Question 1
The first phase of the NIST Incident Response Lifecycle is Preparation. What are the other phases? Select three answers. 1 / 1 point
Identify
Containment, Eradication, and Recovery
Correct
The three other phases of the NIST Incident Response Lifecycle are: Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity.
Post-Incident Activity
Correct
The three other phases of the NIST Incident Response Lifecycle are: Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity.
Detection and Analysis
Correct
The three other phases of the NIST Incident Response Lifecycle are: Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity.

Question 2
What type of process is the NIST Incident Response Lifecycle? 1 / 1 point
Linear
Cyclical
Synchronous
Observable
Correct
The NIST Incident Response Lifecycle is a cyclical process. This means that phases in the lifecycle can be revisited or repeated as incident investigations progress.

Question 3
Fill in the blank: An ______ is an observable occurrence on a network, system, or device. 1 / 1 point
analysis
investigation
incident
event
Correct
An event is an observable occurrence on a network, system, or device.

Question 4
A security professional investigates an incident. Their goal is to gain information about the 5 W's, which include what happened and why. What are the other W's? Select three answers. 1 / 1 point
Where the incident took place
Correct
The other W's are: who triggered the incident, when the incident took place, and where the incident took place.
When the incident took place
Correct
The other W's are: who triggered the incident, when the incident took place, and where the incident took place.

Which type of incident it was

Who triggered the incident
Correct
The other W's are: who triggered the incident, when the incident took place, and where the incident took place.