Question 1
A security analyst uses a network protocol analyzer to capture HTTP traffic to analyze patterns. What type of data are they using? 1 / 1 point
Host-based
Signature-based
False positive
Network telemetry
Correct
They are using network telemetry data. Network telemetry refers to the collection and transmission of network data for analysis, such as HTTP traffic.

Question 2
Which statement accurately describes the difference between a network-based intrusion detection system (NIDS) and a host-based intrusion detection system (HIDS)? 1 / 1 point
A NIDS is installed on a network; a HIDS is installed on individual devices.
A NIDS uses signature analysis to detect threats; a HIDS uses agents.
A NIDS is installed on individual devices; a HIDS is installed on a network.
A NIDS only detects known threats; a HIDS detects unknown threats.
Correct
A NIDS is installed on a network and is used to collect and monitor network traffic and network data. A HIDS is installed on a host and is used to monitor the activity of the host.

Question 3
Fill in the blank: The _____ component of an IDS signature includes network traffic information. 1 / 1 point
rule options
action
header
signature ID
Correct
The header component of an IDS signature includes network traffic information. This includes source and destination IP addresses, source and destination ports, protocols, and traffic direction.

Question 4
A security analyst creates a Suricata signature to identify and detect security threats based on the direction of network traffic. Which of the following rule options should they use? 1 / 1 point
Message
Rev
Content
Flow
Correct
They should use flow. The flow option matches the direction of network traffic flow.