

350-201.VCEplus.premium.exam.100q

Number: 350-201
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

350-201

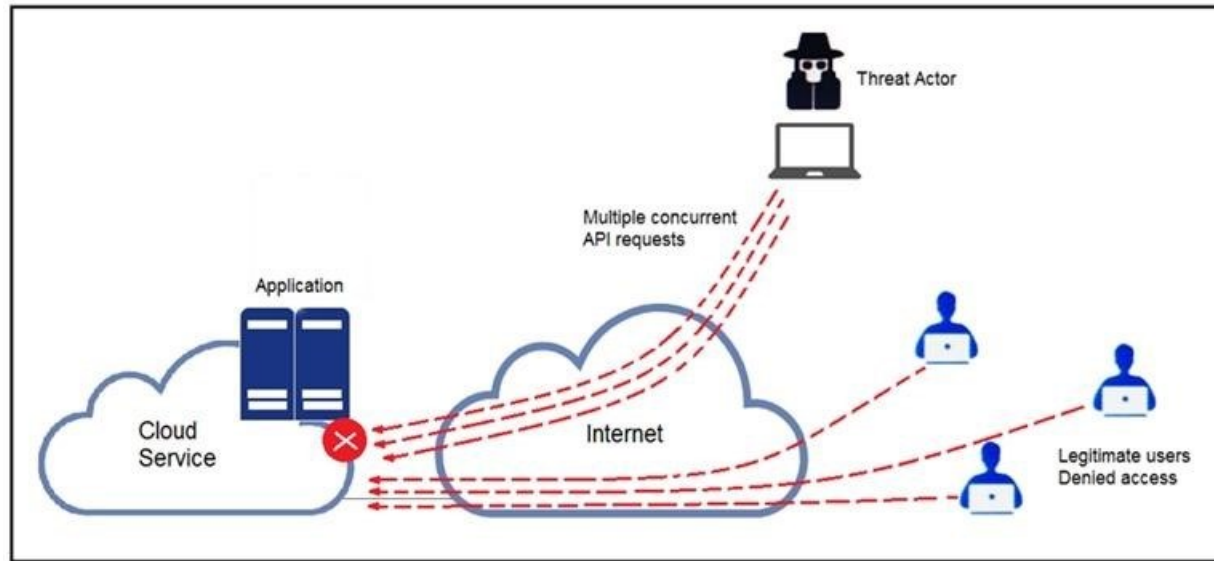
Performing CyberOps Using Cisco Security Technologies



Exam A

QUESTION 1

Refer to the exhibit. A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?



- A. Limit the number of API calls that a single client is allowed to make
- B. Add restrictions on the edge router on how often a single client can access the API
- C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API
- D. Increase the application cache of the total pool of active clients that call the API

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 2

DRAG DROP

An organization lost connectivity to critical servers, and users cannot access business applications and internal websites. An engineer checks the network devices to investigate the outage and determines that all devices are functioning. Drag and drop the steps from the left into the sequence on the right to continue investigating this issue. Not all options are used.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

A threat actor attacked an organization's Active Directory server from a remote location, and in a thirty-minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator's account was disabled. Which activity triggered the behavior analytics tool?

- A. accessing the Active Directory server
- B. accessing the server with financial data
- C. accessing multiple servers
- D. downloading more than 10 files

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

Refer to the exhibit. A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED



- A. packet sniffer
- B. malware analysis
- C. SIEM
- D. firewall manager

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

Analysis Report			
ID	12cbeee21b1ea4	Filename	fpzryrf.exe
OS	7601.1898.amd64fre.win7sp1_gdr.150316-1654	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Started	7/29/16 18:44:43	Analyzed As	exe
Ended	7/29/16 18:50:39	SHA256	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da
Duration	0:05:56	SHA1	a2de85810fd5ebcf29c5da5dd29ce03470772ad
Sandbox	phi-work-02 (pilot-d)	MD5	dd07d778edf8d581ffaadb1610aaa008
Warnings			
+ Executable Failed Integrity Check			
Behavioral Indicators			
+ CTB Locker Detected	Severity: 100	Confidence: 100	
+ Generic Ransomware Detected	Severity: 100	Confidence: 95	
+ Excessive Suspicious Activity Detected	Severity: 90	Confidence: 100	
+ Process Modified a File in a System Directory	Severity: 90	Confidence: 100	
+ Large Amount of High Entropy Artifacts Written	Severity: 100	Confidence: 80	
+ Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90	
+ Decoy Document Detected	Severity: 70	Confidence: 100	
+ Process Modified an Executable File	Severity: 60	Confidence: 100	
+ Process Modified File in a User Directory	Severity: 70	Confidence: 80	
+ Windows Crash Tool Execution Detected	Severity: 20	Confidence: 80	
+ Hook Procedure Detected in Executable	Severity: 35	Confidence: 40	
+ Ransomware 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 has automatically submitted a low prevalence file to the Threat Grid analysis engine for further analysis. What should be concluded from this report?

- A. The prioritized behavioral indicators of compromise do not justify the execution of the “ransomware” because the scores do not indicate the likelihood of malicious ransomware.
- B. The prioritized behavioral indicators of compromise do not justify the execution of the “ransomware” because the scores are high and do not indicate the likelihood of malicious ransomware.
- C. The prioritized behavioral indicators of compromise justify the execution of the “ransomware” because the scores are high and indicate the likelihood that malicious ransomware has been detected.
- D. The prioritized behavioral indicators of compromise justify the execution of the “ransomware” because the scores are low and indicate the likelihood that malicious ransomware has been detected.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

- A. Determine the assets to which the attacker has access
- B. Identify assets the attacker handled or acquired
- C. Change access controls to high risk assets in the enterprise
- D. Identify movement of the attacker in the enterprise

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:**QUESTION 7**

A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

- A. incident response playbooks
- B. asset vulnerability assessment
- C. report of staff members with asset relations
- D. key assets and executives
- E. malware analysis report

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://cloudogre.com/risk-assessment/>

QUESTION 8

URIs:

- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

Refer to the exhibit. At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

- A. exploitation
- B. actions on objectives
- C. delivery
- D. reconnaissance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf>

QUESTION 9

<p><u>Vulnerability #1</u></p> <p>A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions:</p> <ul style="list-style-type: none"> a) Be logged in to the device over telnet or SSH, or through the local console b) Be logged in as a high-privileges administrative user <p>In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device.</p> <p>All software versions are affected Fixes are available now There are no workarounds or mitigations</p>	<p><u>Vulnerability #2</u></p> <p>A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to:</p> <ul style="list-style-type: none"> a) Be able to reach port 80/tcp on an affected device b) The web-based management interface needs to be enabled on the device <p>The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack.</p> <p>All software versions are affected There are no fixes available now Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.</p>
--	---

Refer to the exhibit. How must these advisories be prioritized for handling?



- A. The highest priority for handling depends on the type of institution deploying the devices
- B. Vulnerability #2 is the highest priority for every type of institution
- C. Vulnerability #1 and vulnerability #2 have the same priority
- D. Vulnerability #1 is the highest priority for every type of institution

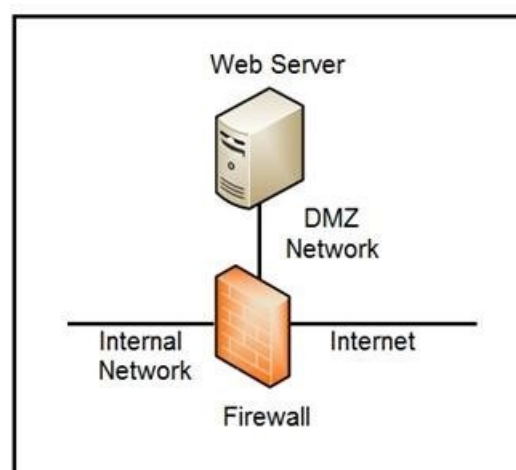
Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10



Refer to the exhibit. Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

- A. Create an ACL on the firewall to allow only TLS 1.3
- B. Implement a proxy server in the DMZ network
- C. Create an ACL on the firewall to allow only external connections
- D. Move the webserver to the internal network

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

DRAG DROP

Drag and drop the phases to evaluate the security posture of an asset from the left onto the activity that happens during the phases on the right.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12 According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?



- A. Perform a vulnerability assessment
- B. Conduct a data protection impact assessment
- C. Conduct penetration testing
- D. Perform awareness testing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf

QUESTION 13

A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?

- A. Classify the criticality of the information, research the attacker's motives, and identify missing patches
- B. Determine the damage to the business, extract reports, and save evidence according to a chain of custody
- C. Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploited
- D. Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation plan

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14 A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

- A. Identify the business applications running on the assets
- B. Update software to patch third-party software
- C. Validate CSRF by executing exploits within Metasploit
- D. Fix applications according to the risk scores

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

An engineer is analyzing a possible compromise that happened a week ago when the company ? (Choose two.)

- A. firewall
- B. Wireshark
- C. autopsy
- D. SHA512
- E. IPS

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16 A European-based advertisement company collects tracking information from partner websites and stores it on a local server to provide tailored ads. Which standard must the company follow to safeguard the resting data?

- A. HIPAA
- B. PCI-DSS
- C. Sarbanes-Oxley
- D. GDPR

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.thesststore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/>

QUESTION 17

An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

- A. Host a discovery meeting and define configuration and policy updates
- B. Update the IDS/IPS signatures and reimage the affected hosts
- C. Identify the systems that have been affected and tools used to detect the attack
- D. Identify the traffic with data capture using Wireshark and review email filters

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

An engineer is going through vulnerability triage with company management because of a recent malware outbreak from which 21 affected assets need to be patched or remediated. Management decides not to prioritize fixing the assets and accepts the vulnerabilities. What is the next step the engineer should take?

- A. Investigate the vulnerability to prevent further spread
- B. Acknowledge the vulnerabilities and document the risk
- C. Apply vendor patches or available hot fixes
- D. Isolate the assets affected in a separate network

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?

- A. Conduct a risk assessment of systems and applications
- B. Isolate the infected host from the rest of the subnet
- C. Install malware prevention software on the host
- D. Analyze network traffic on the host's subnet

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?

- A. diagnostic
- B. qualitative
- C. predictive
- D. statistical

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://insights.principa.co.za/4-types-of-data-analytics-descriptive-diagnostic-predictive-prescriptive>

QUESTION 22 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Analysis Report			
ID	12cbeee21b1ea4	Filename	ee482400446236cb315ad7ed035bd77ad4014039ec9bfebc8f2.eml
OS	Windows 7 64-bit	Magic Type	SMTP mail, ASCII text
Started	10/13/20 06:22:43	Analyzed As	eml
Ended	10/13/20 06:29:19	SHA256	ee482400446236cb3f5ad7ed035bd77add40140058b6d0e6ffe639ec9bfebc8f2
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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

An organization is using a PKI management server and a SOAR platform to manage the certificate lifecycle. The SOAR platform queries a certificate management tool to check all endpoints for SSL certificates that have either expired or are nearing expiration. Engineers are struggling to manage problematic certificates outside of PKI management since deploying certificates and tracking them requires searching server owners manually. Which action will improve workflow automation?

- A. Implement a new workflow within SOAR to create tickets in the incident response system, assign problematic certificate update requests to server owners, and register change requests.
- B. Integrate a PKI solution within SOAR to create certificates within the SOAR engines to track, update, and monitor problematic certificates.
- C. Implement a new workflow for SOAR to fetch a report of assets that are outside of the PKI zone, sort assets by certification management leads and automate alerts that updates are needed.
- D. Integrate a SOAR solution with Active Directory to pull server owner details from the AD and send an automated email for problematic certificates requesting updates.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

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:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 26

Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

- A. **chmod 666**
- B. **chmod 774**
- C. **chmod 775**
- D. **chmod 777**

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.pluralsight.com/blog/it-ops/linux-file-permissions>

QUESTION 27

A SIEM tool fires an alert about a VPN connection attempt from an unusual location. The incident response team validates that an attacker has installed a remote access tool on a user's laptop while traveling. The attacker has the user's credentials and is attempting to connect to the network.

What is the next step in handling the incident?

- A. Block the source IP from the firewall
- B. Perform an antivirus scan on the laptop
- C. Identify systems or services at risk
- D. Identify lateral movement

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28 A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company's infrastructure. Which steps should an engineer take at the recovery stage?

- A. Determine the systems involved and deploy available patches
- B. Analyze event logs and restrict network access
- C. Review access lists and require users to increase password complexity
- D. Identify the attack vector and update the IDS signature list

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

A patient views information that is not theirs when they sign in to the hospital's online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue. An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real-time. What is the first step the analyst should take to address this incident?

- A. Evaluate visibility tools to determine if external access resulted in tampering
- B. Contact the third-party handling provider to respond to the incident as critical
- C. Turn off all access to the patient portal to secure patient records
- D. Review system and application logs to identify errors in the portal code

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 30

```
def map_to_lowercase_letter(s):
    return ord('a') + ((s-ord('a')) % 26)
def next_domain(domain):
    dl = [ord(x) for x in list(domain)]
    dl[0] = map_to_lowercase_letter(dl[0] + dl[3])
    dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
    dl[2] = map_to_lowercase_letter(dl[0] + dl[2] - 1)
    dl[3] = map_to_lowercase_letter(dl[1] + dl[2] + dl[3])
    return ".join([chr(x) for x in dl])
def isBanjoriTail(seed):
    for c0 in xrange(97,123):
        for c1 in xrange(97, 123):
            for c2 in xrange(97,123):
                for c3 in xrange(97,123):
                    domain = chr(c0)+chr(c1)+chr(c2)+chr(c3)
                    domain = next_domain(domain)
                    if seed.startswith(domain):
                        return False
    return True
seeds = {
    "nhcisatformalisticirekb.com",
    "egfesatformalisticirekb.com",
    "qwfusatformalisticirekb.com",
    "eijhsatformalisticirekb.com",
    "siowsatformalisticirekb.com",
    "dhansatformalisticirekb.com",
    "zvogsatformalisticirekb.com",
    "yaewsatformalisticirekb.com",
    "wgxfusatformalisticirekb.com",
    "vfxlsatformalisticirekb.com",
    "usjssatformalisticirekb.com",
    "selzsatformalisticirekb.com",
    "nzjqsatformalisticirekb.com",
    "kencsatformalisticirekb.com",
    "fzkxsatformalisticirekb.com",
    "babysatformalisticirekb.com",
}
for seed in seeds:
    print seed,isBanjoriTail(seed)
```



Refer to the exhibit. What results from this script?

- A. Seeds for existing domains are checked
- B. A search is conducted for additional seeds
- C. Domains are compared to seed rules
- D. A list of domains as seeds is blocked

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

DRAG DROP

Drag and drop the threat from the left onto the scenario that introduces the threat on the right. Not all options are used.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

```
<employees>
  <employee>
    <lastname>Smith</lastname>
    <firstname>Richard</firstname>
  </employee>
  <employee>
    <lastname>Witzel</lastname>
    <firstname>Sevan</firstname>
  </employee>
</employees>
```

Refer to the exhibit. Which data format is being used?

- A. JSON
- B. HTML
- C. XMLD. CSV

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 33

The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident handling guide?

- A. Contain the malware
- B. Install IPS software
- C. Determine the escalation path
- D. Perform vulnerability assessment

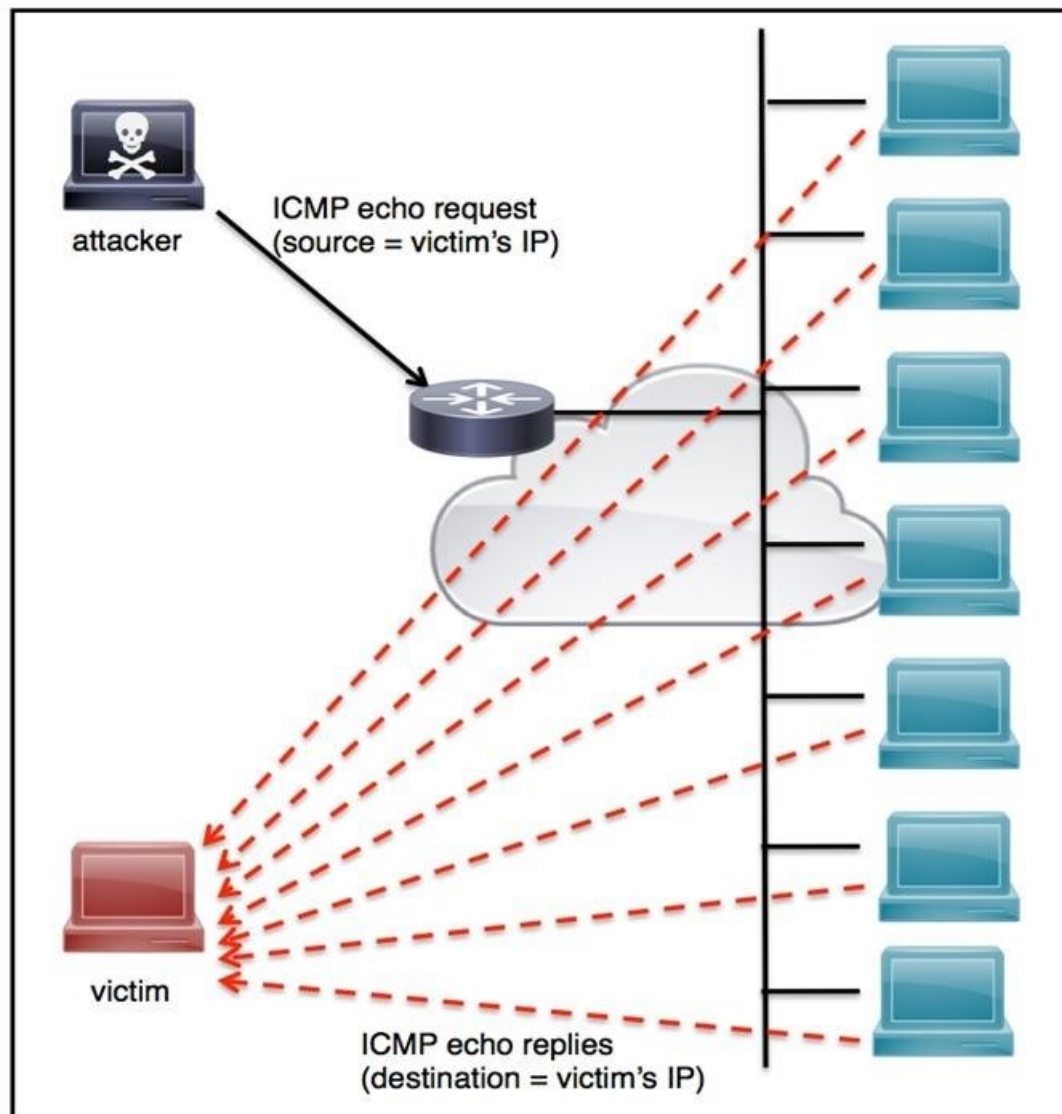
Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34



Refer to the exhibit. An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action does the engineer recommend?

- A. Use command **ip verify reverse-path interface**
- B. Use global configuration command **service tcp-keepalives-out**
- C. Use subinterface command **no ip directed-broadcast**
- D. Use logging trap 6

Correct Answer: A

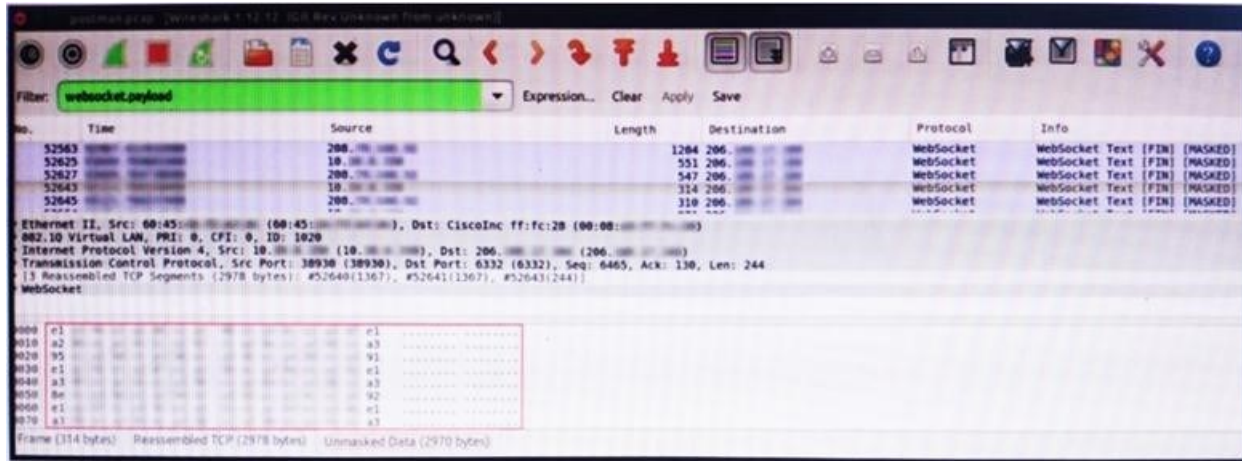
Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.ccexpert.us/pix-firewall/ip-verify-reversepath-command.html>

QUESTION 35



Refer to the exhibit. An engineer is analyzing this Vlan0386-int12-117.pcap file in Wireshark after detecting a suspicious network activity. The origin header for the direct IP connections in the packets was initiated by a google chrome extension on a WebSocket protocol. The engineer checked message payloads to determine what information was being sent off-site but the payloads are obfuscated and unreadable. What does this STIX indicate?

- A. The extension is not performing as intended because of restrictions since ports 80 and 443 should be accessible
- B. The traffic is legitimate as the google chrome extension is reaching out to check for updates and fetches this information
- C. There is a possible data leak because payloads should be encoded as UTF-8 text
- D. There is a malware that is communicating via encrypted channels to the command and control server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 36

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

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 37

An engineer received an alert of a zero-day vulnerability affecting desktop phones through which an attacker sends a crafted packet to a device, resets the credentials, makes the device unavailable, and allows a default administrator account login. Which step should an engineer take after receiving this alert?

- A. Initiate a triage meeting to acknowledge the vulnerability and its potential impact
- B. Determine company usage of the affected products
- C. Search for a patch to install from the vendor
- D. Implement restrictions within the VoIP VLANS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

```
def get_umbrella_dispos(domains):
    # put in right format to pass as argument in POST request
    values = str(json.dumps(domains))
    req = requests.post(investigate_url, data=values, headers=headers)
    # time for timestamp of verdict domain
    time = datetime.now().isoformat()
    # error handling if true then the request was HTTP 200, so successful
    if(req.status_code == 200):
        print("SUCCESS: request has the following code: 200\n")
        output = req.json()

        if(domain_status == -1):
            print("The domain %(domain)s is found MALICIOUS at %(time)s\n" % {'domain': domain, 'time': time})
        elif(domain_status == 1):
            print("The domain %(domain)s is found CLEAN at %(time)s\n" %
                  {'domain': domain, 'time': time})
        else:
            print("The domain %(domain)s is found UNDEFINED / RISKY at %(time)s\n" %
                  {'domain': domain, 'time': time})
    else:
        print("An error has occurred with the following code %(error)s, please consult the following link:
              https://docs.umbrella.com/investigate-api/%"
              {'error': req.status_code})
```

Refer to the exhibit. Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined? A.

```
for domain in domains[:]:
    domain_status = domain_output["status"]

while domain in domains:
    domain_status = domain_output["status"]

for domain in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]

while domains in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```

B.

C.

D.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

An engineer receives an incident ticket with hundreds of intrusion alerts that require investigation. An analysis of the incident log shows that the alerts are from trusted IP addresses and internal devices. The final incident report stated that these alerts were false positives and that no intrusions were detected. What action should be taken to harden the network?

- A. Move the IPS to after the firewall facing the internal network
- B. Move the IPS to before the firewall facing the outside network
- C. Configure the proxy service on the IPS
- D. Configure reverse port forwarding on the IPS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

A SOC team is informed that a UK-based user will be traveling between three countries over the next 60 days. Having the names of the 3 destination countries and the user's working hours, what must the analyst do next to detect an abnormal behavior?

- A. Create a rule triggered by 3 failed VPN connection attempts in an 8-hour period
- B. Create a rule triggered by 1 successful VPN connection from any nondestination country
- C. Create a rule triggered by multiple successful VPN connections from the destination countries
- D. Analyze the logs from all countries related to this user during the traveling period

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41 An engineer receives a report that indicates a possible incident of a malicious insider sending company information to outside parties. What is the first action the engineer must take to determine whether an incident has occurred?

- A. Analyze environmental threats and causes
- B. Inform the product security incident response team to investigate further
- C. Analyze the precursors and indicators
- D. Inform the computer security incident response team to investigate further

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach. Which indicator generated this IOC event?

- A. ExecutedMalware.ioc
- B. Crossrider.ioc
- C. ConnectToSuspiciousDomain.ioc

D. W32 AccesschkUtility.ioc

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

Refer to the exhibit. Which command was executed in PowerShell to generate this log?

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

A. Get-EventLog -LogName*

B. Get-EventLog -List

C. Get-WinEvent -ListLog* -ComputerName localhost

D. Get-WinEvent -ListLog*

Correct Answer: A

Section: (none)

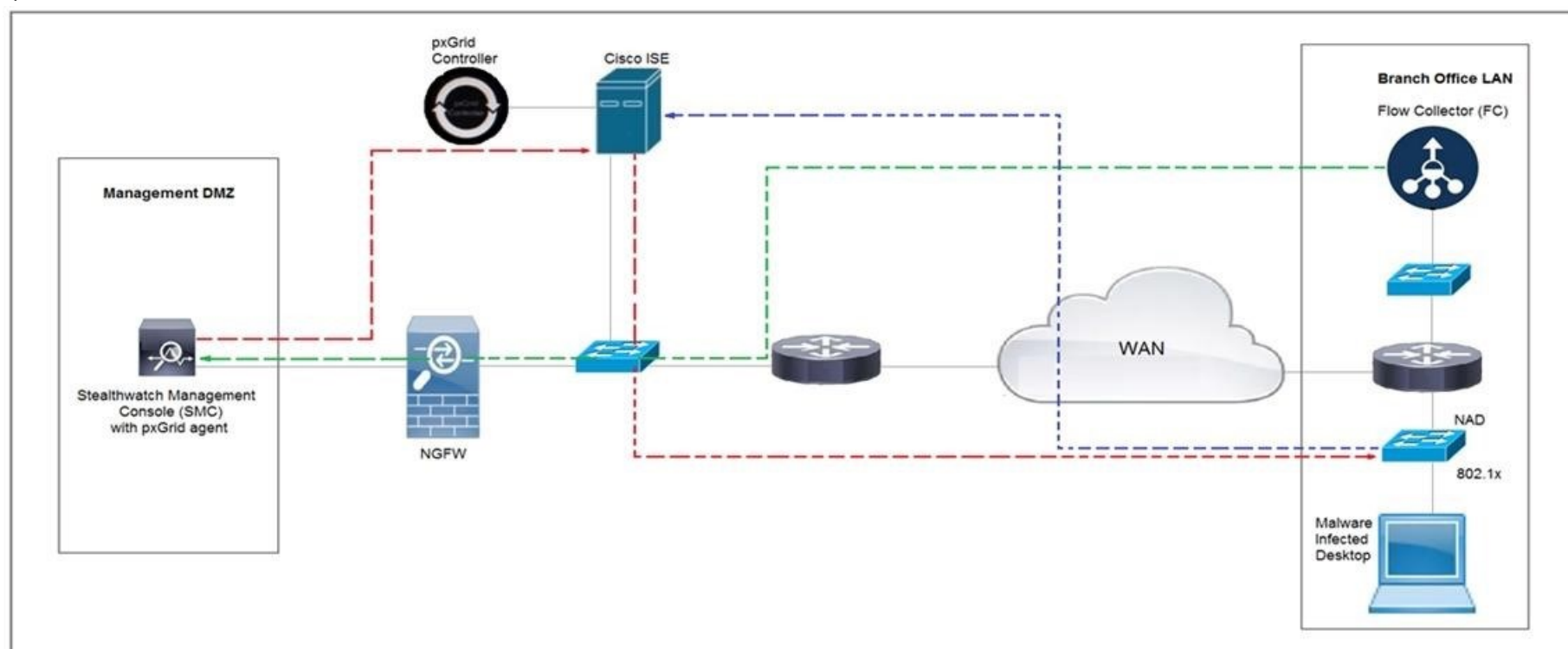
Explanation

Explanation/Reference:

Reference: <https://lists.xymon.com/archive/2019-March/046125.html>



QUESTION 44



Refer to the exhibit. Cisco Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a Quarantine VLAN using Adaptive Network Control policy. Which telemetry feeds were correlated with SMC to identify the malware?

- A. NetFlow and event data
- B. event data and syslog data
- C. SNMP and syslog data
- D. NetFlow and SNMP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

A security architect is working in a processing center and must implement a DLP solution to detect and prevent any type of copy and paste attempts of sensitive data within unapproved applications and removable devices. Which technical architecture must be used?

- A. DLP for data in motion
- B. DLP for removable data
- C. DLP for data in use
- D. DLP for data at rest

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.endpointprotector.com/blog/what-is-data-loss-prevention-dlp/>



QUESTION 46

A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory. What is the next step the analyst should take?

- A. Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
- B. Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities
- C. Review the server backup and identify server content and data criticality to assess the intrusion risk
- D. Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

A security expert is investigating a breach that resulted in a \$32 million loss from customer accounts. Hackers were able to steal API keys and two-factor codes due to a vulnerability that was introduced in a new code a few weeks before the attack. Which step was missed that would have prevented this breach?

- A. use of the Nmap tool to identify the vulnerability when the new code was deployed
- B. implementation of a firewall and intrusion detection system
- C. implementation of an endpoint protection system
- D. use of SecDevOps to detect the vulnerability during development

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://securityintelligence.com/how-to-prioritize-security-vulnerabilities-in-secdevops/>

QUESTION 48

An API developer is improving an application code to prevent DDoS attacks. The solution needs to accommodate instances of a large number of API requests coming for legitimate purposes from trustworthy services. Which solution should be implemented?

- A. Restrict the number of requests based on a calculation of daily averages. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.
- B. Implement REST API Security Essentials solution to automatically mitigate limit exhaustion. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.
- C. Increase a limit of replies in a given interval for each API. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.
- D. Apply a limit to the number of requests in a given time interval for each API. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.whoishostingthis.com/resources/http-status-codes/>

QUESTION 49

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 ( msg:"PROTOCOL-  
IMAP login brute force attempt";  
flow:to_server,established,no_stream;  
content:"LOGIN",fast_pattern,nocase; detection_filter:track  
by_dst, count 5, seconds 900; metadata:ruleset community;  
service:imap; reference:url,attack.mitre.org/techniques/T1110;  
classtype:suspicious-login; sid:2273; rev:12; )
```

Refer to the exhibit. IDS is producing an increased amount of false positive events about brute force attempts on the organization's mail server. How should the Snort rule be modified to improve performance?

- A. Block list of internal IPs from the rule
- B. Change the rule content match to case sensitive
- C. Set the rule to track the source IP
- D. Tune the count and seconds threshold of the rule

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 50**

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51 An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

- A. Modify the alert rule to "output alert_syslog: output log"
- B. Modify the output module rule to "output alert_quick: output filename"
- C. Modify the alert rule to "output alert_syslog: output header"
- D. Modify the output module rule to "output alert_fast: output filename"

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20201231%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20201231T141156Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=e122ab6eb1659e13b3bc6bb2451ce693c0298b76c1962c3743924bc5fd83d382

QUESTION 52

DRAG DROP

Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.

Select and Place:

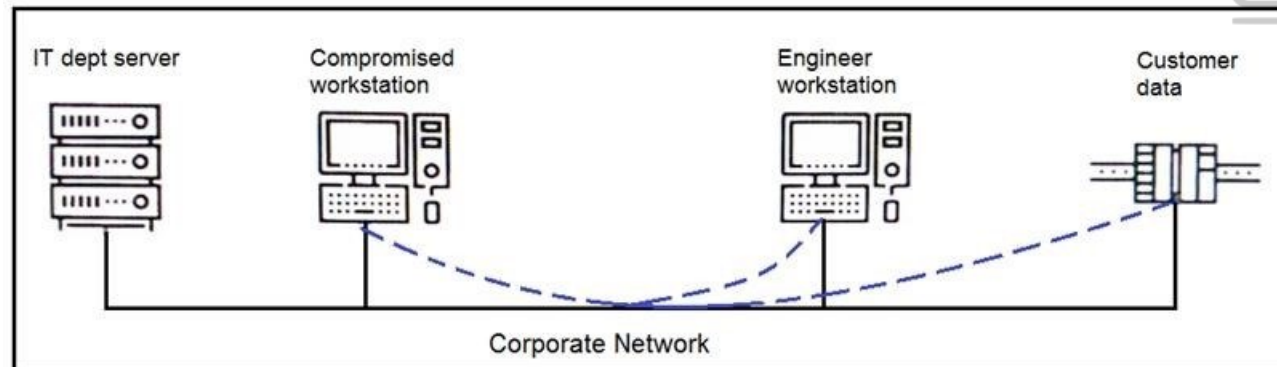
Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53



Refer to the exhibit. An engineer received a report that an attacker has compromised a workstation and gained access to sensitive customer data from the network using insecure protocols. Which action prevents this type of attack in the future?

- A. Use VLANs to segregate zones and the firewall to allow only required services and secured protocols
- B. Deploy a SOAR solution and correlate log alerts from customer zones
- C. Deploy IDS within sensitive areas and continuously update signatures
- D. Use syslog to gather data from multiple sources and detect intrusion logs for timely responses

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54 How does Wireshark decrypt TLS network traffic?

- A. with a key log file using per-session secrets
- B. using an RSA public key
- C. by observing DH key exchange
- D. by defining a user-specified decode-as

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://wiki.wireshark.org/TLS>

QUESTION 55

```
#!/usr/bin/env python3

import re

def (username, minlen):
    if type(username) != str:
        raise TypeError
    if minlen < 3:
        raise ValueError
    if len(username) < minlen:
        return False
    if not re.match('[a-z0-9._]*$', username):
        return False
    if username[0].isnumeric():
        return False
    return True
```



Refer to the exhibit. An organization is using an internal application for printing documents that requires a separate registration on the website. The application allows format-free user creation, and users must match these required conditions to comply with the company's user creation policy:

- minimum length: 3
- usernames can only use letters, numbers, dots, and underscores
- usernames cannot begin with a number

The application administrator has to manually change and track these daily to ensure compliance. An engineer is tasked to implement a script to automate the process according to the company user creation policy. The engineer implemented this piece of code within the application, but users are still able to create format-free usernames. Which change is needed to apply the restrictions?

- A. modify code to return error on restrictions `def return false_user(username, minlen)`
- B. automate the restrictions `def automate_user(username, minlen)`
- C. validate the restrictions, `def validate_user(username, minlen)`
- D. modify code to force the restrictions, `def force_user(username, minlen)`

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

An engineer implemented a SOAR workflow to detect and respond to incorrect login attempts and anomalous user behavior. Since the implementation, the security team has received dozens of false positive alerts and negative feedback from system administrators and privileged users. Several legitimate users were tagged as a threat and their accounts blocked, or credentials reset because of unexpected login times and incorrectly typed credentials. How should the workflow be improved to resolve these issues?

- A. Meet with privileged users to increase awareness and modify the rules for threat tags and anomalous behavior alerts
- B. Change the SOAR configuration flow to remove the automatic remediation that is increasing the false positives and triggering threats
- C. Add a confirmation step through which SOAR informs the affected user and asks them to confirm whether they made the attempts
- D. Increase incorrect login tries and tune anomalous user behavior not to affect privileged accounts

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com, realm=0, isRealm=0, realmDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Refer to the exhibit. Where does it signify that a page will be stopped from loading when a scripting attack is detected?

- A. x-frame-options
- B. x-content-type-options
- C. x-xss-protection
- D. x-test-debug

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/customize-http-security-headers-ad-fs>

QUESTION 58 What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

- A. 401
- B. 402
- C. 403
- D. 404
- E. 405

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

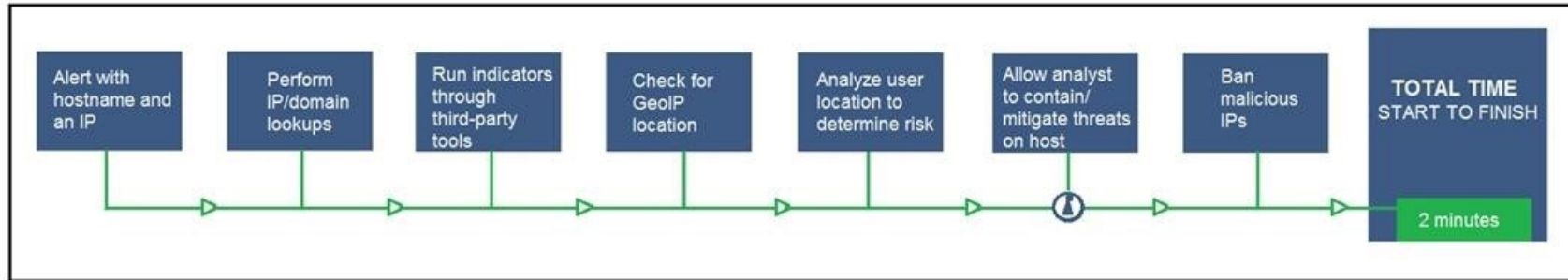
Reference: <https://airbrake.io/blog/http-errors/401-unauthorized-error#:~:text=The%20401%20Unauthorized%20Error%20is,client%20could%20not%20be%20authenticated.>

QUESTION 59 What is a principle of Infrastructure as Code?

- A. System maintenance is delegated to software systems
- B. Comprehensive initial designs support robust systems
- C. Scripts and manual configurations work together to ensure repeatable routines
- D. System downtime is grouped and scheduled across the infrastructure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 60



Refer to the exhibit. An engineer configured this SOAR solution workflow to identify account theft threats and privilege escalation, evaluate risk, and respond by resolving the threat. This solution is handling more threats than Security analysts have time to analyze. Without this analysis, the team cannot be proactive and anticipate attacks. Which action will accomplish this goal?

- A. Exclude the step “BAN malicious IP” to allow analysts to conduct and track the remediation
- B. Include a step “Take a Snapshot” to capture the endpoint state to contain the threat for analysis
- C. Exclude the step “Check for GeoIP location” to allow analysts to analyze the location and the associated risk based on asset criticality
- D. Include a step “Reporting” to alert the security department of threats identified by the SOAR reporting engine

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 61
 DRAG DROP

Drag and drop the telemetry-related considerations from the left onto their cloud service models on the right.

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 62

A company’s web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and vulnerabilities. Which additional element is needed to calculate the risk?

- A. assessment scope
- B. event severity and likelihood
- C. incident response playbook
- D. risk model framework

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63

DRAG DROP

Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://www.densify.com/resources/continuous-integration-delivery-phases>

QUESTION 64

An employee who often travels abroad logs in from a first-seen country during non-working hours. The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs out. The investigation concludes that the external domain belongs to a competitor. Which two behaviors triggered UEBA? (Choose two.)

- A. domain belongs to a competitor
- B. log in during non-working hours
- C. email forwarding to an external domain
- D. log in from a first-seen country
- E. increased number of sent mails

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:



QUESTION 65 How is a

SIEM tool used?

- A. To collect security data from authentication failures and cyber attacks and forward it for analysis
- B. To search and compare security data against acceptance standards and generate reports for analysis
- C. To compare security alerts against configured scenarios and trigger system responses
- D. To collect and analyze security data from network devices and servers and produce alerts

Correct Answer: D

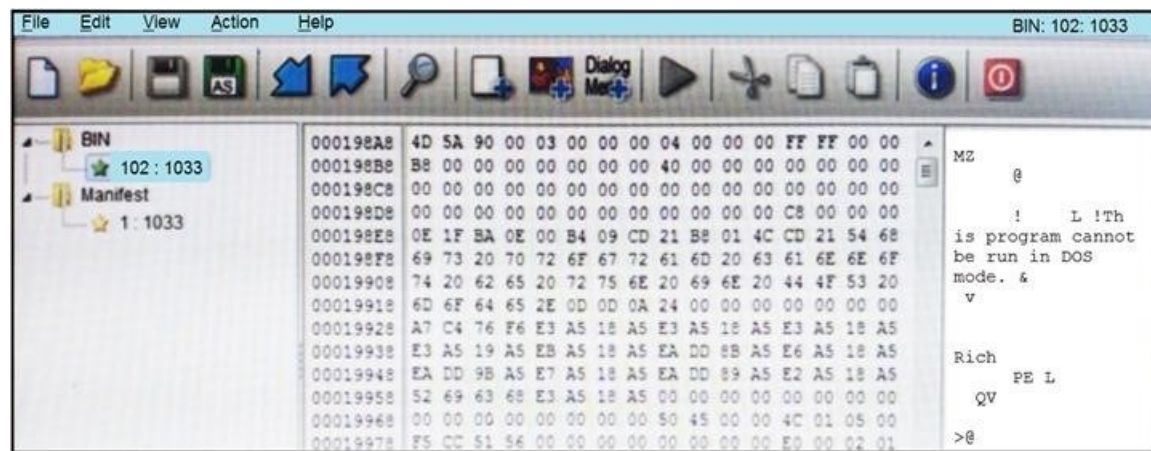
Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.varonis.com/blog/what-is-siem/>

QUESTION 66



Refer to the exhibit. An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

- A. a DOS MZ executable format
- B. a MS-DOS executable archive
- C. an archived malware
- D. a Windows executable file

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://stackoverflow.com/questions/2577545/why-is-this-program-cannot-be-run-in-dos-mode-text-present-in-dll-files#:~:text=The%20linker%20places%20a%20default,using%20the%20%2FSTUB%20linker%20option.&text=This%20information%20enables%20Windows%20to,has%20an%20MS-DOS%20stub>.

QUESTION 67

```
try
{
    using (MemoryStream memoryStream = new MemoryStream())
    {
        memoryStream.Position = 32L;
        using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
        {
            aesCryptoServiceProvider.KeySize = 128;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = key;
            aesCryptoServiceProvider.GenerateIV();
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aesCryptoServiceProvider.CreateEncryptor(), CryptoStreamMode.Write))
            {
                memoryStream.Write(aesCryptoServiceProvider.IV, 0, aesCryptoServiceProvider.IV.Length);
                cryptoStream.Write(input, 0, input.Length);
                cryptoStream.FlushFinalBlock();
                using (HMACSHA256 hMACSHA = new HMACSHA256(bytes))
                {
                    byte[] array = hMACSHA.ComputeHash(memoryStream.ToArray(), 32, memoryStream.ToArray().Length - 32);
                    memoryStream.Position = 0L;
                    memoryStream.Write(array, 0, array.Length);
                }
            }
        }
        result = memoryStream.ToArray();
    }
}
catch
{
}
```

Refer to the exhibit. An engineer is performing a static analysis on a malware and knows that it is capturing keys and webcam events on a company server. What is the indicator of compromise?

- A. The malware is performing comprehensive fingerprinting of the host, including a processor, motherboard manufacturer, and connected removable storage.
- B. The malware is a ransomware querying for installed anti-virus products and operating systems to encrypt and render unreadable until payment is made for file decryption.
- C. The malware has moved to harvesting cookies and stored account information from major browsers and configuring a reverse proxy for intercepting network activity.
- D. The malware contains an encryption and decryption routine to hide URLs/IP addresses and is storing the output of loggers and webcam captures in locally encrypted files for retrieval.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

An audit is assessing a small business that is selling automotive parts and diagnostic services. Due to increased customer demands, the company recently started to accept credit card payments and acquired a POS terminal. Which compliance regulations must the audit apply to the company?

- A. HIPAA
- B. FISMAC. COBIT
- D. PCI DSS

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://upserve.com/restaurant-insider/restaurant-pos-pci-compliance-checklist/>

QUESTION 69

A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device. Which should be disabled to resolve the issue?

- A. SNMPv2
- B. TCP small services
- C. port UDP 161 and 162
- D. UDP small services

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://nvd.nist.gov/vuln/detail/CVE-2018-0161>

QUESTION 70

DRAG DROP

Drag and drop the mitigation steps from the left onto the vulnerabilities they mitigate on the right.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 71

Refer to the exhibit. Which indicator of compromise is represented by this STIX?

```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--d81f86b9-9f",
      "created": "2020-08-10T13:49:37.079Z",
      "modified": "2020-08-10T13:49:37.079Z",
      "name": "Malicious site hosting downloader",
      "indicator_types": [
        "malicious-activity"
      ],
      "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
      "pattern_type": "stix",
      "valid_from": "2020-08-10T13:49:37.079Z"
    },
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware--162d9 a",
      "created": "2020-08-13T09:15:17.182Z",
      "modified": "2020-08-13T09:15:17.182Z",
      "name": "y2z7atc backdoor",
      "malware_types": [
        "backdoor",
        "remote-access-trojan"
      ],
      "is_family": false,
      "kill_chain_phases": [
        {
          "kill_chain_name": "mandant-attack-lifecycle-model",
          "phase_name": "establish-foothold"
        }
      ]
    }
  ],
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--864af2e5",
    "created": "2020-08-15T18:03:58.029Z",
    "modified": "2020-08-15T18:03:58.029Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4",
    "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
  }
]
```



- A. website redirecting traffic to ransomware server
- B. website hosting malware to download files
- C. web server vulnerability exploited by malware
- D. cross-site scripting vulnerability to backdoor server

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

Refer to the exhibit. What is occurring in this packet capture?

No.	Time	Source	Destination	Protocol	Length	Info
2389	848.622259	10.31.133.235	10.25.129.5	TCP	66	61118 → 80 [SYN] Seq=0 Win=8192
2389	848.622273	10.25.129.5	10.31.133.235	TCP	66	80 → 61118 [SYN, ACK] Seq=0 Acc=
2389	848.622351	10.31.133.235	10.25.129.5	TCP	60	30745 → 80 [RST] Seq=1 Win=0
2389	848.622719	10.31.133.235	10.25.129.5	TCP	60	30746 → 80 [RST] Seq=1 Win=0
2389	848.622889	10.31.133.235	10.25.129.5	TCP	60	30748 → 80 [RST] Seq=1 Win=0
2389	848.623250	10.31.133.235	10.25.129.5	TCP	60	30747 → 80 [RST] Seq=1 Win=0
2389	848.623545	10.31.133.235	10.25.129.5	TCP	60	30749 → 80 [RST] Seq=1 Win=0
2389	848.623882	10.31.133.235	10.25.129.5	TCP	60	30750 → 80 [RST] Seq=1 Win=0
2389	848.624295	10.31.133.235	10.25.129.5	TCP	60	30751 → 80 [RST] Seq=1 Win=0
2389	848.624880	10.31.133.235	10.25.129.5	TCP	60	30752 → 80 [RST] Seq=1 Win=0
2389	848.625424	10.31.133.235	10.25.129.5	TCP	60	30753 → 80 [RST] Seq=1 Win=0
2389	848.625729	10.31.133.235	10.25.129.5	TCP	60	30754 → 80 [RST] Seq=1 Win=0
2389	848.626842	10.31.133.235	10.25.129.5	TCP	60	30755 → 80 [RST] Seq=1 Win=0
2389	848.627352	10.31.133.235	10.25.129.5	TCP	60	30756 → 80 [RST] Seq=1 Win=0

- A. TCP port scan
- B. TCP flood
- C. DNS flood
- D. DNS tunneling

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 73

DRAG DROP

Drag and drop the cloud computing service descriptions from the left onto the cloud service categories on the right.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.128.0.2	TCP	54	3341 -> 80 [SYN] Seq=0 Win=512 Len=0
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	80 -> 3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
3	0.005514	10.128.0.2	10.0.0.2	TCP	54	80 -> 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
4	0.008429	10.0.0.2	10.128.0.2	TCP	54	3342 -> 80 [SYN] Seq=0 Win=512 Len=0
5	0.010233	10.128.0.2	10.0.0.2	TCP	58	80 -> 3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	80 -> 3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
7	0.016830	10.0.0.2	10.128.0.2	TCP	54	3343 -> 80 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	80 -> 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9	0.023496	10.128.0.2	10.0.0.2	TCP	58	80 -> 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
10	0.025243	10.0.0.2	10.128.0.2	TCP	58	3344 -> 80 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	80 -> 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	0.028038	10.128.0.2	10.0.0.2	TCP	58	80 -> 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
13	0.030523	10.128.0.2	10.0.0.2	TCP	58	80 -> 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)

Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2

Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0

Source port: 3341
Destination port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 1023350804
0101 = Header Length: 20 bytes (5)

Flags: 0x002 (SYN)
Window size value: 512
[Calculated window size: 512]
Checksum: 0x8d5a [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]

Refer to the exhibit. What is the threat in this Wireshark traffic capture?

- A. A high rate of SYN packets being sent from multiple sources toward a single destination IP
- B. A flood of ACK packets coming from a single source IP to multiple destination IPs
- C. A high rate of SYN packets being sent from a single source IP toward multiple destination IPs
- D. A flood of SYN packets coming from a single source IP to a single destination IP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 75 An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

- A. data clustering
- B. data regression
- C. data ingestion
- D. data obfuscation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 76 What is a benefit of key risk indicators?

- A. clear perspective into the risk position of an organization
- B. improved visibility on quantifiable information
- C. improved mitigation techniques for unknown threats

D. clear procedures and processes for organizational risk

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: [https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20\(ERM\)-,Overview,and%20mitigate%20them%20in%20time.](https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20(ERM)-,Overview,and%20mitigate%20them%20in%20time.)

QUESTION 77

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

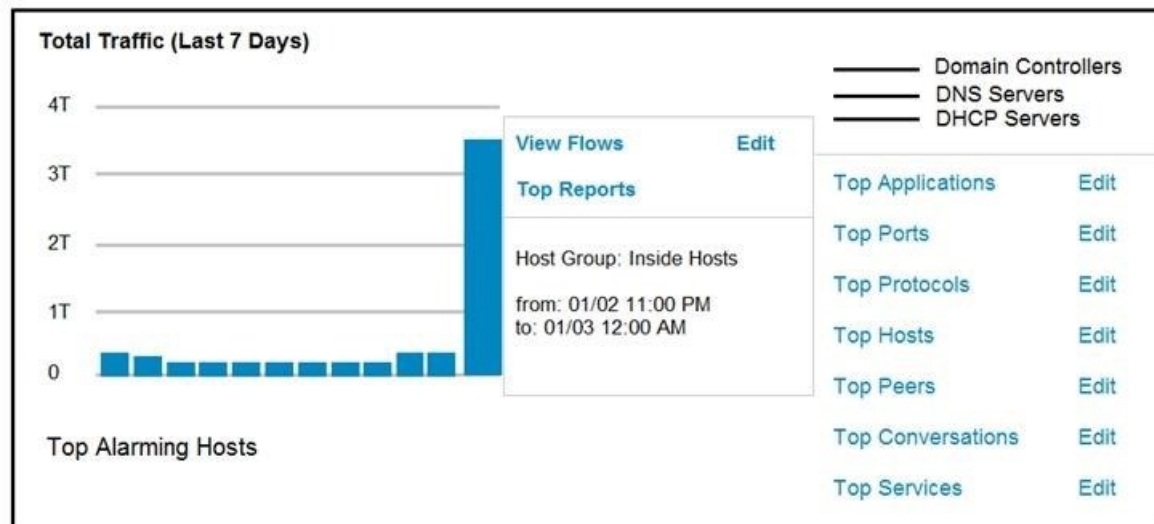
Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78



Refer to the exhibit. An engineer notices a significant anomaly in the traffic in one of the host groups in Cisco Secure Network Analytics (Stealthwatch) and must analyze the top data transmissions. Which tool accomplishes this task?

- A. Top Peers
- B. Top Hosts
- C. Top Conversations
- D. Top Ports

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKSEC-3014.pdf>

QUESTION 79

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80 An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

- A. `chmod +x ex.sh`
- B. `source ex.sh`
- C. `chroot ex.sh`
- D. `sh ex.sh`

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.redhat.com/sysadmin/exit-codes-demystified>



QUESTION 81

An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

- A. phishing
- B. dumpster diving
- C. social engineering
- D. privilege escalation

Correct Answer: C

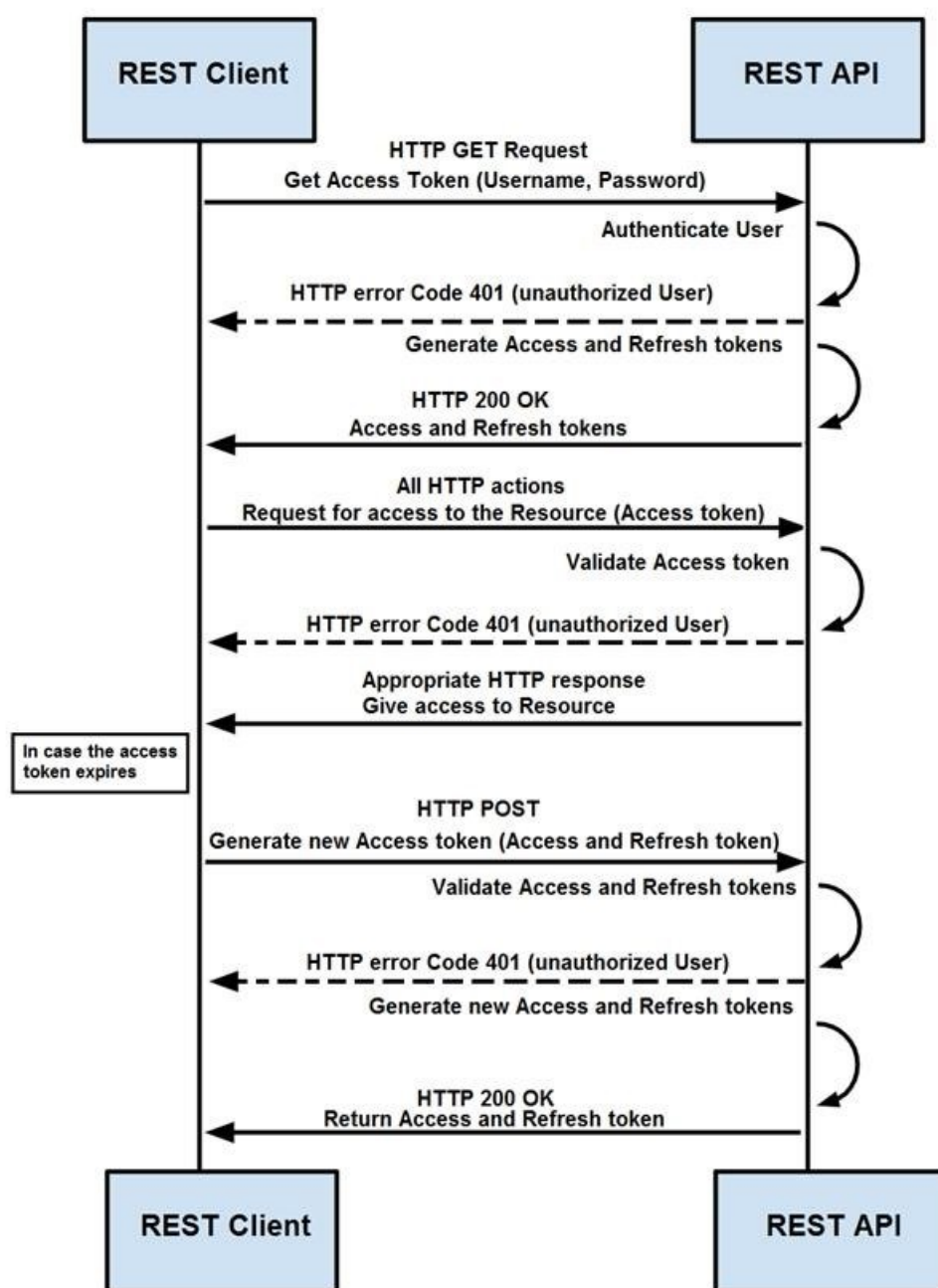
Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

Token-Based Authentication



Refer to the exhibit. How are tokens authenticated when the REST API on a device is accessed from a REST API client?

- A. The token is obtained by providing a password. The REST client requests access to a resource using the access token. The REST API validates the access token and gives access to the resource.
- B. The token is obtained by providing a password. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.
- C. The token is obtained before providing a password. The REST API provides resource access, refreshes tokens, and returns them to the REST client. The REST client requests access to a resource using the access token.
- D. The token is obtained before providing a password. The REST client provides access to a resource using the access token. The REST API encrypts the access token and gives access to the resource.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 83


```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com, realm=0, isRealm=0, realDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

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

- A. x-frame-options
- B. x-xss-protection
- C. x-content-type-options
- D. x-test-debug

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

QUESTION 84

DRAG DROP

Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 85

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 86

What is a limitation of cyber security risk insurance?

- A. It does not cover the costs to restore stolen identities as a result of a cyber attack

- B. It does not cover the costs to hire forensics experts to analyze the cyber attack
- C. It does not cover the costs of damage done by third parties as a result of a cyber attack
- D. It does not cover the costs to hire a public relations company to help deal with a cyber attack

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://tplinsurance.com/products/cyber-risk-insurance/>

QUESTION 87

An engineer returned to work and realized that payments that were received over the weekend were sent to the wrong recipient. The engineer discovered that the SaaS tool that processes these payments was down over the weekend. Which step should the engineer take first?

- A. Utilize the SaaS tool team to gather more information on the potential breach
- B. Contact the incident response team to inform them of a potential breach
- C. Organize a meeting to discuss the services that may be affected
- D. Request that the purchasing department creates and sends the payments manually

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 88

An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

- A. Command and Control, Application Layer Protocol, Duqu
- B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu
- C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu
- D. Discovery, System Network Configuration Discovery, Duqu

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 89

DRAG DROP

Drag and drop the function on the left onto the mechanism on the right.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 90

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

- A. Run the **sudo sysdiagnose** command
- B. Run the **sh** command
- C. Run the **w** command
- D. Run the **who** command

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://eclecticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/>

QUESTION 91

A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

- A. Run and analyze the DLP Incident Summary Report from the Email Security Appliance
- B. Ask the company to execute the payload for real time analysis
- C. Investigate further in open source repositories using YARA to find matches
- D. Obtain a copy of the file for detonation in a sandbox

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 92

A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.861.2117.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet. What is the cause of the issue?

- A. DDoS attack
- B. phishing attack
- C. virus outbreak
- D. malware outbreak

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 93

Max (K)	Retain	OverflowAction	Entries	Log
-----	-----	-----	-----	---
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

Refer to the exhibit. An employee is a victim of a social engineering phone call and installs remote access software to allow an “MS Support” technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https. What should be determined regarding data loss between the employee’s laptop and the remote technician’s system?

- A. No database files were disclosed
- B. The database files were disclosed
- C. The database files integrity was violated
- D. The database files were intentionally corrupted, and encryption is possible

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 94

Refer to the exhibit. Which asset has the highest risk value?

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

- A. servers
- B. website
- C. payment process
- D. secretary workstation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 95

DRAG DROP

Stealthwatch cisco.local																
128.107.78.8																
Hosts																
Sorted by overall severity																
Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
128.107.78.8		12/15/16 5:26 PM	1/27/17 9:13 PM												United States	United States
First Previous 1 Next Last																

Refer to the exhibit. The Cisco Secure Network Analytics (Stealthwatch) console alerted with “New Malware Server Discovered” and the IOC indicates communication from an end-user desktop to a Zeus C&C Server. Drag and drop the actions that the analyst should take from the left into the order on the right to investigate and remediate this IOC.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 96 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 97

A company launched an e-commerce website with multiple points of sale through internal and external e-stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

- A. Mask PAN numbers
- B. Encrypt personal data
- C. Encrypt access
- D. Mask sales details

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 98

An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

- A. aligning access control policies
- B. exfiltration during data transfer
- C. attack using default accounts
- D. data exposure from backups

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 99

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 100



Refer to the exhibit. An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior. Which type of compromise is occurring?

- A. compromised insider
- B. compromised root access
- C. compromised database tables
- D. compromised network

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference: