350-201$^{\text{Q\&As}}$

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

A. continuous delivery

B. continuous integration

C. continuous deployment

D. continuous monitoring

Correct Answer: A

QUESTION 2

Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

A. customer data

B. internal database

C. internal cloud

D. Internet

Correct Answer: D

QUESTION 3

A SOC engineer discovers that the organization had three DDOS attacks overnight. Four servers are reported offline, even though the hardware seems to be working as expected. One of the offline servers is affecting the pay system reporting times. Three employees, including executive management, have reported ransomware on their laptops. Which steps help the engineer understand a comprehensive overview of the incident?

A. Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.

B. Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.

C. Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.

D. Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.

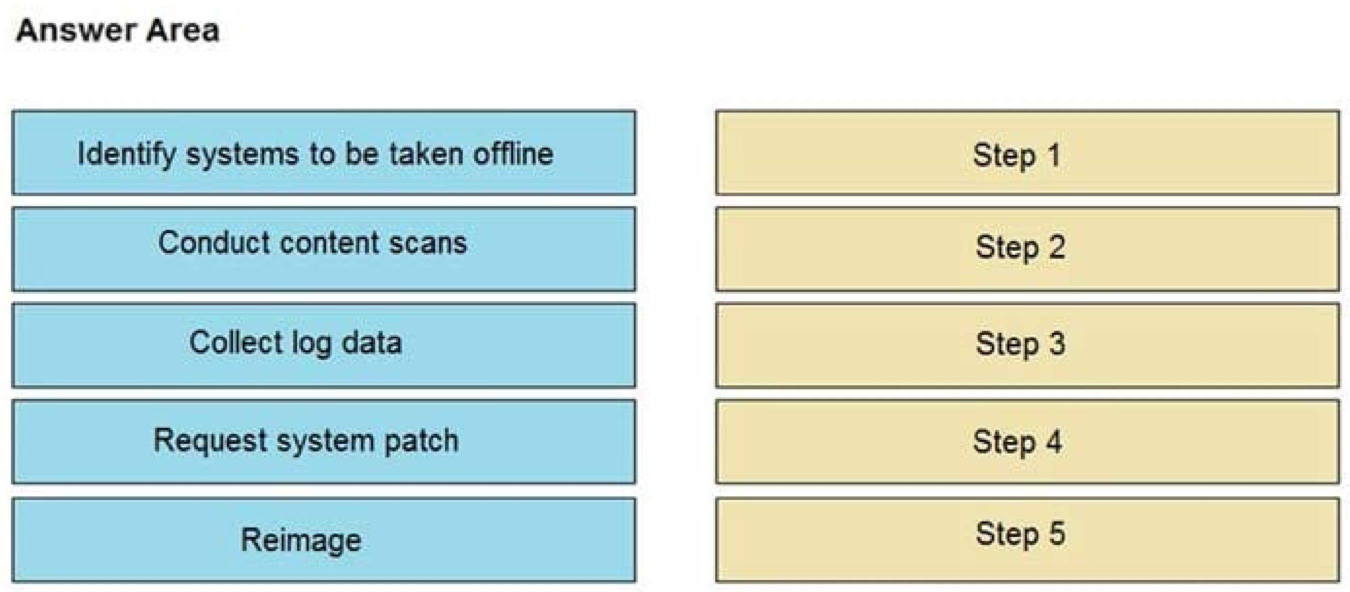
Correct Answer: D

QUESTION 4

DRAG DROP

An engineer notices that unauthorized software was installed on the network and discovers that it was installed by a dormant user account. The engineer suspects an escalation of privilege attack and responds to the incident. Drag and drop the activities from the left into the order for the response on the right.

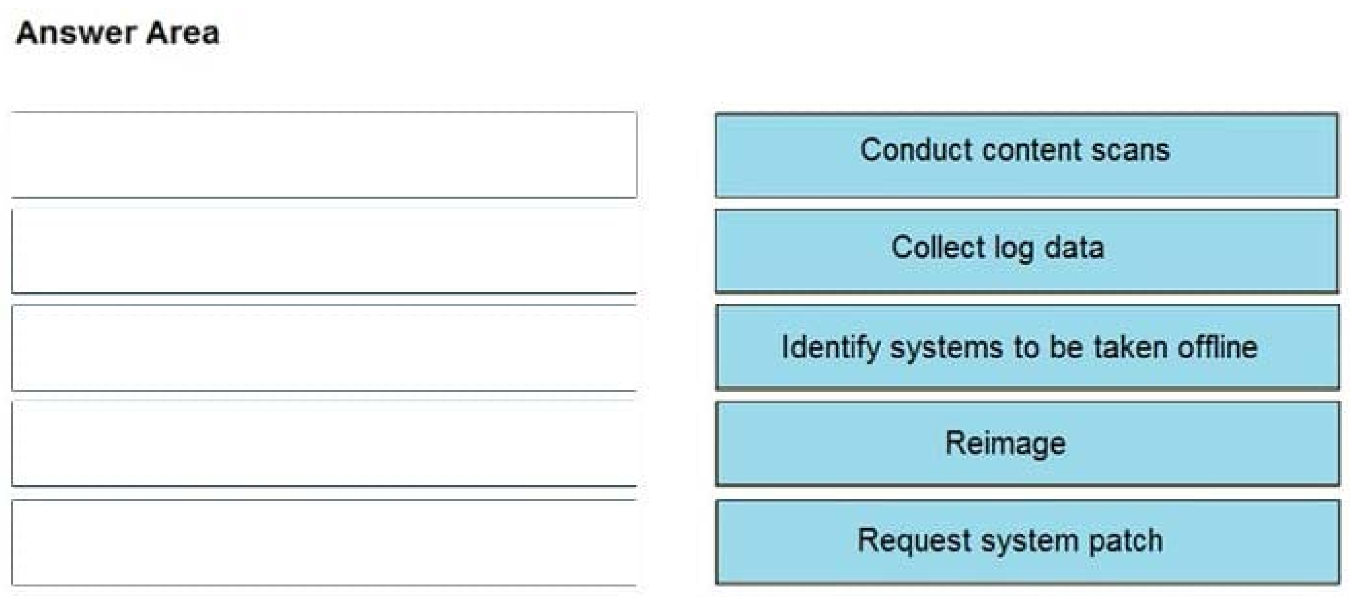
Select and Place:



Answer Area

Identify systems to be taken offline	Step 1
Conduct content scans	Step 2
Collect log data	Step 3
Request system patch	Step 4
Reimage	Step 5

Correct Answer:



Answer Area

	Conduct content scans
	Collect log data
	Identify systems to be taken offline
	Reimage
	Request system patch

QUESTION 5

A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server.

Which security solution is needed at this stage to mitigate the attack?

A. web security solution

B. email security solution

C. endpoint security solution

D. network security solution

Correct Answer: D

QUESTION 6

A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

A. Assess the network for unexpected behavior

B. Isolate critical hosts from the network

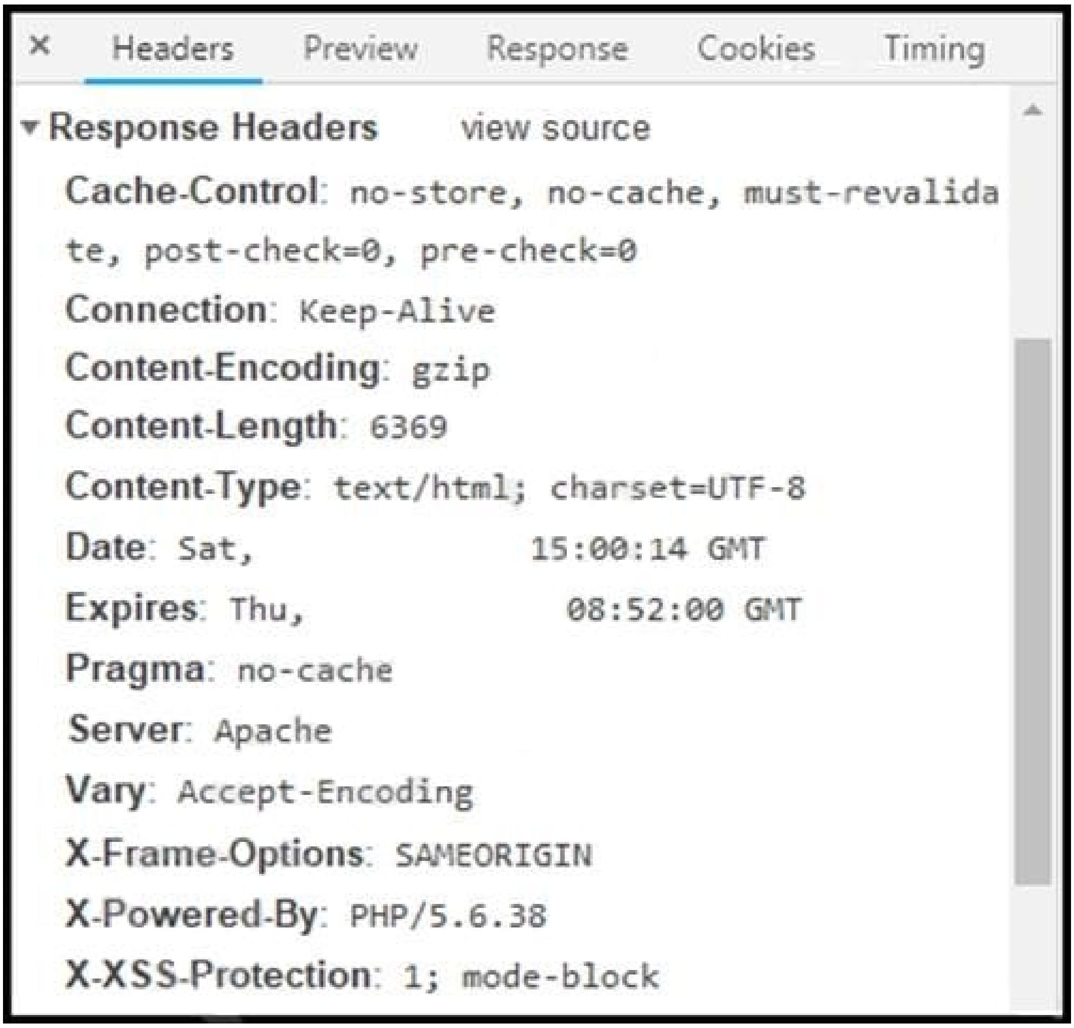
C. Patch detected vulnerabilities from critical hosts

D. Perform analysis based on the established risk factors

Correct Answer: B

QUESTION 7

Refer to the exhibit. Where are the browser page rendering permissions displayed?



▾ Response Headers

```
Cache-Control: no-store, no-cache, must-revalida
te, post-check=0, pre-check=0
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 6369
Content-Type: text/html; charset=UTF-8
Date: Sat,              15:00:14 GMT
Expires: Thu,              08:52:00 GMT
Pragma: no-cache
Server: Apache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Powered-By: PHP/5.6.38
X-XSS-Protection: 1; mode-block
```

A. X-Frame-Options

B. X-XSS-Protection

C. Content-Type

D. Cache-Control

Correct Answer: C

QUESTION 8

What do 2xx HTTP response codes indicate for REST APIs?

A. additional action must be taken by the client to complete the request

B. the server takes responsibility for error status codes

C. communication of transfer protocol-level information

D. successful acceptance of the client\\'s request

Correct Answer: D

Reference: https://restfulapi.net/http-status-codes/#:~:text=HTTP%20defines%20these%20standard%20status,results%20of%20a%20client%27s%20request.andtext=2xx%3A%20Success%20?20Indicates%20that%20the,order%20to%20complete%20their%20request.

QUESTION 9

An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions

B. Unpack the file in a sandbox to see how it reacts

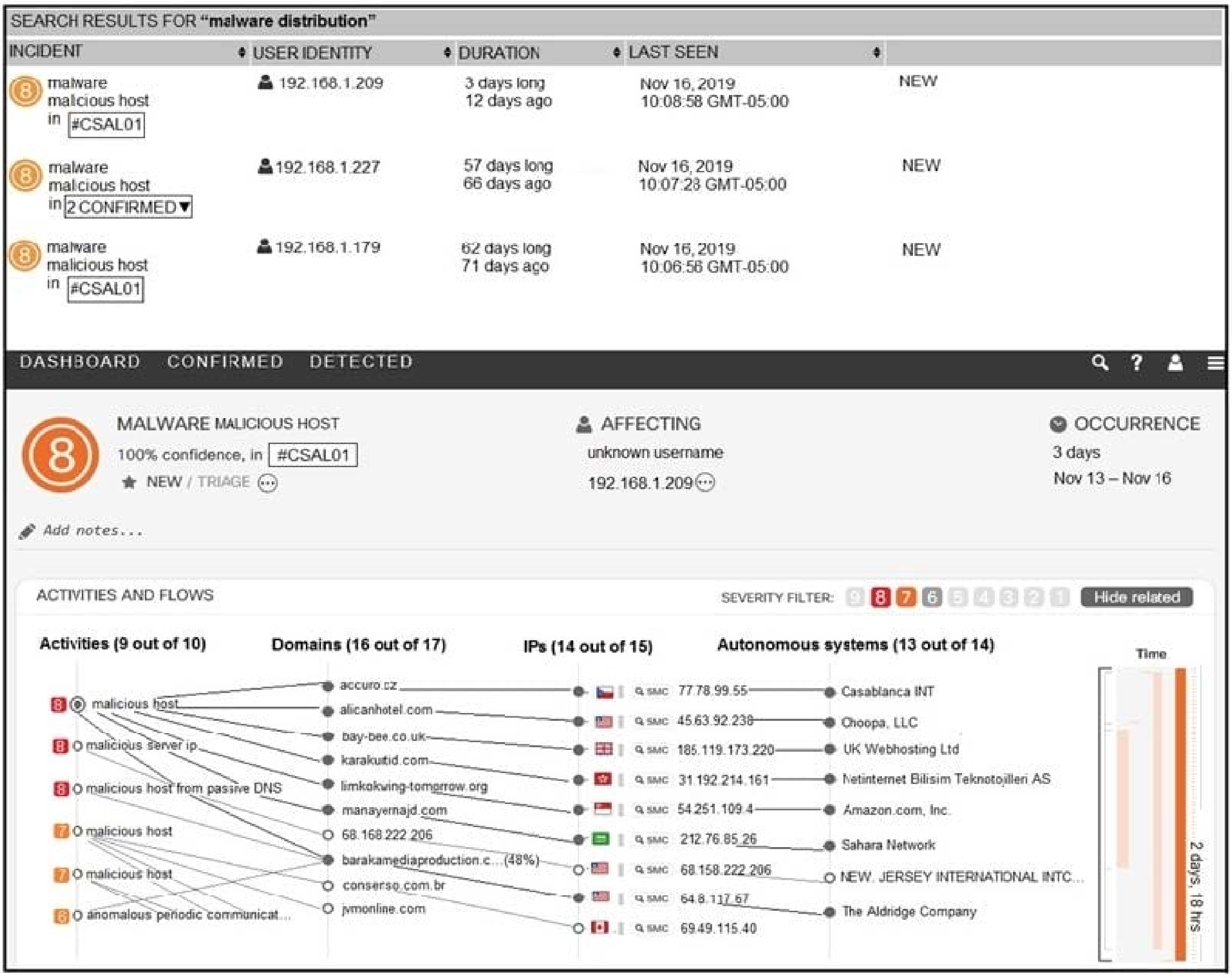
C. Research the malware online to see if there are noted findings

D. Disassemble the malware to understand how it was constructed

Correct Answer: C

QUESTION 10

Refer to the exhibit. For IP 192.168.1.209, what are the risk level, activity, and next step?



SEARCH RESULTS FOR "**malware distribution**"

INCIDENT	USER IDENTITY	DURATION	LAST SEEN	
8 malware malcious host in #CSAL01	192.168.1.209	3 days long 12 days ago	Nov 16, 2019 10:08:58 GMT-05:00	NEW
8 malware malcious host in 2 CONFIRMED ▾	192.168.1.227	57 days long 66 days ago	Nov 16, 2019 10:07:28 GMT-05:00	NEW
8 malware malicious host in #CSAL01	192.168.1.179	62 days long 71 days ago	Nov 16, 2019 10:06:58 GMT-05:00	NEW

DASHBOARD CONFIRMED DETECTED

8 MALWARE MALICIOUS HOST
100% confidence, in #CSAL01
NEW / TRIAGE

AFFECTING
unknown username
192.168.1.209

OCCURRENCE
3 days
Nov 13 – Nov 16

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Hide related

A. high risk level, anomalous periodic communication, quarantine with antivirus

B. critical risk level, malicious server IP, run in a sandboxed environment

C. critical risk level, data exfiltration, isolate the device

D. high risk level, malicious host, investigate further

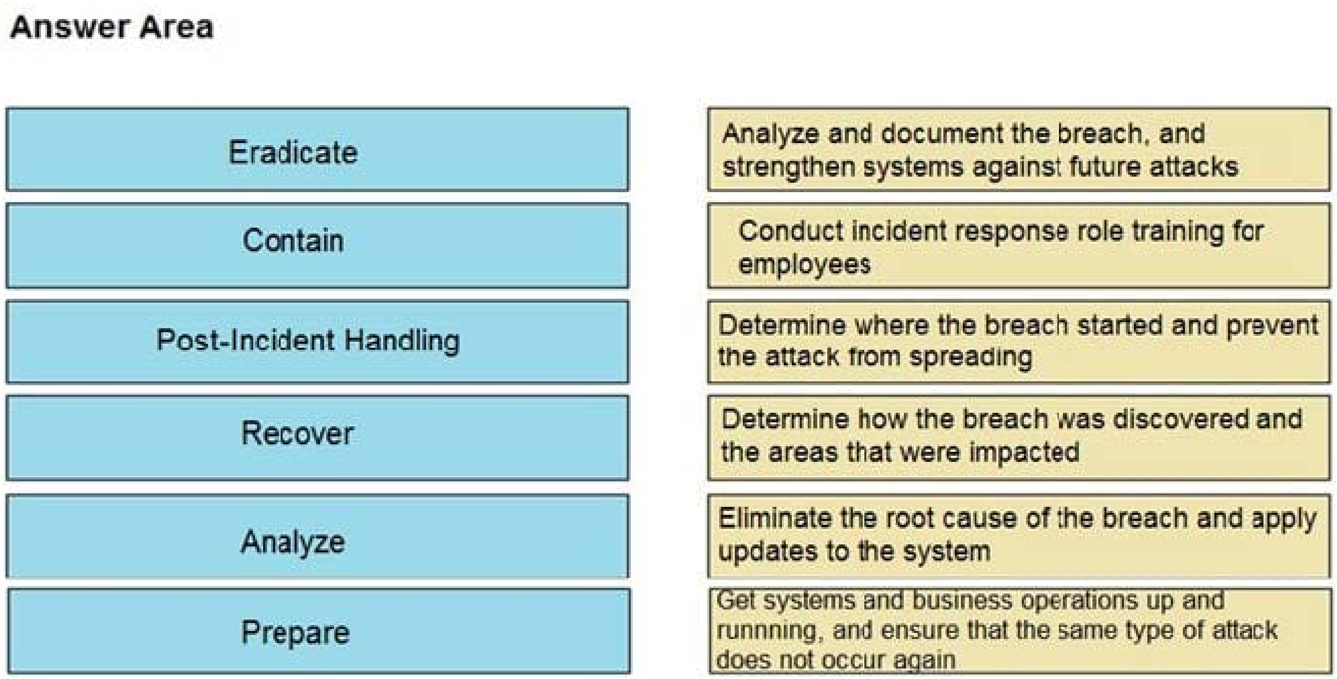
Correct Answer: A

QUESTION 11

DRAG DROP

Drag and drop the NIST incident response process steps from the left onto the actions that occur in the steps on the right.

Select and Place:



Answer Area

Eradicate

Contain

Post-Incident Handling

Recover

Analyze

Prepare

Analyze and document the breach, and strengthen systems against future attacks

Conduct incident response role training for employees

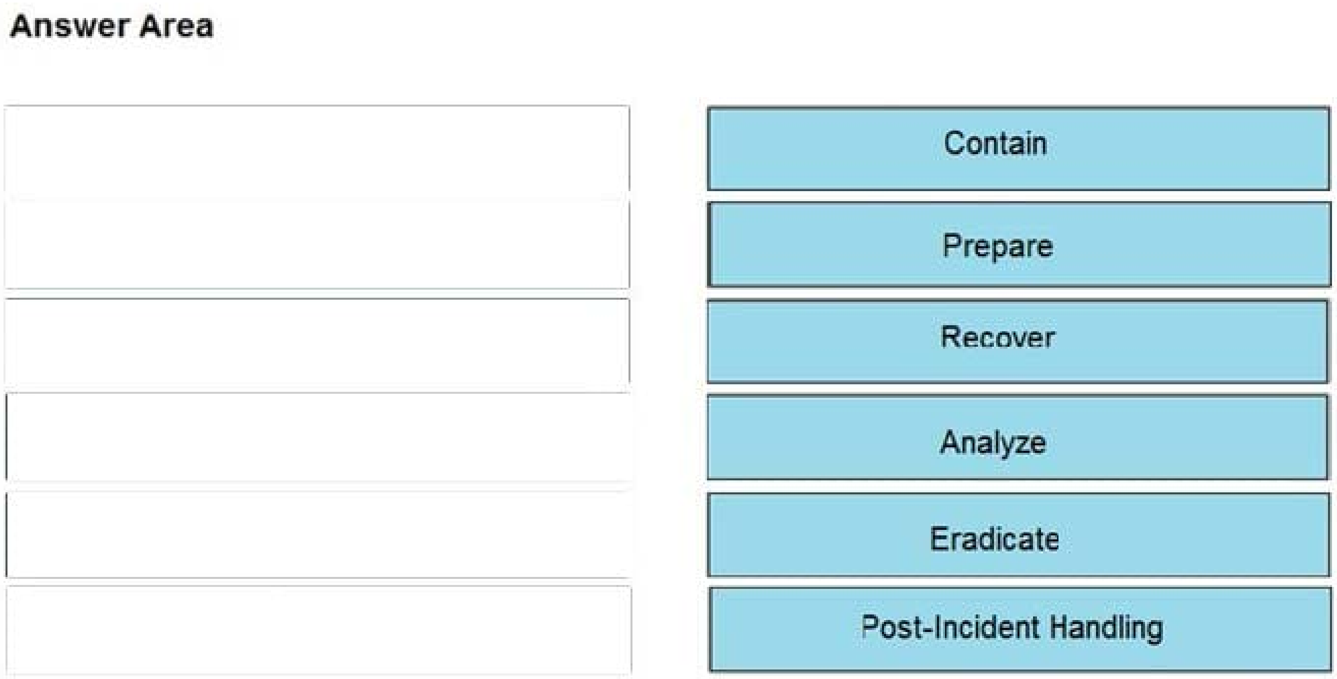
Determine where the breach started and prevent the attack from spreading

Determine how the breach was discovered and the areas that were impacted

Eliminate the root cause of the breach and apply updates to the system

Get systems and business operations up and runnning, and ensure that the same type of attack does not occur again

Correct Answer:



Answer Area

Contain

Prepare

Recover

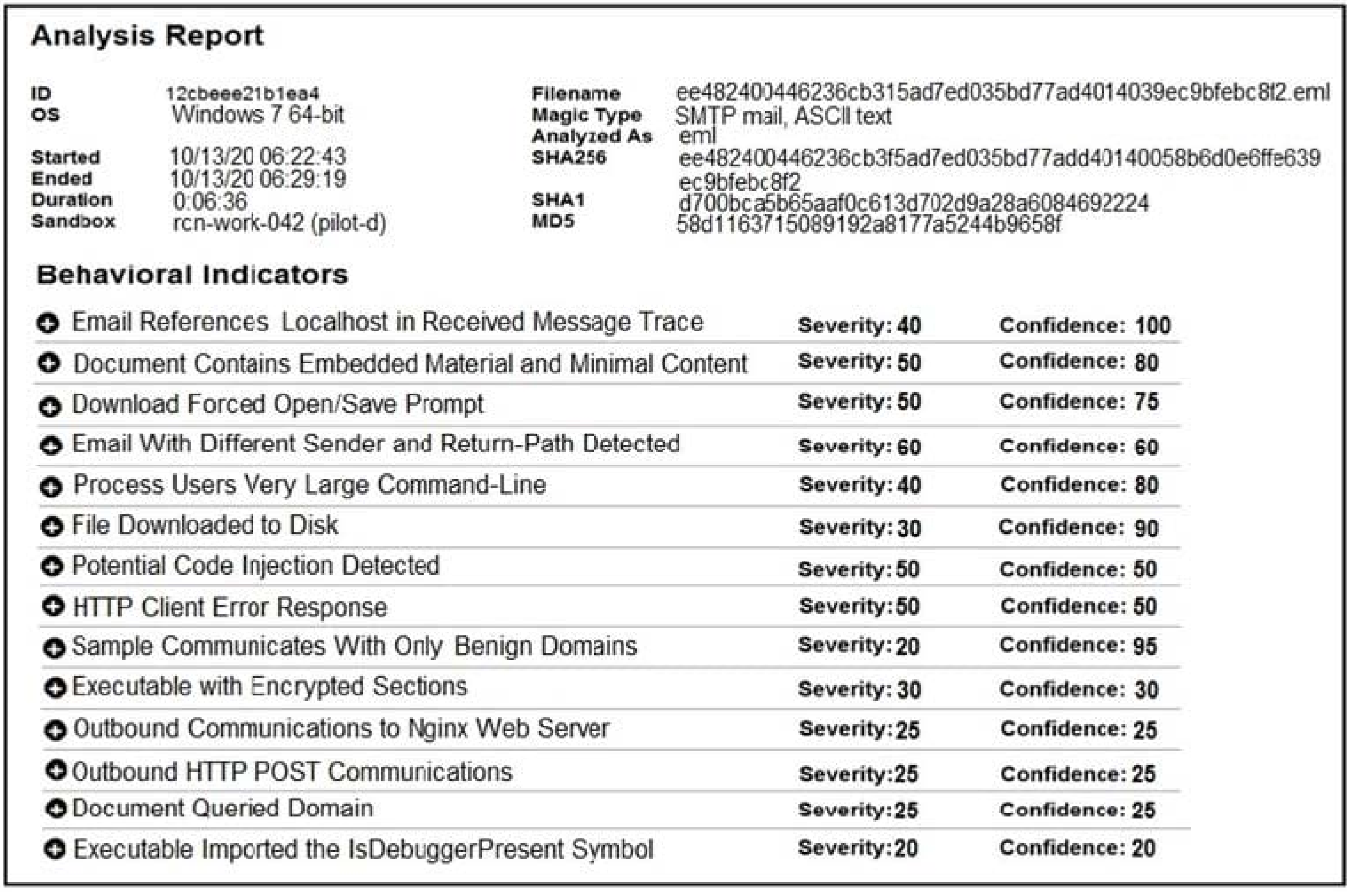
Analyze

Eradicate

Post-Incident Handling

Reference: https://www.securitymetrics.com/blog/6-phases-incident-response-plan

QUESTION 12



Analysis Report

ID	12cbeee21b1ea4	Filename	ee482400446236cb315ad7ed035bd77ad4014039ec9bfebc8f2.eml
OS	Windows 7 64-bit	Magic Type	SMTP mail, ASCII text
		Analyzed As	eml
Started	10/13/20 06:22:43	SHA256	ee482400446236cb3f5ad7ed035bd77add40140058b6d0e6ffe639 ec9bfebc8f2
Ended	10/13/20 06:29:19		
Duration	0:06:36	SHA1	d700bca5b65aaf0c613d702d9a28a6084692224
Sandbox	rcn-work-042 (pilot-d)	MD5	58d1163715089192a8177a5244b9658f

Behavioral Indicators

Email References Localhost in Received Message Trace	Severity: 40	Confidence: 100
Document Contains Embedded Material and Minimal Content	Severity: 50	Confidence: 80
Download Forced Open/Save Prompt	Severity: 50	Confidence: 75
Email With Different Sender and Return-Path Detected	Severity: 60	Confidence: 60
Process Users Very Large Command-Line	Severity: 40	Confidence: 80
File Downloaded to Disk	Severity: 30	Confidence: 90
Potential Code Injection Detected	Severity: 50	Confidence: 50
HTTP Client Error Response	Severity: 50	Confidence: 50
Sample Communicates With Only Benign Domains	Severity: 20	Confidence: 95
Executable with Encrypted Sections	Severity: 30	Confidence: 30
Outbound Communications to Nginx Web Server	Severity: 25	Confidence: 25
Outbound HTTP POST Communications	Severity: 25	Confidence: 25
Document Queried Domain	Severity: 25	Confidence: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20

Refer to the exhibit. Cisco Advanced Malware Protection installed on an end-user desktop automatically submitted a low prevalence file to the Threat Grid analysis engine. What should be concluded from this report?

A. Threat scores are high, malicious ransomware has been detected, and files have been modified

B. Threat scores are low, malicious ransomware has been detected, and files have been modified

C. Threat scores are high, malicious activity is detected, but files have not been modified

D. Threat scores are low and no malicious file activity is detected

Correct Answer: B

QUESTION 13

Employees report computer system crashes within the same week. An analyst is investigating one of the computers that crashed and discovers multiple shortcuts in the system\\'s startup folder. It appears that the shortcuts redirect users to malicious URLs.

What is the next step the engineer should take to investigate this case?

A. Remove the shortcut files

B. Check the audit logs

C. Identify affected systems

D. Investigate the malicious URLs

Correct Answer: C

QUESTION 14

A company recently started accepting credit card payments in their local warehouses and is undergoing a PCI audit. Based on business requirements, the company needs to store sensitive authentication data for 45 days. How must data be stored for compliance?

A. post-authorization by non-issuing entities if there is a documented business justification

B. by entities that issue the payment cards or that perform support issuing services

C. post-authorization by non-issuing entities if the data is encrypted and securely stored

D. by issuers and issuer processors if there is a legitimate reason

Correct Answer: C

QUESTION 15

What is the purpose of hardening systems?

A. to securely configure machines to limit the attack surface

B. to create the logic that triggers alerts when anomalies occur

C. to identify vulnerabilities within an operating system

D. to analyze attacks to identify threat actors and points of entry

Correct Answer: A