[October-2022NSE5_EDR-5.0 VCE and PDF NSE5_EDR-5.0 30Q Instant Download in Braindump2go[Q1-Q20

October/2022 Latest Braindump2go NSE5 EDR-5.0 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go NSE5 EDR-5.0 Real Exam Questions! Question: 1What is the purpose of the Threat Hunting feature? A. Delete any file from any collector in the organization B. Find and delete all instances of a known malicious file or hash in the organization C. Identify all instances of a known malicious file or hash and notify affected users D. Execute playbooks to isolate affected collectors in the organization Answer: CQuestion: 2How does FortiEDR implement post-infection protection? A. By preventing data exfiltration or encryption even after a breach occurs B. By using methods used by traditional EDRC. By insurance against ransomware D. By real-time filtering to prevent malware from executing Answer: DQuestion: 3Exhibit.



Based on the forensics data shown in the exhibit which two statements are true? (Choose two.) A. The device cannot be remediatedB. The event was blocked because the certificate is unsignedC. Device C8092231196 has been isolatedD. The execution prevention policy has blocked this event. Answer: B, CQuestion: 4What is the benefit of using file hash along with the file name in a threat hunting repository search?A. It helps to make sure the hash is really a malwareB. It helps to check the malware even if the malware variant uses a different file nameC. It helps to find if some instances of the hash are actually associated with a different fileD. It helps locate a file as threat hunting only allows hash searchAnswer: C Question: 5Exhibit.



Based on the event shown in the exhibit which two statements about the event are true? (Choose two.)A. The device is moved to isolation.B. Playbooks is configured for this event.C. The event has been blockedD. The policy is in simulation modeAnswer: B, DQuestion: 6An administrator needs to restrict access to the ADMINISTRATION tab in the central manager for a specific account.What role should the administrator assign to this account?A. AdminB. UserC. Local AdminD. REST APIAnswer:

CQuestion: 7Refer to the exhibit.



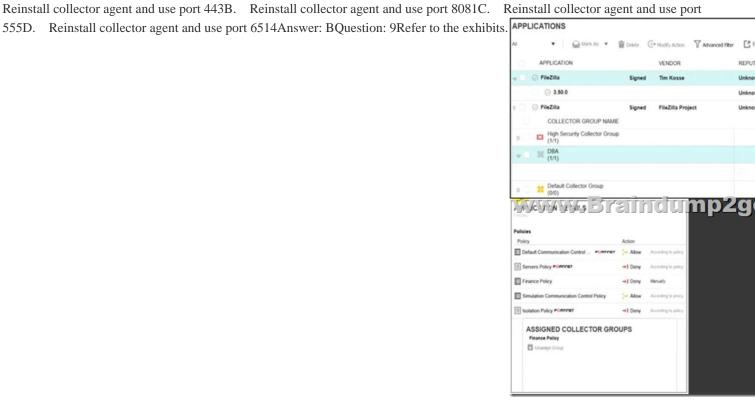
Based on the event shown in the exhibit, which two statements about the event are true? (Choose two.)A. The NGAV policy has blocked TestApplication exeB. TestApplication exe is sophisticated malwareC. The user was able to launch TestApplication exe

D. FCS classified the event as maliciousAnswer: A, BQuestion: 8Refer to the exhibits.

C002221116 -1196 Administrative Statement Forew 2010 19 19 16 11 10 00 00 64 A 32 41 00 - 41 0 51	0EV	CE NAME L	AST LOGGED	05	,	MAC ADDRESS	VERSON
	CBO	12231196	. 1196 Administrator		10 160 6 110	00-50-56-A1-32-81, 00	410.361
	A	BARAB	1-1-1	e un v		1124	9,5
tive Connections				20115		1124	
tive Connections Proto Local Address Foreign Address State		onnections				11:24	
	tive C Proto	onnections Local Address	Fore	ign Address	State		
Proto Local Address Foreign Address State TCP 0.0.0.135 0.0.0.0:0 LISTENING TCP 0.0.0.0:245 0.0.0.0:0 LISTENING	Proto TCP TCP	onnections Local Address 0.0.0.0:135	Fore 0.0.1	ign Address 0.0:0	State LISTEN	016	
Proto Local Address Foreign Address State TCP 0.0.0.0:135 0.0.0.0:0 LISTENING	Proto TCP TCP	onnections Local Address 0.0.0.0:135 0.0.0.0:445	Fore 0,0.1 0.0	ign Address 0.0:0 0.0:0	State LISTEN LISTEN	ING	
Proto Local Address Foreign Address State TCP 0.0.0.135 0.0.0.0:0 LISTENING TCP 0.0.0.0:445 0.0.0.0:0 LISTENING	Proto TCP TCP TCP	onnections Local Address 0.0.0.0:135 0.0.0.0:445 0.0.0.0:5985	Fore 0.0.1 0.0.1 0.0.1	ign Address 0.0:0 0.0:0 0.0:0	State LISTEN LISTEN LISTEN	ING ING ING	
Proto Local Address Foreign Address State TCP 0.0.0.0:135 0.0.0.0:0 LISTENING TCP 0.0.0.0:245 0.0.0.0:0 LISTENING TCP 0.0.0.0:1995 0.0.0.0:0 LISTENING	Proto TCP TCP TCP TCP TCP	onnections Local Address 0.0.0.0:135 0.0.0.0:445 0.0.0.0:5985 0.0.0.0:49692	Fore 0.0.1 0.0.1 0.0.1 0.0.1	ign Address 0.0:0 0.0:0 0.0:0 0.0:0	State LISTEN LISTEN LISTEN LISTEN	1NG 1N6 1N6 1N6	
Proto Local Address Foreign Address State TCP 0.0.0.0:135 0.0.0.0:0:0 LISTENIG CP 0.0.0.0:425 0.0.0.0:0 LISTENIG TCP 0.0.0.0:4265 0.0.0.0:0 LISTENIG TCP 0.0.0.0:1995 0.0.0.0:0 LISTENIG TCP 0.0.0:19902 0.0.0.0:0 LISTENIG	Ctive C Proto TCP TCP TCP TCP TCP TCP	onnections Local Address 0.0.0.0:135 0.0.0.0:455 0.0.0.0:5905 0.0.0.0:49692 10.160.6.110:135	Fore 0.0.1 0.0.1 0.0.1 0.0.1 9 0.0.1	ign Address 0.0:0 0.0:0 0.0:0 0.0:0 0.0:0	State LISTEN LISTEN LISTEN LISTEN LISTEN	Ding Ding Ding Ding Ding Ding	
Proto Local Address Foreign Address State TCP 0.0.0.0135 0.0.0.0:0 LISTENING TCP 0.0.0.0:45 0.0.0.0:0 LISTENING TCP 0.0.0.0:45 0.0.0.0:0 LISTENING TCP 0.0.0.0:005 0.0.0.0:0 LISTENING TCP 0.0.0.0:0092 0.0.0.0:0 LISTENING TCP 0.00.0:0:0192 0.0.0.0:0 LISTENING TCP 0.00.0:0:0192 0.0.0.0:0 LISTENING	Proto TCP TCP TCP TCP TCP TCP TCP TCP	onnections Local Address 0.0.0.0:135 0.0.0.0:445 0.0.0.0:5985 0.0.0.0:49692 10.160.6.110:13 10.160.6.110:50	Fore 0.0.1 0.0.1 0.0.1 9.0.1 9.0.0.1 853.10.1	ign Address 0.0:0 0.0:0 0.0:0 0.0:0 0.0:0 50.6.100:8080	State LISTEN LISTEN LISTEN LISTEN SYN_SE	DNG ING ING ING IT	99

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address

10.160.6.100 using default port.Based on the netstat command output what must you do to resolve the connectivity issue?A.



The exhibits show application policy logs and application details Collector C8092231196 is a member of the Finance groupWhat must an administrator do to block the FileZilia application?A. Deny application in Finance policyB. Assign Finance policy to DBA groupC. Assign Finance policy to Default Collector GroupD. Assign Simulation Communication Control Policy to DBA groupAnswer: D Question: 10Refer to the exhibit.

This page was exported from - <u>Braindump2go Free Exam Dumps with PDF and VCE Collection</u> Export date: Thu Nov 21 14:06:18 2024 / +0000 GMT

Query Name	Query pro	film.					
	and he	-					
Description							
Tags	+						
Full Query							
Category		Device	31156	2			
All Compositions		C8090	21196	,		Dere	
All Compositions	w.	C8090	ain	du	mo	2010	con
All Compositions	W.	C8090	ะ กไก	du	mp	2go	con
All Compositions	w.	C8090	ain	du	mp	2go	.con
All Compositions	w.	C8090	ain	rciun	mp	290	.con
Al Calegores	W-	C8090	ann	rcitum	mp	2go	.con
Al Categores	Query ()	C8090	aiin	rciun	mp	2go	.con
Al Calegores	Query ()	C8090	aitn	rcitur	mpź	290	.con
Al Categores	avery () avery ()	C8090	artn	r ci u n	mp	290	.con
Al Caregores	Query () Query () Query ()	Br	anna 2111A	ici un	mp	290	con

Based on the threat hunting query shown in the exhibit which of the following is true?A. RDP connections will be blocked and classified as suspiciousB. A security event will be triggered when the device attempts a RDP connectionC. This query is included in other organizationsD. The query will only check for network categoryAnswer: BQuestion: 11Which connectors can you use for the FortiEDR automated incident response? (Choose two.)A. FortiNACB. FortiGateC. FortiSiemD. FortiSandboxAnswer: B, CQuestion: 12What is true about classifications assigned by Fortinet Cloud Sen/ice (FCS)?A. The core is responsible for all classifications if FCS playbooks are disabledB. The core only assigns a classification if FCS is not availableC. FCS revises the classification of the core based on its databaseD. FCS is responsible for all classificationsAnswer: CQuestion: 13

Refer to the exhibit. Administrator Command Prompt



Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR collector are true? (Choose two.)A. The collector device has windows firewall enabledB. The collector has been installed with an incorrect port numberC. The collector has been installed with an incorrect registration passwordD. The collector device cannot reach the central managerAnswer: B, DQuestion: 14A company requires a global communication policy for a FortiEDR multi-tenant environment. How can the administrator achieve this?A. An administrator creates a new communication control policy and shares it with other organizationsB. A local administrator creates new a communication control policy and shares it with other organizationsC. A local administrator creates a new communication control policy and assigns it globally to all organizationsD. An administrator creates a new communication control policy for each organizationAnswer: C Question: 15Refer to the exhibit.

This page was exported from - <u>Braindump2go Free Exam Dumps with PDF and VCE Collection</u> Export date: Thu Nov 21 14:06:19 2024 / +0000 GMT

EVENT EXCEPTIONS	
EVENTEAGETION	5
Exceptions for event 44878	
Exception 1 +	
Created from Raw Data Item 64	41717447 of event 44575
Last updated at 10-Dec-2021, 2	22.52 By FortinetCloudServices
Collector groups	
	Al groups
Destinations	
	- All destrutions
www.Br	aindump2go.com
	 Allusers
Trippered Rules	<u> </u>
Pile Encryptor	• ·
FortnetCloudServices, at 10-D The Ne Update exe is classifie	ec-3021, 22 52 59 d as Good. On the device "C8092231196"
	Renover Exception
At the Raw Data items an	e covered Carcel

Based on the event exception shown in the exhibit which two statements about the exception are true? (Choose two)A. A partial exception is applied to this eventB. FCS playbooks is enabled by Fortinet supportC. The exception is applied only on device C8092231196D. The system owner can modify the trigger rules parametersAnswer: A, CQuestion: 16Which two statements are true about the remediation function in the threat hunting module? (Choose two.)A. The file is removed from the affected collectors B. The threat hunting module sends the user a notification to delete the fileC. The file is quarantinedD. The threat hunting

module deletes files from collectors that are currently online. Answer: B, CQuestion: 17Exhibit.

tere 1999	C terr			
· W/W/W	.Bra	ind	um	<u>p2</u>
CONTRACT AND PRODUCTS OF AND	FARE FARENT PROCESS-CREATION	Helpit Roccis clonos	NAME A PROCESSION	Net NOCES OF

Based on the forensics data shown in the exhibit, which two statements are true? (Choose two.)A. An exception has been created for this eventB. The forensics data is displayed m the stacks viewC. The device has been isolatedD. The exfiltration prevention policy has blocked this eventAnswer: C, DQuestion: 18The FortiEDR axe classified an event as inconclusive, out a few seconds later FCS revised the classification to malicious. What playbook actions ate applied to the event?A. Playbook actions applied to inconclusive eventsB. Playbook actions applied to handled eventsC. Playbook actions applied to suspicious eventsD. Playbook actions applied to malicious eventsAnswer: DQuestion: 19Which threat hunting profile is the most resource intensive?A. ComprehensiveB. InventoryC. DefaultD. Standard CollectionAnswer: AQuestion: 20Which two types of remote authentication does the FortiEDR management console support? (Choose two.)A. RadiusB. SAMLC. TACACSD. LDAPAnswer: A, DResources From:1.2022 Latest Braindump2go NSE5_EDR-5.0 Exam Dumps (PDF & VCE) Free Share:

https://www.braindump2go.com/nse5-edr-5-0.html2.2022 Latest Braindump2go NSE5_EDR-5.0 PDF and NSE5_EDR-5.0 VCE Dumps Free Share:https://drive.google.com/drive/folders/1CJgO_BfQSuot7WsvGWbiEpNGJwTDPrDd?usp=sharing3.2021 Free Braindump2go NSE5_EDR-5.0 Exam Questions Download:

https://www.braindump2go.com/free-online-pdf/NSE5_EDR-5.0-PDF-Dumps(1-20).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!