Vendor: Fortinet

Exam Code: FCSS_SOC_AN-7.4

Exam Name: FCSS - Security Operations 7.4 Analyst

Version: DEMO

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.

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.

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.

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.

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:
During the Containment phase of incident handling according to the NIST cybersecurity framework, the goal is to limit the scope and magnitude of an incident. This includes isolating or quarantining compromised systems to prevent the adversary from further exploiting them or using them as a launch pad for attacks on additional systems. This phase is crucial for stopping the spread of the incident and preventing further damage.

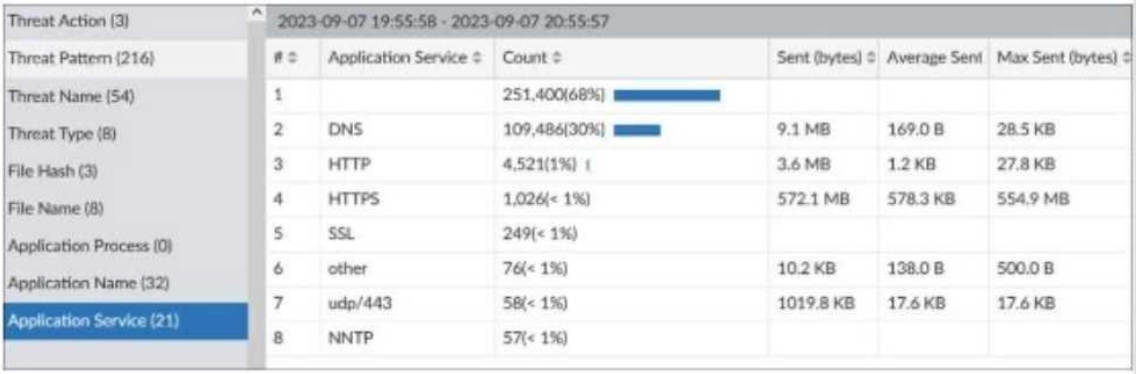
QUESTION 5
Which FortiAnalyzer connector can you use to run automation stitches9

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.
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.
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.

QUESTION 6
Refer to the exhibits. What can you conclude from analyzing the data using the threat hunting module?

Threat Hunting Monitor



Threat Action (3)	2023-09-07 19:55:58 - 2023-09-07 20:55:57				
Threat Pattern (216)	#	Application Service	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
Threat Name (54)	1		251,400(68%)			
Threat Type (8)	2	DNS	109,486(30%)	9.1 MB	169.0 B	28.5 KB
File Hash (3)	3	HTTP	4,521(1%)	3.6 MB	1.2 KB	27.8 KB
File Name (8)	4	HTTPS	1,026(< 1%)	572.1 MB	578.3 KB	554.9 MB
Application Process (0)	5	SSL	249(< 1%)			
Application Name (32)	6	other	76(< 1%)	10.2 KB	138.0 B	500.0 B
Application Service (21)	7	udp/443	58(< 1%)	1019.8 KB	17.6 KB	17.6 KB
	8	NNTP	57(< 1%)			

Threat Hunting Monitor

#	Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

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.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**