Exam Code: 642-544

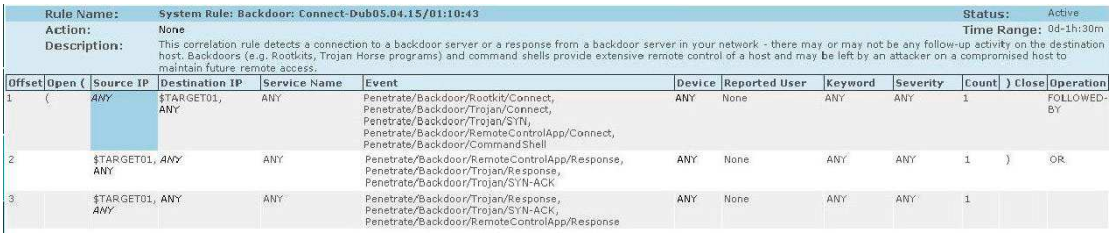
Exam Name: Implementing Cisco Security Monitoring, Analysis and Response System

Vendor: CISCO

Version: DEMO

Part: A

1: Refering to the rule shown on the MARS GUI screen, which two of the following statements are correct?(Choose two.)



Rule Name: System Rule: Backdoor: Connect-Dub05.04.15/01:10:43 — Status: Active
Action: None — Time Range: 0d-1h:30m
Description: This correlation rule detects a connection to a backdoor server or a response from a backdoor server in your network - there may or may not be any follow-up activity on the destination host. Backdoors (e.g. Rootkits, Trojan Horse programs) and command shells provide extensive remote control of a host and may be left by an attacker on a compromised host to maintain future remote access.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1	(	ANY	$TARGET01, ANY	ANY	Penetrate/Backdoor/Rootkit/Connect, Penetrate/Backdoor/Trojan/Connect, Penetrate/Backdoor/Trojan/SYN, Penetrate/Backdoor/RemoteControlApp/Connect, Penetrate/Backdoor/CommandShell	ANY	None	ANY	ANY	1		FOLLOWED-BY
2		$TARGET01, ANY	ANY	ANY	Penetrate/Backdoor/RemoteControlApp/Response, Penetrate/Backdoor/Trojan/Response, Penetrate/Backdoor/Trojan/SYN-ACK	ANY	None	ANY	ANY	1	)	OR
3		$TARGET01, ANY	ANY	ANY	Penetrate/Backdoor/Trojan/Response, Penetrate/Backdoor/Trojan/SYN-ACK, Penetrate/Backdoor/RemoteControlApp/Response	ANY	None	ANY	ANY	1		

A.This rule will fire if the offset 1 condition occurs "OR" if the offset 2 condition occurs.
B.This rule will fire if the offset 3 condition occurs.
C.The expressions between cells are "AND' while the expressions between items in the same cell are "OR".
D.This is a user-defined rule.
E.This rule can be deleted after changing its status to "inactive."
Correct Answers: C

2: To configure a Microsoft Windows IIS server to publish logs to the Cisco Security MARS, which log agent is installed and configured on the Microsoft Windows IIS server?
A.pnLog agent
B.Cisco Security MARS agent
C.SNARE
D.None. Cisco Security MARS is an agentless device.
Correct Answers: C

4: A Cisco Security MARS appliance cannot access certain devices through the default gateway. Troubleshooting has determined that this is a Cisco Security MARS configuration issue. Which additional Cisco Security MARS configuration will be required to correct this issue?
A.use the Cisco Security MARS GUI or CLI to enable a dynamic routing protocol
B.use the Cisco Security MARS CLI to add a static route
C.use the Cisco Security MARS GUI to configure multiple default gateways
D.use the Cisco Security MARS GUI or CLI to configure multiple default gateways
Correct Answers: B

5: Which action enables the Cisco Security MARS appliance to ignore false-positive events by either dropping the events completely, or by just logging them to the database?
A.creating system inspection rules using the drop operation
B.creating drop rules
C.inactivating the rules
D.inactivating the events
E.deleting the false-positive events from the Incidents page
F.deleting the false-positive events from the Event Management page
Correct Answers: B

6: Which three of the following statements are correct regarding the Query shown on the MARS GUI screen?(Choose three.)
A.Query will match any source IP address.
B.Query will only match a source IP address of 10.10.10.10.
C.Query will only match a destination IP address range from 10.1.1.1 to 10.1.1.25.
D.Query will only match a destination IP address of 10.1.1.1 OR 10.1.1.25.
E.Query will only not match any services since both TCP-highPort and UDP-highPort service groups are specified in the Service field.
F.Query will only match any services using the TCP-highPort OR UDP-highPort service groups.
Correct Answers: F

7: Which three statements are true about Cisco Security MARS rules? (Choose three.)
A.There are three types of rules.
B.Rules can be saved as reports.
C.Rules can be deleted.
D.Rules trigger incidents.
E.Rules can be defined using a seed file.
F.Rules can be created using a query.
Correct Answers: A D F

8: Which two are required to enable Cisco Security MARS Level 3 operations? (Choose two.)
A.global controller
B.vulnerability scanning
C.NetFlow
D.SNMP community string
E.administrative access to the device
F.Cisco Security Manager
Correct Answers: D E

9: What is a zone?
A.A zone represents all the local controllers each global controller is monitoring.
B.A zone is a logical partition within a local controller. Configuring zones allows the local controller to scale to cover large networks.
C.A zone is an area of a customer network related to one local controller. Each local controller represents a specific zone.
D.Each zone within the global controller is configured and managed independently.
E.Each zone within the local controller is configured and managed independently.
Correct Answers: C

10: In what two ways can the Cisco Security MARS present the incident data to the user graphically from the Summary Dashboard? (Select two)
A.event type group matrix
B.incident firing information

C.path information
D.compromised topology information
E.incident vector information
F.system-confirmed true positive information
Correct Answers: C E