risk against a specific asset. It is presented as:

$$\mathbf{SLE = AV^{*} EF}$$

- **Annualized rate of occurrence (ARO):** ARO is the expected frequency of occurrence of a risk per year.
- **Annualized loss expectancy (ALE):** ALE is the total annual loss incurred due to a specific risk and is computing as:

$$\mathbf{ALE = SLE^{*} ARO}$$

On the other hand, qualitative risk analysis ranks the assets. Famous qualitative risk analysis techniques include brainstorming, Delphi techniques, surveys, questionnaires, checklists, interviews, and meetings. However, the Delphi technique is a standard and most preferred technique used for qualitative assessment. In this technique, the participants anonymously write their feedback and submit it to a single meeting room.

Based on this analysis, risks are prioritized before mitigating them. The security operations team creates a risk matrix to analyze the probability of likelihood of a security incident with its impact on the business. Like risk assessment, risk

Table 21.2 Qualitative risk analysis

	Impact				
Likelihood	Insignificant	Minor	Moderate	Major	Severe
Very likely	Medium	Medium	High	High	High
Likely	Medium	Medium	Medium	High	High
Possible	Low	Low	Medium	High	High
Unlikely	Low	Low	Medium	Medium	Medium
Rare	Low	Low	Medium	Medium	Medium

analysis can also be performed qualitatively or quantitatively. Table 21.2 presents a simple example of qualitative risk analysis according to which if the likelihood of occurrence of a risk is “very likely” and its impact is “moderate,” then the risk associated is “high.”

Risk analysis aids security operations teams to enhance the decision-making process by identifying gaps in security and improving security policies and procedures. It also helps to understand the financial impacts of potential security risks.

21.6.4 Risk Mitigation and Monitoring

Risk mitigation follows a layered security approach to avoid, accept, transfer, spread, or reduce risk, and it is complemented by a classic principle involving “*four D’s*” (deter, deny, detect, delay) that protects assets from any adversarial attempt by the attacker [11]. A risk mitigation policy is prepared by the following international standards and organizational guidelines. The security operations team considers several points to implement a risk mitigation policy. Some imperative considerations include acceptable use policy, patching, hardening, end-point security, antivirus programs, CIA (Confidentiality, Integrity, Availability) triad, AAA (Authentication, Authorization, Accounting) principle, and encrypted data storage. Mitigation strategies do not mark the end of the risk management process, as it needs to be continuously monitored for new threats and vulnerabilities. Risk monitoring identifies critical trends and responds to security incidents accordingly.

21.6.5 Risk Review and Update

Finally, the security operations team reviews the lessons learned to update the risk management policy so that new risks are identified, and the process is repeated. Lessons learned report is used to redefine risk strategies, analyze and report trends, and profile risks.

21.7 Incident Response Management

Incident response management is the fifth component of the security operations architecture. Incident response is the underpinning of the security operations that collects, correlates, detects, analyzes, and responds to security incidents. Detecting and responding to security incidents is the core functionality provided by security operations. The team performing security operations monitors the assets and reacts to security events and incidents to recognize indicators of compromise. For example, identifying a beaconing activity indicates that a system in the network is compromised and is communicating to a command-and-control server. The incident response management starts with detecting an incident by analyzing the logs collected from different sources and involves processes, people, and technology. A typical incident response process is presented in Fig. 21.6 which sheds light on different phases of handling an incident [12].

Preparation The aim of preparing for an incident response is to reduce the likelihood and impact of future incidents. The security operations team gathers hardware, software, and information needed to investigate an incident. It includes preparing a forensic toolkit and a team of personnel who will participate in the investigation.

Detection and analysis This is one of the difficult phases which involves detecting major event indicators such as alerts, logs, publicly available vulnerability information, and people (internal and external). As soon as a security incident is detected, the security operations team starts analyzing logs using SIEM to reduce its consequences.

Containment, eradication, and recovery After completing the assessment in the previous phase, the security team takes measures designed to contain the effects of the incident, eradicate it from the network, and recover the normal operations. Several strategies are adopted to contain incidents, such as segmentation, removal, or isolation of compromised systems.

Post-incident The security operations team conducts a lesson-learned review to understand what has happened and how. The purpose of this phase is to determine

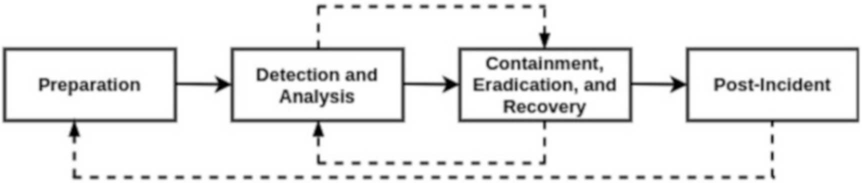


Fig. 21.6 Phases of incident response. Source: NIST SP 800-61: Computer Security Incident Handling Guide

the corrective actions that can prevent similar incidents in future. The security team also drafts a data retention policy to save the incident data for a period.

21.8 Special Issues and Challenges in SO

With unprecedented upsurge in sophisticated cyberattacks, the focus of security operations has shifted from merely preventing a new security incident to developing new technologies and integrating with existing frameworks. This allows the security operations team to identify, manage, and contain an incident in order to minimize its impact on business. Apart from increasing volume of security alerts, proliferation of online users, interteam communication gap; identification of complex and sophisticated attacks, database correlation and analysis, and integrity and interoperability with multiple platforms, following are the special issues and challenges for security operations:

(a) **Integral technology:** Security operations expect emerging technologies such as SIEM, UEBA, and SOAR to integrate their detection and analysis capabilities. This enables security experts to centrally monitor the plethora of security alerts generated by numerous security tools used. Nevertheless, high investment in these technologies is the biggest roadblock for many organizations.

(b) **Shortage of skilled personnel:** Although security operations deploy prominent technological solutions, yet incompetent staff cannot utilize the full potential of automated cybersecurity solutions. Contemporary attacks are more complex and stealthier and need special background knowledge to thwart them. The problem gets intensified when the inappropriately qualified staff is unable to analyze and manage all the critical data to make quick decisions.

(c) **False positives and false negatives:** False alerts are the result of collecting logs from several devices. Factors such as misconfigurations and tuning policies to raise alarms contribute to false positives and false negatives [13].

(d) **Processes and compliance:** Security operations teams bear a major burden of following manual and repeated processes and complying with rigid security policies laid by organizations that are relieved by automated technology such as SIEM.

(e) **Workload or burnout:** Majority of researchers have identified workload as the major challenge for the security operations team. Increased workload leads to deteriorating performance, vigilance, and response capabilities.

These challenges are evaluated using several important performance metrics as reported in the past research [14, 15]. These metrics include amount of time taken to create and resolve tickets, number of tickets raised, quality of incident report, number of incidents, number of alerts analyzed/unanalyzed, experience level of analyst, and average time taken to raise or detect the incident. The mapping between challenges and performance metrics reveals that there is a sound relationship between security operations and emerging technologies used to collect, analyze, and report incident data. However, most of the performance metrics used in the past are quantitative in nature and focus only on the outcome of efforts. There is little or no consideration of efforts behind the detection, analysis, and reporting of complex incidents/alerts.

Some important observations are derived based on the discussion of challenges and performance metrics. First, it is interpreted that analyzing issues and challenges help to identify current loopholes and develop new techniques that address these loopholes. Second, including qualitative measures to determine performance will facilitate management to motivate the security operations' team to achieve the objectives. Third, voluminous log data collected by security operations tools requires an extensive amount of correlation and analysis time. It increases further if the attackers mask the log data by mixing it with non-malicious data. Therefore, it is the need for the hour to integrate emerging technologies to improve the data analysis process. Finally, analyst burnout is one of the major causes of an analyst leaving a job. Mismanagement and vicious life cycle of security operations are regarded as the root causes of burnout [16, 17]. Thereby, it is important to acknowledge the tremendous efforts of the security operations team to avoid analyst burnout.

21.9 Related Emerging Technologies

Security operations cannot work without technology. The emerging technologies facilitate less experienced security analysts to automatically orchestrate, analyze, and respond to security incidents. Therefore, it becomes easier for the security operations team to reduce false alerts and work fatigue which helps to improve the performance.

Traditional SIEM has been an inseparable part of security operations ever since its inception into the third generation. SIEM is a combination of Security Information Management (SIM) and Security Event Management (SEM), where SIM collects, analyzes, and reports log data, and SEM analyzes that log and real-time event data to provide threat modeling, event correlation, and incident response. However, the next-generation SIEM is built upon big data, machine learning, advanced behavior analysis, and automatic incident response. It can detect advanced security events that none of the traditional security tools (firewalls and intrusion detection/prevention systems) can discover. Modern SIEM solutions are expected to possess the following main features [18]:

- Collect data from multiple data sources, such as cloud-based storage, logs, Bring Your Own Device (BYOD) data, and network data.
- Based on voluminous data collected, the need for big data architecture to scale data and perform data science operations.
- Include real-time visualization tools to understand high-risk activities.
- Compliance of regulatory frameworks for risk prioritization and management.

- User and Entity Behavior Analysis (UEBA) through statistical analysis, machine learning, and behavioral modeling.
- Automatic security orchestration and response.

Security Orchestration, Automation, and Response (SOAR) is the second emerging technology that includes two key areas: orchestration and automation. Orchestration refers to the integration of several security tools and technologies to automate streamlined processes. SOAR helps SIEM technology to become big data driven by correlating the behavior of big data collected from multiple sources. It also introduces automated responses to incidents in order to reduce the disruption caused by breaches. Automation makes the security operations team more efficient and frees up their time for other important activities such as modeling threats and creating playbooks.

Another emerging technology in security operations is UEBA that monitors and analyzes user behavior in an organization. The primary functionality of UEBA is to identify insider threats. It works by using advanced machine learning techniques to profile user behavior to identify malicious activities such as compromised user accounts. UEBA has proved its worth to identify attackers' tactics, techniques, and procedures (TTPs). It forms a baseline to mark normal behavior and then uses it to distinguish anomalous user and entity behavior. UEBA differs from traditional SIEM that works on rule-based correlation for threat detection.

Figure 21.7 presents the core components of SIEM, SOAR, and UEBA and their interconnection. Finally, next-generation SIEM, SOAR, and UEBA are the three pillars that can transform the security operations and incident response capability. Adopting these three pillars in any organization, irrespective of size, will inevitably minimize the threat hunting time and reduce the risk involved in security incidents. As an innovation in the emerging technologies, these tools can be integrated so that their advantages add up to improve the security operations.

In addition to emerging technologies, there are certain anthropological studies in which students are embedded as a trained security analyst to understand the operational fieldwork of a security operations team [14]. The students are provided with a real operational world to observe the challenges faced by security operations. These

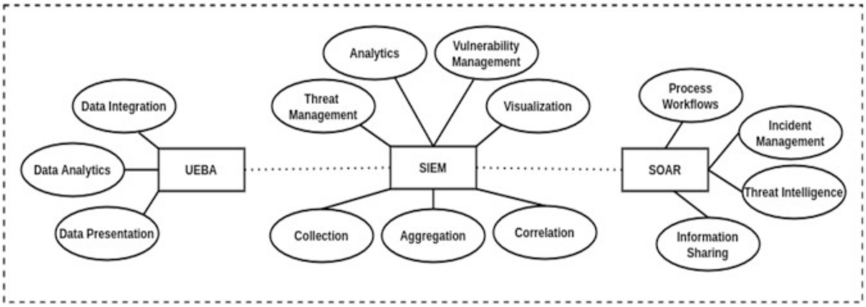


Fig. 21.7 Core components of emerging technologies

studies help improve the operational efficiency of security operations by resolving continuous human conflicts that may arise at any time [16]. The anthropological studies make use of activity theory to analyze data collected through the fieldwork and profile security analyst's behavior [19]. The tools used for conflict resolution are supposed to be dynamic in nature so that they can be adapted, especially to resolve the burnout problem [20].

21.10 Summary

Security operations play a multifunctional role in detecting modern cyberattacks by managing organizational assets, performing vulnerability analyses, modeling threats, mitigating risks, and responding to security incidents. Security operations emphasize on containing severe cyberattacks rather than identifying attackers. With improving technological solutions day by day, security operations are better able to centrally manage people and processes to continuously monitor and improve an organization's security posture. However, there are still some paramount challenges associated with security operations that need to be addressed. Although researchers have proposed anthropological studies to enhance security operations and manage people and processes in a better way, more efforts are needed to resolve the issues.

References

1. *What is WannaCry ransomware?* (2020). Kaspersky. Retrieved September 2020, from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
2. Pace, C. (2018). *The threat intelligence handbook: A practical guide for security teams to unlocking the power of intelligence*. CyberEdge Group.
3. *5G/SOC: SOC generations*. (2013). Business white paper, HP ESP Security Intelligence and Operations Consulting Services (pp. 1–12).
4. Muniz, J., McIntyre, G., & AlFardan, N. (2015). *Chapter 1: Introduction to security operations and the SOC*. Cisco Press. Retrieved September 2020, from https://www.oreilly.com/library/view/security-operations-center/9780134052083/ch01.html.
5. Onwubiko, C. (2015). Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. In *Proc. 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–10). London. https://doi.org/10.1109/CyberSA.2015.7166125
6. Zimmerman, C. (2014). *Ten strategies of a world-class cybersecurity operations center*. MITRE.
7. Chapple, M., Stewart, J. M., & Gibson, D. (2018). Certified information systems security professional. In *Official study guide* (8th ed.). Sybex.
8. Miloslavskaya, N., Tolstoy, A., & Zapechnikov, S. (2016). Taxonomy for unsecure big data processing in security operations centers. In *Proc. 2016 4th International Conference on Future Internet of Things and Cloud Workshops* (pp. 154–159). Vienna.
9. *Threat Modeling Recipe for a state-of-the-art SOC*. (2019). Hawkeye. Retrieved September 2020, from https://www.hawk-eye.io/2019/05/threat-modeling-recipe-for-a-state-of-the-art-soc/

10. Sancho, J. C., Caro, A., Ávila, M., & Bravo, A. (2020). New approach for threat classification and security risk estimations based on security event management. *Future Generation Computer Systems, 113*, 488–505.
11. Peterson, K. E. (2010). Chapter 27: Security risk management. In *The professional protection officer: Practical security strategies and emerging trends* (pp. 315–330). Elsevier.
12. *NIST SP 800-61 Rev. 2: Computer security incident handling guide*. (2012). Retrieved September 2020, from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
13. Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2019). Challenges and performance metrics for security operations center analysts: A systematic review. *Journal of Cyber Security Technology, 4*(3), 125–152. https://doi.org/10.1080/23742917.2019.1698178.
14. Sundaramurthy, S. C., Case, J., Truong, T., Zomlot, L., & Hoffmann, M. (2014). A tale of three security operation centers. In *Proceedings of the 2014 ACM Workshop on Security Information Workers* (pp. 43–50).
15. Shah, A., Ganesan, R., & Jajodia, S. (2019). A methodology for ensuring fair allocation of CSOC effort for alert investigation. *International Journal of Information Security, 18*, 199–218.
16. Sundaramurthy, S. C. (2017). *An anthropological study of security operations centers to improve operational efficiency* (pp. 1–108). Doctorate dissertation, University of South Florida. Retrieved December 2020, from https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=8155&context=etd
17. Hull, J. L. (2017). *Analyst burnout in the cyber security operation center—CSOC: A phenomenological study*. Doctorate dissertation, Colorado Springs (CO): Colorado Technical University.
18. Cassetto, O. (2018). *10 Must-have features to be a modern SIEM*. Retrieved September 2020, from https://www.exabeam.com/siem/next-gen-siem/
19. Sundaramurthy, S. C., McHugh, J., Ou, X., Wesch, M., Bardas, A. G., & Rajagopalan, S. R. (2016). Turning contradictions into innovations or: How we learned to stop whining and improve security operations. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (pp. 237–251).
20. Sundaramurthy, S. C., Wesch, M., Ou, X., McHugh, J., Rajagopalan, S. R., & Bardas, A. (2017). Humans are dynamic. Our tools should be too. Innovations from the Anthropological Study of Security Operations Centers. *IEEE Internet Computing*, 1. Retrieved December 2020, from https://doi.org/10.1109/MIC.2017.265103212