CCNA Cyber Ops (Version 1.1) – Chapter 1 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-1-exam-answers-full.html

May 13, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. A computer is presenting a user with a screen requesting payment before the user data is allowed to be accessed by the same user. What type of malware is this?

- A type of virus
- A type of logic bomb
- **A type of ransomware**
- A type of worm

C. Ransomware commonly encrypts data on a computer and makes the data unavailable until the computer user pays a specific sum of money

2. What is cyberwarfare?

- It is an attack only on military targets.
- It is an attack on a major corporation.
- It is an attack that only involves robots and bots.
- **It is an attack designed to disrupt, corrupt, or exploit national interests.**

D. Cyberwarfare is a subset of information warfare (IW). Its objective is to disrupt (availability), corrupt (integrity), or exploit (confidentiality or privacy). It can be directed against military forces, critical infrastructures, or other national interests, such as economic targets. It involves several teams that work together. A botnet might be one of several tools used for launching the attack.

3. How can a security information and event management system in an SOC be used to help personnel fight against security threats?

- **By collecting and filtering data**

- By filtering network traffic
- By authenticating users to network resources
- By encrypting communications to remote sites

A. A security information and event management system (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.

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

- Proxy service
- User authentication
- **Threat intelligence**
- **Security monitoring**
- Intrusion prevention
- **Event collection, correlation, and analysis**

C, D, F. Technologies in a SOC should include the following:
Event collection, correlation, and analysis
Security monitoring
Security control
Log managementVulnerability assessment
Vulnerability tracking
Threat intelligence
Proxy server, user authentication, and intrusion prevention systems (IPS) are security devices and mechanisms deployed in the network infrastructure and managed by the network operations center (NOC).

5. What name is given to hackers who hack for a political or social cause?

- White hat
- Hacker
- **Hacktivist**
- Blue hat

C. The term is used to describe gray hat hackers who rally and protect for a cause.

6. Which organization is an international nonprofit organization that offers the CISSP certification?

- **(ISC)2**
- IEEE
- GIAC

- CompTIA

A. (ISC)2 is an international nonprofit organization that offers the CISSP certification.

7. After a security incident is verified in a SOC, an incident responder reviewsthe incident but cannot identify the source of the incident and form an effective mitigation procedure. To whom should the incident ticket be escalated?

- A cyberoperations analyst for help
- **An SME for further investigation**
- An alert analyst for further analysis
- The SOC manager to ask for other personnel to be assigned

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

8. The term Alert Analyst refers to which group of personnel in an SOC?

- **Tier 1 personnel**
- Tier 2 personnel
- Tier 3 personnel
- SOC managers

A. In a typical SOC, the Tier 1 personnel are called alert analysts, also known as cyberoperations analysts.

9. What is a rogue wireless hotspot?

- It is a hotspot that was set up with outdated devices.
- It is a hotspot that does not encrypt network user traffic.
- It is a hotspot that does not implement strong user authentication mechanisms.
- **It is a hotspot that appears to be from a legitimate business but was actually set up by someone without the permission from the business.**

D. A rogue wireless hotspot is a wireless access point running in a business or an organization without the official permission from the business or organization.

10. What is a potential risk when using a free and open wireless hotspot in a public location?

- Too many users trying to connect to the Internet may cause a network traffic jam.
- The Internet connection can become too slow when many users access the wireless hotspot.

- **Network traffic might be hijacked and information stolen.**
- Purchase of products from vendors might be required in exchange for the Internet access.

Explanation: Many free and open wireless hotspots operate with no authentication or weak authentication mechanisms. Attackers could easily capture the network traffic in and out of such a hotspot and steal user information. In addition, attackers might set up a “rogue” wireless hotspot to attract unsuspecting users to it and then collect information from those users.

11. How does a security information and event management system (SIEM) in a SOC help the personnel fight against security threats?

- by integrating all security devices and appliances in an organization
- by analyzing logging data in real time
- **by combining data from multiple technologies**
- by dynamically implementing firewall rules

A security information and event management system (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.

12. Which statement best describes a motivation of hacktivists?

- **They are part of a protest group behind a political cause.**
- They are curious and learning hacking skills.
- They are trying to show off their hacking skills.
- They are interested in discovering new exploits.

Each type of cybercriminal has a distinct motivation for his or her actions.

13. If a SOC has a goal of 99.999% uptime, how many minutes of downtime a year would be considered within its goal?

- **Approximately 5 minutes per year.**
- Approximately 10 minutes per year.
- Approximately 20 minutes per year.
- Approximately 30 minutes per year.

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 99.999% of time, the downtime needs to be controlled under 525,600 x (1-0.99999) = 5.256 minutes a year.

14. Why do IoT devices pose a greater risk than other computing devices on a network?

- Most IoT devices do not require an Internet connection and are unable to receive new updates.
- IoT devices cannot function on an isolated network with only an Internet connection.
- **Most IoT devices do not receive frequent firmware updates.**
- IoT devices require unencrypted wireless connections.

IoT devices commonly operate using their original firmware and do not receive updates as frequently as laptops, desktops, and mobile platforms.

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

- **managing comprehensive threat solutions**
- ensuring secure routing packet exchanges
- responding to data center physical break-ins
- **monitoring network security threats**
- providing secure Internet connections

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.

16. Users report that a database file on the main server cannot be accessed. A database administrator verifies the issue and notices that the database file is now encrypted. The organization receives a threatening email demanding payment for the decryption of the database file. What type of attack has the organization experienced?

- man-in-the-middle attack
- DoS attack
- **ransomware**
- Trojan horse

A cybersecurity specialist needs to be familiar with the characteristics of the different types of malware and attacks that threaten an organization.

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

- IEEE
- **CompTIA**
- (ISC)²

- GIAC

Explanation: The CompTIA Cybersecurity Analyst (CySA+) certification is a vendor-neutral security professional certification.

18. What was used as a cyberwarfare weapon to attack a uranium enrichment facility in Iran?

- DDoS
- SQL injection
- PSYOPS
- **Stuxnet**

The Stuxnet malware program is an excellent example of a sophisticated cyberwarfare weapon. In 2010, it was used to attack programmable logic controllers that operated uranium enrichment centrifuges in Iran.

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

- firewall appliance
- **security monitoring**
- **log management**
- intrusion prevention
- proxy service
- **threat intelligence**

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
Proxy server, VPN, and IPS are security devices deployed in the network infrastructure.

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

- SOC Manager
- Tier 2 personnel
- Tier 3 personnel
- **Tier 1 personnel**

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

21. Which statement describes cyberwarfare?

- Cyberwarfare is an attack carried out by a group of script kiddies.
- It is a series of personal protective equipment developed for soldiers involved in nuclear war.
- It is simulation software for Air Force pilots that allows them to practice under a simulated war scenario.
- **It is Internet-based conflict that involves the penetration of information systems of other nations.**

Cyberwarfare is Internet-based conflict that involves the penetration of the networks and computer systems of other nations. Organized hackers are typically involved in such an attack.

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

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

In a SOC, a ticketing system is typically used for a work flow management system.

23. What name is given to an amateur hacker?

- red hat
- **script kiddie**
- black hat
- blue team

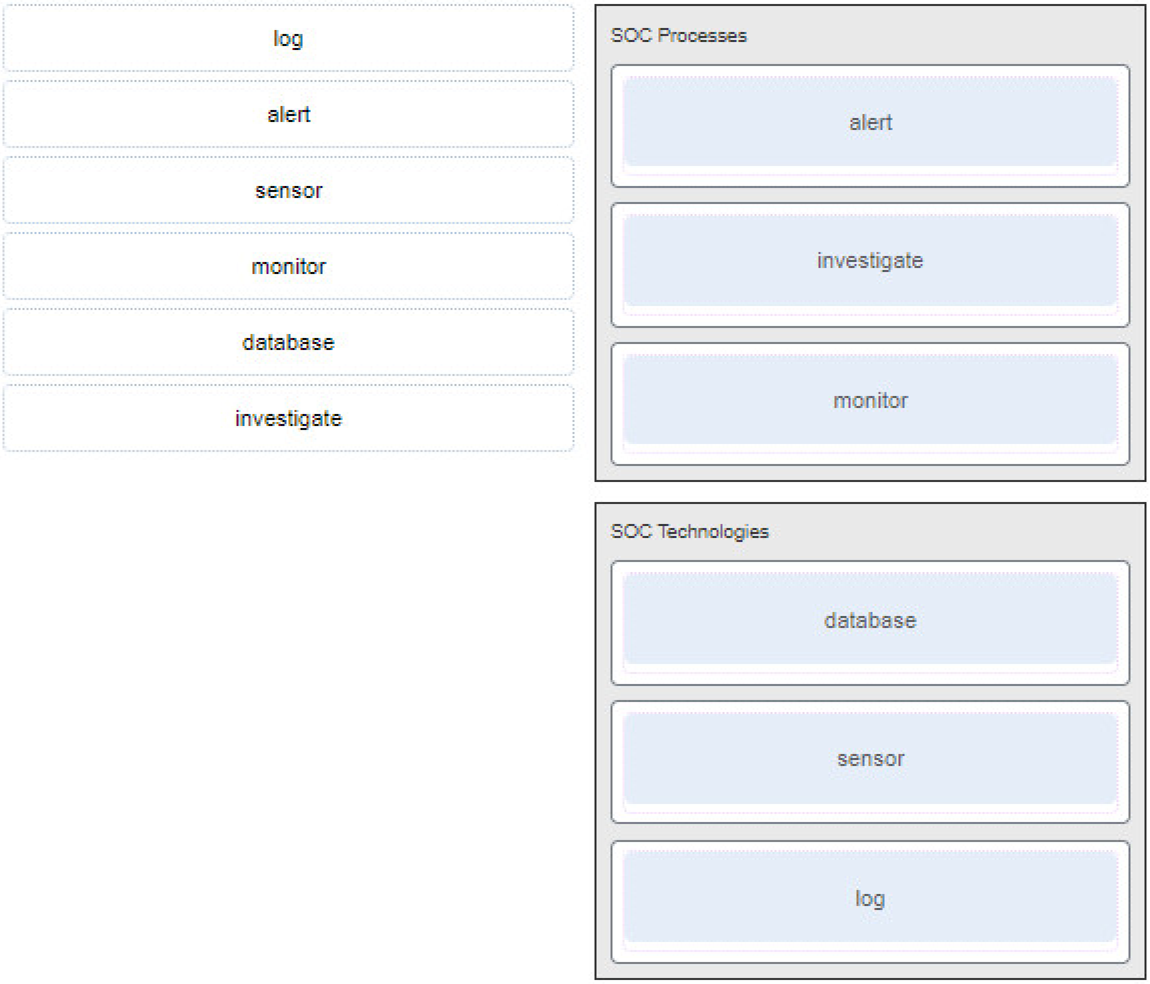
Script kiddies is a term used to describe inexperienced hackers

24. Which personnel in a SOC are assigned the task of hunting for potential threats and implementing threat detection tools?

- Tier 1 Analyst
- SOC Manager
- Tier 2 Incident Reporter
- **Tier 3 SME**

In a SOC, Tier 3 SMEs have expert-level skills in network, endpoint, threat intelligence, and malware reverse engineering (RE). They are deeply involved in hunting for potential security threats and implementing threat detection tools.

25. Match the components to the major categories in a SOC.



log

alert

sensor

monitor

database

investigate

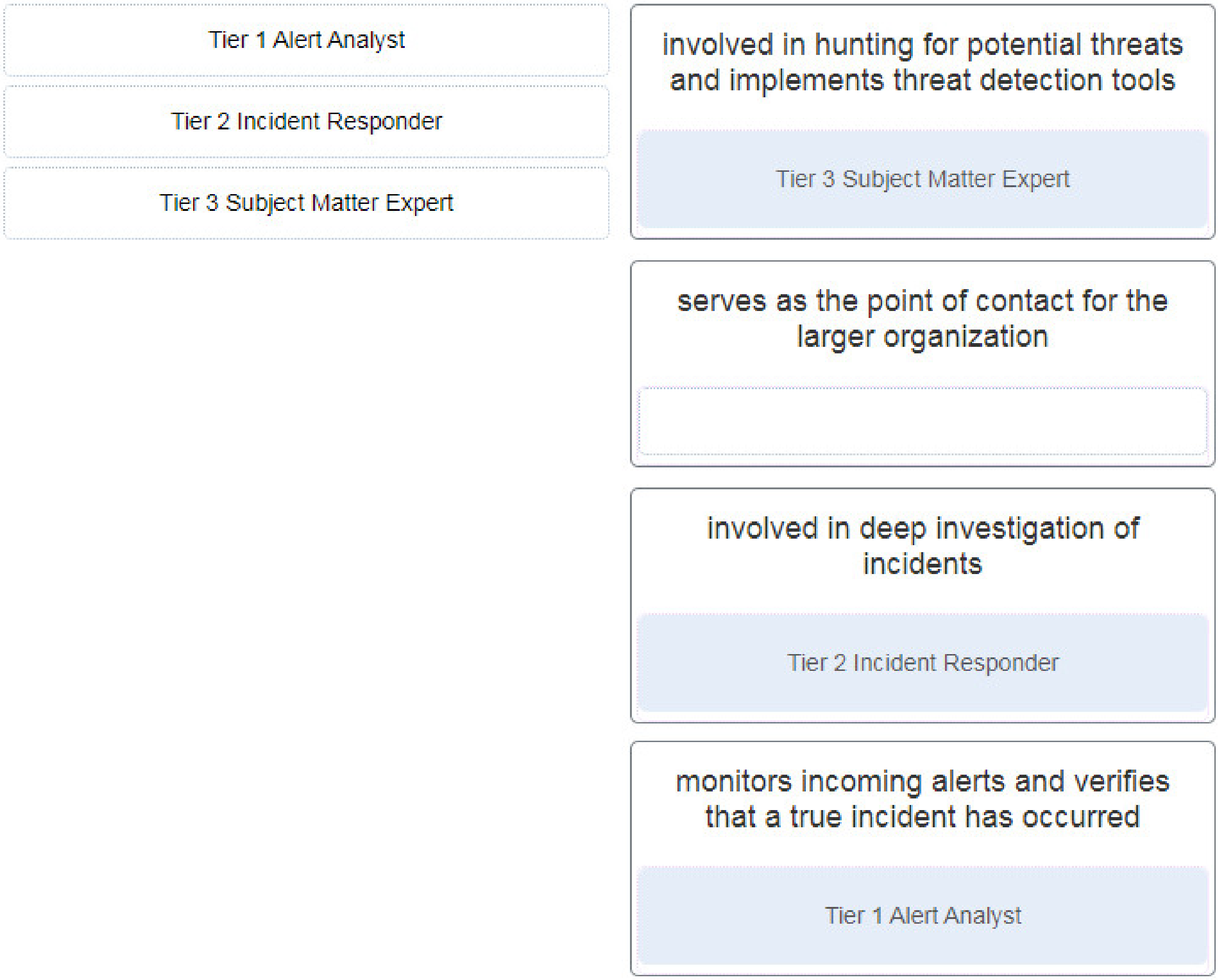
SOC Processes

- alert
- investigate
- monitor

SOC Technologies

- database
- sensor
- log

26. Match the job titles to SOC personnel positions. (Not all options are used.)



Tier 1 Alert Analyst

Tier 2 Incident Responder

Tier 3 Subject Matter Expert

involved in hunting for potential threats and implements threat detection tools

Tier 3 Subject Matter Expert

serves as the point of contact for the larger organization

involved in deep investigation of incidents

Tier 2 Incident Responder

monitors incoming alerts and verifies that a true incident has occurred

Tier 1 Alert Analyst

- Tier 1 Alert Analyst —> monitors incoming alerts & verifies that a true incident has occured
- Tier 2 Incident Responder —> involved in deep investigation of incident
- Tier 3 Subject Matter Expert —> involved in hunting for potential threads & implements thread detection tools
- (not use) —> serve as the point of contact for the large organitazion

27. What name is given to a amateur hacker?

- blue team
- red hat
- **script kiddie**
- black hat

Explanation: Script kiddies is a term used to describe inexperienced hackers.