Question #1 *Topic 1*

Sophia manages data ingestion for her organization's SIEM. The data science team wants to perform real-time analytics on security data and asks Sophia for a copy of all new endpoint telemetry from the current point forward. The SIEM currently collects 15TB of endpoint telemetry every day.Which of the following solutions can Sophia use to best help the data science team?

A. Export the last 12 months of telemetry data from the SIEM in OCSF.

B. Use a message bus to send data to both the SIEM and data science team.

C. Export the last 12 months of telemetry data from the SIEM in JSON format.

D. Configure the SIEM to export a CSV report of all new telemetry data every night.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

To ensure leadership is aware of the security team's performance, which measurements should be presented on a regular basis? (Choose all that apply.)

A. Patch compliance percentage

B. Mean time to contain

C. Number of emergency change requests

D. Mean time to respond

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Justin has just finished successfully importing data from the CMDB platform into the SIEM. While validating data, he discovers a host with a MAC address (35:33:33:20:76) that does not have the same OUI (03:83:71) as the rest of the deployed devices.Which of the following is the most likely explanation for this discrepancy?

A. CMDB contains data from personal devices managed under MDM

B. CMDB data was normalized during the SIEM import process

C. CMDB data was corrupted during the export process

D. CMDB contains data related to dynamic VPN pool addresses

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Which of the following are common criteria used for the evaluation of threat intelligence feeds? (Choose all that apply.)

A. TLP

B. Industry

C. Source

D. Severity

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Which MLTK command can be combined with tstats in an ES detection to apply a machine learning model to search results?

A. Summary

B. Fit

C. Cluster

D. Sample

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

An architect is planning for a net new SIEM deployment.Which of the following data sources will provide the most immediate security value?

A. Physical access control logs

B. Active Directory logs

C. CMDB logs

D. Security tool alerts

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

How can a threat intelligence team discover additional Indicators Of Compromise (IOCs) from threat actor payloads?

A. Submit the payload to Splunk Intelligence Management.

B. Submit the payload to Mission Control.

C. Submit the payload to Behavioral Analytics.

D. Submit the payload to Splunk Attack Analyzer.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which of the following is the most direct way to measure a detection engineering practice to understand what gaps may exist in security controls and program effectiveness?

A. Measure Mean Time to Detect (MTTD) threats.

B. Measure the number of true positive security alerts created per environment.

C. Measure security control coverage against industry frameworks and organizational risks.

D. Measure the number of detections created per quarter.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Buttercup games has implemented over 100 detections in their SOC. These detections consist mostly of vendor provided signatures and field matching that have been tuned, with a few that have been custom built.What more advanced detection methods should they deploy?

A. Define breaches of static thresholds

B. Enrich with asset and identity information

C. Use an outlier based algorithm

D. Use automation to pull additional data

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

What strategies enable data-driven approaches to evaluating tool efficacy? (Choose all that apply.)

A. Clearly defined outcomes and success criteria

B. Relying on public testimonials and vendor marketing materials

C. Early identification of prioritized requirements and use cases

D. Continuous operational monitoring and metrics collection

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Emma is a security architect helping migrate her organization's on-premises SIEM to a newer version of the same SIEM running in a cloud provider. The newer version includes enhanced capabilities for writing detection content. The detection engineering team has built hundreds of rules in the on-premises SIEM over the years.As Emma starts planning for the migration, what should she do about moving the detection rules to the new platform?

A. Export half of the rules from the SIEM and manually convert them.

B. Nothing, the newer version's default detection content will cover the organization's needs.

C. Export all of the rules from the SIEM in Sigma format and import them into the new platform.

D. Review which rules are still relevant to the organization's threat models to prioritize for migration.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

What is a SBOM?

A. A comprehensive list of components, libraries, and dependencies

B. A comprehensive list of search heads, indexers, and forwarders

C. A comprehensive list of indicators, detections, and alerts

D. A comprehensive list of searches, macros, and reports

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Bocklava, Inc. is looking to launch their Software as a Service in an environment that is accredited against a specific control framework (i.e. PCI, ISO).What is the most effective way to ensure the appropriate controls of this environment are properly funded and implemented?

A. Create a business case for the environment to meet all required controls.

B. Hire a red team assessment to identify gaps.

C. Align the cost of the controls to the revenue generated by the new environment.

D. Ensure all requirements are entered in the ticketing system.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Of the following options, which is the best approach to implementing an effective business continuity plan?

A. Develop the plan based on IT infrastructure.

B. Create a one-time plan.

C. Store data backups offsite.

D. Define recovery objectives and regularly test the plan.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

An alert has generated for a malicious file tied to a previously unknown malware.In order to protect the integrity of the investigation, how can the response team automate collection of evidence?

A. Pull the file from the system and detonate in a sandbox.

B. Pull the file directly from the system and store in a vault.

C. Send the Indicators of Compromise to the law enforcement agency.

D. Quarantine and shut down the system.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

A cybersecurity team is looking to leverage DevSecOps best practices. They want to test new security policies with a small subset of users while monitoring for unusual access patterns or failures.Which of the following techniques will support this? (Choose all that apply.)

A. Infrastructure-as-Code

B. Blue-Green Deployments

C. Canary Releases

D. Automated Rollbacks

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Carter is an architect at an organization drafting design and support documents for a net new SOAR deployment.What does Carter have to take into consideration? (Choose all that apply.)

A. SOAR deployment can connect to the required destinations.

B. Write a request for proposal.

C. The organization has an agreed upon RACI.

D. RBAC controls have been properly defined.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Brian is a security architect at an organization and wants to test the efficacy of the security controls currently being used.Which of the following is the best way this can be achieved?

A. Establish a Red vs Blue program

B. Establish a Red vs Purple program

C. Establish a Blue vs Blue program

D. Establish a Blue vs Purple program

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Which of the following best explains how quantifying the financial impact of a cybersecurity incident can help justify and secure additional budget for the cybersecurity team? (Choose all that apply.)

A. It demonstrates the potential cost savings by preventing incidents, making a strong business case for increased funding.

B. It indicates that only technical improvements matter, not financial considerations.

C. It shows that cybersecurity incidents are unavoidable, so additional budget is necessary.

D. It highlights that cybersecurity spending should be reduced to save costs.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

How can an organization's identity and access management (IAM) architecture enable security orchestration?

A. IAM system logs provide valuable alerts for security orchestration.

B. Allows normal users to bypass IAM controls for faster response to authentication and authorizations.

C. Provides granular permissions to automate disabling accounts, resetting passwords, or changing privileges.

D. Performs changes to IAM system settings to alter authentication methods.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

A SOC engineer, is evaluating how to use artificial intelligence in order to improve how their organization responds to security threats.Which of the following benefits can the engineer realize from augmenting incident response with artificial intelligence?

A. AI will require security analysts to spend more time writing detection rules.

B. AI will automatically respond to and remediate all security events without supervision.

C. AI can write incident reports that analysts do not need to review before publishing.

D. AI can reduce the amount of time analysts spend collecting and correlating data from security tools.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

In a DevSecOps workflow, what is the primary purpose of an automated security gate that detects critical vulnerabilities during a build or deployment?

A. To provide developers with optional warnings about potential security risks without affecting the build or deployment process.

B. To replace manual security audits and eliminate the need for developer security training.

C. To accelerate the software release cycle by bypassing security checks for minor issues.

D. To ensure that only code meeting defined security standards is deployed to production, automatically failing the build or deployment if critical issues are found.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

An organization seeks to improve its cybersecurity posture and risk management strategy by implementing and adhering to NIST CSF Functions (Identify, Protect, Detect, Respond, Recover, Govern) as a shared set of practices and standard vocabulary.In what order should these CSF functions be addressed?

A. In CSF provided order (first to last)

B. Concurrently

C. In a cyclical manner

D. As needed

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

A national retail chain is planning to implement a SIEM to improve its PCI compliance in response to an audit finding.What is a benefit that the SIEM should provide to the organization?

A. Cardholder data is encrypted both in transit and at rest using the latest TLS and AES standards to prevent eavesdropping.

B. Access to cardholder networks and system resources is monitored continuously, and alerts are produced in the case of access anomalies.

C. Card transactions are recorded in a central location for financial reporting.

D. Security controls are routinely tested to ensure they are implemented correctly and continue to function properly.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Yokoco has contracted with Helpime to perform a penetration test. The scope of the test is all web facing internet applications. Helpime has completed the test and provided its report to Yokoco.What should be done with the unremediated findings of this report?

A. They should be shared with regulatory authorities to add to their risk register.

B. They should be entered and tracked in the risk register.

C. They should be reviewed and saved for future reference.

D. They should immediately be shared with all teams that are affected.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

What data normalization standards should be used to enable a wider integration across Splunk's security products? (Choose all that apply.)

A. JSON

B. Open Cybersecurity Schema Framework (OCSF)

C. ORC

D. Common Information Model (CIM)

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Kevin is a SOC analyst working with the SRE team to investigate a report of slow responses from a customer-facing web application. While looking at load balancer and WAF logs, Kevin has discovered that one of the web servers hosting the application has gone offline. He does not see any alerts in the WAF or from the endpoint detection and response agent running on the web server.As part of triaging this incident, what should they do next? (Choose all that apply.)

A. Change the WAF from blocking mode to alert-only mode.

B. Review recently scheduled requests in the company's change management system that may affect the same server.

C. Provision a new server behind the load balancer to return the application to full service.

D. Review system logs collected from the server to identify who last logged into it.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

How can an organization best improve its Mean Time to Respond (MTTR) metrics?

A. Automatically page incident responders when low severity alerts occur.

B. Implement SOAR playbooks to automatically isolate infected endpoints.

C. Use a message bus to stream data to a data lake for trend analysis.

D. Automatically empty spam folders from end users' mailboxes every 30 days.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Which of the following tasks takes the largest portion of a data scientist's time?

A. Building AI agents

B. Data cleaning and preparation

C. Building ML infrastructure

D. Data analysis and modeling

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Buttercup Games' incident response team has found IOC's related to the "Water Curse" campaign within their dev environment. Suspicious activity shows unauthorized access to developer workstations and potential manipulation to their source code in their version control software, GitLow. Given "Water Curse's" known weaponization of open-source dependencies, a forensic investigation is required to determine the breach's full scope, identify affected systems, and collect evidence.To support a forensic investigation into the "Water Curse" compromise at Buttercup Games, what triage steps should be performed? (Choose all that apply.)

A. Immediately re-image all potentially compromised developer workstations.

B. Review recent commits and pull requests from potentially compromised developers.

C. Collect volatile memory and disk images.

D. Analyze the network traffic and focus on deep packet inspection to identify command and control activity.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

A threat hunter is looking for suspicious login activity across multiple different authentication systems and cloud providers. Today, the threat hunter has to query multiple different data sources with unique logic to gather basic information about authentication events.What method provides a simple way to standardize data formats, and look for common activity across different sources?

A. Risk-based alerting

B. Adaptive Response Actions

C. Calculated fields

D. Data normalization

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

A corporation chooses to engage in a Request for Information (RFI) / Request for Proposal (RFP) process.What is a major advantage of this type of formal procurement process?

A. Standardizes vendor responses, making it easier to compare solutions against specific requirements.

B. Speeds up the time it takes to evaluate and stack rank solutions by only consulting third-party analyst rankings.

C. Allows vendors to provide bespoke responses based on a framework that highlights their capabilities best.

D. Eliminates significant amounts of internal paperwork and streamlines the evaluation process.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

Buttercup Games needs to provide its SOC team access to a wide range of security data sources located across different regions and cloud providers.Which architectural solution allows the SOC analysts to query these data sources as a single logical source without having to migrate or copy all the raw data?

A. Data mesh

B. Message bus

C. Centralized data warehouse

D. Federated search

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

An architect is consulting with an organization that requires data to be sent to various destination data stores based on a combination of criteria. This includes, but is not limited to, the presence of personally identifiable information (PII), specific key/value pairs in each event, and the required retention duration for specific data sources.Which of the following types of technology would be most appropriate to address these requirements?

A. Data Vault

B. Data Router

C. Data Warehouse

D. Data Lake

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

A U.S. based company has recently purchased a German company. The U.S. organization is planning to consolidate their customer rewards program globally and begin collecting purchasing information on the German customers to send back to their U.S. data center.Which data privacy law would they violate if they did not update the German End User Agreement?

A. FERPA

B. GDPR

C. HIPAA

D. CCPA

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

While working with the Security Automation team, an architect is reviewing a playbook that automates the handling of compromised credentials. The playbook contains the following stages:Examine account to ensure that it is not a service or control account.Access all identity platforms and lock the user account.Revoke all current sessions (email, VPN, etc.).The architect points out the potential for the compromised credentials to be used remotely again.Which of the following actions need to be added to the playbook to alleviate this?

A. Revoke all users MFA tokens.

B. Create service desk ticket for the locked account.

C. Quarantine compromised users endpoint.

D. Revoke access to code repositories.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

Danielle is a security architect at a multinational retail company. She is evaluating threat intelligence feeds to add to her company's security monitoring program.What is the primary benefit that threat intelligence data can provide?

A. Reduce long term data storage needs.

B. Enrich detections with internal asset information.

C. Add context to detection content.

D. Correlate user activity to security alerts.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Melinda's team is responsible for maintaining detection content for a large organization. Her team consists of ten detection engineers, who need to log in to multiple SIEMs in order to make any changes to rules. Melinda wants to evaluate a "detection as code" methodology using the organization's version control and continuous integration systems.What benefits can detection as code provide her team? (Choose all that apply.)

A. Automated integration can reduce manual errors and speed up deployment.

B. Version control adds the ability to audit and rollback changes.

C. Security events can be triaged and closed more quickly.

D. Reusable components can reduce duplication and simplify rule writing.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Which of the following are key advantages of providing “paved road” security engineering templates? (Choose all that apply.)

A. They enable rapid onboarding of new projects by offering standardized, security-hardened infrastructure patterns.

B. They can integrate with CI/CD pipelines to ensure security and compliance checks are automated as part of the development workflow.

C. They eliminate the need for teams to perform any additional security reviews or testing after initial deployment.

D. They help enforce consistent security controls across diverse environments and reduce human error in manual configuration.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

A new vulnerability has been announced in a software library. Leadership would like to understand what exposure this has caused.What can be used to determine which vendor provided executables use that library?

A. Git file list

B. Vulnerability scan results

C. Release notes

D. Software Bill of Materials

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

The internet facing WAF for a new customer facing application has been identified as a potential telemetry collection point.Which of the following best describes this data prior to any tuning or curation efforts?

A. High Value/Low Noise

B. High Value/High Noise

C. Low Value/High Noise

D. Low Value/Low Noise

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

An organization has decided to implement a new endpoint security product. The CISO has concerns about the rollout due to the nature of the varied endpoint builds and installed applications.After initial testing in lab has shown no issues, what next step should the architect perform to ensure the success of their rollout?

A. Update all applications to their newest versions then perform testing.

B. Iterative testing in lab for each build and then each installed application.

C. Build new “golden” image for testing then deploy it to all hosts.

D. Test with subsets of users from each cross section of builds and applications.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

Which of the following describes CIS controls?

A. A prioritized list of technical security controls that map to ISO standards

B. A collection of administrative security controls that map to NIST guidelines

C. A prioritized list of technical security controls that protect against the most common attack vectors

D. A collection of administrative and technical security controls that map to specific threat models

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

Kevin, a security architect, is planning a long-term retention strategy for security logs (e.g.7+ years) for compliance and forensic purposes.Which storage solutions are cost-effective for this requirement and still allow future access? (Choose all that apply.)

A. Cloud object storage with infrequent access

B. SAN with cold storage tiers

C. SQL data warehouse

D. High performant SSD storage

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

A critical legacy application server runs on an unsupported OS and IT cannot install a security agent or forward logs on this server. This application processes sensitive data.What is the best strategy to continuously monitor the server's activities?

A. Analyze network traffic via a tap.

B. Disconnect the application from the network.

C. Copy and review the access logs on a scheduled basis.

D. Install MCP Security Monitoring.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

TighCo is a multi-national application delivery company that delivers content across the world to millions of users. The company requires all solutions are highly resilient and provide maximum uptime. They are looking to deploy a new security solution to help with authentication abuse. They have identified a solution that can meet their needs with a single appliance.How should they architect this solution?

A. Ensure backups are collected on a nightly basis should the appliance fail.

B. Deploy in the cloud using an auto scaling group.

C. Deploy as a virtual machine.

D. Use object storage as the underlying storage layer for global availability.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

What is the most effective approach to ensure coordinated response and clear communication during a large-scale security incident?

A. Rely on automatic system notifications for all incident communication.

B. Assign an incident commander function and use defined processes and communication channels.

C. Allow teams to respond independently and share updates as needed.

D. Wait to communicate until the incident is fully resolved.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

Hannah is building a data lifecycle management strategy for her organization. She is evaluating data retention requirements such as how and when to delete or destroy data as part of that strategy.What factors must Hannah consider as part of defining data destruction requirements? (Choose all that apply.)

A. The organization can archive data to reduce storage costs without ever needing to delete or destroy it.

B. Compliance and privacy regulations may require that data must be deleted upon customer request.

C. Legal regulations require that data be kept for a minimum period of time.

D. The organization may want to keep data forever in case of future use.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

Britney is an architect designing a network security pattern for deployment across an organization. This will include major sites such as the corporate headquarters in New York and London, as well as smaller sites distributed across the globe. She is considering the requirements for firewalls, intrusion prevention systems, and content filtering systems.What factors does Britney need to address during the design phase to ensure scalability and repeatability across all sites? (Choose all that apply.)

A. Function of device

B. Topological placement of device

C. Vendor of device

D. Model of device

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

When acquiring forensic artifacts, what is a critical step to ensure admissibility in court?

A. Chain of custody

B. Chain of authenticity

C. Chain of authority

D. Chain of artifacts

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

Camille is building the high-level architecture and organizational requirements for a SOC modernization and automation initiative. The organization would like to use Splunk SOAR as the foundation of its new vision and strategy.What are some of the primary objectives this initiative should seek to achieve?

A. Reduced MTTD, Increased MTTR, Reduced Organizational Risk, Broader NIST CSF Coverage

B. Reduced MTTD, Reduced MTTR, Reduced Signal-to-Noise, Increased Analyst Productivity

C. Reduced MTTD, Reduced MTTR, Reduced Alert Fatigue, Increased Analyst Productivity

D. Increased MTTD, Increased MTTR, Reduced Alert Fatigue, Increased Analyst Productivity

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

Which security tool should be implemented as a control during the code check-in and commit process to scan code for vulnerabilities?

A. Style and Development Guide

B. Dynamic Application Security Tool

C. Code Enforcement Management Software

D. Static Application Security Tool

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

What are the benefits of having data in a normalized schema? (Choose all that apply.)

A. Standard field names to reference

B. Data can easily be summarized and/or accelerated

C. Easy to write detections against

D. All raw data fields are searchable

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

Which combination of practices and technologies most effectively creates a scalable, secure “paved road” for cloud-native application development?

A. Using Open Policy Agent (OPA) for policy-as-code enforcement, maintaining versioned architecture blueprints, and creating standardized CI/CD pipeline templates which require vault service usage.

B. Deploying infrastructure-as-code templates for cloud resources, integrating static analysis in the CI pipeline to identify leaked secrets.

C. Adopting Kubernetes network policies for traffic control, recommending use of security scanners in documentation, and allowing teams to select their own methods for policy enforcement.

D. Implementing AWS Identity and Access Management (IAM) policies, publishing infrastructure guidelines on an internal wiki, and using manual peer review to check compliance.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

During a recent incident investigation an analyst noted intellectual property being shared externally with unauthorized parties. Upon reporting this through the appropriate channels, the compliance team has engaged an architect to implement controls to alert on and prevent these email communications.Which type of technical control can be implemented to ensure only authorized intellectual property sharing?

A. SPF

B. DKIM

C. DMARC

D. DLP

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

A corporate cybersecurity team operating within the retail sector finds that its existing cyber threat intelligence (CTI) feeds are noisy and lack relevance to the environment.What type of CTI provider feed, shared among other retail organizations, should they consider to improve their CTI effectiveness?

A. Open Source

B. STIX/TAXII

C. Industry ISAC

D. Internal

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

During a security code review, one of the senior developers complains to the security architect that there have been unauthorized modifications to the code going into the nightly builds.Which of the following methods can ensure only authorized code modifications are part of the nightly builds?

A. Configure the main branch to be protected.

B. Add MFA to developer authentication.

C. Require developer signed commits.

D. Incorporate SAST and DAST into CI/CD pipeline.

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

Which stage in the DevOps CI/CD pipeline is the most effective to generate an SBOM?

A. During the build phase to capture all the dependencies as they are assembled

B. During the UAT phase to capture any inconsistencies

C. When the application is pushed into production

D. During the requirements gathering phase to ensure legal is involved early on in the process

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

An architect is designing controls for an application about to go to production. The architect implemented code scanning early in the pipeline. Now they are looking for a tool that will provide a blackbox analysis of the application at runtime.Which of the following tool types would fit this need?

A. Code Repository YAML (CRY)

B. Repository Analysis Tool (RAT)

C. Static Application Security Tool (SAST)

D. Dynamic Application Security Tool (DAST)

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

Which of the following can be used to identify weak passwords? (Choose all that apply.)

A. ntdsutil

B. Bloodhound

C. Idifde

D. Hashcat

Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!