Chapter 1

Introduction to Security Operations and the SOC

"It's better to light a candle than curse the darkness."

This book focuses on the best practices to develop and operate a security operations center (SOC). The journey begins with a review of important concepts relevant to information security and security operations. This chapter opens with a discussion about the continuously evolving security landscape and how new cybersecurity challenges impact how we perceive security operations. The discussion then turns to information assurance and its link to both risk management and security operations. This chapter does not cover information assurance and risk management in depth, but instead provides you with sufficient background information on these topics while relating them to security operations. The chapter then covers incident response and how it is used by security operations. The chapter concludes by introducing a number of concepts associated with the core topics of the book: planning, designing, building, and operating a SOC.

Cybersecurity Challenges

Security attacks are becoming increasingly complex and exhibiting increasingly sophisticated capabilities. So, addressing the complexity and sophistication of such attacks must include not only investing in preventive measures but also the development of intelligent and integrated monitoring capabilities incorporated into an incident response program.

Arguably, getting compromised at some point is inevitable. As the previous CEO of Cisco Systems, John Chambers, said, "There are two types of companies: those who have been hacked and those who don't yet know they have been hacked." So, be warned: A security breach is not an *if* but a *when*. The good news is that a breach does not necessarily mean that the business will immediately experience negative impact, because attackers usually need time to accomplish their objectives beyond gaining unauthorized access to the network. Discovering and preventing this type of behavior is just one of the many reasons organizations develop a SOC.

One exercise to help people understand the inevitability of cyberthreats is to ask this question: If you knew you were going to be breached, would you perform security differently within your organization? This leads to a series of questions that you should ask leadership within your organization about how your business deals with a security compromise. Somebody needs to be responsible for answering these questions; for most organizations, those people run the SOC or have security operations responsibilities.

If you need to justify a SOC budget, here are some questions focused on dealing with a security compromise:

- How can you detect a compromise?
- How severe is the compromise?
- What is the impact of the compromise to your business?
- Who is responsible for detecting and reacting to a compromise?
- Who should be informed or involved and when do you deal with the compromise once detected?
- How and when should you communicate a compromise internally or externally, and is that needed in the first place?

The OODA Loop¹ is one methodology that addresses some of these questions. The concept was first developed by military strategist and USAF Colonel John Boyd.² Colonel Boyd created a four-step approach designed to determine the appropriate response to a problem. An OODA Loop, as shown in Figure 1-1, consists of the following steps: observe, orient, decide, and act. In the context of cybersecurity, the four steps are as follows:

- **Observe:** Monitor, collect, and store data from various points in your network as the first step in the OODA Loop.
- Orient: Analyze collected data in search of suspicious activities. This usually involves the use of tools to process and analyze incoming and stored data.
- Decide: Determine an action course based on the results of the analysis phase and the experience you have gained from previous loop iterations.
- Act: Execute the action course you determined in the preceding step.

Cybersecurity Challenges 3



Figure 1-1 The OODA Loop

The OODA Loop assumes that continuous improvement is an integrated part of the process, allowing you to learn from your previous experiences, feeding lessons learned into the loop activities to achieve better performance every time you complete the four steps. Continuous monitoring and enforcement concepts are an ongoing theme throughout this book.

The OODA Loop may have been designed to deal with military attacks, but the concepts apply to defending any form of attack, including cyberthreats. For our next model, let's switch to the attacker's viewpoint by reviewing the *cyber kill chain*. The cyber kill chain,³ developed by Lockheed Martin's Computer Incident Response Team and shown in Figure 1-2, describes the progression an attacker follows when planning and executing an attack against a target. This model helps security professionals identify security controls and actions that can be implemented or improved to detect, deny, and contain an attack scenario.



Figure 1-2 The Cyber Kill Chain

The various phases of the cyber kill chain are as follows:

- Phase 1, Reconnaissance: Research, identification, and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for e-mail addresses, social relationships, or information on specific technologies.
- Phase 2, Weaponization: Coupling a remote-access Trojan with an exploit into a deliverable payload, typically by means of an automated tool also known as a weaponizer.

- 4 Chapter 1: Introduction to Security Operations and the SOC
 - Phase 3, Delivery: Transmission of the weapon to the targeted environment.
 - Phase 4, Exploitation: Triggers the intruder's code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.
 - Phase 5, Installation: Installation of a remote-access Trojan or back door on the victim system enables the adversary to maintain persistence inside the environment.
 - Phase 6, Command and Control: Beacon outbound to an Internet controller server to establish a command and control channel.
 - Phase 7, Actions and Objectives: Intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration that involves collecting, encrypting, and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

These models make up a high-level way to look at cybersecurity attack and defense concepts. According to the cyber kill chain, attackers perform reconnaissance to identify the easiest and most effective way to breach a network. Defense teams using the OODA Loop may catch this behavior during the observing or orientation stage and decide to react by locking down security or raising awareness of a possible threat from an identified source. An attacker may move to Phase 4 of the cyber kill chain by weaponizing and delivering an exploit against a target. The OODA Loop may once again identify the attack during the observe or orientation stage and react through containing the threat and patching the weakness to avoid future attacks. So essentially, the OODA Loop is a defense strategy against every phase of the cyber kill chain.

Developing security operations and security incident response capabilities is critical to breaking or reducing the impact of an attacker executing the cyber kill chain against your organization. The OODA Loop is just one conceptual model that you can use to break the chain or contain the chain of events during an incident. The important question to ask is this: How does your organization apply the OODA Loop or similar concepts against different stages of the cyber kill chain when an attack against your organization occurs? Most SOCs execute a variation of the OODA Loop by using controls associated with these three elements: people, processes, and technology.

Threat Landscape

The Verizon 2015 Data Breach Investigation Report (DBIR)⁴ showed that 60 percent of businesses being breached happened within minutes or less. The report also showed that half of these incidents took anywhere from months to even years before being

uncovered. So in summary, breaches tend to happen very quickly and on average take a long time to be detected by the targeted organization. These numbers demonstrate the importance of having an effective security operations program in which a mature SOC plays a significant role. Figure 1-3, taken from the DBIR, compares the time spans of when organizations are compromised versus when they are able to discover the breach.



Figure 1-3 2015 DBIR Comparing Breach and Discovery Time

As the security landscape continues to evolve, new and automated offensive tools become readily available for a larger audience. Well-organized libraries of offensive tools are now packaged on free-to-download-and-use Linux distributions such as Backtrack⁵ and Kali,⁶ making it possible for almost anyone to test and develop tools and exploits. Attackers known as Script Kiddies might not understand the details of how the attack works, but packaged offensive tools make launching sophisticated attacks as simple as point-and-click execution. An analogy to this scenario is that the average person cannot build a telephone but can make a phone call as long as the system is prebuilt and ready to use. Many attack tools are developed in a point-and-click fashion, such as shown in Figure 1-4, which showcases a weaponized denial-of-service (DoS) attack application known as Low Orbit Ion Cannon (LOIC).





Why are security products unable to stop these threats? Aren't governments and big businesses investing significant amounts of money into developing countermeasures to cyberattacks? The answer is yes; however, there is a reason why defense technologies need to continue to evolve. Just like solution providers, attackers have labs for researching products. If a "silver bullet" or single solution hits the market and is effective at preventing cyberattacks, that product will become popular and purchased by many organizations, along with their adversaries. Hackers will test various exploits against the new product until one succeeds, and will then either sell the exploit on underground markets, weaponize it for less-skilled attackers, or use it for some other malicious purpose.

Security researchers saw this pattern when the sandbox concept was introduced to detect malicious software. Administrators put a sandbox security product hosting various vulnerable applications at the edge of their inside network with the intention of making it the first target malware would strike during a breach. Malware would launch inside that monitored sandbox, giving away its identity, and thus the other security products could be made aware of the attack. Attackers learned about this technology and developed techniques such as targeting specific systems versus attacking the most vulnerable system, delaying the attack long enough to bypass the sandbox and so on. Figure 1-5 shows an article⁷ from Networkworld.com explaining how hackers are now bypassing sandbox technology. This is why the attack and defense innovations continue to be a cat-and-mouse game, meaning both sides will develop a technique that eventually the other side will adapt to.



Figure 1-5 Networkworld.com Article on Bypassing Sandbox Technology

Where are these exploits being sold once developed? Many new exploits can be found on underground and notably growing commercial zero-day vulnerability markets operated by private brokers. Examples of boutique exploit vendors that sell *known-unknown* zero-day flaws include the French firm VUPEN Security,⁸ Netragard,⁹ ReVuln,¹⁰ and Endgame Systems.¹¹ NSS Labs¹² estimates that on a yearly basis more than 100 *knownunknown* zero-day vulnerabilities are available for sale. To find examples of underground markets selling zero-day exploits, download the Tor browser from https:// www.torproject.org/download/download, access the Darknet, and go to the Hidden Wiki at http://wikitjerrta4qgz4.onion/. Figure 1-6 shows a list of websites marketing anything from contract killers to the infamous Silk Road marketplace.



Figure 1-6 Darknet Marketing Sources

Warning Access the Darknet at your own risk! Because of the anonymous nature of hosting and accessing websites via Tor, many onion network resources contain malicious techniques not found on the Internet.

Business Challenges

In addition to the technical security threat landscape, legal and business-imposed decisions impact the way organizations operate information security. Examples of such decisions include moving services and information to the cloud; meeting compliancy requirements; the proliferation of bring your own device (BYOD); and the rise of the Internet of Everything (IoE), which brings people, processes, things, and data together by combining machine-to-machine (M2M), person-to-machine (P2M), and person-toperson (P2P) connections. For example, the IoE networked connection of people, processes, data, and things, shown in Figure 1-7, introduces challenges related to collecting, processing, storing, and analyzing large volumes of data generated at high velocity and with a variety of formats (that is, big data analytics, as discussed later in this chapter and in Chapter 2, "Overview of SOC Technologies."



Figure 1-7 Networked Connection of People, Process, Data, Things (Source: Cisco Internet of Everything Report¹³)

The Cloud

Cloud services are here to stay and evolve. Over the past decade, there has been a steady increase in the adoption of cloud services by small, medium, and large organizations from various industries. This trend maps to the economic gains expected from consuming cloud-based services.

According to various studies related to cloud adoption, security is one of the top concerns for chief information officers (CIO) for migrating their services to the cloud. For example, a study conducted by ChangeWave Research in April 2014¹⁴ identified security concerns as being the leading reason why both large companies (more than 1000 employees) and small- to medium-sized companies (fewer than 1000 employees) are not moving to the cloud. Another study conducted by the firm McKinsey in conjunction with the World Economic Forum in May 2014¹⁵ revealed that "some 70 percent of the respondents said that security concerns had delayed the adoption of public cloud computing by a year or more, and 40 percent said such concerns delayed enterprise-mobility capabilities by a year or more."

The exact security concerns vary from the ability of cloud service providers guaranteeing basic access control and confidentiality all the way to achieving audit and compliance requirements. Adoption rates also vary between the use of public and private cloud because private cloud tends to have more security based on being dedicated to a single client or company. What this book addresses is how to operate your SOC in an environment where cloud services are being consumed for business purposes regardless of the cloud model. You learn more about cloud services later in this book.

Compliance

Being compliant with mandatory or discretionary information security or privacy standards requires not only an investment in technology but also, in almost all cases, a fair amount of culture change. Required changes can also include a reform to the model by which information is managed and how security operations are conducted.

Typically, standards mandate reactive and preventive security measures to protect information. This means that all regulatory and discretionary security standards explicitly highlight the need for information security operations. In some cases, this is referred to as the need for continuous monitoring of the information security posture.

Examples of security standards many organizations must comply with include the following:

- The Payment Card Industry Data Security Standard (PCI DSS),¹⁶ a standard set by the PCI Security Standards Council (PCI SSC) that applies to all entities that store, process, and/or transmit cardholder data, mandates a number of technical and operational security requirements. The standard mandates, under the "regularly monitor and test networks" control objective mapped to PCI DSS requirements 10 and 11, that organizations must regularly monitor and test networks to find and fix vulnerabilities.
- ISO/IEC 27001:2013, a standard that organizations can adopt to manage information security as a program, requires organizations to operate information security technical and nontechnical controls under the umbrella of an information security management system (ISMS) in which a plan, do, check, and act (PDCA) lifecycle is operated and maintained. Annex A.10.10 of the standard, titled "Monitoring," lists a number of important operation controls in the areas of audit logging, monitoring system use, and so on. The check phase of the PDCA lifecycle requires you to assess and, where applicable, measure process performance against ISMS policies, objectives and practical experience, and report the results to management for review.

PCI DSS and ISO/IEC 27001:2013, along with other information security and privacy standards, demand that security controls be properly monitored and that information security events and incidents be appropriately handled. Failure to comply with standards may lead to large fines or jail time for all persons held accountable for information assurance.

Privacy and Data Protection

In addition to business-centric standards, organizations must adhere to countryspecific laws and regulations related to privacy and data protection. Examples of country-specific laws and regulations include the following:

United States: US-EU Safe Harbor on Data Protection directive went into effect in October 1998 and prohibits the transfer of personal data to non-European Union countries that do not meet the EU-defined *adequacy* standard for privacy protection.

- 10 Chapter 1: Introduction to Security Operations and the SOC
 - Germany: The Federal Data Protection Act¹⁷ (Bundesdatenschutzgesetz in German, BDSG) covers a range of data protection issues. For example, according to the act, organizations must have policies, procedures, and controls in place to protect all data types and categories that are under the BDSG umbrella. In addition, each German state has a data protection law of its own.
 - Japan: The Act on the Protection of Personal Information¹⁸ (APPI) prescribes the duties to be observed by entities handling personal information with the objective of protecting the rights and interests of individuals.
 - United Kingdom: The Data Protection Act 1998¹⁹ governs the protection of personal data in the UK.

Developing security operations capabilities is critical to supporting an organization's compliance state with such regulations; these same capabilities also allow organizations to react appropriately to security incidents that might result in an infringement of the law. Being compliant with these and other mandatory laws and regulations comes in direct support to ensuring that information is protected and monitored against potential attacks that would impact its availability, integrity, authentication, and confidentiality. In many cases, *reasonable effort* (as legally understood) must be used to protect sensitive data; otherwise, persons responsible for information assurance face potential fines or even jail time.

Let's now review the concepts underlying information assurance.

Introduction to Information Assurance

According to the U.S. Department of Defense (DoD) Directive 8500.01E,²⁰ information assurance (IA) refers to "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The National Institute of Standards and Technology (NIST) SP 800-59²¹ and other NIST documents use the same definition for IA.

Taking a United Kingdom (UK) perspective to IA, the UK Home Office defines IA²² as "the practice of managing information-related risks around the confidentiality, integrity and availability of information, particularly sensitive information. It covers information whilst in storage, processing, use or transit; and the risks created by both malicious and non-malicious actions." The UK Cabinet Office has a slightly different definition for IA, stating that "the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users" and that "information systems include any means of storing, processing or disseminating information including IT systems, media and paper-based systems." Most requirements for IA will contain similar characteristics in the language used for protecting

various aspects of data handled by your organization. It is extremely important to know exactly how IA is defined in your country and all associated requirements your organization must meet to avoid legal ramifications.

A question that is often asked is this: What is the difference between IA and information security? Taking NIST as our reference, NIST 800-53²³ defines information security as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." You should notice that a close relationship exists between IA and information security. Considering the NIST definitions of IA and information security, you can think of IA as a superset that covers information security. In general, IA tries to address the different risks associated with information systems or media, encompassing technical, procedural, and human factor aspects involved in delivering physical and digital protection for information systems or media.

Before trying to address IA or information security requirements, it is imperative to understand the security risks associated with your environment. This is where the risk management discipline becomes relevant. It is worth noting that establishing a SOC supports the basic requirement of managing the security risk of an organization. So, the next section introduces risk management concepts.

Introduction to Risk Management

Let's start by defining what *risk* is. A common definition of risk is the *probability* of a *threat* executing on *vulnerability* and the *impact* resulting from successful exploitation. This definition of risk is similar to the one listed in the NIST guide for conducting risk assessments.²⁴ Dealing with risk cannot be achieved without understanding the organization-specific threat landscape and vulnerability status. This can be achieved using various types of security services such as a risk assessment.

A risk assessment is the process used to assign some value to risk associated with assets. The output of a risk assessment can then be used to make better-informed decisions on how to deal with risk. Decisions include one or more of the following: *mitigate*, *trans-fer*, *accept*, or *avoid*. Risk management involves combining the output of risk assessment with the decision on how to address risk.

Examples of frameworks that try to formalize the topic of risk management include ISO/IEC 27005:2010, ISO/IEC 31000:2009, NIST SP 800-39, OWASP Risk Rating Methodology, and the DoD Risk Management Framework (RMF). These frameworks use similar processes for managing risks, as shown in Figure 1-8, taken from the ISO/IEC 31000:2009 standard. Taking the DoD RMF as an example, the framework assumes a six-step process. The process starts with risk categorization and ends with effectiveness measurement through security controls monitoring.



Figure 1-8 Risk Management Framework (As per ISO/IEC 31000:2009)

The task of assessing and managing risk should not be regarded as only a point-in-time exercise, but rather a continuous process that accepts input from various real-time and offline sources. Information generated by security operations is a vital source to the riskassessment process. Consider the example in which security operations identified that a malformed IP packet destined for a critical system has caused this system to crash. The sequence of events should be investigated, and the risk associated with this system, and possibly other similar systems, should be reviewed. Changes made to the environment will have an effect on risk associated with individual assets and the overall security posture of the organization. For example, how should the organization react to the resignation of a system administrator who has responsibilities over privileged access systems? The proactive actions taken by the organization should be based on predefined processes that have been created to address new risk values introduced by this event. Another example is the public announcement of a new security vulnerability affecting a number of internal assets that are not publicly accessible. What should the new risk values associated with these internal assets be as a result of this vulnerability discovery? Let's consider the latter scenario to assess the risk associated with the internal assets based on the new security vulnerability announcement, using the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) risk-assessment methodology that was first developed by the Software Engineering Institute (SEI)²⁵ at Carnegie Mellon University. Table 1-1 demonstrates going through an OCTAVE risk-assessment exercise.

Risk Component	Description		
Vulnerability	A new vulnerability affecting internal assets has been announced. The analysis shows that a number of critical internal assets are indeed vulnerable.		
Threat description	Vulnerable assets are classified as critical. The attack can be easily executed on an asset if the attacker can access the service over the network.		
Existing controls	The internal assets are not connected to the Internet. The assets are protected by a firewall that allows internal users only. The assets are protected by an intrusion prevention system (IPS); however, the IPS vendor has not released signatures that can protect the assets from being exploited through the newly announced vul- nerability.		
Probability	Unlikely. The assets can be only exploited by internal users who have access to the assets over the internal network.		
Impact	Critical. Exploiting the vulnerability results in the attacker gaining full admin- istrative access to the system.		

Table 1-1 Example of a Risk-Assessment Exercise

Next, we will map the information in Table 1-1 to a risk heat map that we can use to identify the priority of this event based on the *probability* of it occurring and *impact* to the business if the event occurs. The risk heat map is a simple color-based representation using a two-dimensional matrix calculating probability and impact levels to identify the organization's level of concern for the event. Figure 1-9 depicts a four-level severity risk heat map using low, medium, high, and extreme as the depth levels of concern.

In the next risk heat map example, we assessed the probability to be unlikely and the impact to be critical, resulting in a moderate priority course of action. It is important to note that the impact, probability, and the priority values presented in Figure 1-9 should be clearly defined and understood when designing your security assessment methodology. For example, a moderate action plan could be the implementation of the required system patches following the standard process of evaluating the patches in the test environment, following the standard change management process, and then applying the patches in production during a standard change window. You learn how to create different forms of heat maps and calculating different risk values in Chapter 7, "Vulnerability Management."

		Impact			
		Negligible	Marginal	Critical	Catastrophic
	Certain	HIGH	HIGH	EXTREME	EXTREME
ility	Likely	MEDIUM	HIGH	HIGH	EXTREME
Probab	Possible	LOW	MEDIUM	HIGH	EXTREME
	Unlikely	LOW	LOW	MEDIUM	EXTREME
	Rare	LOW	LOW	MEDIUM	HIGH

Figure 1-9 Simple Risk Heat Map

Information Security Incident Response

Detecting and responding to information security incidents is at the core of security operations. The team assigned to security operations is expected to monitor the organization's assets within scope and react to security events and incidents, including the detection and investigation of what would be considered indicators of compromise (IOC). IOCs are technical and nontechnical security compromise signals that could be detected with technology, processes, and people. For example, detecting a user accessing files from a USB memory device on an enterprise desktop machine can indicate that a policy related to restricting the use of USB memory devices has been violated and that a security control has been circumvented. Another example is detecting the IP address of an Internet botnet command-and-control server inside your network probably indicates that one or more of your systems have been compromised.

Responding to incidents starts by first detecting that an incident has actually occurred and is within the scope assigned to the security operations team. An example is capturing some IOCs with a monitoring system and either investigating the events or handing off the forensic tasks to another party. This process typically involves different internal and potentially external entities depending on factors such as the tools used, type of event, skills of parties involved, and location triggering the alarms. Preparing a SOC to manage incidents extends to cover people, processes, and of course, technology. For example, a SOC is usually expected to educate users about how they must report security incidents and keep informed of the channels available for users to report what is perceived as a security incident. The exact sequence of steps to follow and the parties to involve depend on the nature of the incident. A typical incident-handling process follows the list of steps presented in the incident response (IR) timeline in Figure 1-10. Let's look at *detection*, which is the second stop on the incident response timeline.



Figure 1-10 Incident Response Timeline

Incident Detection

Detection refers to the phase in which an incident is observed and reported by people or technology, and the process that handles the reporting aspects. A sample process for handling incoming incident reports is shown in Figure 1-11. For the process to be effective, the following must be documented and formalized:

- Identify the sources, such as people and technology, that are responsible for detecting and reporting computer security incidents.
- Identify the channels through which computer security incidents should be reported.
- Identify the steps that should be taken to accept and process computer security incident reports.
- Identify the requirements on people and technology for the process to work.

The steps described in the sections that follow outline the actions you expect to take after an incident has been reported, regardless of the channel through which the incident has been reported. Let's look at what follows detection, starting with triage.



Figure 1-11 Incident Detection Phase

Incident Triage

Incident triage represents the initial actions taken on a detected event that is used to determine the remaining steps according to the incident response plan. The triage phase consists of three subphases: *verification*, *initial classification*, and *assignment*. An example of applying these phases is receiving an alert about an unauthorized system accessing a sensitive part of the network. The administrator would verify whether the alarm is something that should be investigated, classify the risk level for the event, and assign responsibility for handling the incident based on the level of associated risk.

The triage phase is concerned with answering questions such as the following:

- Is the incident within the scope of the program?
- Is it a new incident, or is it related to a previous reported one?
- What category should the incident be assigned to?
- What severity level should be assigned to the incident?
- Who should be assigned to analyze and investigate the incident (that is, the incident handler)?
- Is there a timeframe associated with the incident?

The triage process needs to be developed to prioritize incidents and move them along the incident response timeline to be analyzed and eventually conclude with some form of resolution. This usually involves placing the incident in a *category* for organization and assignment purposes along with applying a *severity level* so that incidents can be prioritized. Let's look at categorizing incidents and then at applying severity levels.

Incident Categories

All computer security incidents should be assigned a category. The category value identifies the type of the incident and its potential type of impact. Assigning a category value helps the SOC allocate the appropriate resources to analyze and investigate a computer security incident. Table 1-2 shows a sample list of categories that you could use for categorizing incidents.

Note that some incidents might have more than one category and that the category can change as the incident progresses or as the investigation of the incident unfolds new findings.

Category Number	Name	Description
0	Exercise	This is used when conducting an approved exercise such as an authorized penetration test.
1	Unauthorized Access	This represents when an individual gains logical or physical access without permission to a client network, system, application, data, or other resource.
2	Denial of Service This is used when an attack successfully prevents impairs the normal authorized functionality of n works, systems, or applications by exhausting re	
3	Malicious Code	This identifies when there is a successful installation of malicious software, such as a virus, worm, Trojan horse, or other code-based malicious entity, that infects an OS or application.
4	Scans/Probes/ Attempted Access	This includes any activity that seeks to access or iden- tify a client computer, open ports, protocols, service, or any combination for a future attack.
5	Investigation	This includes unconfirmed incidents that are potentially malicious or anomalous activity deemed by the report- ing entity to warrant further review.

Table 1-2 Computer Security Incident Categories

Incident Severity

Severity levels are based on the expected or observed impact of an incident. This is used for the prioritization of the incident, taking into account the amount of resources that should be assigned, and determines the escalation process to follow. Note that the severity level of an incident may change as the investigation unfolds. Chapter 7 covers calculating severity levels.

Table 1-3 shows a list of sample severity values. Levels can be more or less granular depending on your operational requirements.

Level	Description
High Incidents that have severe impact on operations	
Medium	Incidents that have a significant impact, or the potential to have a severe impact, on operations
Low	Incidents that have a minimal impact with the potential for significant or severe impact on operations

 Table 1-3
 Computer Security Incident Severity Levels

Once you categorize an incident and apply a severity level, you can decide how to resolve the incident. Let's review this stage of the incident response timeline.

Incident Resolution

The lifecycle of an incident should eventually lead to some form of resolution. This may include data analysis, resolution research, a proposed or performed action, and recovery. The objective of this phase is to discover the root cause of the incident, while working on containing the incident at the earliest stage possible.

During the analysis phase, the SOC team and the other teams should collaborate to achieve the quickest and best form of resolution. Access to some systems might be required to conduct necessary investigation activities. Figure 1-12 shows a sample process for handling the analysis tasks.



Figure 1-12 Incident Analysis Phase Process

The analysis and investigation phase involves the activities undertaken by SOC and by other teams for the purpose of

- Identifying compromised systems and accounts
- Understanding the impact of the computer security incident
- Identifying unauthorized access attempts to confidential data
- Understanding the chain of events that have led to the computer security incident

The containment phase involves the actions performed to quickly stop a computer security incident from escalating or spreading to other systems (that is, minimizing the potential damage caused by a computer security incident). Note that depending on the computer security incident and its impact, the containment phase can happen before, during, or after the analysis phase.

The process shown in Figure 1-13 is a sample containment process. You may, however, proceed with containment before or during the incident analysis.



Figure 1-13 Incident Containment Phase Process

The exact steps to follow to contain a computer security incident vary depending on the nature of the incident and business criticality of the asset. Examples of containment actions include the following:

- Disconnecting a system from the network
- Moving an infected system to the quarantine network
- Stopping a service or a process
- Disabling an account
- Adding a firewall rule
- Adding an intrusion prevention system (IPS) signature/rule that would detect and block the attack's specific vector

Incident Closure

Closing a computer security incident refers to the eradication phase in which vulnerabilities that lead to the incident have been closed and all the incident traces have been cleansed. The closure process also includes testing systems to ensure that the eradication steps and controls were effective and that the vectors used by the attack do not exist anymore or are ineffective. Predefined actions to consider include applying any final information about the event, its final classification, any external notifications, and archiving information about the incident.

If the incident involved violating regulatory requirements or resulted in the infringement of law, the SOC might be obliged to notify external entities. The SOC should have processes in place so that this communication is timely, accurate, and contains all information required for such notification.

The exact steps to follow when eradicating a computer security incident will vary depending on the nature of the incident. Examples of eradication actions include the following:

- System reconfiguration
- System re-imaging or rebuild
- Patching of systems
- Software update
- Deletion of accounts
- Deletion of files

In many cases, the closure and containment phases are closely coupled.

Post-Incident

This is the "lessons-learned" phase in which you seek to improve the IR processes and reflect on other people, processes, and technology controls. Post-incident activities will vary depending on the severity of the computer security incident. Valuable knowledge gained from computer security incidents can be useful to prevent/mitigate future incidents in the form of proactive services such as enhancing security features of functions within defenses.

In general, the process of post-analysis starts after incident closure and mainly includes documenting proposals of improvements in linkage to the different areas of the SOC: people, processes, and technology. In addition, recommendations for improving the SOC capabilities might result from a scheduled or an ad hoc risk-assessment exercise.

In summary, following an incident response timeline, the SOC team would handle a number of critical tasks, from incident detection to closure. Each stage of an incident can have its own processes and involve other groups within the organization. It is important that the plan, design, and build phases for incident response be defined, documented, and sponsored by the right authorities within the organization. Incident response is all about timing, and the worst time to figure out responsibilities and incident-handling process is during an active attack. Now that we have covered a general overview of the responsibilities of the SOC, let's take a look at the history of SOC generations to get a better idea of how SOCs have matured over time.

SOC Generations

Our understanding of SOC components and expected services has changed over time. This is a reflection to the adjustment in our perception of the criticality of information assurance and security operations. This transformation comes in response to the ever-changing security threat landscape, in addition to our increasingly adopting formal information security standards, requiring the establishment and management of a formal security operations model and review processes.

The SOC's journey for the past 15 years can be broken to four *incremental* generations, shown in Figure 1-14. Ideally, an organization that uses technologies from the fourth generation, such as big data security analytics, should have adopted most of the SOC services from the previous generations. This might not always be the case in practice, though.



Figure 1-14 The SOC: Four Generations

The four generations reflect SOC capabilities in response to increasingly sophisticated attacks. Refer to the description of the generations to identify which SOC generation service your organization might be offering. Let's look at the details of the services offered in each SOC generation.

First-Generation SOC

In this generation, the wider IT operations team delivered what would be considered as SOC functions and services. This team was not necessarily skilled or trained to handle information security events and incidents. Security operations were not delivered by the establishment of a formal SOC, but in many cases by an IT operations individual or a team who focused on a blend of tasks. This could be responsibility for device and network health monitoring, managing antivirus security across the organization, and log collection. Log collection for the first-generation SOC was limited in the number of sources and types of devices capable of producing logs, such as firewalls. In many cases, storing logging messages was done locally. In other cases, a central logging facility was provisioned to receive log information, mainly in the form of unencrypted syslog or Simple Management Network Protocol (SNMP) messages.

In this generation, logging messages were rarely proactively analyzed, and were instead referred to if an incident was reported or some sort of troubleshooting was required. In addition, the concept of information security incident response was not formally established or appreciated. The process of identifying, communicating, and reacting to potential information security incidents was generally slow (and in many cases, ad hoc).

Let's look at an example of how a first-generation SOC would operate. Consider, for instance, that a number of systems have reported a substantial and relatively abnormal number of failed login attempts for the Microsoft Windows Active Directory domain administrator account within what is considered to be a short period of time. No evidence indicates suspicious activity or that a system compromise has been reported.

In the first generation of SOC, logging messages would most likely be locally saved on each system rather than stored on a centralized collection system such as a security information and event management (SIEM). The unsuccessful login attempt events would be saved to the local Windows security log store and buried under a large number of events generated by other various activities. Unless the Microsoft Active Directory system administrator manually accessed and analyzed the logs, the events in this example would have likely gone unnoticed, overlooking what could potentially be an account compromise and leading to what could be considered a major security incident.

Second-Generation SOC

This is the generation in which SIEM tools started to emerge. Early generations of SIEM providers such as netForensics, Network Intelligence (later acquired by EMC), and Cisco Security Monitoring, Analysis, and Response System (MARS) promised to detect network threats, releasing administrators from the complex and in many cases impossible task of manually analyzing huge amounts of log information. The early providers

of such tools focused on security threat management (STM), also referred to as security event management (SEM), which delivers real-time log analysis for the purpose of threat detection. These tools accept log information generated by various sources in different formats, speeding up the process of detecting potential security incidents. The basic idea of SEM is to first aggregate log information in the form of events from various sources such as operating systems, security devices, and applications. Events are then correlated so that possible relationships between them are identified, indicating the potential occurrence of incidents. Incidents are then reported in the form of a dashboard alert to the operator to investigate further.

This SEM function was eventually consolidated with the security information management (SIM) function to produce what is known today as SIEM. SIM tools focused on searching through large amounts of acquired log data. This historical data could be then analyzed for different purposes, such as performing digital investigations or meeting a number of compliance requirements related to log retention and compliancy report generation.

Another important operational aspect introduced in the second-generation SOC was security incidents case management. SIEM operators can create and assign cases for security incidents reported by the tools. In some cases, this is integrated with the organization's service ticketing systems.

Taking the same multiple failed login attempts example used in the discussion about first-generation SOC, the Microsoft Windows systems would most likely be configured to forward logged events to a SIEM tool. The SIEM tool should be capable of receiving, parsing, normalizing, and correlating the different events and eventually alerting a security analyst that there have been multiple login failures for the account "administrator" on multiple systems. This behavior could indicate a possible brute-force attack, assuming that the SIEM tool is configured with correlation rules that can detect and assign a relevant and meaningful alert to this suspicious activity. You learn how correlation rules are created and tuned in Chapter 2.

Third-Generation SOC

As SIEM tools further established their importance, other security services started to find their way to the SOC. In this generation, the SOC team would handle tasks related to vulnerability management, in addition to being heavily involved in formalizing and executing tasks related to incident response.

Vulnerability management refers to the practice in which vulnerabilities are discovered and confirmed, their impact is evaluated, corrective measures are identified and executed, and their status is tracked and reported until closure. This definition is similar to the one used in the NIST SP 800-40 standard.²⁶

It is critical that the impact evaluation phase for discovered vulnerabilities be associated with the organization's risk-assessment practice. This means referring to the whole process of managing vulnerabilities instead of running vulnerability scanning tools against IT assets only. Vulnerability scanning is an activity that is part of vulnerability management and is usually executed during the vulnerability discovery, confirmation, and tracking phases. Some commercial products, such as Qualys²⁷, nCircle²⁸ (acquired in 2013 by Tripwire), and Rapid7 Nexpose²⁹ have evolved from being predominately vulnerability scanners to automating the vulnerability management process. The SOC team would either operate the vulnerability management process, working with other units, or would be assigned some of its tasks. You learn more about vulnerability management best practices in Chapter 7.

Fourth-Generation SOC

This generation of SOC introduces a number of advanced security services that attempt to tackle new security threats. The first new concept is expanding on the limited event correlation seen in previous generations of SIEM to big data security. Big data security analytics can be defined as "the ability to analyze large amount of data over long periods of time to discover threats and then present and visualize the results." Big data platforms are now being deployed to consume data from any source at high speed and with high volume, while being able to perform real-time or offline sophisticated security analytics. An example of using big data is ingesting large threat intelligence feeds about attacks seen all over the world rather than limiting event correlation to internal threats. Attack data could be website reputation data, malicious sources, volumetric trends for identifying distributed denial-of-service (DDoS) attacks, and so on. You learn more about big data security in Chapter 2.

Another new fourth-generation SOC concept is data enrichment through the use of sources such as geo data, Domain Name System (DNS) data, network access control integration, and IP and domain reputation service. Network telemetry information is also being used for sophisticated network and security monitoring, essentially turning common network equipment into security sensor ports.

New technologies are being used by the SOC for forensics and identifying network breaches also known as breach-detection solutions. Cross-product integration is being leveraged to automate remediation, such as an intrusion detection product identifying a threat and leveraging a network access control technology to automatically perform remediation.

In summary, fourth-generation SOC is expanding threat data sources, layering different security capabilities to battle more advanced threats, and automating security to improve reaction time to incidents. This generation of SOC also includes policies to evaluate their capabilities as a continuous process for optimization and enhancement purposes. To better understand the latest SOC generation, let's review the characteristics of an effective SOC.

Characteristics of an Effective SOC

To build and operate an effective SOC, organizations must account for a number of critical success factors. Some practices found in almost all organizations running a successful SOC are as follows:

Executive sponsorship: The SOC program must have executive sponsorship. This sponsorship should be in the form of the sponsor signing the SOC mission, and the SOC team providing periodic updates to the sponsor, who is expected to be

involved in major decisions taken by or for the SOC (for example, the acquisition of new tools or the expansion of the SOC team). The CIO and in some cases the CEO make ideal internal executive sponsors for the SOC program. There are also cases in which the SOC is established as part of the organization's risk management program. For these environments, the head of the security risk steering committee can oversee the SOC sponsorship.

- Governance: Establishing a governance structure is critical to the success of any security program. Metrics must be established to measure the effectiveness of the SOC capabilities. These metrics should provide sufficient and relevant visibility to the organization's management team on the performance of the SOC and should identify areas where improvements and investments are needed.
- Operate SOC as a program: Organizations should operate the SOC as a program rather than a single project. Doing so relies on the criticality and the amount of resources required to design, build, and operate the various services offered by the SOC. Having a clear SOC service strategy with clear goals and priorities would shape the size of the SOC program, timeline, and the amount of resources required to deliver the program objectives.
- Collaboration: The different units in an organization must collaborate during the plan, design, build, and operate phases of the SOC. The exact collaboration and interdepartmental relationships must be formally defined during the SOC design and build phases.
- Access to data and systems: Access to the required data and systems must be provided to the SOC team so that they can perform their tasks: before, during, and after a security incident. The exact definition of *access* must be established during the SOC design and build phases. This can be, for example, access to log data or extended to gaining access to system configuration. At a minimum, SOC tools should receive logging messages from various systems and applications.
- Applicable processes and procedures: The SOC team must be equipped with established processes and knowledge, augmented with the appropriate set of tools. The processes created during the SOC design and build phases should consider the current and desired capabilities.
- Skill set and experience: The SOC team must be equipped with the appropriate skill set that enables them to perform their tasks in terms of operating technologies and investigating incidents. The organization must consider training existing staff or acquiring the required skill set through a hiring process. This process should be continuous with the ability to rotate the SOC staff.
- Budget: The subject of budget is relative. The budget assigned to the build and operate phases would vary depending on a number factors, such as the following:
 - In-house versus SOC outsourcing
 - The services provided by the SOC

- The SOC operation hours
- The skill set gap
- The desired capability level roadmap

The characteristics of an effective SOC are connected such that the successful implementation of one is required to support the others. For example, the lack of executive sponsorship would lead to difficulties in implementing the required level of governance, establishing a collaborative environment, and allocating budget for the SOC. Figure 1-15 presents the relationship between the different characteristics.



Figure 1-15 The Characteristics of an Effective SOC

Introduction to Maturity Models

Maturity models are IT governance tools used to describe management processes with respect to standardization, repeatable processes and results, and measurement of effectiveness. Examples of such models include the Control Objectives for Information and related Technology (COBIT) Maturity Model (MM), described in Table 1-4, and the Carnegie Mellon Software Engineering Institute (SEI) Capability Maturity Model³⁰ (CMM), now under the CMMI Institute, described in Table 1-5. Referring to Table 1-4 and Table 1-5, notice the slight difference between the two models.

Scores for the maturity model are based on an assignment of a 0–5 score. These scoring metrics are used in the next sections to provide a general understanding of maturity in each of the identified security management areas. Table 1-4 shows the maturity scores and associated descriptions for the COBIT MM.

Maturity Level	Process Criteria	
0	Complete lack of any recognizable processes. The organization has not recognized there is an issue to be addressed.	
Nonexistent		
1 Initial/Ad Hoc	There is evidence that the organization has recognized that the issues exist and need to be addressed. There are, however, no standardized pro- cesses, but instead there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to manage- ment is disorganized.	
2 Repeatable but Intuitive	Processes have developed to the stage where similar procedures are fol- lowed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowl- edge of individuals, and therefore errors are likely.	
3 Defined Process	Procedures have been standardized, documented, and communicated through training. It is, however, left to the individual to follow these pro- cesses, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.	
4 Managed and Measurable	It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.	

 Table 1-4
 COBIT MM Scoring

Maturity Level	Process Criteria		
5	Processes have been refined to a level of best practice, based on the		
Optimized	results of continuous improvement and maturity modeling with other organizations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enter- prise quick to adapt.		

Maturity Level	Process Criteria
0	No security policy exists.
Nonexistent	
1 Initial: Process is unpredictable, poorly controlled, and reactive.	Processes are usually ad hoc and chaotic. The organi- zation usually does not provide a stable environment to support processes. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven pro- cesses.
2 Managed: Process is characterized by projects and is often reactive.	The document exists, and has been validated and dis- seminated, but it is incomplete or does not fit the con- text of the organization.
3 Defined: Process is characterized as a defined process.	The document exists, is complete, has been validated and disseminated, and fits the context of the organization.
4 Quantitatively managed: Process is measured and controlled.	Controls are set up to assess the application of the validated document.
5 Optimized: Focus is on continuous process improvement.	A regular review process allows assessing the applica- tion of the previously validated document and enables the organization to regularly update it.

Table 1-5	SEI Maturity	Levels
-----------	--------------	--------

 Table 1-4
 continued

Using a maturity model helps you measure your current capabilities and track progress against goals. To achieve this, processes and capabilities must be first identified so that maturity level values are assigned and a roadmap is then formalized. The exact set of capabilities to measure depends on the discipline you are trying to evaluate. Figure 1-16 shows maturity level values assigned to a number of security operation capabilities.



Figure 1-16 Capability Level: Security Operations

Applying Maturity Models to SOC

No single reference formalizes SOC capabilities. Here we propose a set of SOC-specific capabilities in three areas that could be evaluated. We use these capabilities as our reference for the rest of this book:

- People
 - Structure
 - Relative SOC knowledge and experience
 - Training and awareness
- Process
 - Incident triage
 - Incident reporting
 - Incident analysis

- 30 Chapter 1: Introduction to Security Operations and the SOC
 - Incident closure
 - Post-incident
 - Vulnerability discovery
 - Vulnerability remediation
 - Technology
 - Network infrastructure readiness
 - Events collection, correlation, and analysis
 - Security monitoring
 - Security control
 - Log management
 - Vulnerability assessment
 - Vulnerability tracking
 - Threat intelligence

Similar to Figure 1-16, the capabilities listed here can be graphically represented. For example, Figure 1-17 shows process-related SOC capabilities.



Figure 1-17 SOC Capabilities: Process

Phases of Building a SOC

This section introduces the sequence of phases that you expect to undergo when establishing a SOC: namely, plan, design, build, operate, and optionally, transfer. Each part of the book represents a SOC phase, with practices related to that phase. Although we use this chronological approach in the book to cover the different SOC topics, you can easily refer to any of these phases depending on where you are in your SOC program. For example, you might already be operating a SOC and looking to methodologies that you can use to assess your SOC's effectiveness in detecting and responding to various suspicious activity categories, or you might be looking to explore ideas related to people retention and skill development.

Delivering on each SOC phase requires having a set of relevant skills and the engagement of a number of internal and potentially external entities. The type of engagement varies from active involvement and actual service delivery to more of an executive and financial type of support.

A sequential approach in building a SOC does not necessarily mean following a rigid sequence of activities; instead, it gives you the opportunity to identify and consider the specific environment that your SOC will eventually operate within. How you plan and design your SOC will largely impact, positively or negatively, the time and cost you spend in deploying and operating your SOC. Properly planning for your SOC gives you enough visibility needed to formalize your SOC requirements before hiring resources or approaching technology vendors, some of whom are happy to sell you unnecessary modules of their SIEM solution, for example. In general, it is critical that SOC capabilities be developed and customized so that they are applicable to the organization's threat landscape, perceived risk, and compliancy needs.

Each phase consists of a number of activities that are performed in accordance with the organization's exact requirements. The list of phases is summarized in Figure 1-18 as an iterative process in which emerging security challenges introduced by the continuously evolving threat landscape are addressed. The following chapters extensively discuss each of these phases.



Figure 1-18 Phases of Building a SOC

Challenges and Obstacles

Although the success of any security program like the SOC relies heavily on proper planning, there are almost always challenges that are specific to the organization. These challenges are introduced because of issues related to governance, collaboration, skill sets, and so on. Such challenges must be identified and treated, or at least acknowledged, at an early stage of a SOC establishment program. They should be then tracked during each stage of the SOC. Chapter 3, "Assessing Security Operations Capabilities," discusses this topic in detail.

Summary

Establishing and maintaining a SOC is a continuous process of planning, designing, building, and operating a center that can detect and respond to security incidents. The establishment of the SOC requires developing various capabilities and maintenance related to people, processes, and technology. Understanding and formalizing the roles of the SOC program in the overall information security management system of an organization is paramount to the success of the SOC.

To set the stage for the rest of the book, this chapter provided a general overview of a SOC. Next we look at SOC operations, covering the tools and techniques found in most SOC environments.

References

- 1. The OODA Loop, http://en.wikipedia.org/wiki/OODA loop
- 2. John Boyd http://en.wikipedia.org/wiki/John Boyd (military strategist)
- 3. The Lockheed Martin cyber kill chain model, http://www.lockheedmartin.com/ content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- 4. Verizon 2015 Data Breach Report, http://www.verizonenterprise.com/DBIR/2015/
- 5. Backtrack Linux Distribution, http://www.backtrack-linux.org
- 6. Kali Linux Distribution, http://www.kali.org
- http://www.networkworld.com/article/2164758/network-security/malwaredetecting--sandboxing--technology-no-silver-bullet.html
- 8. VUPEN Security, http://www.vupen.com
- 9. Netragard, http://www.netragard.com
- 10. ReVuln Ltd., http://www.revuln.com
- 11. Endgame, http://www.endgame.com
- The Known Unknowns Report by NSS, https://www.nsslabs.com/reports/knownunknowns-0
- Internet of Everything, http://www.cisco.com/web/about/ac79/docs/IoE/IoE-AAG.pdf
- Bitglass Cloud Adoption Report Summary, http://www.bitglass.com/company/ news/press releases/cloud-security-adoption-report-2014
- 15. The rising strategic risks of cyberattacks research by McKinsey, http:// www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_ cyberattacks
- PCI Quick Reference Guide, https://www.pcisecuritystandards.org/documents/ pci ssc quick guide.pdf
- 17. Germany—Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG), http://www.iuscomp.org/gla/statutes/BDSG.htm
- Japan—Act on the Protection of Personal Information, http://www.cas.go.jp/jp/ seisaku/hourei/data/APPI.pdf
- 19. UK Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/ contents
- 20. Department of Defense Directive on Information Assurance (IA), http:// dodcio.defense.gov/Portals/0/Documents/DIEA/850001p.pdf
- NIST Special Publication 800-59, http://csrc.nist.gov/publications/nistpubs/800-59/ SP800-59.pdf
- http://lincs.police.uk/Library/Freedom-of-Information/Publication-Scheme/Our-Policies-And-Procedures/Information-Management-Strategy.pdf

- 34 Chapter 1: Introduction to Security Operations and the SOC
 - 23. NIST Special Publication 800-53 Revision 4, http://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-53r4.pdf
 - 24. Guide for Conducting Risk Assessments, http://csrc.nist.gov/publications/ nistpubs/800-30-rev1/sp800_30_r1.pdf
 - 25. Software Engineering Institute, http://www.sei.cmu.edu
 - 26. NIST SP 800-40 Version 2.0 Creating a Patch and Vulnerability Management Program, http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
 - 27. Qualys, http://www.qualys.com
 - 28. Tripwire, http://www.tripwire.com
 - 29. Rapid7, http://www.rapid7.com
 - 30. SEI Capability Maturity Model Integration (CMMI), http://www.sei.cmu.edu/cmmi