

# Cisco

## Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)



NEW QUESTION 1

Refer to the exhibit.

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

Which command was executed in PowerShell to generate this log?

- A. Get-EventLog -LogName\*
- B. Get-EventLog -List
- C. Get-WinEvent -ListLog\* -ComputerName localhost
- D. Get-WinEvent -ListLog\*

Answer: A

NEW QUESTION 2

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

Answer: D

NEW QUESTION 3

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

Answer: B

NEW QUESTION 4

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.

Answer Area

vulnerability assessment	gathering information on a target for future use
persistence	probing the target to discover operating system details
exploit	confirming the existence of known vulnerabilities in the target system
cover tracks	using previously identified vulnerabilities to gain access to the target system
reconnaissance	inserting backdoor access or covert channels to ensure access to the target system
enumeration	erasing traces of actions in audit logs and registry entries

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

vulnerability assessment	persistence
persistence	reconnaissance
exploit	vulnerability assessment
cover tracks	exploit
reconnaissance	enumeration
enumeration	cover tracks

NEW QUESTION 5

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	End-user desktops allow the execution of non-approved applications that include malicious code
Use multifactor authentication for remote access or accessing sensitive information	Application security vulnerabilities can be used to execute malicious code
Change backup and store software and configuration settings for at least three months	Privilege accounts have full rights to information systems
Patch applications including flash, web browsers, and PDF viewers	User verification is weak and based on a single factor
Utilize application control to stop malware delivery and execution	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	Utilize application control to stop malware delivery and execution
Use multifactor authentication for remote access or accessing sensitive information	Patch applications including flash, web browsers, and PDF viewers
Change backup and store software and configuration settings for at least three months	Restrict administrative access to operating systems and applications in accordance with job duties
Patch applications including flash, web browsers, and PDF viewers	Use multifactor authentication for remote access or accessing sensitive information
Utilize application control to stop malware delivery and execution	Change backup and store software and configuration settings for at least three months

### NEW QUESTION 6

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 7

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

**Answer:** D

### NEW QUESTION 8

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 9

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

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

**Answer:** C

#### NEW QUESTION 10

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

**Answer:** D

#### NEW QUESTION 14

Refer to the exhibit.

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

Which data format is being used?

- A. JSON
- B. HTML
- C. XML
- D. CSV

**Answer:** B

#### NEW QUESTION 18

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 22

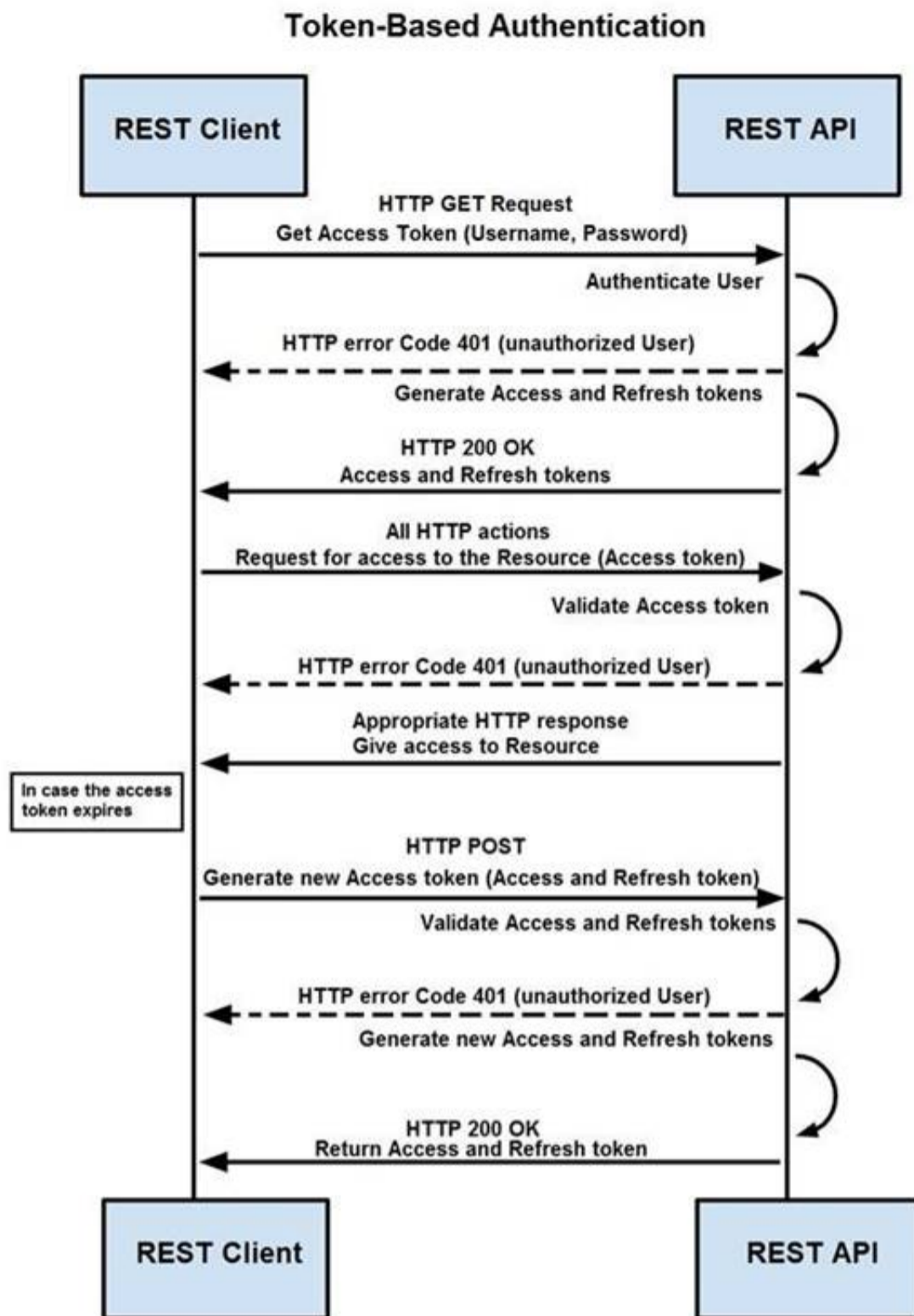
What is a limitation of cyber security risk insurance?

- 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 24

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 26

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 28

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

Answer: C

NEW QUESTION 29

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 reimagine 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

Answer: C

NEW QUESTION 30

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 35

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 40

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

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

Answer: A

NEW QUESTION 44

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 46

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 48

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.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area

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

NEW QUESTION 53

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 55

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

Answer Area

spoofing attack	installing network devices
broken authentication attack	developing new code
injection attack	implementing a new application
man-in-the-middle attack	changing configuration settings
privilege escalation attack	
default credential attack	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

spoofing attack	man-in-the-middle attack
broken authentication attack	injection attack
injection attack	privilege escalation attack
man-in-the-middle attack	default credential attack
privilege escalation attack	
default credential attack	

NEW QUESTION 60

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

Answer: B

NEW QUESTION 61

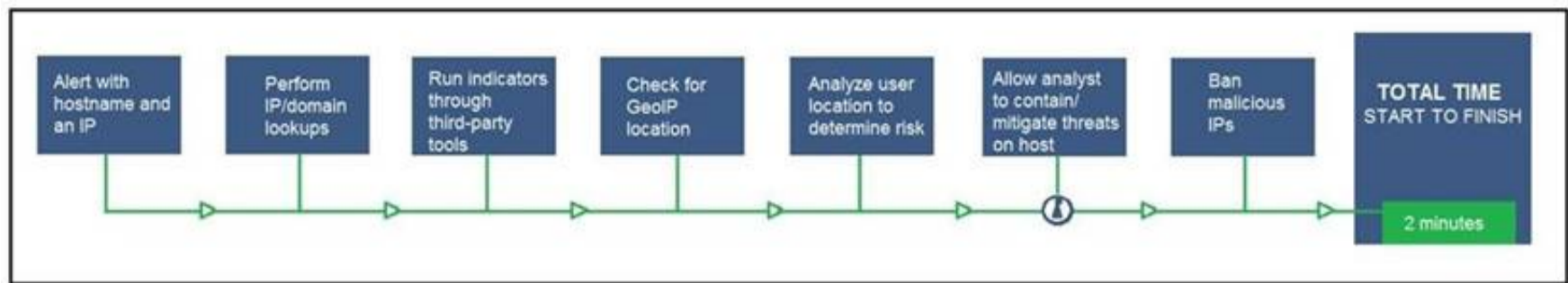
An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

- A. continuous delivery
- B. continuous integration
- C. continuous deployment
- D. continuous monitoring

Answer: A

NEW QUESTION 65

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

Answer: A

NEW QUESTION 67

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.

Answer: C

NEW QUESTION 69

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

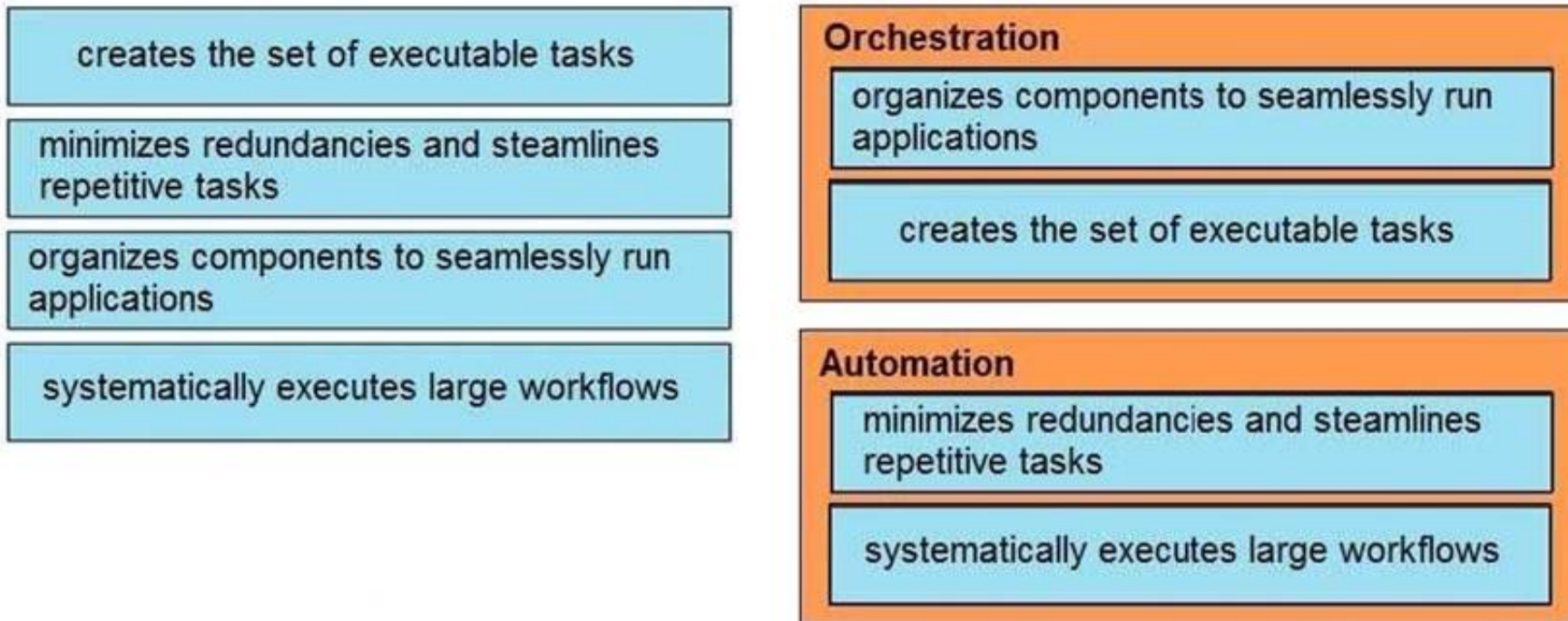
Automation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area



### NEW QUESTION 71

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 73

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 74

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 79

Refer to the exhibit.

```
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; )
```

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

**Answer: B**

#### NEW QUESTION 82

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

**Answer: D**

#### NEW QUESTION 86

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 88**

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 89**

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 90  
Refer to the exhibit.

<div><div> Stealthwatch <span>cisco.local</span></div><div><div>Dashboards</div><div>Monitor</div><div>Analyze</div><div>Jobs</div><div>Configure</div><div>Deploy</div></div><div>128.107.78.8</div></div>																
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

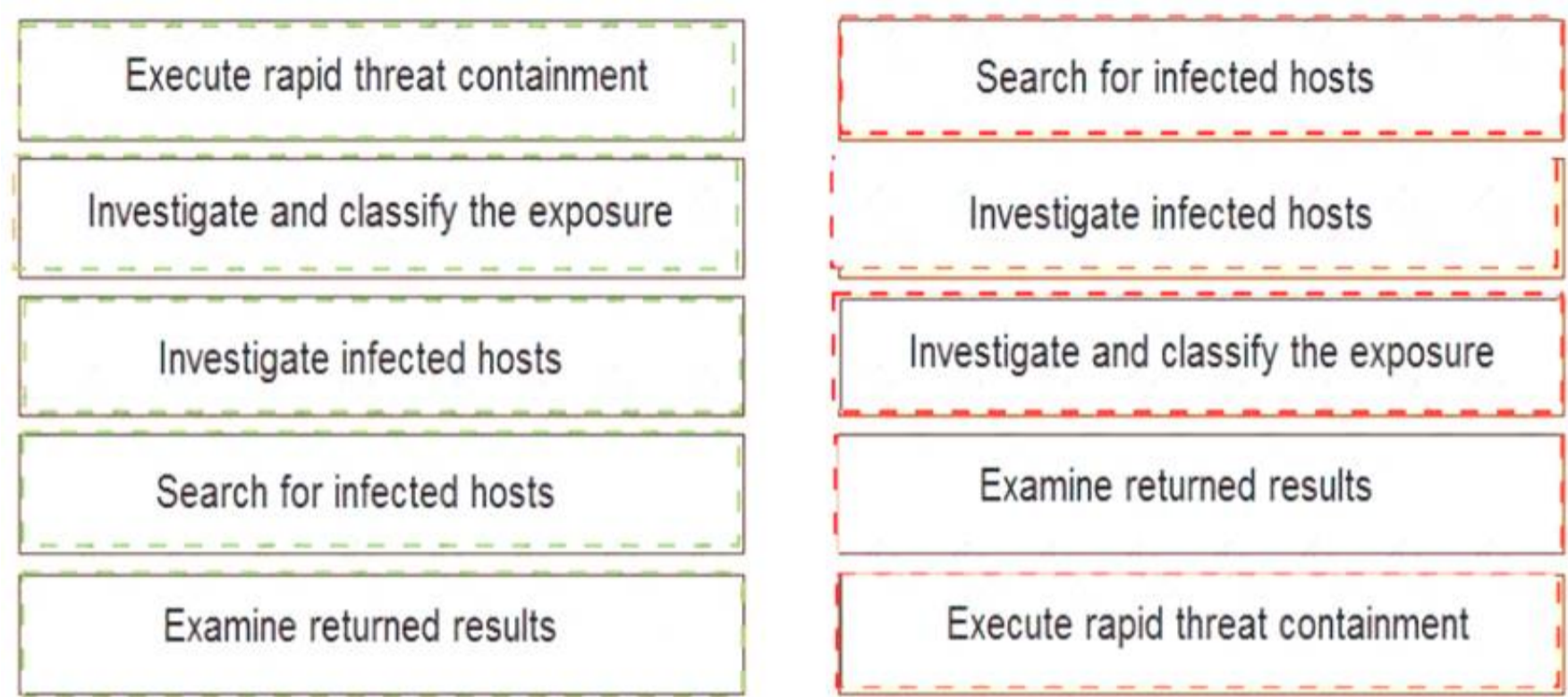
Step 5

- A. Mastered
- B. Not Mastered

Answer: A

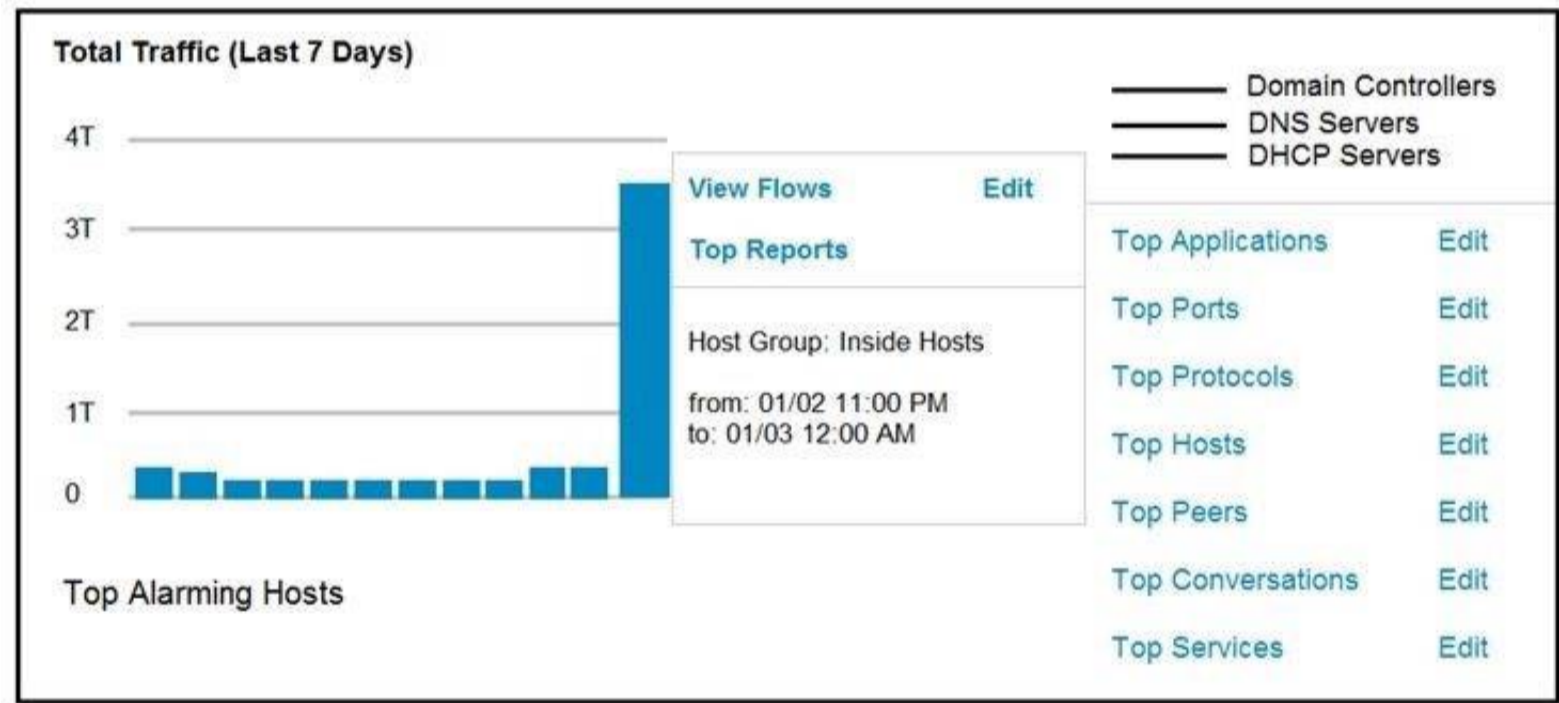
Explanation:

Answer Area



NEW QUESTION 91

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

Answer: B

NEW QUESTION 92

Refer to the exhibit.

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 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?

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

**Answer: A**

#### NEW QUESTION 94

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=1
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 96

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 99**

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 100**

.....

## 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](#)**