Question 1
Which tool collects and analyzes log data to monitor critical activities in an organization? 1 / 1 point
Intrusion prevention system (IPS) tool
Intrusion detection system (IDS) tool
Security information and event management (SIEM) tool
Playbook
Correct
SIEM tools collect and analyze log data to monitor critical activities in an organization.

Question 2
Fill in the blank: Security orchestration, automation, and response (SOAR) is a collection of applications, tools, and workflows that uses automation to _____ security events. 1 / 1 point
respond to
interact with
collect
remediate
Correct
SOAR is a collection of applications, tools, and workflows that uses automation to respond to security events.

Question 3
Which step in the SIEM process transforms raw data to create consistent log records? 1 / 1 point
Normalize data
Collect and aggregate data
Analyze data
Centralize data
Correct
During the normalize data step in the SIEM process, raw data is transformed to create consistent log records. The normalization process involves cleaning the data and removing non-essential attributes.

Question 4
What is the process of gathering data from different sources and putting it in one centralized place? 1 / 1 point
Aggregation
Notification
Analysis
Normalization
Correct
Aggregation is the process of gathering data from different sources and putting it in one centralized place.