✓ **Good job!**

You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

×

Show Menu

2 Fighters in the War A
Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

Fighters in the War Against Cybercrime Summary

2.3.1

What Did I Learn in this Module?

The Modern Security Operations Center

Major elements of the SOC include people, processes, and technologies. Job roles are rapidly evolving and include tiers based on expertise and experience. These roles include a Tier 1 Alert Analyst, a Tier 2 Incident Responder, a Tier 3 Threat hunter, and an SOC Manager. A Tier 1 Analyst will monitor incidents, open tickets, and perform basic threat mitigation.

SEIM systems are used for collecting and filtering data, detecting and classifying threats, and analyzing and investigating threats. SEIM and SOAR are often paired together. SOAR is similar to SIEM. SOAR goes a step further by integrating threat intelligence and automating incident investigation and response workflows based on playbooks developed by the security team. Key Performance Indicators (KPI) are devised to measure different aspects of SOC performance. Common metrics include Dwell Time, Meant Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), and Time to Control.

There must be a balance between security and availability of the networks. Security cannot be so strong that it interferes with employees or business functions.

13 Attackers and Their T

CyberC

Good job!

You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

2 Fighters in the War A
Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

Becoming a Defender

Certification, (ISC)2 Information Security Certifications, Global Information Assurance Certification (GIAC), and others. Job sites include Indeed.com, CareerBuilder.com, USAJobs.gov, Glassdoor, and LinkedIn. You may also want to consider internships and temporary agencies to gain experience and begin your career. In addition, Linux and Python programming skills will add to your desirability in the job market.

2.3.2

Module 2: Fighters in the War Against Cybercrime Quiz

1. Which personnel in a SOC is assigned the task of verifying whether an alert triggered by monitoring software represents a true security incident?

✓ Topic 2.1.0 - In a SOC, the job of a Tier 1 Alert Analyst includes monitoring incoming alerts and verifying that a true security incident has occurred.

○ Tier 1 personnel

○ SOC Manager

○ Tier 2 personnel

○ Tier 3 personnel

13 Attackers and Their T

Show Menu

2 Fighters in the War A… Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

✓ **Good job!**

You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

×

2. After a security incident is verified in a SOC, an … nt but cannot … form an … om should

✓ Topic 2.1.0 - An incident responder is a Tier 2 security professional in a SOC. If the responder cannot resolve the incident ticket, the incident ticket should be escalated to the next tier support, a Tier 3. A Tier 3 SME would further investigate the incident.

○ a SME for further investigation

○ an alert analyst for further analysis

○ the SOC manager to ask for other personnel to be assigned

○ a cyberoperations analyst for help

3. Which two services are provided by security operations centers? (Choose two.)

✓ Topic 2.1.0 - Security operations centers (SOCs) can provide a broad range of services to defend against threats to information systems of an organization. These services include monitoring threats to network security and managing comprehensive solutions to fight against threats. Ensuring secure routing exchanges and providing secure Internet connections are tasks typically performed by a network operations center (NOC). Responding to facility break-ins is typically the function and responsibility of the local police department.

□ ensuring secure routing packet exchanges

☑ monitoring network security threats

□ responding to data center physical break-ins

□ providing secure Internet connections

☑ managing comprehensive threat solutions

13 Attackers and Their T

Show Menu

2 Fighters in the War A Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

Good job!

You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

4. Which metric is used in SOCs to evaluate the at valid network?

y metrics w long it takes personnel to locate, stop, and remediate security incidents.

- Dwell Time
- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- Mean Time to Contain (MTTC)
- Time to Control

○ Dwell Time

○ MTTD

○ MTTC

○ MTTR

5. Which KPI metric does SOAR use to measure the length of time that threat actors have access to a network before they are detected and the access of the threat actors stopped?

✓ Topic 2.1.0 - The common key performance indicator (KPI) metrics compiled by SOC managers are as follows:
- Dwell Time: the length of time that threat actors have access to a network before they are detected and the access of the threat actors 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

○ MTTD

○

MTTR

13 Attackers and Their T

Show Menu

2 Fighters in the War Ag
Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

Good job!

You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

✓ Topic 2.1.0 - A security information and event management system (SIEM) makes sense of all of the data that firewalls, network appliances, intrusion detection systems, and other devices generate. SIEMs 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.

○ to analyze all the network packets for any malware signatures and update the vulnerabilities database

○ to analyze all the network packets for any malware signatures and synchronize the signatures with the Federal Government databases

○ to analyze any OS vulnerabilities and apply security patches to secure the operating systems

○ to analyze all the data that firewalls, network appliances, intrusion detection systems, and other devices generate and institute preventive measures

13 Attackers and Their T

Show Menu

2 Fighters in the War A
Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

Good job!

You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

7. What is a characteristic of the SOAR security

platforms

omponent
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 predefined playbooks that enable automatic response to specific threats

○ to include predefined playbooks that enable automatic response to specific threats

○ to provide a means to synchronize the vulnerabilities database

○ to interact with the Federal Government security sites and update all vulnerability platforms

○ to provide a user friendly interface that uses the Python programming language to manage security threats

8. A network security professional has applied for a Tier 2 position in a SOC. What is a typical job function that would be assigned to a new employee?

✓ Topic 2.1.0 – In a typical SOC, the job of a Tier 2 incident responder involves deep investigation of security incidents.

○ further investigating security incidents

○ serving as the point of contact for a customer

○ monitoring incoming alerts and verifying that a true security incident has occurred

○ hunting for potential security threats and implementing threat detection tools

13 Attackers and Their T

Show Menu

2 Fighters in the War A
Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

✓ **Good job!**
You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

×

9. If a SOC has a goal of 99.99% uptime, how many … considered

…here are … 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.

○ 52.56
○ 60.56
○ 50.38
○ 48.25

10. Which organization offers the vendor-neutral CySA+ certification?

✓ Topic 2.2.0 - The CompTIA Cybersecurity Analyst (CySA+) certification is a vendor-neutral security professional certification.

○ (ISC)²
○ IEEE
○ CompTIA
○ GIAC

11. In the operation of a SOC, which system is frequently used to let an analyst select alerts from a pool to investigate?

✓ Topic 2.1.0 - In a SOC, a ticketing system is typically used for a work flow management system.

○ security alert knowledge-based system
○ registration system
○ ticketing system
○ syslog server

13 Attackers and Their T

Show Menu

2 Fighters in the War A
Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

Good job!

You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

12. How can a security information and event
d to help
s?

mation
(SIEM)
combines data from multiple sources to help SOC personnel collect and filter data, detect and classify threats, analyze and investigate threats, and manage resources to implement preventive measures.

○ by filtering network traffic

○ by encrypting communications to remote sites

○ by authenticating users to network resources

○ by collecting and filtering data

13. Which three technologies should be included in a security information and event management system in a SOC? (Choose three.)

✓ Topic 2.1.0 - Technologies in a SOC should include the following:

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

Firewall appliances, VPNs, and IPS are security devices deployed in the network infrastructure.

☑ vulnerability tracking

☑ threat intelligence

☐ intrusion prevention

☐ VPN connection

☑ security monitoring

☐ firewall appliance

13 Attackers and Their T

Show Menu

Good job!

You have successfully identified the correct answers.

You answered 13 out of 13 questions correctly.

2 Fighters in the War A
Cybercrime

2.3.1 What Did I Learn in this Module?

2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

10 Network Services

11 Network Communication Devices

12 Network Security Infrastructure

2.2 Becoming a Defender

3.0 Introduction