Question #1 *Topic 1*

A SIEM alert is triggered due to unusual network traffic involving NetBIOS. The System log shows that “The TCP/IP NetBIOS Helper service entered the running state”. Concurrently, Event Code 4624: “An account was successfully logged on” appears for multiple machines within a short time frame. The logon type is identified as 3 (Network logon). Which of the following security incidents is the SIEM detecting?

A. A user connecting to shared files from multiple workstations

B. A malware infection spreading via SMB protocol

C. A network administrator conducting routine maintenance

D. An attacker performing lateral movement within the network

Suggested Answer: *D*

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

Question #2 *Topic 1*

A manufacturing company is deploying a SIEM system and wants to improve both its security monitoring and regulatory compliance capabilities. During the planning phase, the team decides to use an output-driven approach, starting with use cases that address unauthorized access to production control systems. They configure data sources and alert specific to this use case, ensuring they receive actionable alerts without excessive false positives. After validating its success, they move on to use cases related to supply chain disruptions and malware detection. Which of the following best describes the primary advantage of using an output-driven approach in SIEM deployment?

A. The company can collect logs from non-critical systems.

B. The SOC team can respond to all incidents in real time without delays.

C. The SIEM system can automatically block all unauthorized access attempts.

D. The company can create more complex use cases with greater scope.

Suggested Answer: *D*

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

Question #3 *Topic 1*

An attacker attempts to gain unauthorized access to a secure network by repeatedly guessing login credentials. The SIEM is configured to generate an alert after detecting 10 consecutive failed login attempts within a short timeframe. However, the attacker successfully logs in on the 9th attempt, just before the threshold is reached, bypassing the alert mechanism. Security teams only become aware of the incident after detecting suspicious activity post-login, highlighting a gap in the SIEM's detection rules. What type of alert classification does this represent?

A. True Positive

B. False Positive

C. False Negative

D. True Negative

Suggested Answer: *C*

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

Question #4 *Topic 1*

Daniel Clark, a cybersecurity specialist working in the Cloud SOC for a government agency, is responsible for ensuring secure access to cloud applications while maintaining compliance with regulatory frameworks. His team needs a security solution that can enforce access policies to prevent unauthorized access to cloud based applications, monitor and restrict data sharing within SaaS, PaaS, and IaaS environments, ensure compliance with government regulations for data security and privacy, and apply security controls to prevent sensitive data exposure in the cloud. To achieve these objectives, the team has implemented a security technology that governs control over cloud resources, applies security policies, and protects sensitive cloud-stored data. Which Cloud SOC technology is Daniel's team using?

A. Cloud Security Posture Management

B. Cloud-native anomaly detection

C. Cloud Workload Protection Platform

D. Cloud Access Security Broker

Suggested Answer: *D*

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

Question #5 *Topic 1*

A mid-sized healthcare organization is facing frequent phishing and ransomware attacks. They lack an internal SOC and want proactive threat detection and response capabilities. Compliance with HIPAA regulations is essential. The organization seeks a solution that includes both monitoring and rapid response to incidents. Which service best meets their needs?

A. MSSP with 24/7 log monitoring and incident escalation

B. Self-hosted SIEM with in-house SOC analysts

C. MDR with proactive threat hunting and incident containment

D. Cloud-based SIEM with MSSP-Managed services

Suggested Answer: *C*

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

Question #6 *Topic 1*

A Security Operations Center (SOC) analyst receives a high-priority alert indicating unusual user activity. An employee account is attempting to access company resources from a different country and outside of their normal working hours. This behavior raises concerns about potential account compromise or unauthorized access to automate the initial response and quickly restrict access while further investigating the incident, which SOAR Playbook would be relevant to adapt and implement?

A. Deprovisioning Users SOAR Playbook

B. Phishing Investigations SOAR Playbook

C. Alert Enrichment SOAR Playbook

D. Malware Containment SOAR Playbook

Suggested Answer: *A*

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

Question #7 *Topic 1*

A government agency responsible for protecting sensitive information needs to monitor its network for unusual data exfiltration attempts. Since traditional log data alone is insufficient to identify suspicious traffic patterns, the SIEM team decides to integrate traffic flow data into their system. This data will help detect anomalies, such as large data transfers to unauthorized destinations or unexpected traffic spikes. The team must choose the appropriate protocol to collect IP traffic information from network devices like routers and switches. Which protocol should be used to collect this data?

A. Syslog

B. SNMP (Simple Network Management Protocol)

C. IPFIX (IP Flow Information Export)

D. Net Flow (RFC 3954)

Suggested Answer: *C*

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

Question #8 *Topic 1*

SecureTech Solutions, a managed security service provider (MSSP), is optimizing its log management architecture to enhance log storage, retrieval, and analysis efficiency. The SOC team needs to ensure that security logs are stored in a structured or semi-structured format, allowing for easy parsing, querying, and correlation of security events. To achieve this, they decide to implement a log storage format that organizes data in a text file in tabular structure, ensuring each log entry is stored in rows and columns. Additionally, they require a format that supports easy export to databases or spreadsheet-based analysis while maintaining readability. Which log format should the SOC team choose to store logs in a structured or semi structured format for efficient analysis?

A. Syslog Format

B. Cloud Storage

C. Comma-Separated Values (CSV) Format

D. Database

Suggested Answer: *C*

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

Question #9 *Topic 1*

A large web hosting service provider Web4Everyone is responsible for hosting multiple major websites, social media platforms and more. You are working here as a L1 SOC analyst responsible for investigating web server logs for potential malicious activity. Recently, your team detected multiple failed login attempts and unusual traffic patterns targeting the company's web application. To efficiently analyze the logs and identify key details such as the remote host, username, timestamp, requested resource, and HTTP status code, and user-agent you need a structured log format that ensures quick and accurate parsing. Which standardized log format will you choose for this scenario?

A. Extended Log Format (ELF)

B. Tab-Separated Format

C. Common Log Format (CLF)

D. JSON Format

Suggested Answer: *A*

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

Question #10 *Topic 1*

At 10:30 AM, during routine monitoring, SOC's Tier-1 Jennifer detects unusual network traffic and confirms an active LockBit ransomware infection targeting systems in the finance department. She escalates the issue to the SOC lead, Sarah, who activates the Incident Response Team (IRT) and instructs the network team to isolate the finance department's VLAN to prevent further spread across the network. Which phase of the Incident Response process is currently being implemented?

A. Notification

B. Evidence Gathering and Forensic Analysis

C. Eradication

D. Containment

Suggested Answer: *D*

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

Question #11 *Topic 1*

A SOC analyst is responsible for designing a security dashboard that provides real-time monitoring of security threats. The organization wants to avoid overwhelming analysts with excessive information and focus on the most critical security alerts to ensure timely responses to potential threats. Which principle should guide the design of the dashboard?

A. Restrict dashboard access to only network administrators

B. Prioritize critical information and remove unnecessary details

C. Include as much data as possible to ensure complete visibility

D. Use only historical data to avoid real-time inconsistencies

Suggested Answer: *B*

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

Question #12 *Topic 1*

The Security Operations Center (SOC) team at Rapid Response Group, a leading cybersecurity firm, is facing challenges in managing security incidents efficiently. With an increasing volume of alerts and security events being generated daily in their Microsoft Sentinel environment, the team is struggling to respond to threats quickly and consistently. To enhance their incident response capabilities, they aim to automate routine security tasks, such as log collection, alert triaging, remediation steps, and notifications to stakeholders. By implementing automated workflows, they seek to reduce response times, eliminate manual intervention for repetitive actions, and ensure a standardized approach to handling security threats across the organization. Which component of Microsoft Sentinel should they utilize to create these automated workflows for incident response?

A. Playbooks

B. Community

C. Workspace

D. Analytics

Suggested Answer: *A*

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

Question #13 *Topic 1*

The SOC team found a suspicious document file on a user's workstation. Upon initial inspection, the document appears benign, but deeper analysis reveals an embedded PowerShell script. The team suspects the script is designed to download and execute a malicious payload. They need to understand the script's functionality without triggering it. Which malware analysis technique would be recommended technique for the SOC team to understand the PowerShell script's functionality without executing it?

A. Automated behavioral analysis

B. Network traffic analysis

C. Dynamic analysis

D. Static analysis

Suggested Answer: *D*

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

Question #14 *Topic 1*

A major financial institution has strict policies preventing unauthorized data transfers. As a SOC analyst, you are conducting routine log analysis when you detect an anomaly – an employee's workstation is initiating large file transfers outside of business hours. The files in question contain highly sensitive customer financial records. Upon further investigation, you discover that the employee has been remotely accessing the system from an unfamiliar IP address. Security logs also flag an unauthorized USB device connected to the workstation, violating corporate policy. Given the nature of the data involved and the possibility of data exfiltration, you need to act swiftly. What will be your first step in responding to this incident?

A. Isolate employee's workstation and revoke remote access

B. Conduct a full forensic analysis first

C. Inform employee's department and wait for evidence

D. Disable corporate VPN entirely

Suggested Answer: *A*

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

Question #15 *Topic 1*

Jannet works in a multinational corporation that operates multiple data centers, cloud environments, and on-premises systems as a SOC analyst, she notices that security incidents are taking too long to detect and investigate. After analyzing this, she discovers that logs from firewalls, endpoint security solutions, authentication servers, and cloud applications are scattered across different systems in various formats hence her team has to manually convert logs into a readable format before investigating incidents. What approach should she implement to enable accepting the logs from heterogeneous sources with different formats and converting them into common format and improving incident detection and response time?

A. Log normalization

B. Log transformation

C. Log collection

D. Log correlation

Suggested Answer: *A*

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

Question #16 *Topic 1*

A security team is tasked with configuring a newly deployed SIEM system. With limited resources, they must prioritize specific monitoring scenarios that provide the greatest security benefit. The team understands that an effective SIEM relies on well-defined use cases tailored to the organization's environment. Given the evolving threat landscape, they must carefully choose which use cases to implement first to maximize value and threat detection capabilities. Which factor should guide their selection of use cases?

A. Focus on use cases required to meet industry compliance standards.

B. Select use cases based on the availability and quality of data from existing data sources.

C. Prioritize use cases that address zero day attacks.

D. Implement as many use cases as the SIEM supports to cover all threats.

Suggested Answer: *B*

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

Question #17 *Topic 1*

Bob is a SOC analyst in a multinational corporation that relies on a centralized file-sharing system for storing confidential project documents. One morning, he notices that few critical financial records stored on the shared server appear to have been altered without authorization. Upon further analysis, he discovers that the version history confirms unexpected changes made outside of business hours. Now he must investigate by inspecting the logs. Which log should he check to determine who accessed the files and when the modifications occurred?

A. Authentication logs

B. Firewall logs

C. Security logs

D. Network logs

Suggested Answer: *C*

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

Question #18 *Topic 1*

SecureTech Inc., a leading cybersecurity-focused organization, operates its critical infrastructure and applications in AWS. The Security Operations Center (SOC) team is responsible for detecting, investigating, and mitigating security threats within their cloud environment. Recently, the SOC team has observed an increase in suspicious activities, such as unexpected API calls, unusual outbound traffic from instances, and DNS requests to potentially malicious domains. To enhance their threat detection capabilities, they need a fully managed AWS security service that can continuously monitor for malicious activity across their AWS environment, analyze AWS CloudTrail logs, VPC Flow Logs, and DNS query logs, leverage machine learning and threat intelligence to identify advanced threats, and provide actionable security findings to accelerate response efforts. Which AWS service is best suited to help SecureTech Inc. proactively detect and respond to security threats in their AWS environment?

A. AWS Config

B. Amazon GuardDuty

C. AWS Security Hub

D. Amazon Macie

Suggested Answer: *B*

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

Question #19 *Topic 1*

As a SOC Administrator at a mid-sized financial institution, you noticed intermittent network slowdowns and unexplained high memory usage across multiple critical systems. Your initial analysis found no traces of malware, but a forensic investigation revealed unauthorized scheduled tasks that executed during off-peak hours. These tasks ran obfuscated scripts that connected to an external C2 server. Further investigations showed that the adversary had gained access months ago through a compromised VPN account, leveraging stolen credentials from a phishing campaign. Which phase of the Advanced Persistent Threat (APT) lifecycle does this scenario align with?

A. Persistence

B. Cleanup

C. Search and Exfiltration

D. Initial Intrusion

Suggested Answer: *A*

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

Question #20 *Topic 1*

An organization with a complex IT infrastructure is planning to implement a SIEM solution to improve its threat detection and response capabilities. Due to the scale and complexity of its systems, the organization opts for a phased deployment approach to ensure a smooth implementation and reduce potential risks. Which of the following should be the first phase in their SIEM deployment strategy?

A. Configure security analytics to identify potential threats

B. Set up the log management component before deploying the SIEM component

C. Implement User and Entity Behavior Analytics (UEBA)

D. Automate incident response processes

Suggested Answer: *B*

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

Question #21 *Topic 1*

During a routine security audit, analysts discover that several of the organization's web servers are still using a vulnerable third-party library flagged for a zero-day exploit. This vulnerability was identified in a previous audit, and patches were initially deployed to mitigate the risk. However, due to reported application instability and compatibility issues, the application team rolled back the patches, leaving the systems exposed. Despite the known risk, the vulnerability remains unaddressed, and no alternative mitigations have been put in place. Given the state of the web servers and their reliance on outdated, vulnerable software, how should the security team classify this risk in the context of web application security?

A. Vulnerable and Outdated Components

B. Software and Data Integrity Failures

C. Security Logging and Monitoring Failures

D. Insecure Design

Suggested Answer: *A*

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

Question #22 *Topic 1*

The SOC team at a national cybersecurity agency has detected anomalous network traffic originating from a sensitive government server. Initial analysis suggests a potential intrusion, leading the SOC team to escalate the incident to the forensic team for deeper investigation. Upon forensic examination, the team discovers a trojan on the compromised server. The trojan is suspected of engaging in data exfiltration, raising concerns about potential backdoor access and long-term persistence mechanisms employed by the malware. Given the severity of the situation, the lead malware analyst is tasked with conducting an in-depth analysis of the trojan to determine its capabilities (e.g., command execution, privilege escalation, keylogging), its persistence mechanisms (e.g., registry modifications, scheduled tasks, startup entries), and any backdoor functionalities (e.g., remote access, hidden communication channels). However, due to the sensitive nature of the system and the risk of unintended execution, the analyst must analyze the trojan's binary code at the instruction level without actually executing it. Which technique should the forensic analyst use?

A. Malware Disassembly

B. Network Behavior Monitoring

C. Dynamic Code Injection

D. Interactive Debugging

Suggested Answer: *A*

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

Question #23 *Topic 1*

A SOC team at a major financial institution detects unauthorized access attempts on its web application. The security team reviews the logs to find the web application is compromised. To determine the exact attack technique used and implement necessary mitigation measures, the forensic investigators is assessing cookie attributes (such as HttpOnly, Secure, and SameSite) for security weaknesses, and track anomalous request patterns that deviate from normal user behavior. Which of the following attack vectors is the forensic team investigating in the above investigation?

A. SQL Injection

B. Cross-Site Scripting (XSS)

C. Man-in-the-Middle (MITM) Attack

D. Session Poisoning

Suggested Answer: *D*

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

Question #24 *Topic 1*

A security operations center (SOC) team is investigating a phishing attack that targeted multiple employees. During the Containment Phase, they need to determine how users interacted with the malicious email, whether they opened it, clicked on links, downloaded attachments, or entered credentials. This information is critical to assessing the impact and preventing further compromise. Which specific activity helps the SOC team understand user interactions with the phishing email?

A. User action verification.

B. Blocking C2 and email traffic.

C. Monitoring and containment validation.

D. Malware infection check.

Suggested Answer: *A*

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

Question #25 *Topic 1*

Lisa Carter, a SOC analyst at a financial services firm, is performing a risk assessment following a series of suspicious alerts detected by the SIEM (Security Information and Event Management) system. Her task is to evaluate the risk of a potential data breach prioritizing incident response efforts. She assesses three key factors: the likelihood of an attack succeeding based on current threat intelligence, the impact on critical business operations if the breach occurs, and the value of the assets targeted (e.g., customer data, financial systems). Using the standard risk assessment formula, which of the following scenarios represents the highest risk to the organization?

A. Low Likelihood, High Impact, Low Asset Value

B. High Likelihood, High Impact, High Asset Value

C. Low Likelihood, Low Impact, High Asset Value

D. High Likelihood, Low Impact, High Asset Value

Suggested Answer: *B*

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

Question #26 *Topic 1*

A rapidly growing e-commerce company wants to implement a SIEM solution to improve its security posture and comply with PCI DSS requirements. They need a solution that offers both the necessary technological features and the expertise to manage the system effectively. They also need to ensure continuous compliance support and data security assistance. Which of the following SIEM solutions is appropriate for this company?

A. Security analytics

B. Managed SIEM

C. In-house SIEM

D. Cloud-based SIEM

Suggested Answer: *B*

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

Question #27 *Topic 1*

A multinational corporation with strict regulatory requirements (e.g., GDPR, PCI-DSS) needs a SIEM solution to monitor its global network. Data residency laws in certain regions prohibit transferring logs outside local jurisdictions. The company also requires centralized monitoring with 24/7 SOC operations but has limited in-house SIEM expertise. Which SIEM deployment model is appropriate in the given scenario?

A. Cloud, MSSP-Managed

B. Self-hosted, MSSP-Managed

C. Self-hosted, Jointly Managed

D. Hybrid Model, Jointly Managed

Suggested Answer: *B*

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

Question #28 *Topic 1*

You are working as a SOC analyst in a multinational company with multiple data centers and remote offices. Security logs are stored locally at each site, making it difficult to correlate incidents across different locations. Recently, an advanced persistent threat (APT) compromised multiple servers, but due to multiple sources of logs and inconsistent monitoring, the attack was detected only after significant data exfiltration had occurred. To improve visibility, streamline log analysis, and enable faster incident response, you need to implement a solution that aggregates logs from all sources into a unified system. Which solution will you implement for your organization?

A. Local logging

B. Event tracing

C. Distributed logging

D. Centralized logging

Suggested Answer: *D*

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

Question #29 *Topic 1*

The Security Operations Center (SOC) team is investigating a suspected malware incident during the Analysis Phase of their incident response process. Their primary goal is to validate the initial detection, ensure the threat is real, and gather critical intelligence to understand the scope of the attack. Which of the following actions should the SOC team take to confirm their initial findings and eliminate false alarms?

A. Verify generated logs

B. Scan the enterprise environment and update the scope

C. Root-cause analysis

D. Verify false positives

Suggested Answer: *D*

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

Question #30 *Topic 1*

Katie is working in the Cyber Security department of an international Financial Corporation INT FIN Corp. as a SOC analyst. She is responsible for monitoring logs to detect potential security threats in real time. Her team needs to implement a functionality as part of incident response plan such that the system that it continuously scans logs for anomalies, identifies suspicious activities, and want to be notified when predefined security thresholds are reached as well as generate incidents or issue tickets to ensure immediate response and mitigation. It must provide critical details such as the type of event, its duration, the affected device, and its OS version. Which function should she configure to achieve this?

A. Alerting and Reporting

B. Log collection

C. Log parsing

D. Log normalization

Suggested Answer: *A*

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

Question #31 *Topic 1*

A large financial institution receives thousands of security logs daily from firewalls, IDS systems, and user authentication platforms. The SOC team uses an AI-driven SIEM system with NLP capabilities to streamline threat detection. This approach enables faster response times, reduces manual rule creation, and helps detect advanced threats that traditional systems might overlook. Which of the following BEST illustrates the advantage of NLP in SIEM?

A. Enables analysis of text-based data from logs and communications to detect threats

B. Eliminates the need for data normalization and correlation in SIEM systems

C. Allows security analysts to write SIEM rules using complex programming languages

D. Simplifies infrastructure management by reducing hardware dependencies

Suggested Answer: *A*

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

Question #32 *Topic 1*

A large financial organization has recently experienced an increase in sophisticated cyber threats, including zero-day attacks and advanced persistent threats (APTs). The security team is struggling with traditional detection methods, which rely heavily on signature-based detection and manual intervention, causing delays in identifying and mitigating threats. To enhance their security posture, the Chief Information Security Officer (CISO) is exploring AI-driven solutions that can automatically analyze vast datasets, detect anomalies, and adapt to evolving threats in real time. The goal is to implement a system that can identify suspicious activity without predefined signatures, allowing for faster response times and minimal human oversight. Which key AI technology should the organization focus on to achieve this?

A. Natural Language Processing (NLP)

B. Heuristic-based Signature Detection

C. Machine Learning (ML)

D. Static IP Blocking

Suggested Answer: *C*

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

Question #33 *Topic 1*

CyberBank, a leading financial institution, has recently experienced a series of cyberattacks, including phishing campaigns, insider threats, and attempted data breaches targeting customer financial records. The bank operates across multiple regions, making it vulnerable to regional compliance violations, fraud attempts, and advanced persistent threats (APTs). During a board meeting, the CISO proposes a security solution that offers continuous security monitoring, rapid threat detection, and centralized visibility across all branches. Which of the following solution will provide automated alerting, digital forensics capabilities, and active threat hunting?

A. Implementing Security Operation Center (SOC)

B. Deploying a standalone SIEM (Security Information and Event Management) system

C. Implementing SOAR (Security Orchestration, Automation, and Response)

D. Implementing periodic security audit

Suggested Answer: *A*

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

Question #34 *Topic 1*

A SOC analyst receives an alert indicating that the system time on a critical Windows server was changed at 3:00 AM. There are no scheduled maintenance tasks at this time. Unauthorized time changes can be used to evade security controls, such as altering timestamps to obscure malicious activity. The analyst must identify the relevant event codes that log system time modifications and related suspicious behavior. Which of the following Windows Security Event Codes should the analyst review to investigate potential tampering?

A. 4625 and 4634

B. 4616 and 4618

C. 4616 and 4624

D. 4608 and 4609

Suggested Answer: *B*

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

Question #35 *Topic 1*

A security analyst working in a multinational corporation's Threat Intelligence team is tasked with enhancing the organization's ability to detect stealthy malware infections. During an investigation, the analyst observes an unusually high volume of DNS requests directed toward domains that follow patterns commonly associated with Domain Generation Algorithms (DGAs). Recognizing that these automated domain queries could indicate a malware strain attempting to establish communication with its Command & Control (C2) infrastructure, the analyst realizes that existing detection capabilities may not be sufficient. To effectively counter such threats, the security team needs to define intelligence requirements – including identifying critical data sources, refining detection criteria, and improving threat monitoring strategies. Which stage of the Cyber Threat Intelligence (CTI) process does this scenario align with?

A. Requirement Analysis

B. Filtering CTI

C. Intelligence Buy-In

D. Automated tool

Suggested Answer: *A*

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

Question #36 *Topic 1*

A large financial institution, SOC has recently identified a sophisticated phishing campaign targeting its employees, resulting in unauthorized access to sensitive customer data. The SOC team is under pressure to enhance their detection and response capabilities to manage this evolving threat. The organization already uses a SIEM system for log aggregation and alerting, alongside an EDR solution for endpoint visibility. Additionally, they have access to XDR for broader threat detection and XSOAR for security orchestration and automation. As a SOC analyst, you've been asked to recommend an integration strategy to improve real-time threat correlation, streamline incident response workflows, and maximize the use of existing tools. Which of the following integrations would meet these goals?

A. Integrate XDR with SIEM

B. Integrate XDR with XSOAR

C. Integrate EDR with XSOAR

D. Integrate EDR with SIEM

Suggested Answer: *B*

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

Question #37 *Topic 1*

Global Bank, a large financial institution, relies heavily on Microsoft Azure to host its critical banking applications and services, including customer transactions, financial data processing, and risk assessment systems. Given the highly regulated nature of the banking industry, the security operation center team must ensure continuous monitoring, compliance with financial regulations, and real-time threat detection across all Azure resources. To achieve this, the team requires a comprehensive solution that can collect, analyze, and visualize telemetry data from various cloud resources, virtual machines, storage accounts, and applications. The solution must also integrate seamlessly with their security tools, allowing them to detect anomalies, monitor performance, and respond proactively to potential security threats. Which Azure service is best suited to in the given situation?

A. Azure Monitor

B. Azure Policy

C. Azure Firewall

D. Azure Active Directory

Suggested Answer: *A*

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

Question #38 *Topic 1*

DNS logs in the SIEM show an internal host sending many DNS queries with long, encoded subdomains to an external domain. The queries predominantly use TXT records and occur during off-business hours. The external domain is newly registered and has no known business association. Which of the following best explains this behaviour?

A. Monitoring DNS cache poisoning attempts

B. Detecting rogue DNS servers within the internal network

C. Validating DNS records for legitimate business operations

D. Identifying DNS tunneling for data exfiltration

Suggested Answer: *D*

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

Question #39 *Topic 1*

Jennifer, a SOC analyst, initiates an investigation after receiving an alert about potential unauthorized activity on Marcus's workstation. She starts by retrieving EDR logs from the endpoint, analyzing network traffic patterns in the Security Information and Event Management (SIEM) system, and inspecting email gateway logs for signs of malicious attachments. Her objective is to determine whether this alert represents a legitimate security incident. In which phase of the Incident Response process is Jennifer currently operating?

A. Notification

B. Incident Triage

C. Evidence Gathering and Forensic Analysis

D. Incident Recording and Assignment

Suggested Answer: *C*

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

Question #40 *Topic 1*

Secuzin Corp., is a large enterprise performing millions of financial transactions daily, making it critical to analyze security logs efficiently, detect suspicious activities, and respond to incidents in real-time. Its SOC is responsible for managing security logs from various network devices, including firewalls, intrusion detection systems (IDS), authentication servers, and cloud services. As part of their SOC team to fulfill their compliance and regulatory requirements that mandate long-term archival of the logs you need to provide a log storage solution which should be scalable to handle increasing log volumes, provide encryption for data security, and should be seamlessly accessible. Which storage solution you must choose to meet these long-term log storage requirements?

A. Hybrid storage system

B. Cloud storage

C. Distributed storage system

D. Local storage

Suggested Answer: *B*

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

Question #41 *Topic 1*

The SOC team is tasked with enhancing the security of an organization's network infrastructure. The organization's public-facing web servers, which handle customer transactions, need to be isolated from the internal private network containing sensitive employee data and proprietary systems. The goal is to create a buffer zone that limits exposure of internal systems if the web servers are compromised during a cyberattack, such as a DDoS or SQL injection attempt. As a SOC analyst, which network architecture component would you recommend implementing to establish this isolated region?

A. Intrusion Detection Systems (IDS)

B. Honeypot

C. De-Militarized Zone (DMZ)

D. Firewall

Suggested Answer: *C*

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

Question #42 *Topic 1*

The SOC analyst at a national cybersecurity agency detected unusual system behavior on critical infrastructure servers. Initial scans flagged potential malware activity. Due to the sophisticated nature of the suspected attack, which included registry key modifications, process injection, and unauthorized tasks, the case was escalated to the forensic team. The forensic team suspects the malware is designed for stealthy data exfiltration. To fully assess the compromise, they captured system snapshots before and after suspected infection to identify unauthorized changes and anomalies. Which process is the forensic team following by capturing and comparing system snapshots to detect unauthorized changes and anomalies?

A. Host integrity monitoring

B. Signature-based detection

C. Digital forensics

D. Threat intelligence gathering

Suggested Answer: *A*

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

Question #43 *Topic 1*

A security operation center team in a large financial institution is working on implementing a threat intelligence strategy to proactively defend against cyber threats. To ensure the success of this initiative, they need to systematically allocate resources to gather relevant intelligence. The CISO has emphasized that simply collecting data is not enough; the team must focus on assigning specific personnel, tools, and time to gather intelligence that aligns with the organization's most pressing security concerns, such as fraud detection, phishing campaigns, and nation-state threats targeting financial transactions. As part of this structured approach, the team must determine who will be responsible for collecting intelligence, what sources will be monitored, and how frequently data should be gathered. This step ensures that the right resources are applied to the most relevant intelligence efforts. What is this process called?

A. Resources

B. High-Level Requirements

C. Tasking

D. Prioritization

Suggested Answer: *C*

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

Question #44 *Topic 1*

A newly hired SOC analyst has just joined a fast-growing multinational organization that manages a vast IT infrastructure across multiple regions. The analyst's first task is to quickly assess the company's external exposure and identify potential security risks before threat actors can exploit them. To begin the assessment, the analyst considers various techniques, including analyzing publicly available information, scanning for exposed services, reviewing DNS records, and gathering intelligence from external sources. However, given the sheer volume of data spanning multiple subsidiaries, cloud environments, and third- party integrations, the analyst quickly realizes that some methods may not scale well for large, complex infrastructures and may lead to delays or incomplete insights. Which technique is less practical for handling large or diverse data sets in this scenario?

A. OSINT

B. DNS Lookup

C. Web Enumeration

D. Stack Counting

Suggested Answer: *C*

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

Question #45 *Topic 1*

TechSolutions, a software development firm, discovered a potential data leak after an external security researcher reported finding sensitive customer data on a public code repository. Level 1 SOC analysts confirmed the presence of the data and escalated the issue. Level 2 analysts have been tracking the source of the leak, and have found that the data was uploaded from an internal network account. The incident response team has been alerted, and the CISO is demanding a comprehensive analysis of the incident, including the extent of the data breach and the timeline of events. The SOC manager is overwhelmed has to decide whom to assign to the task of the in-depth investigation. To accurately determine timeline, extent, and root cause of the data leak, which of the following SOC role is critical in gathering analyzing the digital evidence?

A. Forensic Analyst

B. Threat Intelligence Analyst

C. Subject Matter Expert

D. SOC Manager

Suggested Answer: *A*

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

Question #46 *Topic 1*

A healthcare organization's SIEM detects a series of unusual HTTP requests targeting its patient portal. The requests originate from a foreign IP address and occur during non-business hours. The methods used are primarily TRACE and OPTIONS, which are rarely seen in normal web traffic. The SIEM correlates these events with an increase in reconnaissance activity on other servers within the same subnet. What is the primary security concern with TRACE and OPTIONS requests?

A. They expose information about server-supported methods and request headers

B. They can be used to upload malicious payloads directly to the server

C. They make Distributed Denial of Service (DDoS) attack easier

D. They allow attackers to bypass authentication controls

Suggested Answer: *A*

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

Question #47 *Topic 1*

A health corporation is implementing an SIEM solution to improve its ability to detect and respond to security incidents and comply with the HIPAA regulatory requirements for protecting sensitive patient data. They need to ensure that the implemented SIEM solution can efficiently collect, analyze, and correlate security events from various sources, including network devices, servers, and security applications, and generate timely alerts for potential HIPAA violations. Which of the following capabilities is needed for a corporation's SIEM solution to meet these needs?

A. Log management and security analytics

B. Threat hunting and intelligence

C. Log collection through agents

D. Centralized SIEM Implementation

Suggested Answer: *A*

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

Question #48 *Topic 1*

A SOC analyst detects multiple instances of powershell.exe being launched with the -ExecutionPolicy Bypass and -NoProfile arguments on a domain controller. The parent process is winrm.exe, and the activity occurs during non-business hours. What should be the analyst's primary focus?

A. Review Event ID 5145 to see if unauthorized network shares were accessed

B. Search for Event ID 4688 to find similar PowerShell executions within the last 24 hours

C. Investigate Event ID 7045 to determine if a malicious service was created

D. Look for Event ID 4625 to check for failed authentication attempts before execution

Suggested Answer: *B*

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

Question #49 *Topic 1*

Jake Carter, a SOC analyst at a financial institution in New York, is responsible for monitoring network traffic to detect potential data exfiltration attempts. His team uses a security solution that inspects data packets in real time as they traverse the network. During an incident response, Jake observes that the solution struggles to analyze encrypted traffic, limiting its effectiveness in identifying threats hidden within secure communications. Which security control, with this known limitation, is the SOC team relying on?

A. SSH

B. Packet filters

C. VPN

D. IPsec

Suggested Answer: *B*

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

Question #50 *Topic 1*

During routine monitoring, the SIEM detects an unusual spike in outbound data transfer from a critical database server. The typical outbound traffic for this server is around 5 MB/hour, but in the past 10 minutes, it has sent over 500 MB to an external IP address. No predefined signatures match this activity, but the SIEM raises an alert due to deviations from the server's normal behavior profile. Which detection method is responsible for this alert?

A. Rule-based detection

B. Signature-based detection

C. Heuristic-based detection

D. Anomaly-based detection

Suggested Answer: *D*

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