Prepare Smart for Success Free Fortinet NSE7_SOC_AR-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 7 - Security Operations 7.6 Architect exam PDF questions now. Get authentic NSE7_SOC_AR-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE7_SOC_AR-7.6 exam pdf questions and answers.

Thank you for Downloading NSE7_SOC_AR-7.6 exam PDF Demo

https://prepbolt.com/NSE7_SOC_AR-7.6.html

Question 1

Question Type: MultipleChoice

Refer to the exhibits.

You configured a spearphishing event handler and the associated rule. However. FortiAnalyzer did not generate an event.

When you check the FortiAnalyzer log viewer, you confirm that FortiSandbox forwarded the appropriate logs, as shown in the raw log exhibit.

What configuration must you change on FortiAnalyzer in order for FortiAnalyzer to generate an event?

Options:

A- In the Log Type field, change the selection to AntiVirus Log(malware).
B- Configure a FortiSandbox data selector and add it tothe event handler.
C- In the Log Filter by Text field, type the value: .5 ub t ype ma Iwa re..
D- Change trigger condition by selecting. Within a group, the log field Malware Kame (mname> has 2 or more unique values.

Answer:

B

Explanation:

Understanding the Event Handler Configuration:

The event handler is set up to detect specific security incidents, such as spearphishing, based on logs forwarded from other Fortinet products like FortiSandbox.

An event handler includes rules that define the conditions under which an event should be triggered.

Analyzing the Current Configuration:

The current event handler is named 'Spearphishing handler' with a rule titled 'Spearphishing Rule 1'.

The log viewer shows that logs are being forwarded by FortiSandbox but no events are generated by FortiAnalyzer.

Key Components of Event Handling:

Log Type: Determines which type of logs will trigger the event handler.

Data Selector: Specifies the criteria that logs must meet to trigger an event.

Automation Stitch: Optional actions that can be triggered when an event occurs.

Notifications: Defines how alerts are communicated when an event is detected.

Issue Identification:

Since FortiSandbox logs are correctly forwarded but no event is generated, the issue likely lies in the data selector configuration or log type matching.

The data selector must be configured to include logs forwarded by FortiSandbox.

Solution:

B . Configure a FortiSandbox data selector and add it to the event handler:

By configuring a data selector specifically for FortiSandbox logs and adding it to the event handler, FortiAnalyzer can accurately identify and trigger events based on the forwarded logs.

Steps to Implement the Solution:

Step 1: Go to the Event Handler settings in FortiAnalyzer.

Step 2: Add a new data selector that includes criteria matching the logs forwarded by FortiSandbox (e.g., log subtype, malware detection details).

Step 3: Link this data selector to the existing spearphishing event handler.

Step 4: Save the configuration and test to ensure events are now being generated.

Conclusion:

The correct configuration of a FortiSandbox data selector within the event handler ensures that FortiAnalyzer can generate events based on relevant logs.

Fortinet Documentation on Event Handlers and Data Selectors FortiAnalyzer Event Handlers

Fortinet Knowledge Base for Configuring Data Selectors FortiAnalyzer Data Selectors

By configuring a FortiSandbox data selector and adding it to the event handler, FortiAnalyzer will be able to accurately generate events based on the appropriate logs.

Question 2

Question Type: MultipleChoice

Refer to the exhibits.

What can you conclude from analyzing the data using the threat hunting module?

Options:

A- Spearphishing is being used to elicit sensitive information.
B- DNS tunneling is being used to extract confidential data from the local network.
C- Reconnaissance is being used to gather victim identity information from the mail server.
D- FTP is being used as command-and-control (C&C) technique to mine for data.

Answer:

B

Explanation:

Understanding the Threat Hunting Data:

The Threat Hunting Monitor in the provided exhibits shows various application services, their usage counts, and data metrics such as sent bytes, average sent bytes, and maximum sent bytes.

The second part of the exhibit lists connection attempts from a specific source IP (10.0.1.10) to a destination IP (8.8.8.8), with repeated 'Connection Failed' messages.

Analyzing the Application Services:

DNS is the top application service with a significantly high count (251,400) and notable sent bytes (9.1 MB).

This large volume of DNS traffic is unusual for regular DNS queries and can indicate the presence of DNS tunneling.

DNS Tunneling:

DNS tunneling is a technique used by attackers to bypass security controls by encoding data within DNS queries and responses. This allows them to extract data from the local network without detection.

The high volume of DNS traffic, combined with the detailed metrics, suggests that DNS tunneling might be in use.

Connection Failures to 8.8.8.8:

The repeated connection attempts from the source IP (10.0.1.10) to the destination IP (8.8.8.8) with connection failures can indicate an attempt to communicate with an external server.

Google DNS (8.8.8.8) is often used for DNS tunneling due to its reliability and global reach.

Conclusion:

Given the significant DNS traffic and the nature of the connection attempts, it is reasonable to conclude that DNS tunneling is being used to extract confidential data from the local network.

Why Other Options are Less Likely:

Spearphishing (A): There is no evidence from the provided data that points to spearphishing attempts,

such as email logs or phishing indicators.

Reconnaissance (C): The data does not indicate typical reconnaissance activities, such as scanning or probing mail servers.

FTP C&C (D): There is no evidence of FTP traffic or command-and-control communications using FTP in the provided data.

SANS Institute: 'DNS Tunneling: How to Detect Data Exfiltration and Tunneling Through DNS Queries' SANS DNS Tunneling

OWASP: 'DNS Tunneling' OWASP DNS Tunneling

By analyzing the provided threat hunting data, it is evident that DNS tunneling is being used to exfiltrate data, indicating a sophisticated method of extracting confidential information from the network.

Question 3

Question Type: MultipleChoice

Which FortiAnalyzer connector can you use to run automation stitches9

Options:

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.

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.

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.

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.

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.

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.

Question 4

Question Type: MultipleChoice

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?

Options:

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.

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.

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

Question Type: MultipleChoice

Which role does a threat hunter play within a SOC?

Options:

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.

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.

Advanced Analytical Skills:

Utilizing advanced analytical skills and tools, threat hunters analyze logs, network traffic, and endpoint data to uncover signs of compromise.

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.

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.

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 6

Question Type: MultipleChoice

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

Options:

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

Answer:

B, D, E

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.

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.

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.

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.

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 7

Question Type: MultipleChoice

Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?

Options:

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.

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 8

Question Type: MultipleChoice

You are trying to create a playbook that creates a manual task showing a list of public IPv6 addresses. You were successful in extracting all IP addresses from a previous action into a variable called ip_list, which contains both private and public IPv4 and IPv6 addresses. You must now filter the results to display only public IPv6 addresses. Which two Jinja expressions can accomplish this task? (Choose two answers)

Options:

A- {{ vars.ip_list | ipv6addr('public') }}
B- {{ vars.ip_list | ipaddr('public') | ipv6 }}
C- {{ vars.ip_list | ipaddr('!private') | ipv6 }}
D- {{ vars.ip_list | ipv6 | ipaddr('public') }}

Answer:

B, D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:

In FortiSOAR 7.6, the playbook engine utilizes the powerful ipaddr family of Jinja filters (derived from the Ansible netaddr library) to manipulate network data. To isolate public IPv6 addresses from a mixed

list, the order of operations in the filter chain ensures the correct data is extracted:

Double Filtering Sequence (B): In the expression {{ vars.ip_list | ipaddr('public') | ipv6 }}, the first filter ipaddr('public') processes the entire list and retains only public addresses, including both IPv4 and IPv6 versions. The second filter in the pipe, | ipv6, then takes that subset of public addresses and filters them again to keep only those that conform to the IPv6 standard. The final result is a list containing only public IPv6 addresses.

Why other options are incorrect:

A (ipv6addr 'public'): While ipv6addr is a valid filter in many Ansible environments, FortiSOAR's standard documentation for manual task creation and data manipulation primarily emphasizes the use of the generic ipaddr filter with specific flags or chained version filters (like | ipv6) to ensure cross-compatibility with the underlying Python libraries used by the SOAR engine.

C (!private syntax): The ipaddr filter utilizes specific keywords for classification. While 'not private' is the logical requirement, the filter expects positive assertions such as 'public', 'private', or 'multicast'. The !private syntax is not a supported or documented operator for this filter within the Fortinet SOC ecosystem.

Thank You for trying NSE7_SOC_AR-7.6 PDF Demo

To try our NSE7_SOC_AR-7.6 practice exam software visit link below

https://prepbolt.com/NSE7_SOC_AR-7.6.html

Start Your NSE7_SOC_AR-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE7_SOC_AR-7.6 preparation with actual exam questions.