Question 1
Which of the following is an essential part of incident escalation? 1 / 1 point
Communicate a potential security incident to a more experienced team member
Make reactive decisions
Maintain data logs that detail previous security events
Create a visual dashboard that details a solution to the security problem
Correct

Question 2
What does attention to detail and following an organization's security event notification process help you with? 1 / 1 point
Incident escalation
Log monitoring
Security data forensics
Vulnerability scanning
Correct

Question 3
Fill in the blank: Entry-level analysts might need to escalate various incident types, including _____. 1 / 1 point
noncompliance of tax laws
improper usage
mismanagement of funds
missing software
Correct

Question 4
An employee attempting to access software on their work device for personal use can be an example of what security incident type? 1 / 1 point
Unauthorized access
Malware infection
Improper usage
Social engineering
Correct

Question 5
You are alerted that a hacker has gained unauthorized access to one of your organization's manufacturing applications. At the same time, an employee's account has been flagged for multiple failed login attempts. Which incident should be escalated first? 1 / 1 point
The best thing to do is escalate the incident that your supervisor advised you to escalate first.
The incident involving the employee who is unable to log in to their account should be escalated first.
The incident involving the malicious actor who has gained unauthorized access to the manufacturing application should be escalated first.
Both security incidents should be escalated at the same time.
Correct

Question 6
What is the best way to determine the urgency of a security incident? 1 / 1 point
Contact the risk assessment team to determine urgency.
Reach out to the organization's Red Team supervisor to determine urgency.
Email the Chief Information Security Officer (CISO) of the company for clarification.
Identify the importance of the assets affected by the security incident.
Correct

Question 7
What security term is defined as a set of actions that outlines who should be notified when an incident alert occurs? 1 / 1 point
A security risk assessor
A vulnerability scan system
An escalation policy
A network architecture alert
Correct

Question 8
Why is it important for analysts to follow a company's escalation policy? Select two answers. 1 / 1 point
An escalation policy instructs analysts on the right person to contact during an incident.
Correct
An escalation policy can help analysts prioritize which security events need to be escalated with more or less urgency.
Correct
An escalation policy can help analysts determine which tools to use to solve an issue.
An escalation policy can help analysts determine the best way to cross-collaborate with other members of their organization.

Question 9
A new security analyst has just been hired to an organization and is advised to read through the company's escalation policy. What kind of information will the analyst be educated on when reading through this policy? 1 / 1 point
They will learn the best way to communicate with stakeholders.
They will learn the best way to create visual dashboards to communicate with executives.
They will learn when and how to escalate security incidents.
They will learn how to use the Linux operating system.
Correct

Question 10
A security analyst receives an alert that someone has gained unauthorized access to a system with PII. Seconds later, the analyst is alerted that an employee has downloaded unapproved software on their work device. Which incident should be escalated first? 1 / 1 point
Both incidents should be escalated at the same time.
The incident involving unauthorized access to the system with PII should be escalated first.
Neither incident needs to be escalated.
The incident involving an employee downloading unapproved software on their work device should be escalated first.
Correct