AREAS OF EXPERTISE IN CYBERSECURITY

Welcome back! We're entering Chapter 2, which focuses on the many disciplines that make up a successful company, their scope of duties, and how those roles come in contact with the SOC.

Additionally, we'll consider the external organizations that the SOC might interact with on a day-to-day basis.

Because a security investigation could involve everyone in an organization, including the CEO, you'll want to understand an SOC's role in the functions of other teams. In particular, we'll consider three sections: information security teams, internal teams, and external teams.

We'll start our probe by looking at information security teams.

Information Security

Organizations are made up of different teams. Just like a Human Resources department might have focused staff for Recruitment, Employee Benefits, and Training and Development, security teams are broken down into specific areas, too.

Accordingly, information security teams, at least in larger organizations, typically consist of three groups:

1. OPERATIONS 2. ENGINEERING 3. ARCHITECTURE

Just like everything in smaller organizations, though, it's possible that one or more of these teams may be combined in an effort to save costs. For example, in small organizations, a handful of cybersecurity professionals might handle all areas mentioned above--and more!

So the size of a company's network usually determines if these responsibilities are handled in-house or outsourced to a third party organization.

Let's look closely at different areas of expertise in cybersecurity for a "big picture" understanding:

AREA OF EXPERTISE	PURPOSE	DETAILS TO KNOW
SECURITY OPERATIONS CENTER (SOC)	• Monitors, investigates, and remediates security events	• If internal, the SOC has higher privileges and more extensive knowledge of the network • If externally sourced to an MSSP, then the incident is reported to the IT team. MSSPs often monitor several
THREAT INTELLIGENCE (TI)	• Researches new threats • Determines if threats are dangerous • Provides details to management and other IT teams	• Usually a smaller team. • Sometimes manages the Threat Intelligence Platform, the single point of collection for indicators of compromise and intelligence reports from multiple intel sources. • Typical intel sources of threat feeds include AlienVault or Talos Intelligence and other open-source Intelligence (OSINT). Commercial threat feeds require a subscription and may be expensive
DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR)	• Takes over incidents from the SOC • Conducts investigations on long and enduring incidents • Often works hand-in-hand with teams outside of the SOC and communicates with executive management concerning high priority cybersecurity incidents	• Acts as subject matter experts • Investigates incidents pertaining to legal, privacy, fraud, or external law enforcement organizations

Areas of Expertise in Cybersecurity

AREA OF EXPERTISE	PURPOSE	DETAILS TO KNOW
SECURITY ARCHITECTURE	• Focuses on enforcing the best security practices and compliance controls • Implements new technology	• Usually present in larger organizations • Typically made up of senior security specialists with several years of experience in cybersecurity • Sometimes outsourced due to limited scope • Commonly has specialists with specific skills. For example, host-based security, network security, virtualization, or cloud security • Represents the typical path for SOC analysts to move up after 7-10 years of cybersecurity experience
SECURITY ENGINEERING	• Deploys, manages, and maintains security tools and appliances • Updates and tunes cybersecurity tools • Serves SOC as their number one customer	• Sometimes combined with SOC analyst positions in small companies • Large companies typically staff internally • One technology area will usually be assigned per engineer • Another area for SOC analysts to advance
VULNERABILITY MANAGEMENT	• Identifies, catalogs, and remediates new and existing vulnerabilities throughout the network • Performs cyclic penetration tests, known as “Red Teams”	• Sometimes outsourced to a consulting company • Uses vulnerability scanners like Nessus, OpenVAS, and BurpSuite • Penetration testing may be outsourced

To neatly summarize the information in this table, you just need to know that most organizations have some combination of these roles and teams. And whether the SOC outsources or owns these responsibilities, every company has these functions.

In fact, you can think of each component as a puzzle piece that comes together to create a well-rounded, rockstar cybersecurity program.

Regardless of what team you work on, remember that they're all important to each other. After all, when a piece is missing, the puzzle isn't complete.

And what technology geek doesn't love a good puzzle?!

With information security behind us, we'll now dive into internal teams and how you'll interact with them as an SOC analyst.

Internal Teams

We've covered the roles you'll interact with as an SOC analyst, and you have a foundational understanding of the teams and a general sense of how they operate.

It's time to uncover and define the roles within an internal team. Here we go!

Like every organization, someone's in charge. Whether that person is the CEO, director, or manager, you'll report to a supervisor.

And this person is often powerful. The buck often stops with them when it comes to making business decisions. Let's look at what that might be for an SOC analyst.

We'll start from the bottom and make our way up the chain.

1. SOC Manager: The SOC manager is the first level of management and represents one of the most difficult jobs in cybersecurity. Generally, the SOC manager:

- Handles your offer letter in the beginning
- Approves your compensation, bonuses, and promotions
- Oversees tim e-off requests, work schedules, and your specific SOC duties
- Generates reports to upper management on the number and type of security events
- Ensures upper management is informed on the latest trends of cybersecurity attacks

While this is a brief introduction, we'll cover the SOC Manager in more detail later in the course.

2. **SOC Director:** This title differs across organizations, but you might hear any of the following:

    - Director of Security Operations
    - Director of Threat Management
    - Director of IT Security

    No matter what you call them, this position supervises the SOC Manager. Their general responsibilities include:

    - Handling the overall strategic decision for cybersecurity, including budgets and staffing approval
    - Reporting to Executive Leadership
    - Coordinating with other directors to plan joint projects

    With these facts in mind, we'll also discuss the SOC Director more later in the course.

3. **Chief Information Security Officer or CISO:** The CISO may have a wide range of responsibilities across different companies, but suffice it to say that they're responsible for high-level decisions regarding information security. The CISO is likely the first executive you'll meet and they often will report to the CEO or CTO. It goes without saying that an excellent first impression with the CISO will be an investment in your future career!

With the management ladder loosely defined, now let's look at the internal teams you will work with as an SOC analyst: risk management, governance and compliance, and privacy and legal.

1. **Risk Management Team** responsibilities include:

    - Measuring, reporting, and mitigating an organization's risk levels
    - Considering the likelihood of a compromise
    - Determining the impact if a compromise occurs
    - Generating a report to management on the risk

    Risk Management focuses on the worst-case scenario. Keep in mind, however, they may not be cybersecurity experts. Their understanding of attacks and compromises may be pretty limited, but they do seek to uncover the dangerous outcomes for an organization and how often that may occur.

2. Governance and Compliance Team responsibilities include:

- Ensuring the overall management approach that board members and senior executives use to control and direct an organization is correct
- Communicating compliance standards to the staff and making sure they meet industry standards
- Understanding global compliance standards and their varying sets of controls
- Securing that proper cybersecurity practices are followed in a uniform manner

With this in mind, some of the most common compliance standards are included here for your reference.

COMPLIANCE STANDARD	WEBSITE
Payment Card Industry Data Security Standard (PCI DSS)	*https://www.pcisecuritystands.org*
International Organization for Standardization (ISO 27001)	*https://www.iso.org/*
Cybersecutiry Maturity Model Certification (CMMC)	*https://www.acq.osd.mil/cmmc/*
health insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule	*https://www.hhs.gov/hippa/for.professionals/security/*
Information Security Registered Assessors Progam (IRAP)	*https://www.cyber.gov.au/irap/*
System and Organization Controls (SOC)	*https://www.aicpa.org/interestareas/frc/*

Can you imagine the regulations that must be followed in all of these areas of compliance?! Thankfully, you won't have to. Governance and Compliance is on the job of ensuring everything is on the up and up so you can focus on your job on the SOC.

As an SOC team member, you may interact with Governance and Compliance during audits because the SOC plays a crucial role in providing compliance evidence. Governance and Compliance may request logs, documentation, and security event walk-throughs from the SOC.

3. Privacy and Legal Team responsibilities include:

- Collecting evidence of a compromise
- Identifying the nature of stolen data
- Informing executive leadership on disclosure requirements, legal obligations, and options for pursuing attackers

Remember the Capital One breach we discussed earlier in the course? A Privacy and Legal team would handle the above responsibilities in a

situation like that. As an SOC analyst, you'd likely interact with Privacy and Legal after some type of serious cybersecurity incident and help provide necessary information.

Whew! There were several Internal Team roles to meet. With an understanding of what goes on inside an organization with an SOC, let's now turn to external teams that you may interact with as a future SOC analyst.

External Teams

For our purposes, any team that doesn't work within your company is an external team. We've talked about how you'll interact with information security and internal teams, but communicating with external teams requires different considerations. Let's look at the potential players on external teams.

1. **Government agencie**s are essential in any country, and it's no different for the good old U S of A. SOCs will find themselves interacting with local or federal governments at some point, whether it's for data breaches, compliance, or privacy law interpretation. We strongly urge you to research laws and regulations in your region so that you know what to expect when interacting with government agencies. Let's look at three specific kinds you'll likely come in contact with:

    - Law enforcement agencies represent the most common interactions you'll have as an SOC analyst, and those will typically include issues like providing evidence of data breaches or insider threats to an investigating agency. These include the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and state and local police. When communicating with agencies like this, remember the following:

        - State the facts
        - Remain professional
        - Show respect
        - Use common terms since they may not be cybersecurity professionals

- Military and intelligence agencies make up the next government entities you may interact with. Since the government buys goods and services from many companies and must follow certain cybersecurity regulations, tighter compliance controls and mandatory reporting requirements come into play. Working with the government ensures shared threat intelligence, and companies can do so by accessing the Defense Industrial Base Cybersecurity (DIB CS) program. DIB CS enables companies to share reports, indicators of compromise, and malware samples, all in one central location. The threat

- Regulatory agencies are government and non-government bodies created by legislature to set a baseline of standards for a particular field of activity in the private sector. The agency's job is to enforce these standards, and they're usually separated by business sectors. For example, the US Department of Health and Human Services regulates HIPAA compliance standards. Regulatory agencies often ask SOC analysts for evidence to prove compliance with regulations.

2. Auditors play a significant role in regulatory compliance and often cause headaches for the SOC and its employees. Their job includes:

- Understanding compliance standards and which security controls must be taken to satisfy those requirements
- Applying their knowledge and expertise
- Comparing a company's security against compliance standards

Depending on the compliance standards, audits could happen anywhere from 3 months to annually. Let's break down an example of how an auditor might interact with an SOC analyst during a compliance engagement:

EXCERPT FROM PCI CSS QUICK GUIDE

GOALS	PCI DSS REQUIREMENTS
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data	3. Protect stored cardholder data.
	4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program	5. Use and regularly update antivirus software or programs.
	6. Develop and maintain secure systems and applications.
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know.
	8. Assign a unique ID to each person with computer access.
	9. Restrict physical access to cardholder data
Regularly monitor and test networks ***This is an example of data an SOC may be asked to provide. The SOC would be the team monitoring access to network resources, and an auditor will likely ask to see the SOC's SIEM. Or some will request a live demo or screenshots of the monitoring platform.***	10. Track and monitor all access to network resources and cardholder data.
	11. Regularly test security systems and processes.
Maintain an information security policy	12. Maintain a policy that addresses information security for employees and contractors.

It's vital to note that an SOC analyst won't likely interact with an auditor directly. Senior analysts or your manager will often handle the contact, and your task may begin with evidence collection.

3. **Vendors** are external product or service providers that have sold your company a product or service. In other words, anything the SOC uses that wasn't created by your company came from a vendor. A vendor might ask you to join a tool demo or proof of concept (POC) evaluation of a security tool. Vendors provide great networking opportunities, providing potential future job opportunities if you ever move away from the SOC.

   Ethically, there are some rules when dealing with vendors. Remember--you represent your company. You can ask for new features, but you want to be sure the company won't be billed before an agreement is made. You also want to avoid promising anything to a vendor.

   When asked, you should provide honest feedback, including constructive criticism, because vendors take this input back to their company for changes. Do be sure to avoid insensitive comments like "we could build this ourselves" or "this adds zero value"--that is, unless you want to be excluded from future vendor conversations.