



# Day 3

## CISCO CYBER OPS

Studied Module 1-2 of Cisco CyberOps Associate.

**Module 1 was all about Introduction, Guide, History, Threat Actor, Threat Impact(PII, PHI, and PSI)**

**Module 2 was about SOC/ Security Analysts. And involved Elements of Soc, People in SOC as TIER wise. Process in the SOC, Technologies in the SOC: SIEM, SOAR. SOC Metrics, Enterprise and Managed Security, Security vs. Availability, Becoming a Defender**

## War Stories

Threat actors can hijack banking sessions and other personal information by using “evil twin” hotspots. Threat actors can target companies, as in the example where opening a pdf on the company computer can install ransomware. Entire nations can be targeted. This occurred in the Stuxnet malware attack.

## Threat Actors

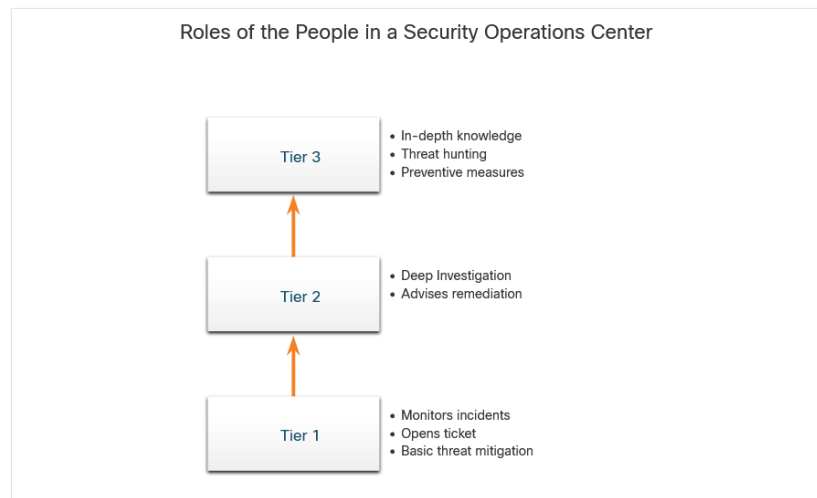
Threat actors include, but are not limited to, amateurs, hackers, organized crime groups, state sponsored, and terrorist groups. The amateur may have little to no skill and often use information found on the internet to launch attacks. Hackers are hackers who protest against a variety of political and social ideas. Much of the hacking activity is motivated by financial gain. Nation states are interested in using cyberspace for industrial espionage. Theft of intellectual property can give a country a significant advantage in international trade. As the Internet of Things (IoT) expands, webcams, routers, and other devices in our homes are also under attack.

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)**. In the European Union the **General Data Protection Regulation (GDPR)** protects a broad range of personal information including health records.

## Threat Impact

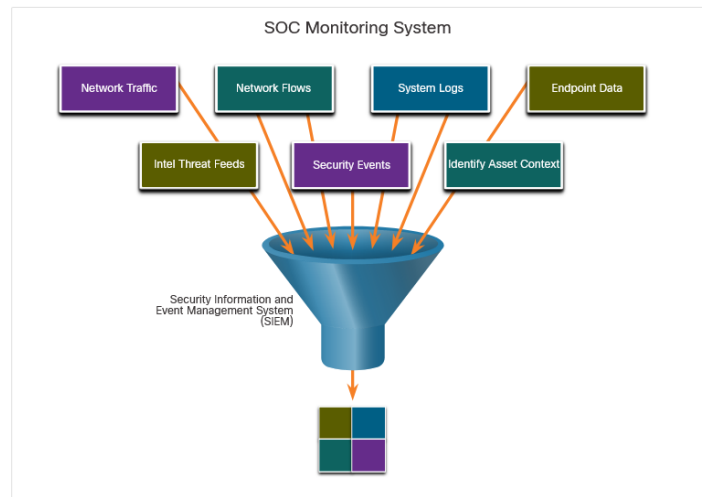
It is estimated that businesses will lose over \$5 trillion annually by 2024 due to cyberattacks. Personally identifiable information (PII), protected health information (PHI), and personal security information (PSI) are forms of protected information that are often stolen. A company can lose its competitive advantage when this information is stolen, including trade secrets. Also, customers lose trust in the company's ability to protect their data. Governments have also been victims of hacking.

- **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 Threat 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. Threat hunters search for cyber threats that are present in the network but have not yet been detected.
- **SOC Manager** – This professional manages all the resources of the SOC and serves as the point of contact for the larger organization or customer



SIEM systems are used for collecting and filtering data, detecting and classifying threats, and analyzing and investigating threats. SIEM systems may also manage 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

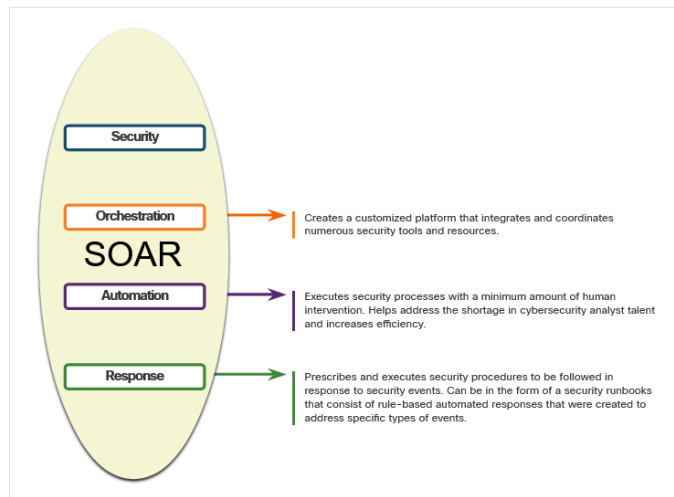


SIEM and security orchestration, automation and response (SOAR) are often paired together as they have capabilities that complement each other.

In system administration, *orchestration* is the automated configuration, coordination, and management of computer systems and software.

Orchestration is the automated configuration, management, and coordination of computer systems, applications, and services

.



SOAR security platforms:

- Gather alarm data from each component of the system.
- Provide tools that enable cases to be researched, assessed, and investigated.
- Emphasize integration as a means of automating complex incident response workflows that enable more rapid response and adaptive defense strategies.
- Include pre-defined playbooks that enable automatic response to specific threats. Playbooks can be initiated automatically based on predefined rules or may be triggered by security personnel.

Several common metrics compiled by SOC managers are:

- **Dwell Time** – the length of time that threat actors have access to a network before they are detected, and their access is stopped.
- **Mean Time to Detect (MTTD)** – the average time that it takes for the SOC personnel to identify valid security incidents have occurred in the network.
- **Mean Time to Respond (MTTR)** – the average time that it takes to stop and remediate a security incident.

- **Mean Time to Contain (MTTC)** – the time required to stop the incident from causing further damage to systems or data.
- **Time to Control** – the time required to stop the spread of malware in the network.

Cisco offers a wide range of incident response, preparedness, and management capabilities including:



- 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

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 table. 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.

 Availability %	 Downtime
<u>99.8%</u>	17.52 hours
<u>99.9%</u> ("three nines").	8.76 hours
<u>99.99%</u> ("four nines").	52.56 minutes
<u>99.999%</u> ("five nines").	5.256 minutes
<u>99.9999%</u> ("six nines").	31.56 seconds
<u>99.99999%</u> ("seven nines").	3.16 seconds

Within a year, there are 365 days x 24 hours a day x 60 minutes per hour = 525,600 minutes. With the goal of uptime 99.99% of time, the downtime needs to be controlled under 525,600 x (1-0.9999) = 52.56 minutes a year.

## Certifications

A variety of cybersecurity certifications that are relevant to careers in SOC's are available from several different organizations.

### Cisco Certified CyberOps Associate

The Cisco Certified CyberOps Associate certification provides a valuable first step in acquiring the knowledge and skills needed to work with a SOC team. It can be a valuable part of a career in the exciting and growing field of cybersecurity operations.

### CompTIA Cybersecurity Analyst Certification

The CompTIA Cybersecurity Analyst (CySA+) certification is a vendor-neutral IT professional certification. It validates knowledge and skills required to configure and use threat detection tools, perform data analysis, interpret the results to identify vulnerabilities, threats and risks to an organization. The end goal is the ability to secure and protect applications and systems within an organization.

### (ISC)<sup>2</sup> Information Security Certifications

(ISC)<sup>2</sup> is an international non-profit organization that offers the highly-acclaimed CISSP certification. They offer a range of other certifications for various specialties in cybersecurity.

### Global Information Assurance Certification (GIAC)

GIAC, which was founded in 1999, is one of the oldest security certification organizations. It offers a wide range of certifications in seven categories.

## Assessment Score

Earned Points: 34

Percentage: 87.2%