Free Questions for Lead-Cybersecurity-Manager

Shared by Green on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Scenario 9: FuroDart ts a leading retail company that operates across Europe With over 5Q0 stores In several countries, EuroDart offers an extensive selection of products, including clothing, electronics, home appliances, and groceries. The company's success stems from its commitment to providing its customers with exceptional support and shopping experience.

Due to the growing threats In the digital landscape. EutoDart puls a lot of efforts in ensuring cybersecurity. The company understands the Importance of safeguarding customer data, protecting Its infrastructure, and maintaining a powerful defense against cyberattacks. As such, EuroDart has Implemented robust cybersecurity measures 10 ensure the confidentiality, integrity, and availability of its systems and data

EuroDart regularly conducts comprehensive testing to enhance its cybersecurity posture. Following a standard methodology as a reference for security testing, the company performs security tests on high-risk assets, utilizing its own data classification scheme. Security tests are conducted regularly on various components, such as applications and databases, to ensure their reliability and integrity.

As part of these activities. EuroDart engages experienced ethical hackers to simulate real-world attacks on its network and applications. The purpose of such activities is to identify potential weaknesses and exploit them within a controlled environment to evaluate the effectiveness of existing security measures. EuroDart utilizes a security information and event management (SIEM) system to centralize log data from various sources within the network and have a customizable view for comprehending and reporting Incidents promptly and without delay The SiEM system enables the company to increase productivity and efficiency by collecting, analyzing, and correlating realtime dat

a. The company leverages different dashboards to report on monitoring and measurement activities that are more tied to specific controls or processes. These dashboards enable the company to measure the progress of its short-term objectives.

EuroDart recognizes that the cybersecurity program needs to be maintained and updated periodically. The company ensures that the cybersecurity manager is notified regarding any agreed actions to be taken. In addition, EuroDart regularly reviews and updates its cybersecurity policies, procedures, and controls. The company maintains accurate and comprehensive documentation of its cybersecurity practices including cybersecurity policy, cybersecurity objectives and targets, risk analysis, incident management, and business continuity plans, based on different factors of change, such as organizational changes, changes in the business scope, incidents, failures, test results, or faulty operations. Regular updates of these documents also help ensure that employees are aware of their roles and responsibilities in maintaining a secure environment.

According to scenario 9. which type of dashboards does EuroDart employ?

Options:

A- Operational and tactical

B- Scorecards or strategic

C- Gages and financial reports

Answer:

A

Explanation:

EuroDart employs operational and tactical dashboards. These types of dashboards are used to monitor and measure activities that are closely tied to specific controls or processes, providing real-time data and insights necessary for day-to-day operations and immediate tactical decisions. They enable the company to track the progress of short-term objectives and enhance productivity and efficiency. Reference for the effective use of such dashboards can be found in ISO/IEC 27004, which provides guidelines for monitoring and measuring the effectiveness of information security management systems.

Question 2

Question Type: MultipleChoice

What is EuroDart aiming to achieve by proactively notifying their cybersecurity manager regarding The cybersecurity program hetore implementing any agreed-upon actions? Refer to scenario 9.

Options:

A- Ensure compliance win data privacy regulations and legal requirements

B- Optimize the procedures by reducing the likelihood of overlooking any risks

C- Enhance customer trust and confidence in the company's cybersecurity measures

Answer:

B

Explanation:

By proactively notifying their cybersecurity manager regarding the cybersecurity program before implementing any agreed-upon actions, EuroDart aims to optimize procedures by reducing the likelihood of overlooking any risks. This approach ensures that all potential risks are considered and addressed, leading to more effective and comprehensive cybersecurity measures. It also helps maintain alignment with organizational goals and regulatory requirements. This practice is aligned with ISO/IEC 27001, which emphasizes the importance of risk management and continuous improvement in information security management systems.

Top of Form

Bottom of Form

Question 3

Question Type: MultipleChoice

Scenario 9: FuroDart ts a leading retail company that operates across Europe With over 5Q0 stores In several countries, EuroDart offers an extensive selection of products, including clothing, electronics, home appliances, and groceries. The company's success stems from its commitment to providing its customers with exceptional support and shopping experience.

Due to the growing threats In the digital landscape. EutoDart puls a lot of efforts in ensuring cybersecurity. The company understands the Importance of safeguarding customer data, protecting Its infrastructure, and maintaining a powerful defense against cyberattacks. As such, EuroDart has Implemented robust cybersecurity measures 10 ensure the confidentiality, integrity, and availability of its systems and data

EuroDart regularly conducts comprehensive testing to enhance its cybersecurity posture. Following a standard methodology as a reference for security testing, the company performs security tests on high-risk assets, utilizing its own data classification scheme. Security tests are conducted regularly on various components, such as applications and databases, to ensure their reliability and integrity.

As part of these activities. EuroDart engages experienced ethical hackers to simulate real-world attacks on its network and applications. The purpose of such activities is to identify potential weaknesses and exploit them within a controlled environment to evaluate the effectiveness of existing security measures. EuroDart utilizes a security information and event management (SIEM) system to centralize log data from various sources within the network and have a customizable view for comprehending and reporting Incidents promptly and without delay The SiEM system enables the company to increase productivity and efficiency by collecting, analyzing, and correlating realtime dat

a. The company leverages different dashboards to report on monitoring and measurement activities that are more tied to specific controls or processes. These dashboards enable the company to measure the progress of its short-term objectives.

EuroDart recognizes that the cybersecurity program needs to be maintained and updated periodically. The company ensures that the cybersecurity manager is notified regarding any agreed actions to be taken. In addition, EuroDart regularly reviews and updates its cybersecurity policies, procedures, and controls. The company maintains accurate and comprehensive documentation of its cybersecurity practices including cybersecurity policy, cybersecurity objectives and targets, risk analysis, incident management, and business continuity plans, based on different factors of change, such as organizational changes, changes in the business scope, incidents, failures, test results, or faulty operations. Regular updates of these documents also help ensure that employees are aware of their roles and responsibilities in maintaining a secure environment.

Based on scenario 9, which of the following capabilities does EuroDart's SIEM solution otter?

Options:

A- Threat intelligence

B- Log data management

C- Security and IT Integrations

Answer:

B

Explanation:

EuroDart's SIEM solution offers the capability of log data management. SIEM systems centralize log data from various sources within the network, allowing for comprehensive analysis, correlation, and reporting of security incidents. This capability helps in promptly identifying and responding to potential security threats by providing a customizable view of the log data and facilitating efficient monitoring and measurement activities. Reference include NIST SP 800-137, which covers continuous monitoring and SIEM capabilities for security management.

Question 4

Question Type: MultipleChoice

Scenario 9: FuroDart ts a leading retail company that operates across Europe With over 5Q0 stores In several countries, EuroDart offers an extensive selection of products, including clothing, electronics, home appliances, and groceries. The company's success stems from its commitment to providing its customers with exceptional support and shopping experience.

Due to the growing threats In the digital landscape. EutoDart puls a lot of efforts in ensuring cybersecurity. The company understands the Importance of safeguarding customer data, protecting Its infrastructure, and maintaining a powerful defense against cyberattacks. As such, EuroDart has Implemented robust cybersecurity measures 10 ensure the confidentiality, integrity, and availability of its systems and data

EuroDart regularly conducts comprehensive testing to enhance its cybersecurity posture. Following a standard methodology as a reference for security testing, the company performs security tests on high-risk assets, utilizing its own data classification scheme. Security tests are conducted regularly on various components, such as applications and databases, to ensure their reliability and integrity.

As part of these activities. EuroDart engages experienced ethical hackers to simulate real-world attacks on its network and applications. The purpose of such activities is to identify potential weaknesses and exploit them within a controlled environment to evaluate the effectiveness of existing security measures. EuroDart utilizes a security information and event management (SIEM) system to centralize log data from various sources within the network and have a customizable view for comprehending and reporting Incidents promptly and without delay The SiEM system enables the company to increase productivity and efficiency by collecting, analyzing, and correlating realtime dat

a. The company leverages different dashboards to report on monitoring and measurement activities that are more tied to specific controls or processes. These dashboards enable the company to measure the progress of its short-term objectives.

EuroDart recognizes that the cybersecurity program needs to be maintained and updated periodically. The company ensures that the cybersecurity manager is notified regarding any agreed actions to be taken. In addition, EuroDart regularly reviews and updates its cybersecurity policies, procedures, and controls. The company maintains accurate and comprehensive documentation of its cybersecurity practices including cybersecurity policy, cybersecurity objectives and targets, risk analysis, incident management, and business continuity plans, based on different factors of change, such as organizational changes, changes in the business scope, incidents, failures, test results, or faulty operations. Regular updates of these documents also help ensure that employees are aware of their roles and responsibilities in maintaining a secure environment.

Based on the scenario above, answer the following question:

Which testing technique does EureDart utilize to identify vulnerabilities of its security controls?

Options:

A- Vulnerability assessment

B- Integration testing

C- Penetration testing

Answer:

C

Explanation:

EuroDart utilizes penetration testing to identify vulnerabilities in its security controls. Penetration testing involves simulating real-world attacks on the network and applications to find and exploit potential weaknesses within a controlled environment. This method helps evaluate the effectiveness of existing security measures by identifying and addressing vulnerabilities before they can be exploited by actual attackers. Reference include ISO/IEC 27001 and NIST SP 800-115, which provide guidelines for conducting penetration testing and other security assessments.

Question 5

Question Type: MultipleChoice

Which of the following best describes a computer security incident?

Options:

A- An attacker exploiting a vulnerability to command a botnet and launch a distributed denial-of-service (DUoS) attack on a web server

B- A system crash caused by a power failure or natural disaster that disrupts network operations

C- A mild network glitch or temporary internet interruption

Answer:

A

Explanation:

A computer security incident is best described as an event where an attacker exploits a vulnerability to command a botnet and launch a distributed denial-of-service (DDoS) attack on a web server. This type of incident involves unauthorized access and malicious activity aimed at disrupting the availability of a web service. Such incidents are typically included in the scope of security incidents because they involve breaches of security policy and pose significant risks to the affected systems. Reference include NIST SP 800-61, which defines and categorizes computer security incidents.

Question 6

Question Type: MultipleChoice

What is an advantage of properly implementing a security operations center (SOC) within an organization?

Options:

A- The SOC ensures immediate and absolute prevention of all cybersecurity incidents

B- The SOC promotes seamless collaboration between different teams and departments, enhancing overall organizational security

C- The SOC facilitates continuous monitoring and analysis of an organization's activities, leading to enhanced security incident detection

Answer:

C

Explanation:

Properly implementing a Security Operations Center (SOC) within an organization has the advantage of facilitating continuous monitoring and analysis of the organization's activities, leading to enhanced security incident detection. The SOC acts as a central hub for monitoring, detecting, and responding to security threats in real-time, which is crucial for maintaining the security of an organization's systems and data. This continuous vigilance helps in early detection and rapid response to incidents, thereby reducing potential damage. Reference include NIST SP 800-61, which provides guidelines for establishing and maintaining effective incident response capabilities, including the role of a SOC.

Question 7

Question Type: MultipleChoice

Which of the following standards provides guidelines 10 plan and prepare for Incident response and extract valuable Insights from such responses?

Options:

A- ISO/IEC 27035-1

B- ISO/IEC 27035-2

C- ISO/IEC 27035 3

Answer:

A

Explanation:

ISO/IEC 27035-1 provides guidelines for planning and preparing for incident response and extracting valuable insights from such responses. It focuses on the principles of incident management and establishes a framework for responding to information security incidents. This standard helps organizations develop and implement effective incident response processes and improve their overall security posture through lessons learned from incidents.