Fortinet

FCSS_SOC_AN-7.4 Exam

FCSS - Security Operations 7.4 Analyst

Questions & Answers
Demo

Version: 4.0

Question: 1

Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?
A. An event handler on FortiAnalyzer executes an automation stitch when an event is created.
B. An automation stitch is configured on FortiAnalyzer and mapped to FortiGate using the FortiOS connector.
C. An event handler on FortiAnalyzer is configured to send a notification to FortiGate to trigger an automation stitch.
D. A security profile on FortiGate triggers a violation and FortiGate sends a webhook call to FortiAnalyzer.

Answer: D

Explanation:

Overview of Automation Stitches: Automation stitches in Fortinet solutions enable automated responses to specific events detected within the network. This automation helps in swiftly mitigating threats without manual intervention.
FortiGate Security Profiles:
FortiGate uses security profiles to enforce policies on network traffic. These profiles can include antivirus, web filtering, intrusion prevention, and more.
When a security profile detects a violation or a specific event, it can trigger predefined actions.
Webhook Calls:
FortiGate can be configured to send webhook calls upon detecting specific security events.
A webhook is an HTTP callback triggered by an event, sending data to a specified URL. This allows FortiGate to communicate with other systems, such as FortiAnalyzer.
FortiAnalyzer Integration:
FortiAnalyzer collects logs and events from various Fortinet devices, providing centralized logging and analysis.
Upon receiving a webhook call from FortiGate, FortiAnalyzer can further analyze the event, generate reports, and take automated actions if configured to do so.
Detailed Process:
Step 1: A security profile on FortiGate triggers a violation based on the defined security policies.
Step 2: FortiGate sends a webhook call to FortiAnalyzer with details of the violation.
Step 3: FortiAnalyzer receives the webhook call and logs the event.
Step 4: Depending on the configuration, FortiAnalyzer can execute an automation stitch to respond to the event, such as sending alerts, generating reports, or triggering further actions.
Reference:
Fortinet Documentation: FortiOS Automation Stitches
FortiAnalyzer Administration Guide: Details on configuring event handlers and integrating with FortiGate.

FortiGate Administration Guide: Information on security profiles and webhook configurations.
By understanding the interaction between FortiGate and FortiAnalyzer through webhook calls and automation stitches, security operations can ensure a proactive and efficient response to security events.

Question: 2

Which three end user logs does FortiAnalyzer use to identify possible IOC compromised hosts? (Choose three.)

A. Email filter logs
B. DNS filter logs
C. Application filter logs
D. IPS logs
E. Web filter logs

Answer: BDE

Explanation:

Overview of Indicators of Compromise (IoCs): Indicators of Compromise (IoCs) are pieces of evidence that suggest a system may have been compromised. These can include unusual network traffic patterns, the presence of known malicious files, or other suspicious activities.
FortiAnalyzer's Role: FortiAnalyzer aggregates logs from various Fortinet devices to provide comprehensive visibility and analysis of network events. It uses these logs to identify potential IoCs and compromised hosts.
Relevant Log Types:
DNS Filter Logs:
DNS requests are a common vector for malware communication. Analyzing DNS filter logs helps in identifying suspicious domain queries, which can indicate malware attempting to communicate with command and control (C2) servers.
Reference: Fortinet Documentation on DNS Filtering FortiOS DNS Filter
IPS Logs:
Intrusion Prevention System (IPS) logs detect and block exploit attempts and malicious activities. These logs are critical for identifying compromised hosts based on detected intrusion attempts or behaviors matching known attack patterns.
Reference: Fortinet IPS Overview FortiOS IPS
Web Filter Logs:
Web filtering logs monitor and control access to web content. These logs can reveal access to malicious websites, download of malware, or other web-based threats, indicating a compromised host.
Reference: Fortinet Web Filtering FortiOS Web Filter
Why Not Other Log Types:
Email Filter Logs:
While important for detecting phishing and email-based threats, they are not as directly indicative of compromised hosts as DNS, IPS, and Web filter logs.
Application Filter Logs:
These logs control application usage but are less likely to directly indicate compromised hosts compared to the selected logs.
Detailed Process:
Step 1: FortiAnalyzer collects logs from FortiGate and other Fortinet devices.

Step 2: DNS filter logs are analyzed to detect unusual or malicious domain queries.
Step 3: IPS logs are reviewed for any intrusion attempts or suspicious activities.
Step 4: Web filter logs are checked for access to malicious websites or downloads.
Step 5: FortiAnalyzer correlates the information from these logs to identify potential IoCs and compromised hosts.
Reference:
Fortinet Documentation: FortiOS DNS Filter, IPS, and Web Filter administration guides.
FortiAnalyzer Administration Guide: Details on log analysis and IoC identification.
By using DNS filter logs, IPS logs, and Web filter logs, FortiAnalyzer effectively identifies possible compromised hosts, providing critical insights for threat detection and response.

Question: 3

Which role does a threat hunter play within a SOC?

A. investigate and respond to a reported security incident
B. Collect evidence and determine the impact of a suspected attack
C. Search for hidden threats inside a network which may have eluded detection
D. Monitor network logs to identify anomalous behavior

Answer: C

Explanation:

Role of a Threat Hunter:
A threat hunter proactively searches for cyber threats that have evaded traditional security defenses. This role is crucial in identifying sophisticated and stealthy adversaries that bypass automated detection systems.
Key Responsibilities:
Proactive Threat Identification:
Threat hunters use advanced tools and techniques to identify hidden threats within the network. This includes analyzing anomalies, investigating unusual behaviors, and utilizing threat intelligence.
Reference: SANS Institute, "Threat Hunting: Open Season on the Adversary" SANS Threat Hunting
Understanding the Threat Landscape:
They need a deep understanding of the threat landscape, including common and emerging tactics, techniques, and procedures (TTPs) used by threat actors.
Reference: MITRE ATT&CK Framework MITRE ATT&CK
Advanced Analytical Skills:
Utilizing advanced analytical skills and tools, threat hunters analyze logs, network traffic, and endpoint data to uncover signs of compromise.
Reference: Cybersecurity and Infrastructure Security Agency (CISA) Threat Hunting Guide CISA Threat Hunting
Distinguishing from Other Roles:
Investigate and Respond to Incidents (A):
This is typically the role of an Incident Responder who reacts to reported incidents, collects evidence, and determines the impact.
Reference: NIST Special Publication 800-61, "Computer Security Incident Handling Guide" NIST Incident Handling
Collect Evidence and Determine Impact (B):

This is often the role of a Digital Forensics Analyst who focuses on evidence collection and impact assessment post-incident.
Monitor Network Logs (D):
This falls under the responsibilities of a SOC Analyst who monitors logs and alerts for anomalous behavior and initial detection.
Conclusion:
Threat hunters are essential in a SOC for uncovering sophisticated threats that automated systems may miss. Their proactive approach is key to enhancing the organization's security posture.
Reference:
SANS Institute, "Threat Hunting: Open Season on the Adversary"
MITRE ATT&CK Framework
CISA Threat Hunting Guide
NIST Special Publication 800-61, "Computer Security Incident Handling Guide"
By searching for hidden threats that elude detection, threat hunters play a crucial role in maintaining the security and integrity of an organization's network.

Question: 4

According to the National Institute of Standards and Technology (NIST) cybersecurity framework, incident handling activities can be divided into phases.
In which incident handling phase do you quarantine a compromised host in order to prevent an adversary from using it as a stepping stone to the next phase of an attack?

A. Containment
B. Analysis
C. Eradication
D. Recovery

Answer: A

Explanation:

NIST Cybersecurity Framework Overview:
The NIST Cybersecurity Framework provides a structured approach for managing and mitigating cybersecurity risks. Incident handling is divided into several phases to systematically address and resolve incidents.
Incident Handling Phases:
Preparation: Establishing and maintaining an incident response capability.
Detection and Analysis: Identifying and investigating suspicious activities to confirm an incident.
Containment, Eradication, and Recovery:
Containment: Limiting the impact of the incident.
Eradication: Removing the root cause of the incident.
Recovery: Restoring systems to normal operation.
Containment Phase:
The primary goal of the containment phase is to prevent the incident from spreading and causing further damage.
Quarantining a Compromised Host:
Quarantining involves isolating the compromised host from the rest of the network to prevent adversaries from moving laterally and causing more harm.

Techniques include network segmentation, disabling network interfaces, and applying access controls.
Reference: NIST Special Publication 800-61, "Computer Security Incident Handling Guide" NIST Incident Handling
Detailed Process:
Step 1: Detect the compromised host through monitoring and analysis.
Step 2: Assess the impact and scope of the compromise.
Step 3: Quarantine the compromised host to prevent further spread. This can involve disconnecting the host from the network or applying strict network segmentation.
Step 4: Document the containment actions and proceed to the eradication phase to remove the threat completely.
Step 5: After eradication, initiate the recovery phase to restore normal operations and ensure that the host is securely reintegrated into the network.
Importance of Containment:
Containment is critical in mitigating the immediate impact of an incident and preventing further damage. It buys time for responders to investigate and remediate the threat effectively.
Reference: SANS Institute, "Incident Handler's Handbook" SANS Incident Handling
Reference:
NIST Special Publication 800-61, "Computer Security Incident Handling Guide"
SANS Institute, "Incident Handler's Handbook"
By quarantining a compromised host during the containment phase, organizations can effectively limit the spread of the incident and protect their network from further compromise.

Question: 5

Which FortiAnalyzer connector can you use to run automation stitches9

A. FortiCASB
B. FortiMail
C. Local
D. FortiOS

Answer: D

Explanation:

Overview of Automation Stitches:
Automation stitches in FortiAnalyzer are predefined sets of automated actions triggered by specific events. These actions help in automating responses to security incidents, improving efficiency, and reducing the response time.
FortiAnalyzer Connectors:
FortiAnalyzer integrates with various Fortinet products and other third-party solutions through connectors. These connectors facilitate communication and data exchange, enabling centralized management and automation.
Available Connectors for Automation Stitches:
FortiCASB:
FortiCASB is a Cloud Access Security Broker that helps secure SaaS applications. However, it is not typically used for running automation stitches within FortiAnalyzer.
Reference: Fortinet FortiCASB Documentation FortiCASB
FortiMail:

FortiMail is an email security solution. While it can send logs and events to FortiAnalyzer, it is not primarily used for running automation stitches.
Reference: Fortinet FortiMail Documentation FortiMail
Local:
The local connector refers to FortiAnalyzer's ability to handle logs and events generated by itself. This is useful for internal processes but not specifically for integrating with other Fortinet devices for automation stitches.
Reference: Fortinet FortiAnalyzer Administration Guide FortiAnalyzer Local
FortiOS:
FortiOS is the operating system that runs on FortiGate firewalls. FortiAnalyzer can use the FortiOS connector to communicate with FortiGate devices and run automation stitches. This allows FortiAnalyzer to send commands to FortiGate, triggering predefined actions in response to specific events.
Reference: Fortinet FortiOS Administration Guide FortiOS
Detailed Process:
Step 1: Configure the FortiOS connector in FortiAnalyzer to establish communication with FortiGate devices.
Step 2: Define automation stitches within FortiAnalyzer that specify the actions to be taken when certain events occur.
Step 3: When a triggering event is detected, FortiAnalyzer uses the FortiOS connector to send the necessary commands to the FortiGate device.
Step 4: FortiGate executes the commands, performing the predefined actions such as blocking an IP address, updating firewall rules, or sending alerts.
Conclusion:
The FortiOS connector is specifically designed for integration with FortiGate devices, enabling FortiAnalyzer to execute automation stitches effectively.
Reference:
Fortinet FortiOS Administration Guide: Details on configuring and using automation stitches.
Fortinet FortiAnalyzer Administration Guide: Information on connectors and integration options.
By utilizing the FortiOS connector, FortiAnalyzer can run automation stitches to enhance the security posture and response capabilities within a network.