Congratulations! You passed!

Grade received 100% To pass 75% or higher

Go to next item

1. How do indicators of compromise (IoCs) help security analysts detect network traffic abnormalities? 1 / 1 point

- They confirm that a security incident happened.
- They define the attacker's intentions.
- They capture network activity.
- They provide a way to identify an attack.

Correct
IoCs help security analysts detect network traffic abnormalities by providing a way to identify an attack. IoCs provide analysts with specific evidence associated with an attack, such as a known malicious IP address, which can help quickly identify and respond to a potential security incident.

2. Fill in the blank: Data _____ is the term for unauthorized transmission of data from a system. 1 / 1 point

- pivoting
- exfiltration
- network traffic
- infiltration

Correct
Data exfiltration is the unauthorized transmission of data from a system.

3. An attacker has infiltrated a network. Next, they spend time exploring it in order to expand and maintain their access. They look for valuable assets such as proprietary code and financial records. What does this scenario describe? 1 / 1 point

- Phishing
- Large internal file transfer
- Lateral movement
- Network data

Correct
This scenario describes lateral movement. Lateral movement, also called pivoting, describes an attacker exploring a network with the goal of expanding and maintaining their access.

4. What can security professionals use network traffic analysis for? Select three answers. 1 / 1 point

- [ ] To secure critical assets
- [x] To understand network traffic patterns

Correct
Network traffic analysis provides security professionals with a way to monitor network activity, identify malicious activity, and understand network traffic patterns.

- [x] To identify malicious activity

Correct
Network traffic analysis provides security professionals with a way to monitor network activity, identify malicious activity, and understand network traffic patterns.

- [x] To monitor network activity

Correct
Network traffic analysis provides security professionals with a way to monitor network activity, identify malicious activity, and understand network traffic patterns.