1. Which of the following statements describe security incidents and events? **1 / 1 point**

- ○ All events are security incidents, but not all security incidents are events.
- ○ Security incidents and events are the same.
- ○ Security incidents and events are unrelated.
- ◉ All security incidents are events, but not all events are security incidents.

✓ **Correct**

2. What is the NIST Incident Response Lifecycle? **1 / 1 point**

- ○ The method of closing an investigation
- ○ The process used to document events
- ○ A system that only includes regulatory standards and guidelines
- ◉ A framework that provides a blueprint for effective incident response

✓ **Correct**

3. Which core functions of the NIST Cybersecurity Framework relate to the NIST Incident Response Lifecycle? **1 / 1 point**

Select two answers.

- ☑ Detect

✓ **Correct**

- ☐ Discover
- ☑ Respond

✓ **Correct**

- ☐ Investigate

4. What are some roles included in a computer security incident response team (CSIRT)? Select three answers. **1 / 1 point**

- ☐ Incident manager
- ☑ Technical lead

✓ **Correct**

- ☑ Security analyst

✓ **Correct**

- ☑ Incident coordinator

✓ **Correct**

5. Fill in the blank: Incident response plans outline the _____ to take in each step of incident response. **1 / 1 point**

- ○ policies
- ○ exercises
- ○ instructions
- ◉ procedures

✓ **Correct**

6. Which of the following best describes how security analysts use security tools? **1 / 1 point**

- ○ They only use detection and management tools during incident investigations.
- ◉ They use a combination of different tools for various tasks.
- ○ They only use documentation tools for incident response tasks.
- ○ They only use a single tool to monitor, detect, and analyze events.

✓ **Correct**

7. Which of the following methods can a security analyst use to create effective documentation? Select two answers. **1 / 1 point**

- [ ] Write documentation using technical language.
- [x] Provide clear and concise explanations of concepts and processes.

Correct

- [ ] Provide documentation in a paper-based format.
- [x] Write documentation in a way that reduces confusion.

Correct

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 monitors system activity and alerts on intrusive activity whereas an IPS stops intrusive activity.
- ○ An IDS and an IPS both have the same capabilities.
- ○ An IDS automates response and an IPS generates alerts.

Correct

9. What is the difference between a security information and event management (SIEM) tool and a security orchestration, automation, and response (SOAR) tool? **1 / 1 point**

- ○ SIEM tools use automation to respond to security incidents. SOAR tools collect and analyze log data, which are then reviewed by security analysts.
- ○ SIEM tools and SOAR tools have the same capabilities.
- ◉ SIEM tools collect and analyze log data, which are then reviewed by security analysts. SOAR tools use automation to respond to security incidents.
- ○ SIEM tools are used for case management while SOAR tools collect, analyze, and report on log data.

Correct

10. What happens during the data collection and aggregation step of the SIEM process? Select two answers. **1 / 1 point**

- [x] Data is centralized in one place.

Correct

- [x] Data is collected from different sources.

Correct

- [ ] Data is cleaned and transformed.
- [ ] Data is analyzed according to rules.