Question 1
How do indicators of compromise (IoCs) help security analysts detect network traffic abnormalities? 1 / 1 point
They capture network activity.
They provide a way to identify an attack.
They define the attacker's intentions.
They confirm that a security incident happened.
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.

Question 2
Fill in the blank: Data _____ is the term for unauthorized transmission of data from a system. 1 / 1 point
exfiltration
infiltration
network traffic
pivoting
Correct
Data exfiltration is the unauthorized transmission of data from a system.

Question 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
Large internal file transfer
Network data
Phishing
Lateral movement
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.

Question 4
What can security professionals use network traffic analysis for? Select three answers. 1 / 1 point
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.
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.
To secure critical assets
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.