Question 1
Which of the following is an example of a security incident? 1 / 1 point
A user installs a device on their computer that is allowed by an organization's policy.
An unauthorized user successfully changes the password of an account that does not belong to them.
A software bug causes an application to crash.
An authorized user successfully logs in to an account using their credentials and multi-factor authentication.
Correct

Question 2
A security team uses the NIST Incident Response Lifecycle to support incident response operations. How should they follow the steps to use the approach most effectively? 1 / 1 point
Complete the steps in any order.
Overlap the steps as needed.
Skip irrelevant steps.
Only use each step once.
Correct

Question 3
Which core functions of the NIST Cybersecurity Framework relate to the NIST Incident Response Lifecycle? Select two answers. 1 / 1 point
Detect
Correct
Respond
Correct
Discover
Investigate

Question 4
What is a computer security incident response team (CSIRT)? 1 / 1 point

A specialized group of security professionals who focus on incident prevention
A specialized group of security professionals who are solely dedicated to crisis management
A specialized group of security professionals who are trained in incident management and response
A specialized group of security professionals who work in isolation from other departments
Correct

Question 5
Fill in the blank: Incident response plans outline the _____ to take in each step of incident response. 1 / 1 point
procedures
policies
instructions
exercises
Correct

Question 6
What are investigative tools used for? 1 / 1 point
Monitoring activity
Documenting incidents
Managing alerts
Analyzing events
Correct

Question 7
Which statement most accurately describes documentation? 1 / 1 point
It is a standardized format used to record information across all industries.
It can be audio, video, or written instructions used for a specific purpose.
It serves as legal documentation and evidence in official settings.
It is always digital and stored in a centralized database.
Correct

Question 8
What is the difference between an intrusion detection system (IDS) and an intrusion prevention system (IPS)? 1 / 1 point
An IDS stops intrusive activity whereas an IPS monitors system activity and alerts on intrusive activity.
An IDS automates response and an IPS generates alerts.
An IDS monitors system activity and alerts on intrusive activity whereas an IPS stops intrusive activity.
An IDS and an IPS both have the same capabilities.
Correct

Question 9
Which process uses a variety of applications, tools, and workflows to respond to security events? 1 / 1 point
Intrusion detection system (IDS)
Security orchestration, automation, and response (SOAR)
Intrusion prevention system (IPS)
Security information and event management (SIEM)
Correct

Question 10
What happens during the data collection and aggregation step of the SIEM process? Select two answers. 1 / 1 point
Data is collected from different sources.
Correct
Data is analyzed according to rules.
Data is centralized in one place.
Correct
Data is cleaned and transformed.