Question 1
A security analyst notices that an employee has installed an app on their work device without getting permission from the help desk. The log indicates that potentially malicious code might have been executed on the host. Which of these security events should the security analyst escalate to a supervisor? 1 / 1 point
The employee installing an app without permission should be escalated.
Neither event should be escalated.
The log indicating malicious code might have been executed on the host should be escalated.
Both events should be escalated.
Correct
Both events should be escalated to a supervisor. There are no issues that are too small or too big. It's always best to err on the side of caution and report events to the appropriate team members.

Question 2
Which are types of data and assets that stakeholders are most interested in protecting? Select two answers. 1 / 1 point
Customers' usernames and passwords
Correct
Sensitive financial data and customers' usernames and passwords are examples of data and assets that stakeholders are most interested in protecting.
Sensitive financial data
Correct
Sensitive financial data and customers' usernames and passwords are examples of data and assets that stakeholders are most interested in protecting.
Company policies
Social media presence

Question 3
Fill in the blank: When a security event results in a data breach, it is categorized as a _____. 1 / 1 point
threat
asset
vulnerability
security incident
Correct
When a security event results in a data breach, it is categorized as a security incident. However, if the event is resolved without resulting in a breach, it is not considered an incident.

Question 4
Which of the following are examples of the potential impact of a security incident involving malicious code? Select three answers. 1 / 1 point
Financial consequences
Correct
Operational downtime, financial consequences, and loss of assets are examples of the potential impact of a security incident involving malicious code.

Data protection

Operational downtime
Correct
Operational downtime, financial consequences, and loss of assets are examples of the potential impact of a security incident involving malicious code.

Loss of assets
Correct
Operational downtime, financial consequences, and loss of assets are examples of the potential impact of a security incident involving malicious code.