

# Cisco

## Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)



### NEW QUESTION 1

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

**Answer: B**

### NEW QUESTION 2

Refer to the exhibit.

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]

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

**Answer: D**

### NEW QUESTION 3

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

**Answer: D**

### NEW QUESTION 4

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

Answer Area

- Restrict administrative access to operating systems and applications in accordance with job duties
- Use multifactor authentication for remote access or accessing sensitive information
- Change backup and store software and configuration settings for at least three months
- Patch applications including flash, web browsers, and PDF viewers
- Utilize application control to stop malware delivery and execution

- End-user desktops allow the execution of non-approved applications that include malicious code
- Application security vulnerabilities can be used to execute malicious code
- Privilege accounts have full rights to information systems
- User verification is weak and based on a single factor
- Data or access loss occurs due to cybersecurity incidents

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

- Restrict administrative access to operating systems and applications in accordance with job duties
- Use multifactor authentication for remote access or accessing sensitive information
- Change backup and store software and configuration settings for at least three months
- Patch applications including flash, web browsers, and PDF viewers
- Utilize application control to stop malware delivery and execution

- Utilize application control to stop malware delivery and execution
- Patch applications including flash, web browsers, and PDF viewers
- Restrict administrative access to operating systems and applications in accordance with job duties
- Use multifactor authentication for remote access or accessing sensitive information
- Change backup and store software and configuration settings for at least three months

NEW QUESTION 5

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



**Answer: C**

#### NEW QUESTION 6

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

**Answer: AB**

#### NEW QUESTION 7

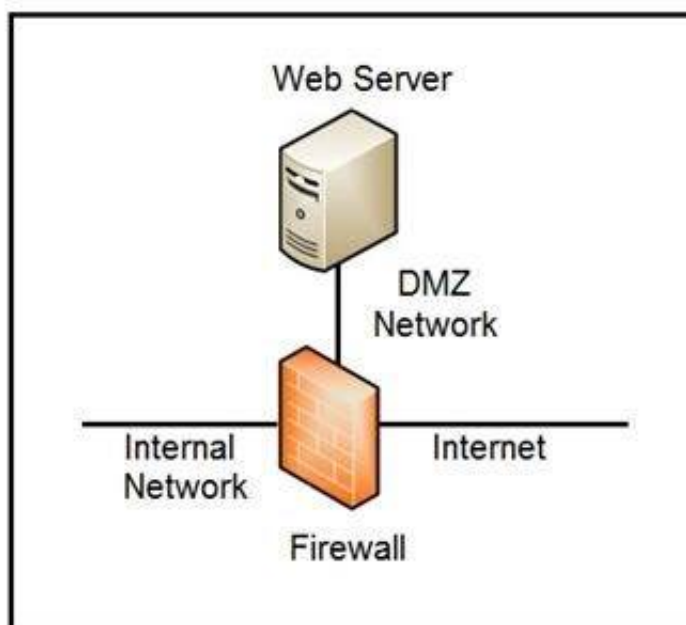
Employees report computer system crashes within the same week. An analyst is investigating one of the computers that crashed and discovers multiple shortcuts in the system's startup folder. It appears that the shortcuts redirect users to malicious URLs. What is the next step the engineer should take to investigate this case?

- A. Remove the shortcut files
- B. Check the audit logs
- C. Identify affected systems
- D. Investigate the malicious URLs

**Answer: C**

#### NEW QUESTION 8

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

**Answer: BD**

#### NEW QUESTION 9

Refer to the exhibit.

URLs:

- /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

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

**Answer: C**

**NEW QUESTION 10**

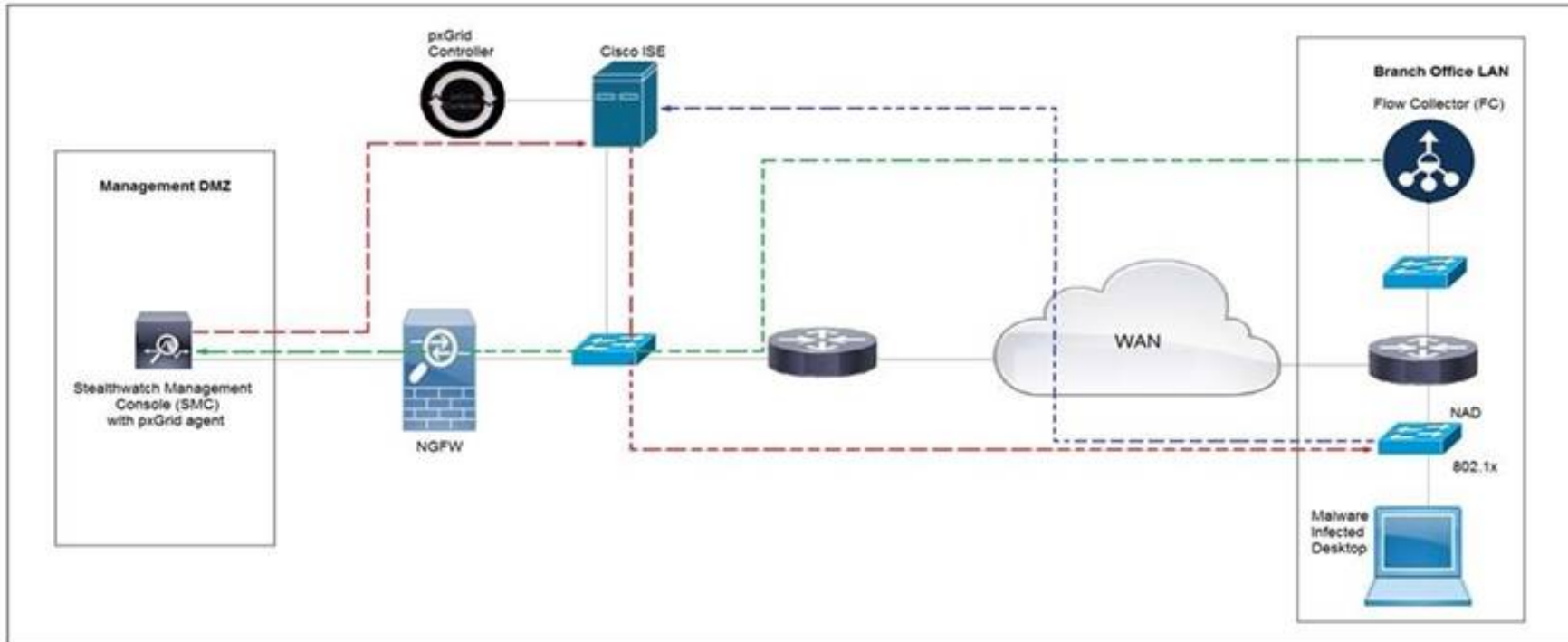
How does Wireshark decrypt TLS network traffic?

- 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

**Answer: A**

**NEW QUESTION 10**

Refer to the exhibit.



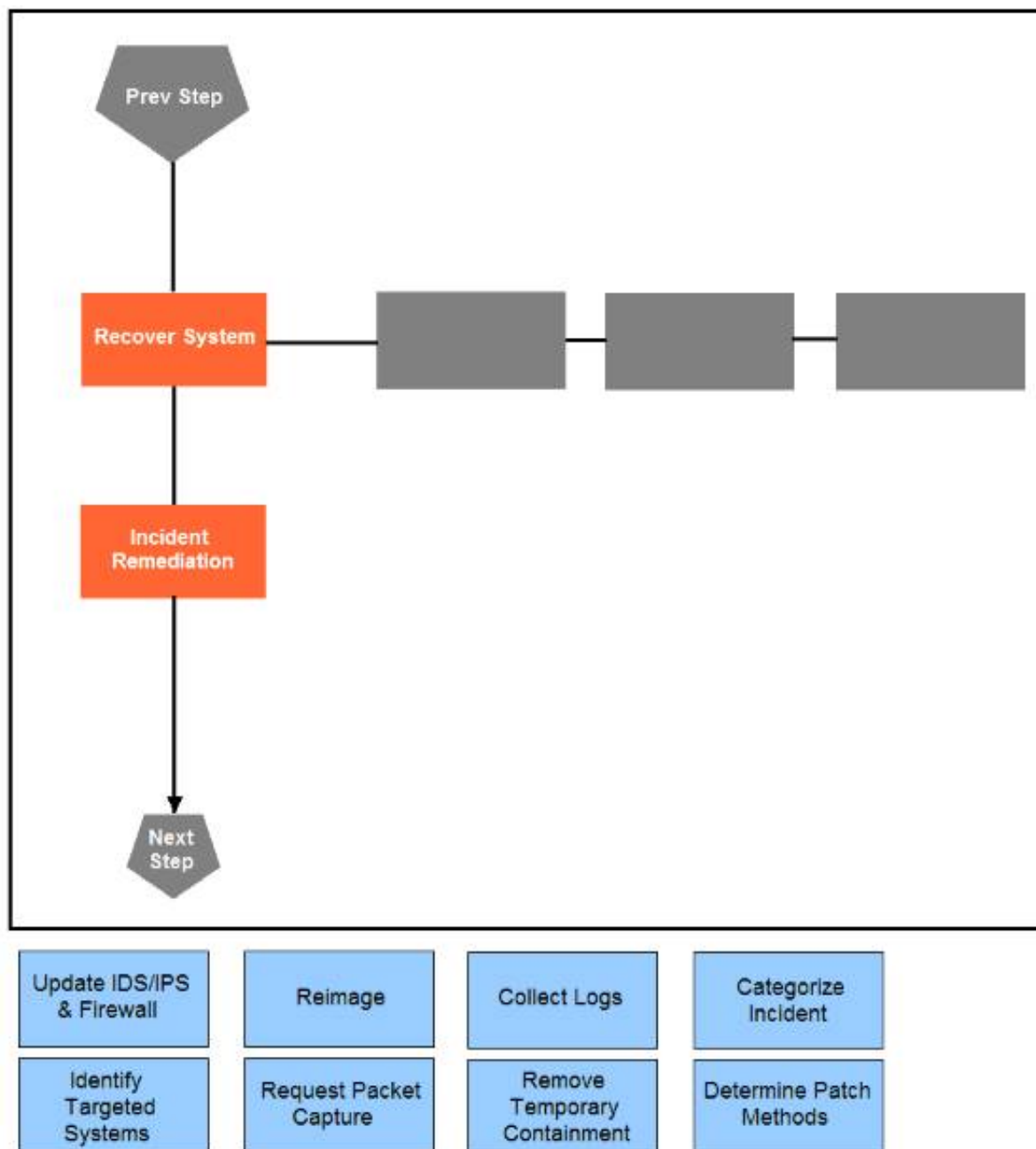
Cisco Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a Quarantine VLAN using Adaptive Network Control policy. Which telemetry feeds were correlated with SMC to identify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

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

**Answer: B**

**NEW QUESTION 15**

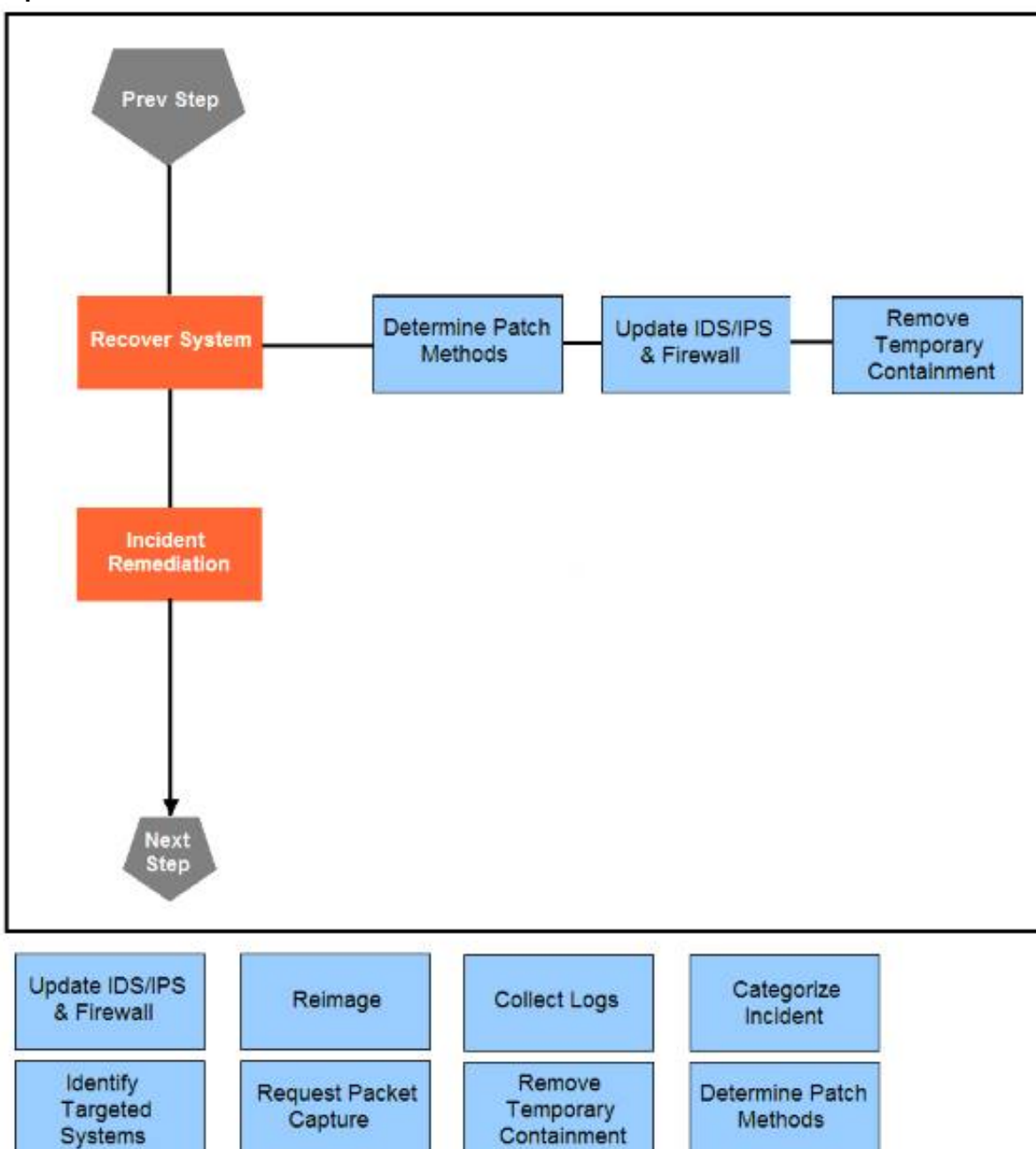
Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 16**

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

**Answer: D**

**NEW QUESTION 18**

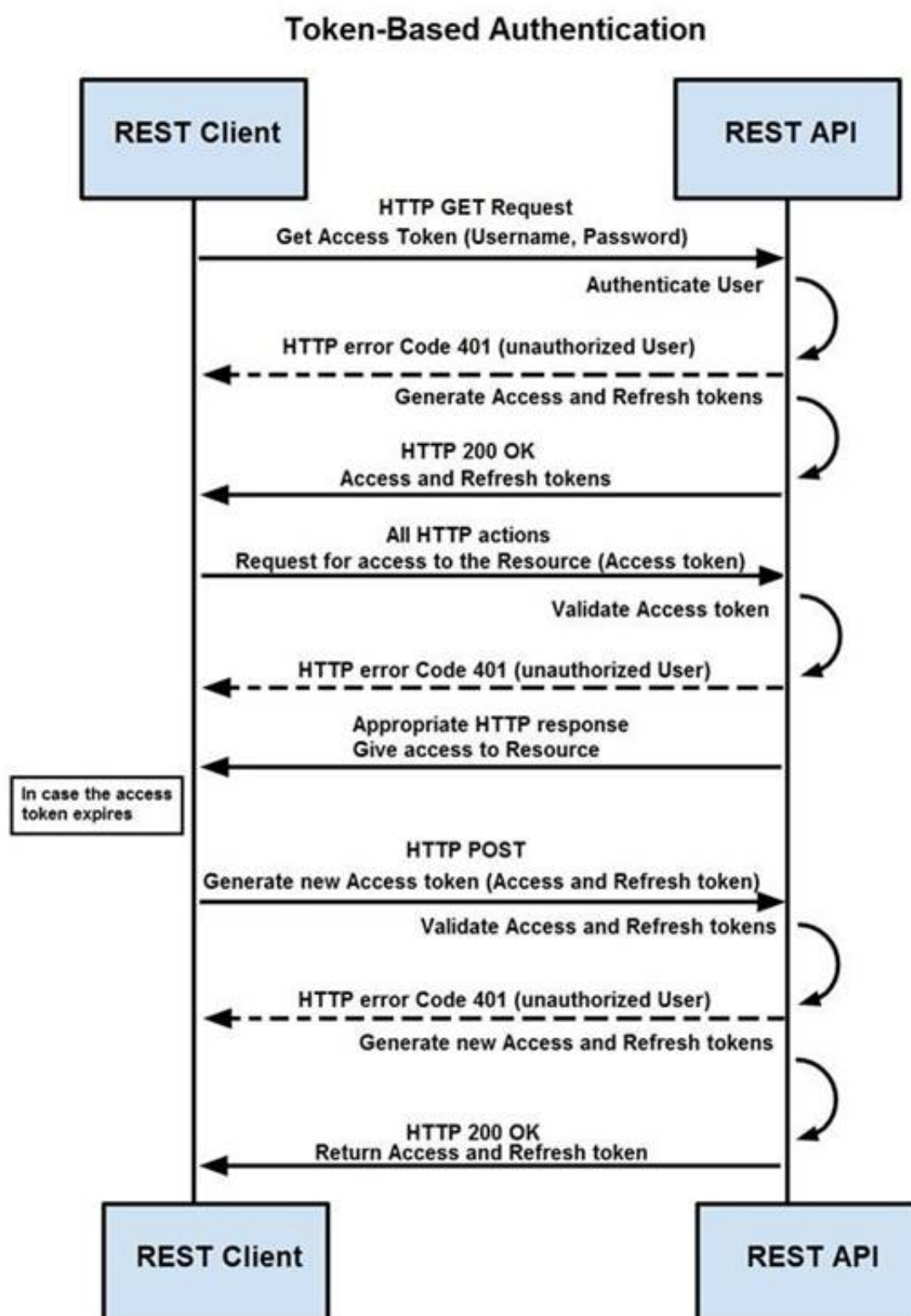
What is a limitation of cyber security risk insurance?

- 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

**Answer: A**

**NEW QUESTION 20**

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



- J. The REST client provides access to a resource using the access token
- K. The REST API encrypts the access token and gives access to the resource.

**Answer:** D

**NEW QUESTION 25**

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`

**Answer:** A

**NEW QUESTION 30**

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

**Answer:** A

**NEW QUESTION 33**

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

**Answer:** C

**NEW QUESTION 37**

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

**Answer:** D

**NEW QUESTION 41**

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

**Answer Area**

triggers a block of code when triggered by a specific event	SaaS
allows renting full servers or virtual machines	PaaS
focuses on developing, testing, and delivering applications	IaaS
allows hosting and managing a virtual environment	FaaS

- A. Mastered
- B. Not Mastered

**Answer:** A

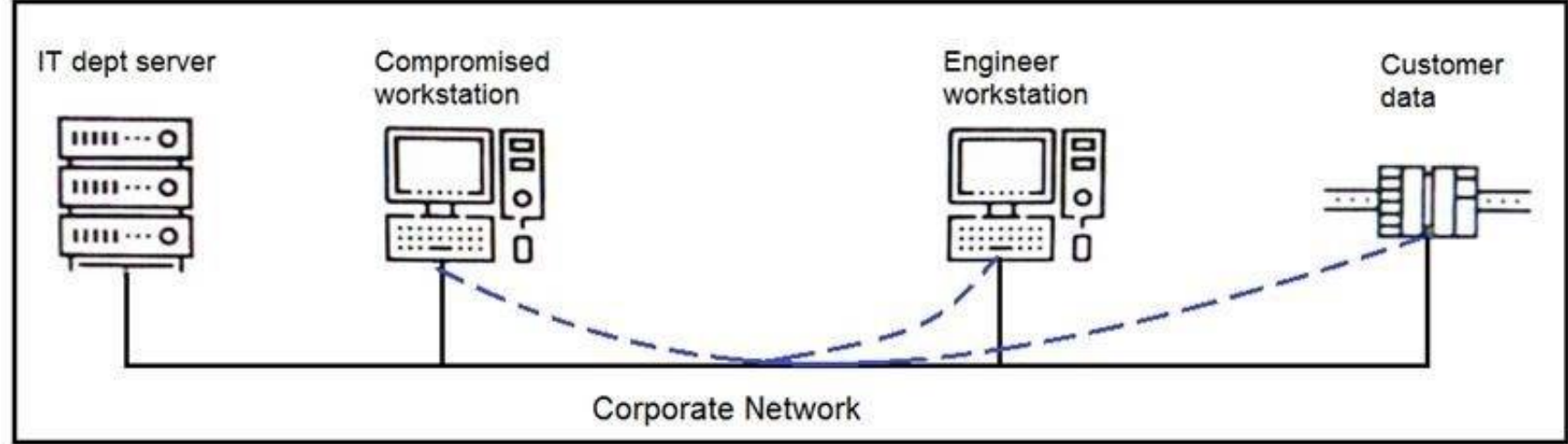
**Explanation:**



Answer Area

triggers a block of code when triggered by a specific event	focuses on developing, testing, and delivering applications
allows renting full servers or virtual machines	allows hosting and managing a virtual environment
focuses on developing, testing, and delivering applications	allows renting full servers or virtual machines
allows hosting and managing a virtual environment	triggers a block of code when triggered by a specific event

NEW QUESTION 46  
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

Answer: A

NEW QUESTION 50

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.

Answer Area

run show access-list	Step 1
run show config	Step 2
validate the file MD5	Step 3
generate the core file	Step 4
verify the image file hash	
check the memory logs	
verify the memory state	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
**Answer Area**

run show access-list	run show config
run show config	check the memory logs
validate the file MD5	verify the memory state
generate the core file	run show access-list
verify the image file hash	
check the memory logs	
verify the memory state	

**NEW QUESTION 54**

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

Answer: A

**NEW QUESTION 59**

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

Answer: C

**NEW QUESTION 63**

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

Answer: C

**NEW QUESTION 66**

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

Answer: C



#### NEW QUESTION 67

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

**Answer: D**

#### NEW QUESTION 72

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

**Answer: B**

#### NEW QUESTION 76

Refer to the exhibit.

### Analysis Report

<b>ID</b>	12cbeee21b1ea4	<b>Filename</b>	fpzryrf.exe
<b>OS</b>	7601.1898.amd64fre.win7sp1_gdr.150316-1654	<b>Magic Type</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>Started</b>	7/29/16 18:44:43	<b>Analyzed As</b>	exe
<b>Ended</b>	7/29/16 18:50:39	<b>SHA256</b>	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da
<b>Duration</b>	0:05:56	<b>SHA1</b>	a2de85810fd5ebcf29c5da5dd29ce03470772ad
<b>Sandbox</b>	phl-work-02 (pilot-d)	<b>MD5</b>	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

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.

**Answer: C**



NEW QUESTION 81

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 average
- B. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.
- C. Implement REST API Security Essentials solution to automatically mitigate limit exhaustio
- D. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.
- E. Increase a limit of replies in a given interval for each AP
- F. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.
- G. Apply a limit to the number of requests in a given time interval for each AP
- H. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Answer: D

NEW QUESTION 82

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. FISMA
- C. COBIT
- D. PCI DSS

Answer: D

NEW QUESTION 85

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

Answer Area

creates the set of executable tasks

minimizes redundancies and steamlines repetitive tasks

organizes components to seamlessly run applications

systematically executes large workflows

Orchestration

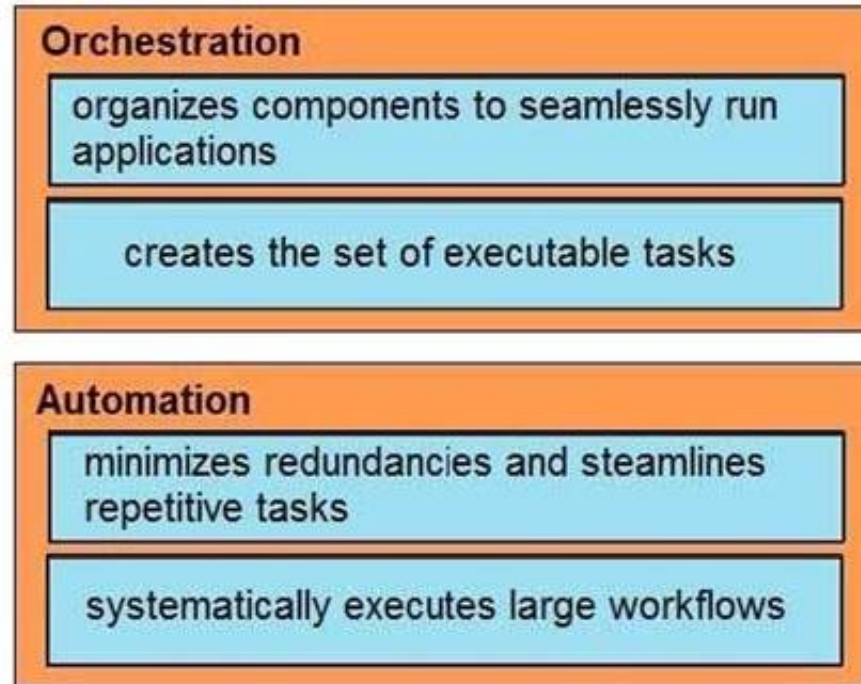
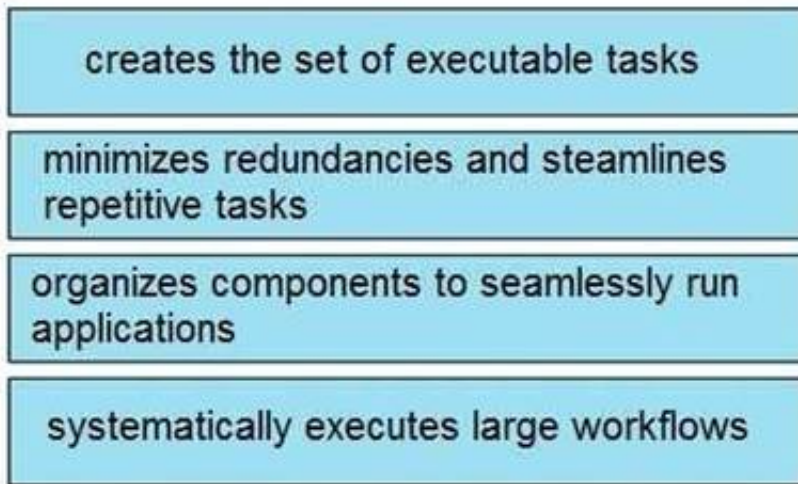
Automation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area



### NEW QUESTION 87

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

Answer: A

### NEW QUESTION 88

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

Answer: C

### NEW QUESTION 92

Refer to the exhibit.

```

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
{
}
  
```

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.

**Answer: B**

#### NEW QUESTION 93

Refer to the exhibit.

```
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)
```

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

**Answer: B**

#### NEW QUESTION 94

Refer to the exhibit.



```
#!/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
```

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)`

**Answer: B**

#### NEW 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

**Answer: B**

#### NEW QUESTION 99

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.

## Answer Area

not visible to the victim
virus scanner turning off
malware placed on the targeted system
open port scans and multiple failed logins from the website
large amount of data leaving the network through unusual ports
system phones connecting to countries where no staff are located
USB with infected files inserted into company laptop

reconnaissance
weaponization
delivery
exploitation
installation
command & control
actions on objectives

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

## Answer Area

not visible to the victim
virus scanner turning off
malware placed on the targeted system
open port scans and multiple failed logins from the website
large amount of data leaving the network through unusual ports
system phones connecting to countries where no staff are located
USB with infected files inserted into company laptop

system phones connecting to countries where no staff are located
malware placed on the targeted system
not visible to the victim
large amount of data leaving the network through unusual ports
USB with infected files inserted into company laptop
virus scanner turning off
open port scans and multiple failed logins from the website

### NEW QUESTION 102

Refer to the exhibit.



Stealthwatch <small>cisco.local</small>																
128.107.78.8																
Cisco																
Dashboards Monitor Analyze Jobs Configure Deploy																
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																

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.

Answer Area

Execute rapid threat containment

Investigate and classify the exposure

Investigate infected hosts

Search for infected hosts

Examine returned results

Step 1

Step 2

Step 3

Step 4

Step 5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Execute rapid threat containment

Investigate and classify the exposure

Investigate infected hosts

Search for infected hosts

Examine returned results

Search for infected hosts

Investigate infected hosts

Investigate and classify the exposure

Examine returned results

Execute rapid threat containment



#### NEW QUESTION 107

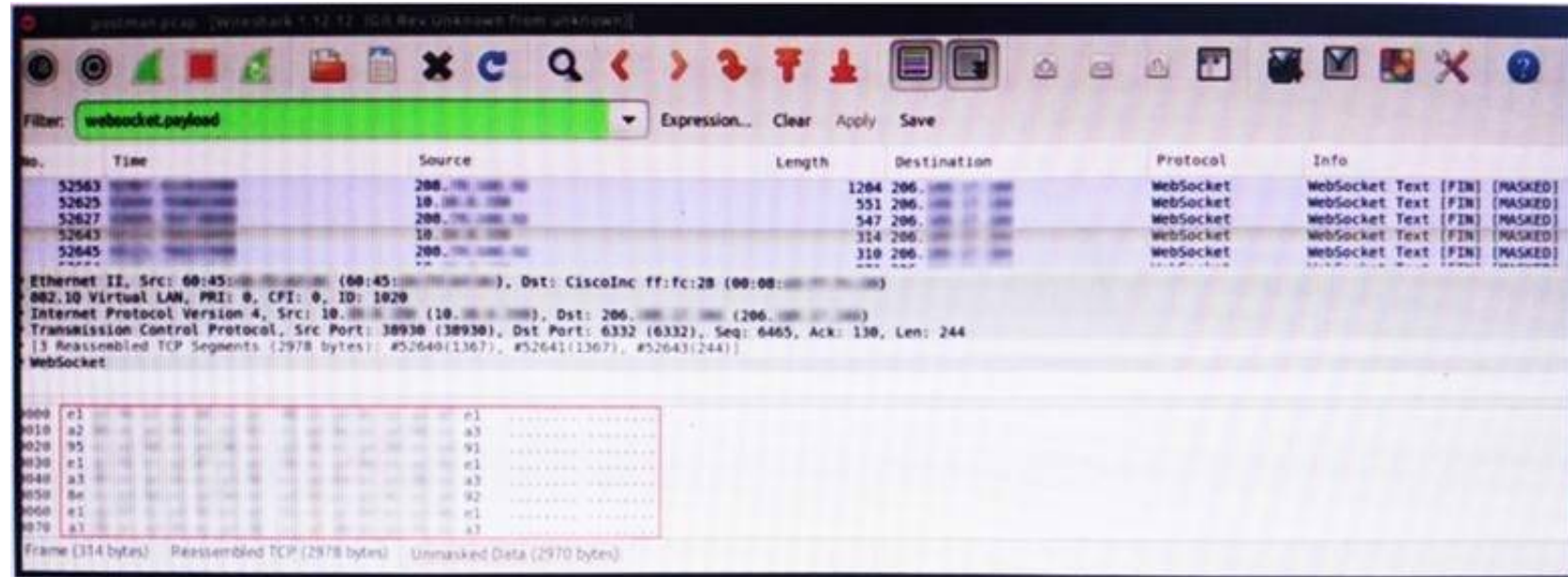
Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

- A. customer data
- B. internal database
- C. internal cloud
- D. Internet

**Answer: D**

#### NEW QUESTION 109

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

**Answer: C**

#### NEW QUESTION 113

Refer to the exhibit.

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 Len=0
2389	848.622719	10.31.133.235	10.25.129.5	TCP	60	30746 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.622889	10.31.133.235	10.25.129.5	TCP	60	30748 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.623250	10.31.133.235	10.25.129.5	TCP	60	30747 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.623545	10.31.133.235	10.25.129.5	TCP	60	30749 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.623882	10.31.133.235	10.25.129.5	TCP	60	30750 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.624295	10.31.133.235	10.25.129.5	TCP	60	30751 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.624880	10.31.133.235	10.25.129.5	TCP	60	30752 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.625424	10.31.133.235	10.25.129.5	TCP	60	30753 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.625729	10.31.133.235	10.25.129.5	TCP	60	30754 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.626842	10.31.133.235	10.25.129.5	TCP	60	30755 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.627352	10.31.133.235	10.25.129.5	TCP	60	30756 → 80 [RST] Seq=1 Win=0 Len=0

What is occurring in this packet capture?

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

**Answer: B**

#### NEW QUESTION 118

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

**Answer: B**

#### NEW QUESTION 120

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

**Answer: C**

#### NEW QUESTION 121

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

**Answer: D**

#### NEW QUESTION 123

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"

**Answer: A**

#### NEW QUESTION 128

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

**Answer: D**

#### NEW QUESTION 132

Refer to the exhibit.

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

Which asset has the highest risk value?

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

**Answer: C**

#### NEW QUESTION 134

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 350-201 Practice Exam Features:

- \* 350-201 Questions and Answers Updated Frequently
- \* 350-201 Practice Questions Verified by Expert Senior Certified Staff
- \* 350-201 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 350-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 350-201 Practice Test Here](#)**