01 CyberSec and SOC

Notebook:	FGA Cyber		
Created:	7/2/2019 10:15 AM	**Updated:**	7/2/2019 12:31 PM
Author:	clink200032@gmail.com		
URL:	https://static-course-assets.s3.amazonaws.com/CyberOps11/en/course/module1/1.1.1.1...		

Hijacked People

Sarah stopped by her favorite coffee shop to grab her afternoon drink. She placed her order, paid the clerk, and waited while the baristas worked furiously to fulfill the backup of orders. Sarah pulled out her phone, opened the wireless client, and connected to what she assumed was the coffee shop's free wireless network.

However, sitting in a corner of the store, a hacker had just set up an open "rogue" wireless hotspot posing as the coffee shop's wireless network. When Sarah logged onto her bank's website, the hacker hijacked her session, and gained access to her bank accounts.

Click here for a quick look at a video posted in 2008 demonstrating how one wireless network was vulnerable to hacking. In this course, you will learn about security technologies that easily prevent this type of attack.

Ransomware Company

Rashid, an employee in the finance department of a major, publicly-held corporation, receives an email from his CEO with an attached PDF. The PDF is about the company's third quarter earnings. Rashid does not remember his department creating the PDF. His curiosity is peaked, so he opens the attachment.

The same scenario plays out across the organization as dozens of other employees are successfully enticed to click the attachment. When the PDF opens, ransomware is installed on the employees' computers and begins the process of gathering and encrypting corporate data. The goal of the attackers is financial gain, because they hold the company's data for ransom until they are paid.

Click here to see a dramatization of how this ransomware attack could happen.

Targeted Nations

Some of today's malware is so sophisticated and expensive to create that security experts believe only a nation state or group of nations could possibly have the influence and funding to create it. Such malware can be targeted to attack a nation's vulnerable infrastructure, such as the water system or power grid.

This was the purpose of the Stuxnet worm, which infected USB drives. These drives were carried by five Iranian component vendors, with the intention of infiltrating nuclear facilities supported by the vendors. Stuxnet was designed to infiltrate Windows operating systems and then target Step 7 software. Step 7 was developed by Siemens for their programmable logic controllers (PLCs). Stuxnet was looking for a specific model of the Siemens PLCs that controls the centrifuges in nuclear facilities. The worm was transmitted from the infected USB drives into the PLCs and eventually damaged many of these centrifuges.

Zero Days, a film released in 2016, attempts to document the development and deployment of the Stuxnet targeted malware attack.

Note: Search for the Zero Days film if the link does not work for your country of residence.

Amateurs

Threat actors include, but are not limited to, amateurs, hacktivists, organized crime groups, state sponsored, and terrorist groups. Threat actors are individuals or a group of individuals who perform cyberattacks against another individual or organization. Cyberattacks are intentional, malicious acts meant to negatively impact another individual or organization.

Amateurs, also known as script kiddies, have little or no skill. They often use existing tools or instructions found on the Internet to launch attacks. Some are just curious, while others try to demonstrate their skills by causing harm. Even though they are using basic tools, the results can still be devastating.

Hacktivists

Hacktivists are hackers who protest against a variety of political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles and videos, leaking sensitive information, and disrupting web services with illegitimate traffic in distributed denial of service (DDoS) attacks

Financial Gain

Much of the hacking activity that consistently threatens our security is motivated by financial gain. These cybercriminals want to gain access to our bank accounts, personal data, and anything else they can leverage to generate cash flow.

Trade secret and global politic

The past several years have seen many stories about nation states hacking other countries, or otherwise interfering withHinternal politics. Nation states are also interested in using cyberspace for industrial espionage. The theft of intellectual property can give a country a significant advantage in international trade.

Defending against the fallout from state-sponsored cyberespionage and cyberwarfare will continue to be a priority for cybersecurity professionals.

How secure is IoT

The Internet of Things (IoT) is all around us and quickly expanding. We are just beginning to reap the benefits of the IoT. New ways to use connected things are being developed daily. The IoT helps individuals connect things to improve their quality of life. For example, many people are now using connected wearable devices to track their fitness activities. How many devices do you currently own that connect to your home network or the Internet?

How secure are these devices? For example, who wrote the firmware? Did the programmer pay attention to security flaws? Is your connected home thermostat vulnerable to attacks? What about your digital video recorder (DVR)? If security vulnerabilities are found, can firmware in the device be patched to eliminate the vulnerability? Many devices on the Internet are not updated with the latest firmware. Some older devices were not even developed to be updated with patches. These two situations create opportunity for threat actors and security risks for the owners of these devices.

In October 2016, a DDoS attack against the domain name provider Dyn took down many popular websites. The attack came from a large number of webcams, DVRs, routers, and other IoT devices that had been compromised by malicious software. These devices formed a "botnet" that was controlled by hackers. This botnet was used to create an enormous DDoS attack that disabled essential Internet services. Dyn has posted a blog here to explain the attack and their reaction to it.

Avi Rubin, professor of Computer Science at Johns Hopkins University, highlights the dangers of not securing all our connected devices. Click here to view his TED talk.

1.1.3 Threat Impact
PII and PHI

The economic impact of cyberattacks is difficult to ascertain with precision; however, according to an article in Forbes, it is estimated that businesses lose $400 billion annually to cyberattacks.

Personally identifiable information (PII) is any information that can be used to positively identify an individual. Examples of PII include:

- Name
- Social security number
- Birthdate
- Credit card numbers
- Bank account numbers
- Government issued ID
- Address information (street, email, phone numbers)

One of the more lucrative goals of cybercriminals is obtaining lists of PII that can then be sold on the dark web. The dark web can only be accessed with special software and is used by cybercriminals to shield their activities. Stolen PII can be used to create fake accounts, such as credit cards and short-term loans.

A subset of PII is protected health information (PHI). The medical community creates and maintains electronic medical records (EMRs) that contain PHI. In the U.S., handling of PHI is regulated by the Health Insurance Portability and Accountability Act (HIPAA). The equivalent regulation in the European Union is called Data Protection.

Most hacks on companies and organizations reported in the news involved stolen PII or PHI. In only three months in 2016, the following attacks occurred:

- In March 2016, a data breach at a health care provider exposed the personal information of 2.2 million patients.
- In April 2016, a laptop and portable drives were stolen from a government agency that included personal information for as many as 5 million people.
- In May 2016, a data breach at a payroll company exposed the payroll, tax, and benefits information of over 600,000 companies.

Lost Competitive Advantage

Companies are increasingly worried about corporate espionage in cyberspace. An additional major concern is the loss of trust that comes when a company is unable to protect its customers' personal data. The loss of competitive advantage may come from this loss of trust rather than another company or country stealing trade secrets.

Politic and National Security

It is not just businesses that get hacked. In February 2016, a hacker published the personal information of 20,000 U.S. Federal Bureau of Investigation (FBI) employees and 9,000 U.S.

Department of Homeland Security (DHS) employees. The hacker was apparently politically motivated.

The Stuxnet worm was specifically designed to impede Iran's progress in enriching uranium that could be used in a nuclear weapon. Stuxnet is a prime example of a network attack motivated by national security concerns. Cyberwarfare is a serious possibility. State-supported hacker warriors can cause disruption and destruction of vital services and resources within an enemy nation. The Internet has become essential as a medium for commercial and financial activities. Disruption of these activities can devastate a nation's economy. Controllers, similar to those attacked by Stuxnet, also are used to control the flow of water at dams and the switching of electricity on the power grid. Attacks on such controllers can have dire consequences.

1.2 Fighter in war against Crime

1.2.1.Modern SOC

Element of SOC

Defending against today's threats requires a formalized, structured, and disciplined approach which is executed by professionals at Security Operations Centers. SOCs provide a broad range of services, from monitoring and management, to comprehensive threat solutions and hosted security that can be customized to meet customer needs. SOCs can be wholly in-house, owned and operated by a business, or elements of a SOC can be contracted out to security vendors, such as Cisco's Managed Security Services.

The major elements of a SOC, shown in the figure, are people, processes, and technology.

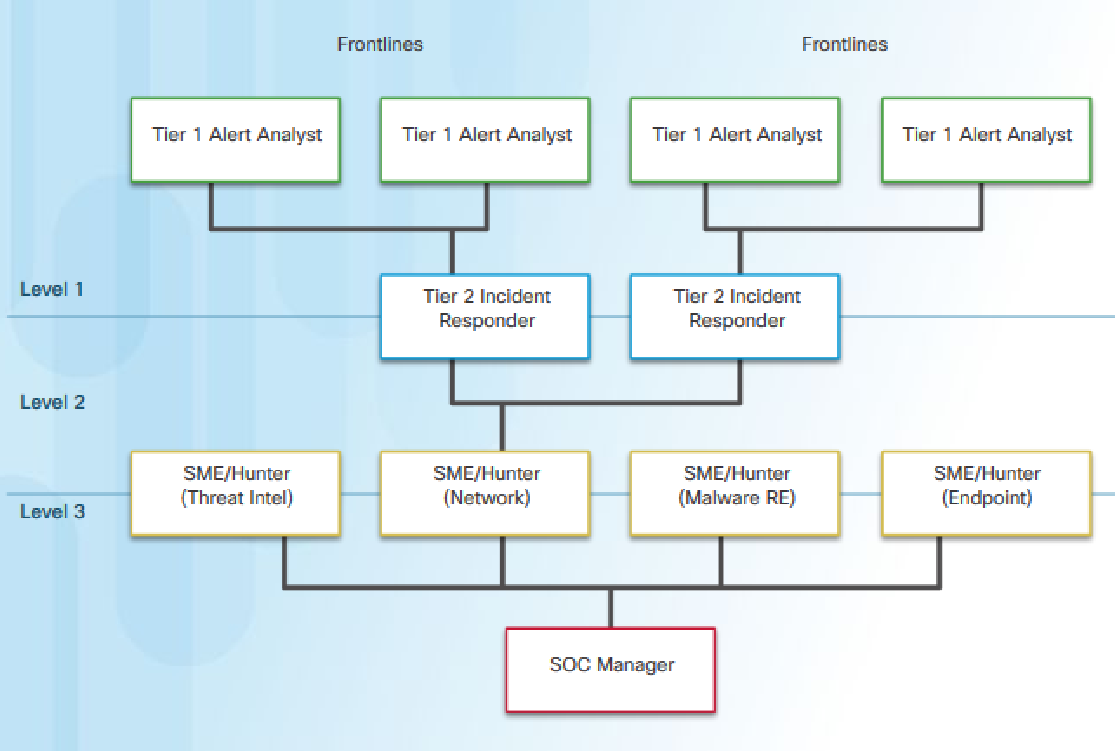
People in SOC

The SANS Institute (www.sans.org) classifies the roles people play in a SOC into four job titles:

- **Tier 1 Alert Analyst** – These professionals monitor incoming alerts, verify that a true incident has occurred, and forward tickets to Tier 2, if necessary.
- **Tier 2 Incident Responder**- These professionals are responsible for deep investigation of incidents and advise remediation or action to be taken.
- **Tier 3 Subject Matter Expert (SME)/Hunter** – These professionals have expert-level skill in network, endpoint, threat intelligence, and malware reverse engineering. They are experts at tracing the processes of the malware to determine its impact and how it can be removed. They are also deeply involved in hunting for potential threats and implementing threat detection tools.
- **SOC Manager** – This professional manages all the resources of the SOC and serves as the point of contact for the larger organization or customer.

This course offers preparation for a certification suitable for the position of Tier 1 Alert Analyst, also known as Cybersecurity Analyst.

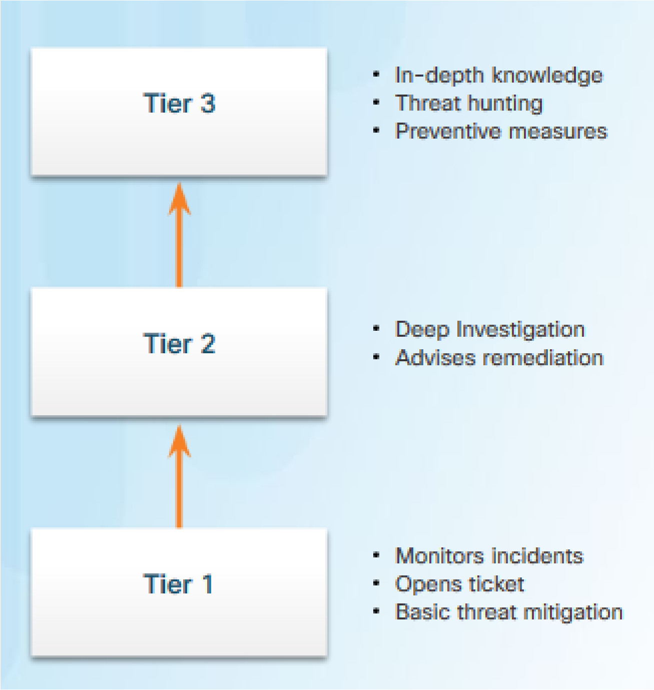
The figure from the SANS institute graphically represents how these roles interact with each other.



Process in SOC

The day of a Tier 1 Analyst begins with monitoring security alert queues. A ticketing system is frequently used to allow analysts to select alerts from a queue to investigate. Because the software that generates alerts can trigger false alarms, one job of the Tier 1 Analyst might be to verify that an alert represents a true security incident. When verification is established, the incident can be forwarded to investigators or other security personnel to be acted upon, or resolved as a false alarm.

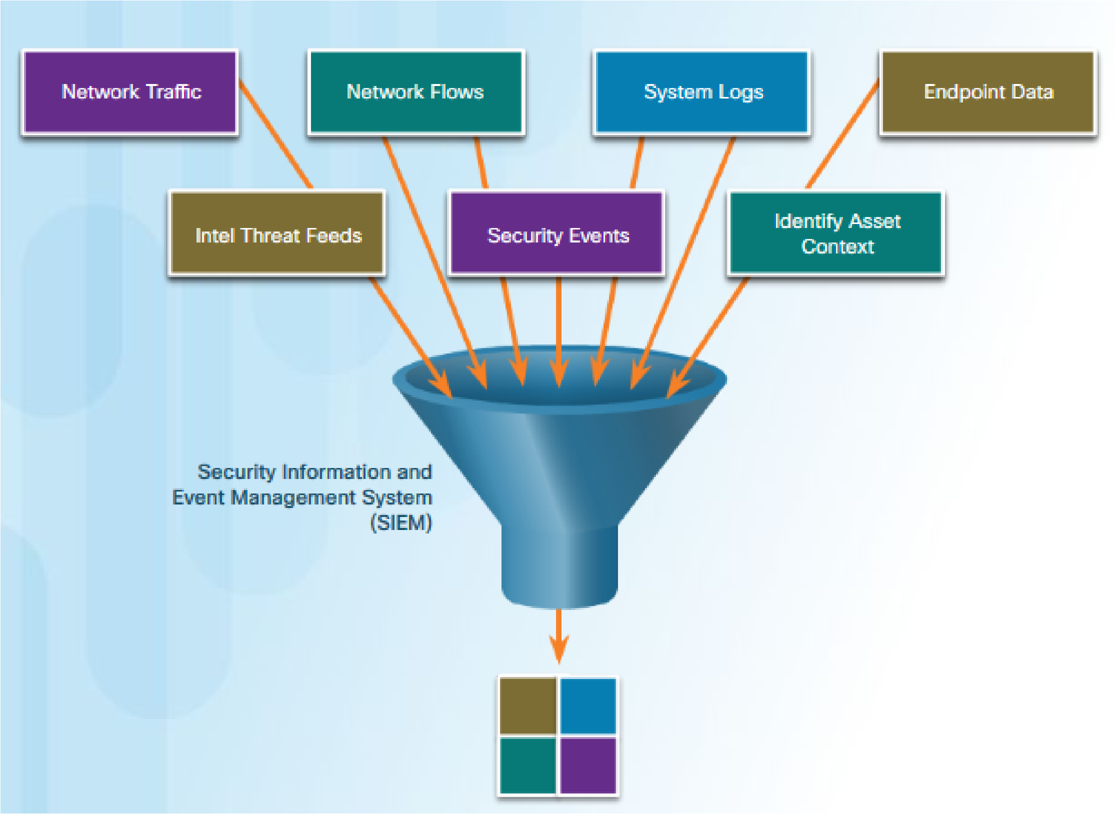
If a ticket cannot be resolved, the Tier 1 Analyst will forward the ticket to a Tier 2 Analyst for deeper investigation and remediation. If the Tier 2 Analyst cannot resolve the ticket, she will forward it to a Tier 3 Analyst with in-depth knowledge and threat hunting skills.



Technology in SOC

As shown in the figure, a SOC needs a security information and event management system (SIEM), or its equivalent. This system combines data from multiple technologies. SIEM systems are used for collecting and filtering data, detecting and classifying threats, analyzing and investigating threats, and managing resources to implement preventive measures and address future threats. SOC technologies include one or more of the following:

- Event collection, correlation, and analysis
- Security monitoring
- Security control
- Log management
- Vulnerability assessment
- Vulnerability tracking
- Threat intelligence



Enterprise and Managed Security

For medium and large networks, the organization will benefit from implementing an enterprise-level SOC. The SOC can be a complete in-house solution. However, many larger organizations will outsource at least part of the SOC operations to a security solutions provider.

Cisco has a team of experts who help ensure timely and accurate incident resolution. Cisco offers a wide range of incident response, preparedness, and management capabilities:

- Cisco Smart Net Total Care Service for Rapid Problem Resolution
- Cisco Product Security Incident Response Team (PSIRT)
- Cisco Computer Security Incident Response Team (CSIRT)
- Cisco Managed Services
- Cisco Tactical Operations (TacOps)
- Cisco's Safety and Physical Security Program

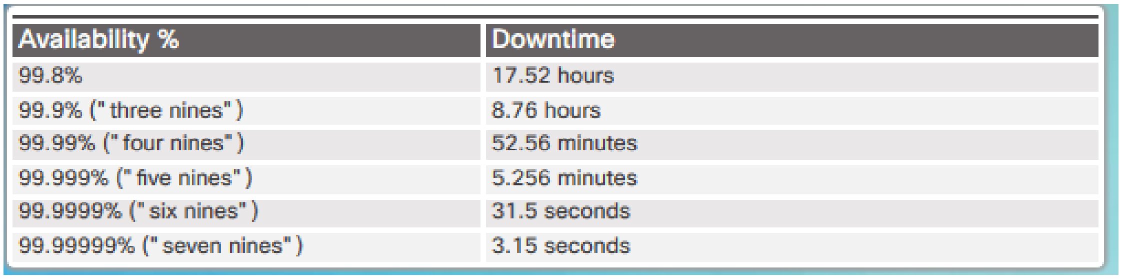
Security vs Availablity

Most enterprise networks must be up and running at all times. Security personnel understand that for the organization to accomplish its priorities, network availability must be preserved.

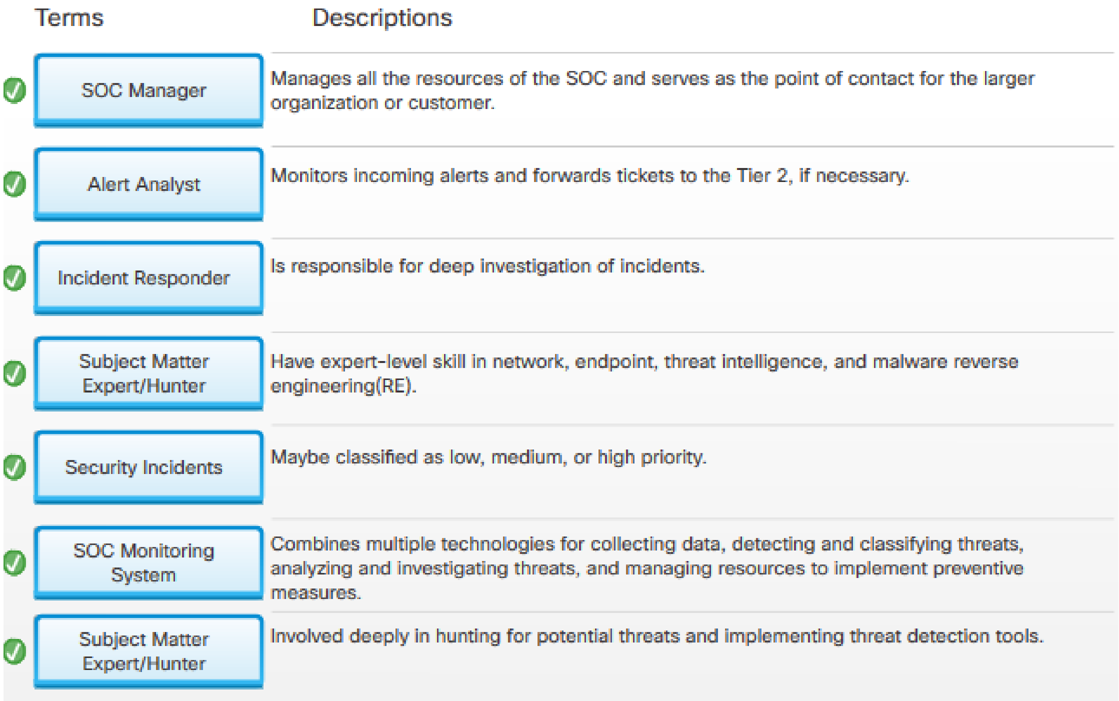
Each business or industry has a limited tolerance for network downtime. That tolerance is usually based upon a comparison of the cost of the downtime in relation to the cost of ensuring against downtime. For example, in a small retail business with only one location, it may be tolerable to have a router as a single point of failure. However, if a large portion of that business's sales are from online shoppers, then the owner may decide to provide a level of redundancy to ensure that a connection is always available.

Preferred uptime is often measured in the number of down minutes in a year, as shown in the figure. For example, a “five nines” uptime means that the network is up 99.999% of the time or down for no more than 5 minutes a year. “Four nines” would be a downtime of 53 minutes a year.

However, security cannot be so strong that it interferes with the needs of employees or business functions. It is always a tradeoff between strong security and permitting efficient business functioning.



Availability %	Downtime
99.8%	17.52 hours
99.9% (" three nines")	8.76 hours
99.99% (" four nines")	52.56 minutes
99.999% (" five nines")	5.256 minutes
99.9999% (" six nines")	31.5 seconds
99.99999% (" seven nines")	3.15 seconds



	Terms	Descriptions
✓	SOC Manager	Manages all the resources of the SOC and serves as the point of contact for the larger organization or customer.
✓	Alert Analyst	Monitors incoming alerts and forwards tickets to the Tier 2, if necessary.
✓	Incident Responder	Is responsible for deep investigation of incidents.
✓	Subject Matter Expert/Hunter	Have expert-level skill in network, endpoint, threat intelligence, and malware reverse engineering(RE).
✓	Security Incidents	Maybe classified as low, medium, or high priority.
✓	SOC Monitoring System	Combines multiple technologies for collecting data, detecting and classifying threats, analyzing and investigating threats, and managing resources to implement preventive measures.
✓	Subject Matter Expert/Hunter	Involved deeply in hunting for potential threats and implementing threat detection tools.

Internships

Internships are an excellent method for gaining entry into the cybersecurity field. Sometimes, internships turn into an offer of full time employment. However, even a temporary internship allows you the opportunity to gain experience in the inner workings of a cybersecurity organization. The contacts you make during an internship can also prove to be a valuable resource as you continue your career. Click here to read an article by Forbes about the 10 best websites for internships.

Cisco Cybersecurity Scholarship

To help close the security skills gap, Cisco introduced the Global Cybersecurity Scholarship program in 2016. Cisco is motivated to increase the pool of talent with critical cybersecurity proficiency. Registration opens in spring and awards are announced in late fall. Click here to learn more about the scholarship.

Temporary Agencies

If you are having difficulty finding your first job, a temporary agency can be a great place to start. Most temporary agencies will help you polish your resume and make recommendations on additional skills you may need to obtain to make yourself more attractive to potential employers.

Many organizations use temporary agencies to fill job openings for the first 90 days. Then, if the employee is a good match, the organization may offer to buy the contract from the temporary agency, converting the employee to a full-time, permanent position.

Your First Job

If you have no experience in the cybersecurity field, then you will most likely look for a company that is willing to train you for a position similar to a Tier 1 Analyst. Working for a call center or support desk may be your first step into gaining the experience you need to move ahead in your career.

How long should you stay in your first job? Generally, you want to make it through a full review cycle before leaving a company. That is, you typically want to make it past 18 months. Potential employers will normally want to know if you met or exceeded expectations in your current or past jobs.

Conclusion

In the beginning of the chapter you learned that people, companies, and even nations can all fall victim to cyberattacks. There are various types of attackers, including amateurs who attack for fun and prestige, hacktivists who hack to further a political cause, and professional hackers who attack for profit. In addition, nations may attack other nations to gain economic advantage through the theft of intellectual property, or to damage or destroy the assets of another country. The networks that are vulnerable to attack are not just business networks of PCs and servers, but also the thousands of devices on the Internet of Things.

Security Operations Centers (SOC) are responsible for preventing, detecting, and responding to cybercrime. SOCs consist of people following processes to use technologies to respond to threats. There are four main roles in the SOC. Tier 1 analysts verify security alerts using network data. Tier 2 responders investigate verified incidents and decide on how to act. Tier 3 SME/Hunters are experts and are able to investigate threats at the highest level. The fourth role is the SOC managers. They manage the resources of the center and communicate with customers. Customers can be internal or external. A SOC may be operated by a single company or may provide services to many companies. Finally, although network security is extremely important, it cannot interfere with the ability of the company and its employees to fulfill the mission of an organization.

In order to work in a SOC, you learned that you can study to earn certifications that are offered by a number of different organizations. In addition, you can pursue degrees in higher education that are relevant to cyber operations, and learn other skills such as programming in Python. Job leads can be found at a number of employment websites, and agencies can help you to find temporary jobs, internships, or permanent employment.