

350-201 Dumps

Performing CyberOps Using Core Security Technologies (CBRCOR)

<https://www.certleader.com/350-201-dumps.html>



NEW QUESTION 1

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 2

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

Answer: D

NEW QUESTION 3

Refer to the exhibit.

Analysis Report

ID	12cbbee21b1ea4	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	phl-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

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 4

Refer to the exhibit.

```
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
```

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

Answer: C

NEW QUESTION 5

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 6

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 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

Answer: BE

NEW QUESTION 8

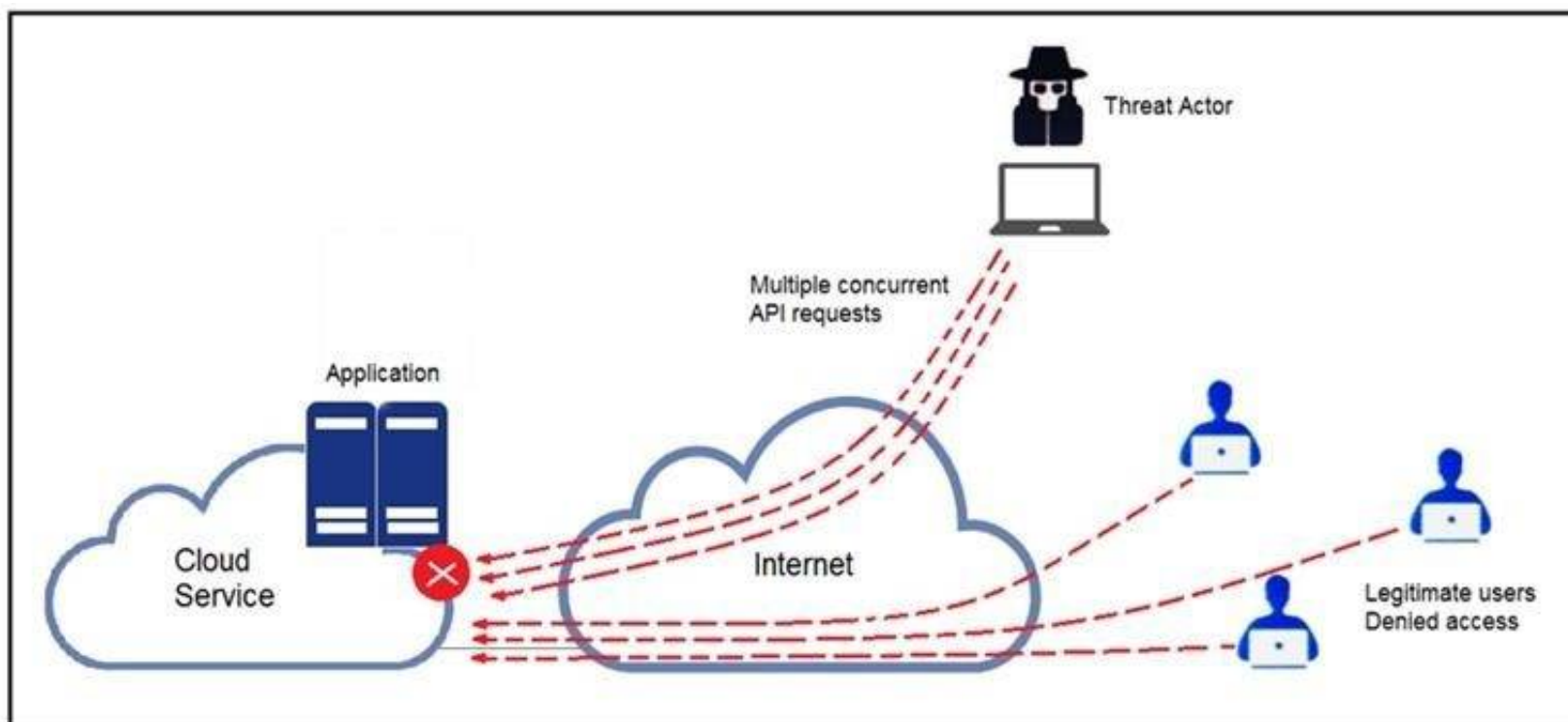
What is the purpose of hardening systems?

- 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 9

Refer to the exhibit.



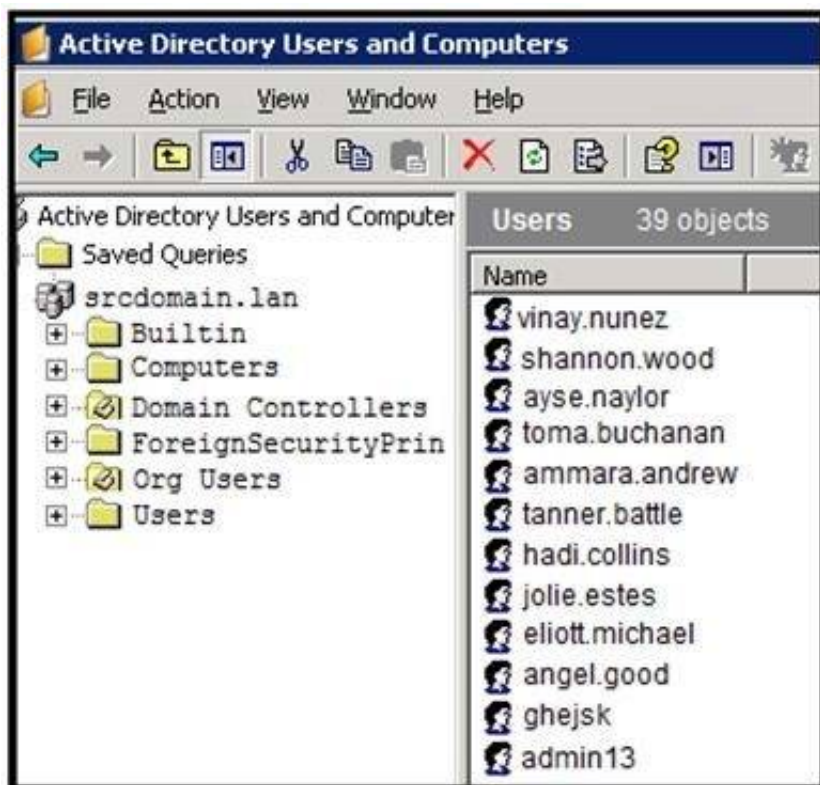
A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?

- 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

Answer: A

NEW QUESTION 10

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

Answer: D

NEW QUESTION 10

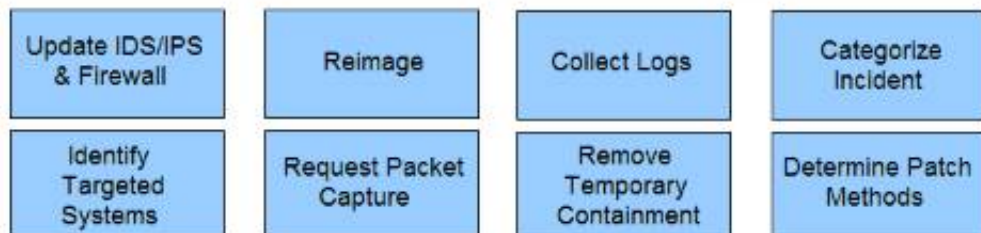
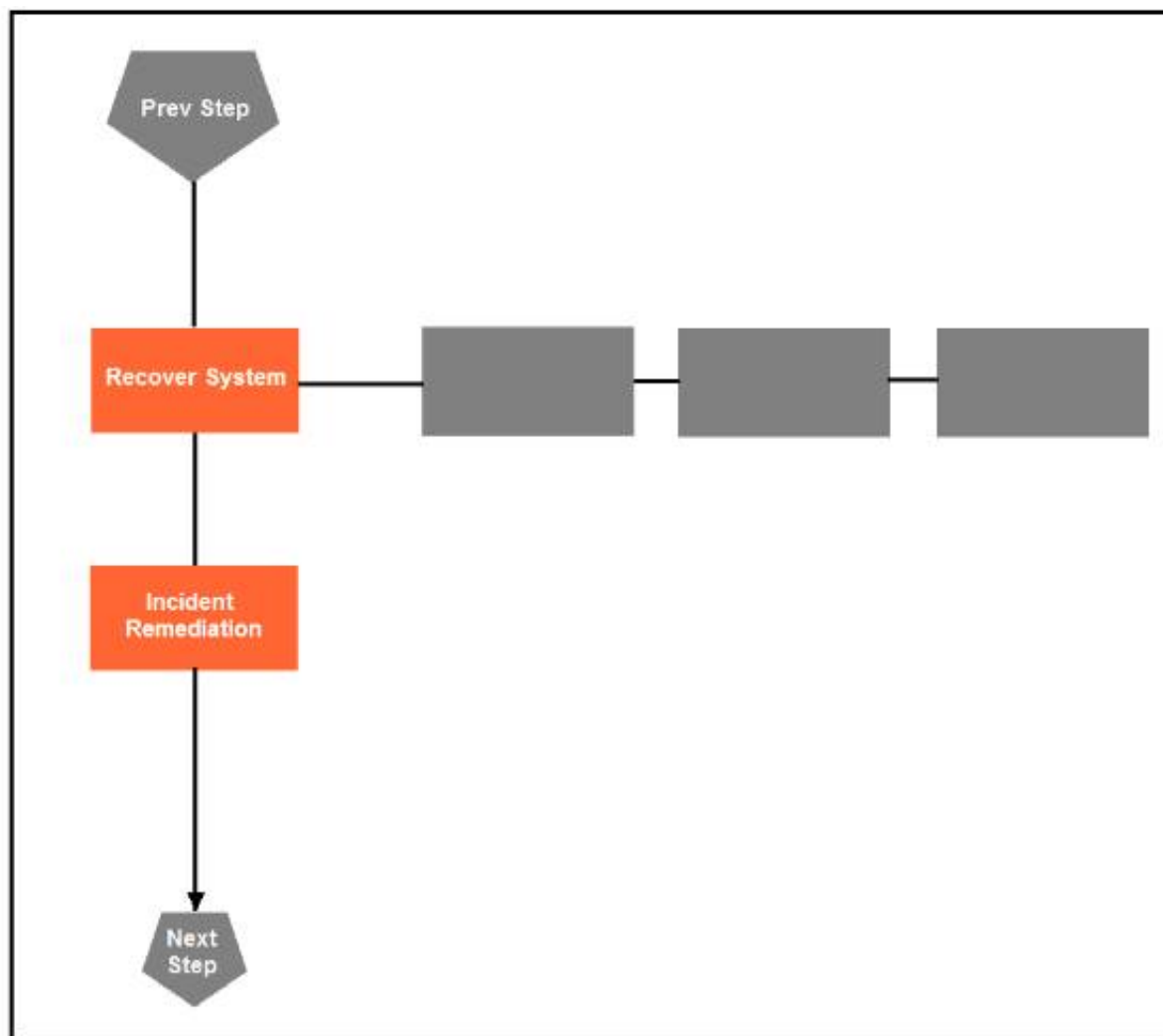
According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

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

Answer: B

NEW QUESTION 11

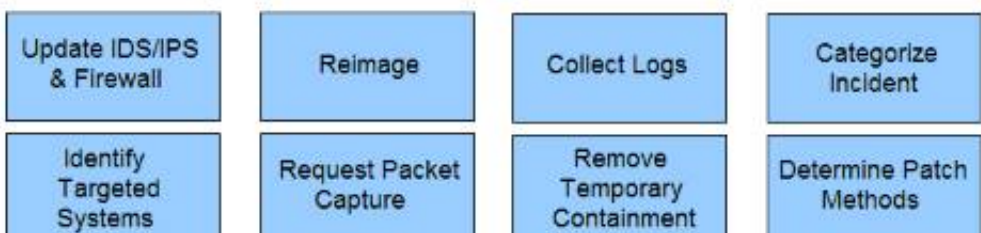
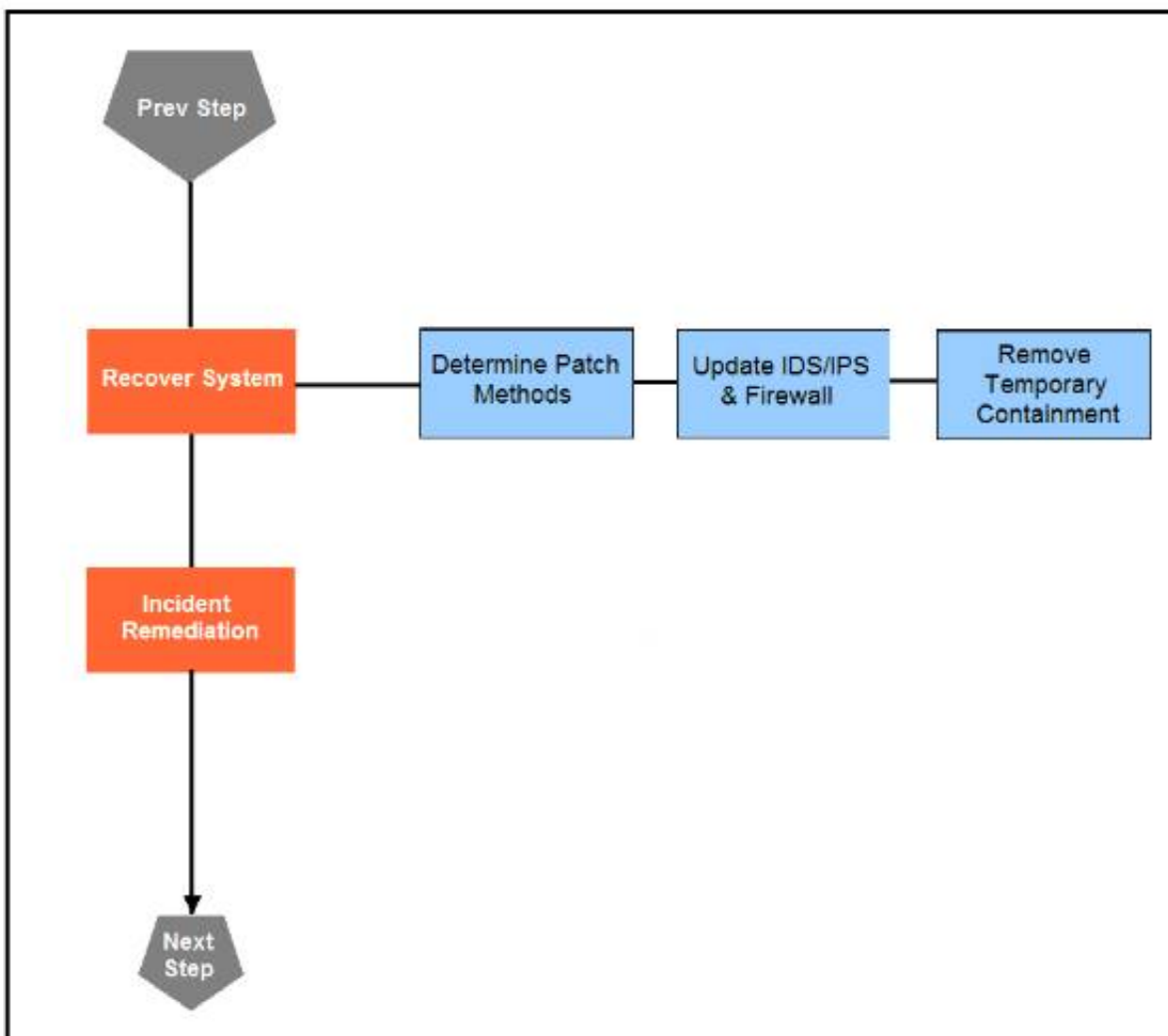
Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 13

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

Answer Area

Eradicate	Analyze and document the breach, and strengthen systems against future attacks
Contain	Conduct incident response role training for employees
Post-Incident Handling	Determine where the breach started and prevent the attack from spreading
Recover	Determine how the breach was discovered and the areas that were impacted
Analyze	Eliminate the root cause of the breach and apply updates to the system
Prepare	Get systems and business operations up and running, and ensure that the same type of attack does not occur again

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Eradicate	Contain
Contain	Prepare
Post-Incident Handling	Recover
Recover	Analyze
Analyze	Eradicate
Prepare	Post-Incident Handling

NEW QUESTION 16

Refer to the exhibit.


```
{
  "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"
  }
]
```

Which indicator of compromise is represented by this STIX?

- 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

Answer: C

NEW QUESTION 17

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

Answer Area

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	SaaS
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	PaaS
Logs, alerts, and events for operating systems are configurable by the customer	IaaS

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	Logs, alerts, and events for operating systems are configurable by the customer
Logs, alerts, and events for operating systems are configurable by the customer	Logs, alerts, and events for application performance monitoring and application health are configurable by the customer

NEW QUESTION 18

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

Answer: A

NEW QUESTION 19

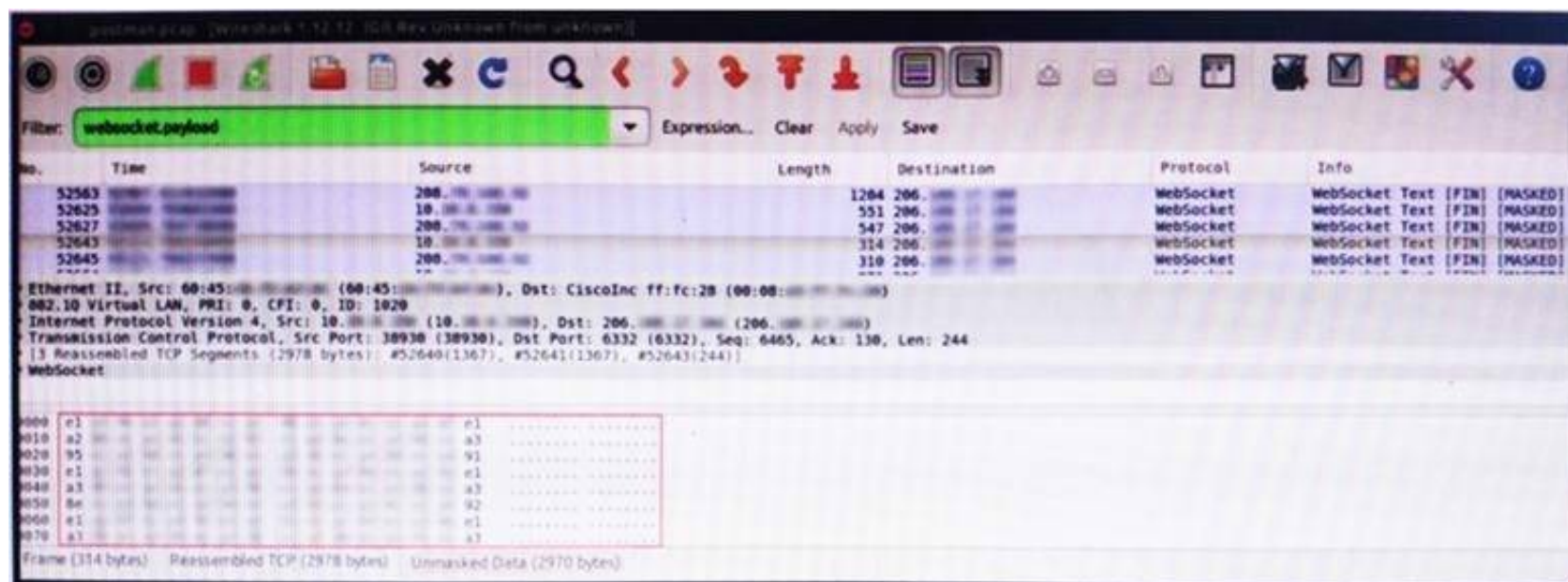
A SOC team is informed that a UK-based user will be traveling between three countries over the next 60 days. Having the names of the 3 destination countries and the user's working hours, what must the analyst do next to detect an abnormal behavior?

- 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 21

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 22

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 27

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 31

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 350-201 Exam with Our Prep Materials Via below:

<https://www.certleader.com/350-201-dumps.html>