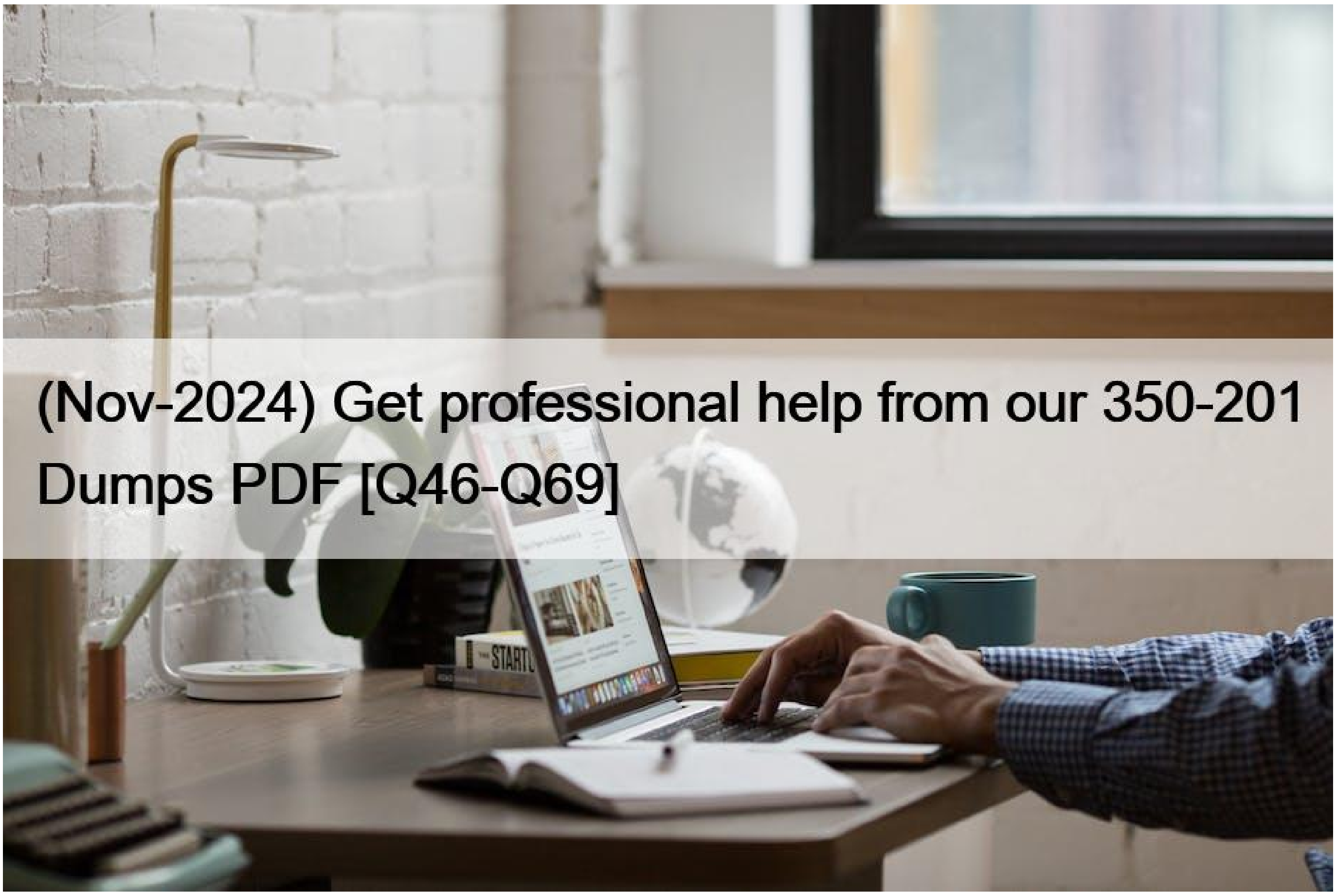
(Nov-2024) Get professional help from our 350-201 Dumps PDF [Q46-Q69



(Nov-2024) Get professional help from our 350-201 Dumps PDF
Give You Free Regular Updates on 350-201 Exam Questions

Cisco 350-201 certification exam is an excellent opportunity for cybersecurity professionals to enhance their skills and knowledge and gain recognition as a Cisco certified professional. With the ever-increasing importance of cybersecurity in today's digital age, obtaining this certification can open up new career opportunities and help individuals stay competitive in the job market.

NEW QUESTION 46

Which action should be taken when the HTTP response code 301 is received from a web application?
* Update the cached header metadata.
* Confirm the resource&#8217;s location.
* Increase the allowed user limit.
* Modify the session timeout setting.

NEW QUESTION 47

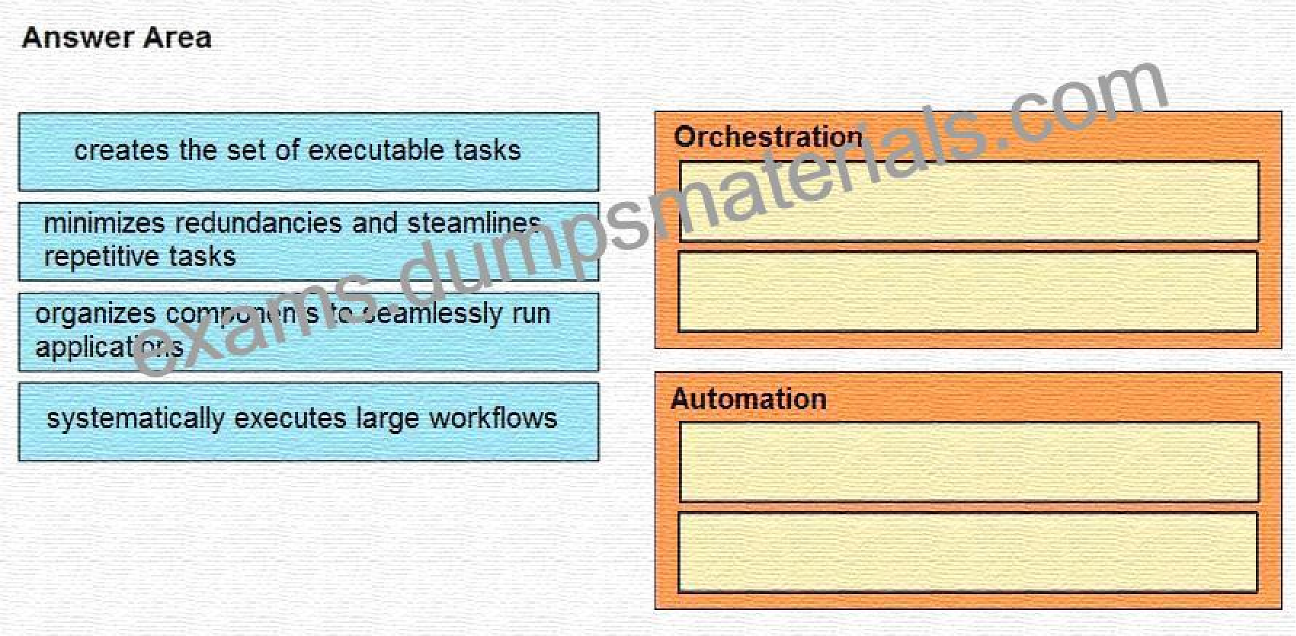
What is a benefit of key risk indicators?

* clear perspective into the risk position of an organization
* improved visibility on quantifiable information
* improved mitigation techniques for unknown threats
* clear procedures and processes for organizational risk

Key risk indicators (KRIs) provide a clear perspective into the risk position of an organization. KRIs are metrics used to proactively measure risks that a business may face. They serve as early warning signs of upcoming crises, which can provide an organization&#8217;s management team time to create an action plan to mitigate that risk&#8217;s potential impact or prevent it from occurring2.

NEW QUESTION 48

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



Answer Area

creates the set of executable tasks

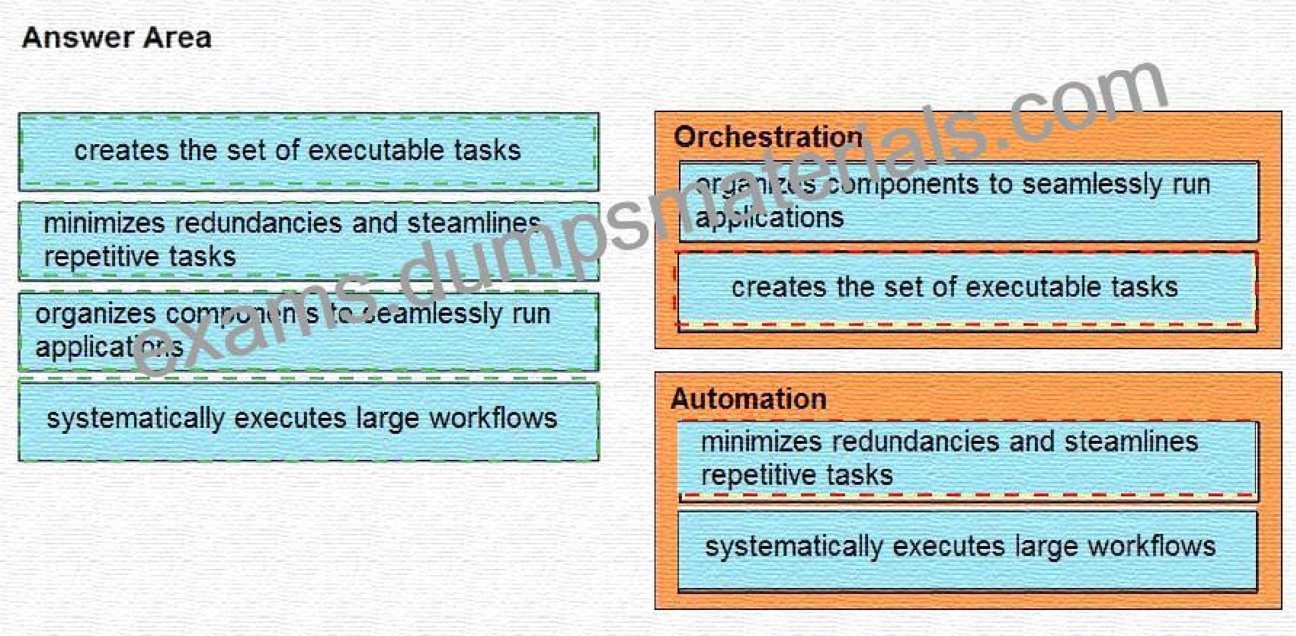
minimizes redundancies and steamlines repetitive tasks

organizes components to seamlessly run applications

systematically executes large workflows

Orchestration

Automation



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

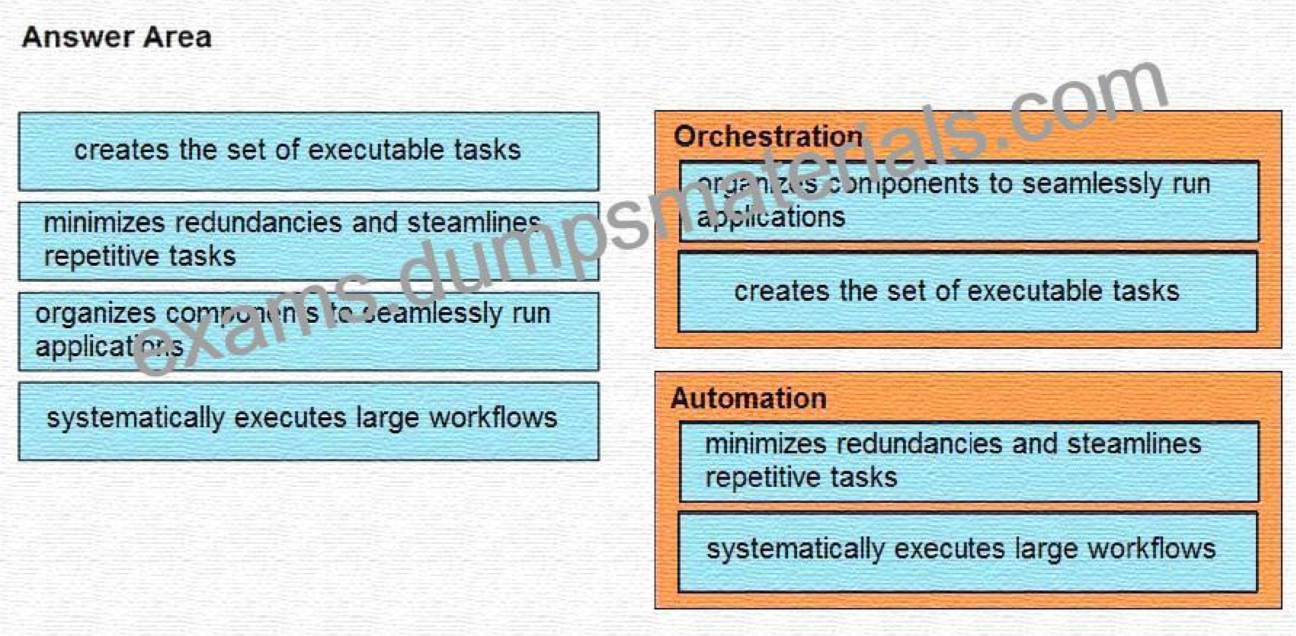
organizes components to seamlessly run applications

creates the set of executable tasks

Automation

minimizes redundancies and steamlines repetitive tasks

systematically executes large workflows



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

organizes components to seamlessly run applications

creates the set of executable tasks

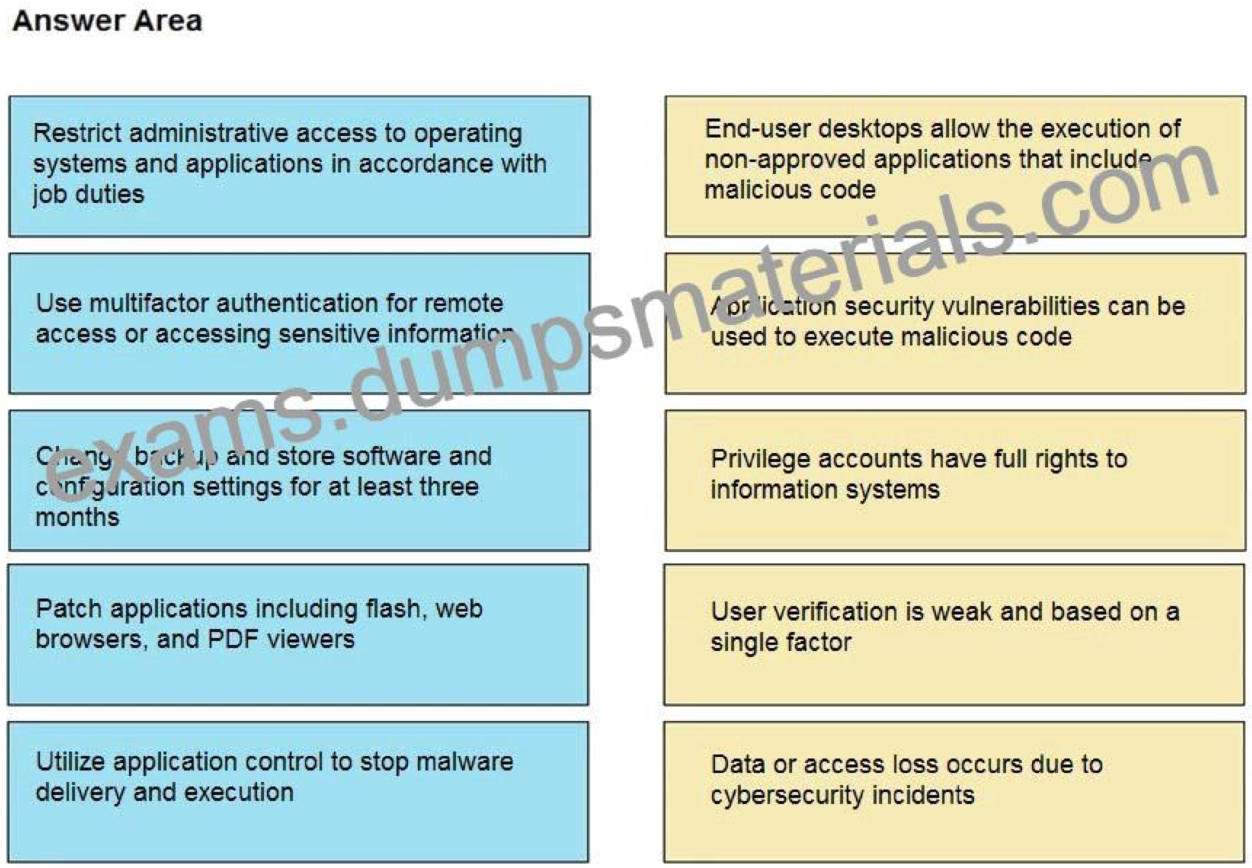
Automation

minimizes redundancies and steamlines repetitive tasks

systematically executes large workflows

NEW QUESTION 49

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

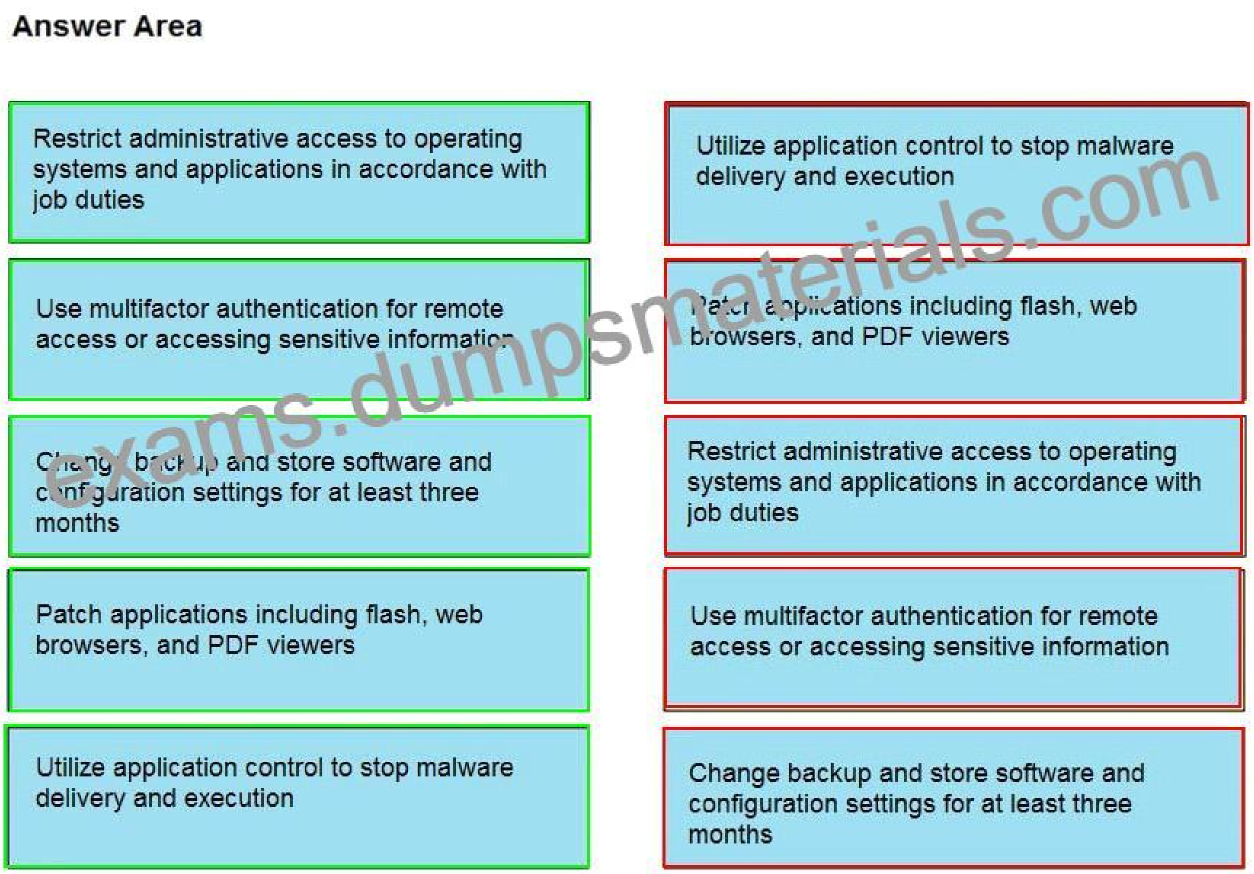
End-user desktops allow the execution of non-approved applications that include malicious code

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



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 50

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?
* Host a discovery meeting and define configuration and policy updates
* Update the IDS/IPS signatures and reimage the affected hosts
* Identify the systems that have been affected and tools used to detect the attack
* Identify the traffic with data capture using Wireshark and review email filters
During the recovery phase of the incident response process, especially after a phishing attack, it&#8217;s crucial to update the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) signatures to detect and prevent similar attacks in the future. Additionally, reimaging the affected hosts ensures that any malware or changes made by the attacker are removed and that the systems are restored to a known good state. This step is essential to eradicate the threat and restore normal operations

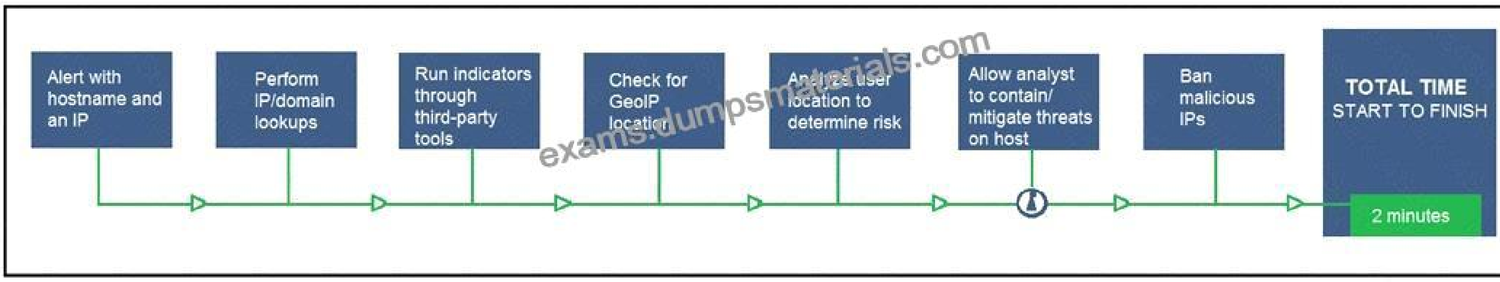
NEW QUESTION 51

A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?
* Classify the criticality of the information, research the attacker&#8217;s motives, and identify missing patches
* Determine the damage to the business, extract reports, and save evidence according to a chain of custody
* Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploited
* Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation plan
When an incident response team receives a report of unexpected changes within software, the immediate steps involve classifying the attack vector, understanding the scope of the event, and identifying the vulnerabilities being exploited. This is a critical part of

the incident response workflow as it helps in determining the nature of the attack and the appropriate containment and eradication strategies3.

NEW QUESTION 52

Refer to the exhibit.


Alert with hostname and an IP
Perform IP/domain lookups
Run indicators through third-party tools
Check for GeoIP location
Analyze user location to determine risk
Allow analyst to contain/ mitigate threats on host
Ban malicious IPs
TOTAL TIME
START TO FINISH
2 minutes

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?
* Exclude the step &#8220;BAN malicious IP&#8221; to allow analysts to conduct and track the remediation
* Include a step &#8220;Take a Snapshot&#8221; to capture the endpoint state to contain the threat for analysis
* Exclude the step &#8220;Check for GeoIP location&#8221; to allow analysts to analyze the location and the associated risk based on asset criticality
* Include a step &#8220;Reporting&#8221; to alert the security department of threats identified by the SOAR reporting engine
Including a step to &#8220;Take a Snapshot&#8221; in the SOAR solution workflow is the most effective action to accomplish the goal of allowing security analysts to be proactive and anticipate attacks. By capturing the endpoint state when a threat is identified, analysts can contain the threat and have a detailed record of the system at the time of the incident. This enables a thorough analysis of the threat, which is essential for understanding attack patterns, identifying potential vulnerabilities, and developing strategies to prevent future incidents.

The other options do not directly contribute to the goal of enabling proactive analysis:

* A. Exclude the step &#8220;BAN malicious IP&#8221;: This would allow threats to persist in the system, potentially

* causing more harm.

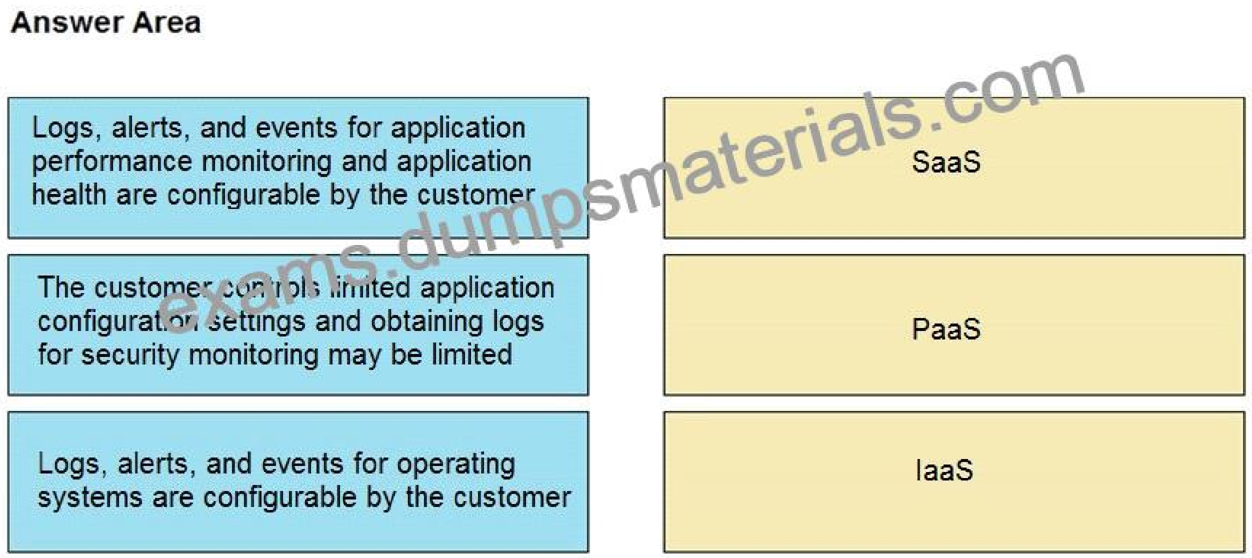
* C. Exclude the step &#8220;Check for GeoIP location&#8221;: GeoIP location is valuable for assessing the risk based on asset criticality and should not be excluded.

* D. Include a step &#8220;Reporting&#8221;: While reporting is important, it does not directly aid in the proactive analysis of threats.

By taking snapshots for analysis, the security team can better understand the nature of the threats and refine their detection and response mechanisms accordingly. This proactive approach is crucial for staying ahead of cyber threats and ensuring the security of the organization&#8217;s assets.

NEW QUESTION 53

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

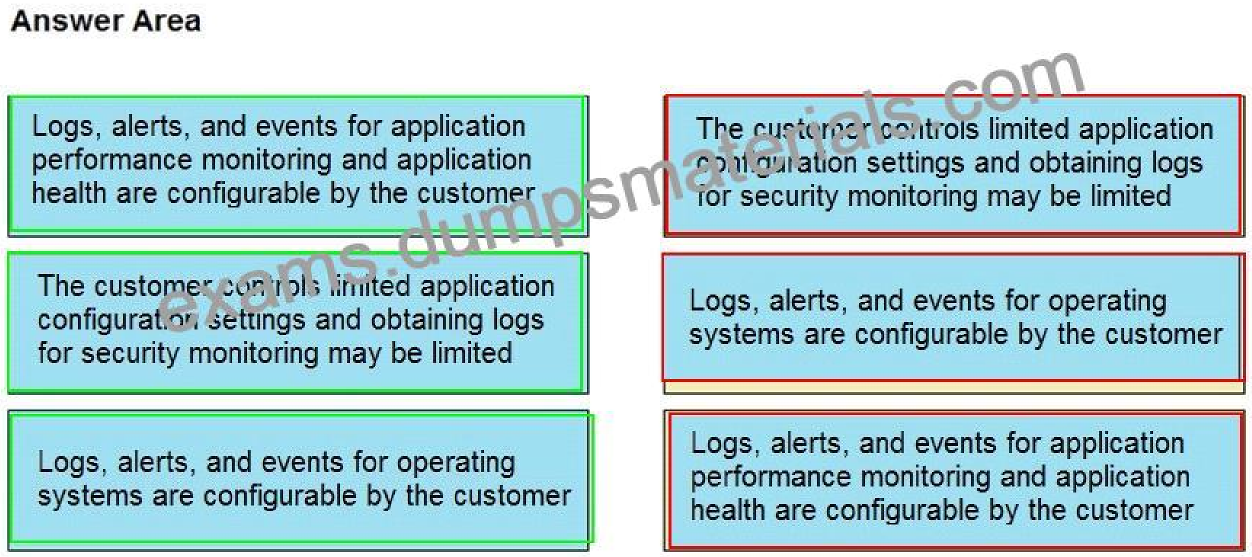
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited

Logs, alerts, and events for operating systems are configurable by the customer

SaaS

PaaS

IaaS



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

Logs, alerts, and events for operating systems are configurable by the customer

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 application performance monitoring and application health are configurable by the customer

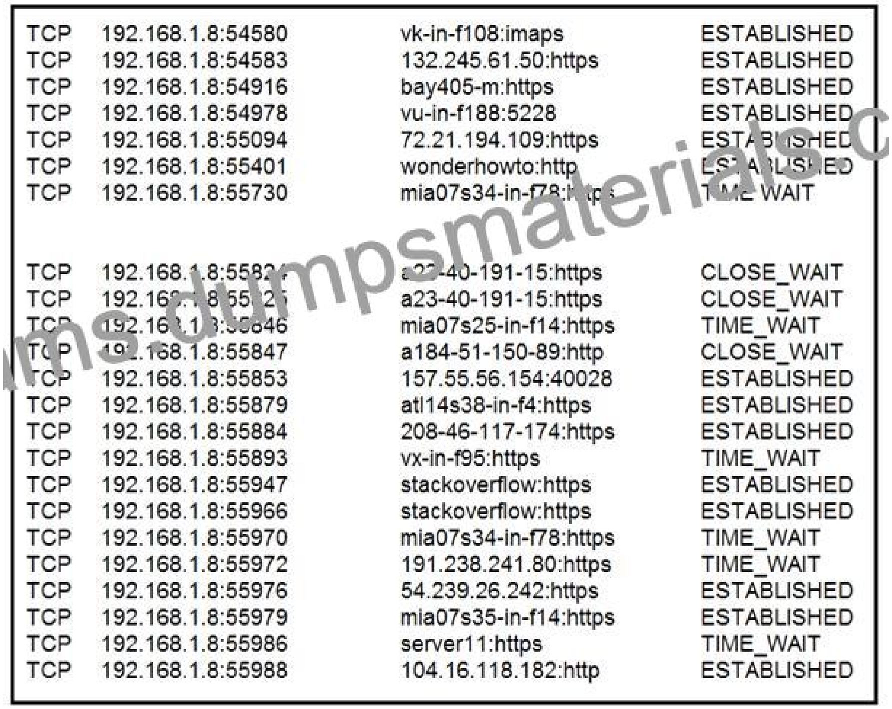
NEW QUESTION 54

A SOC team receives multiple alerts by a rule that detects requests to malicious URLs and informs the incident response team to block the malicious URLs requested on the firewall. Which action will improve the effectiveness of the process?

- Block local to remote HTTP/HTTPS requests on the firewall for users who triggered the rule.
- Inform the user by enabling an automated email response when the rule is triggered.
- Inform the incident response team by enabling an automated email response when the rule is triggered.
- Create an automation script for blocking URLs on the firewall when the rule is triggered.

NEW QUESTION 55

Refer to the exhibit.



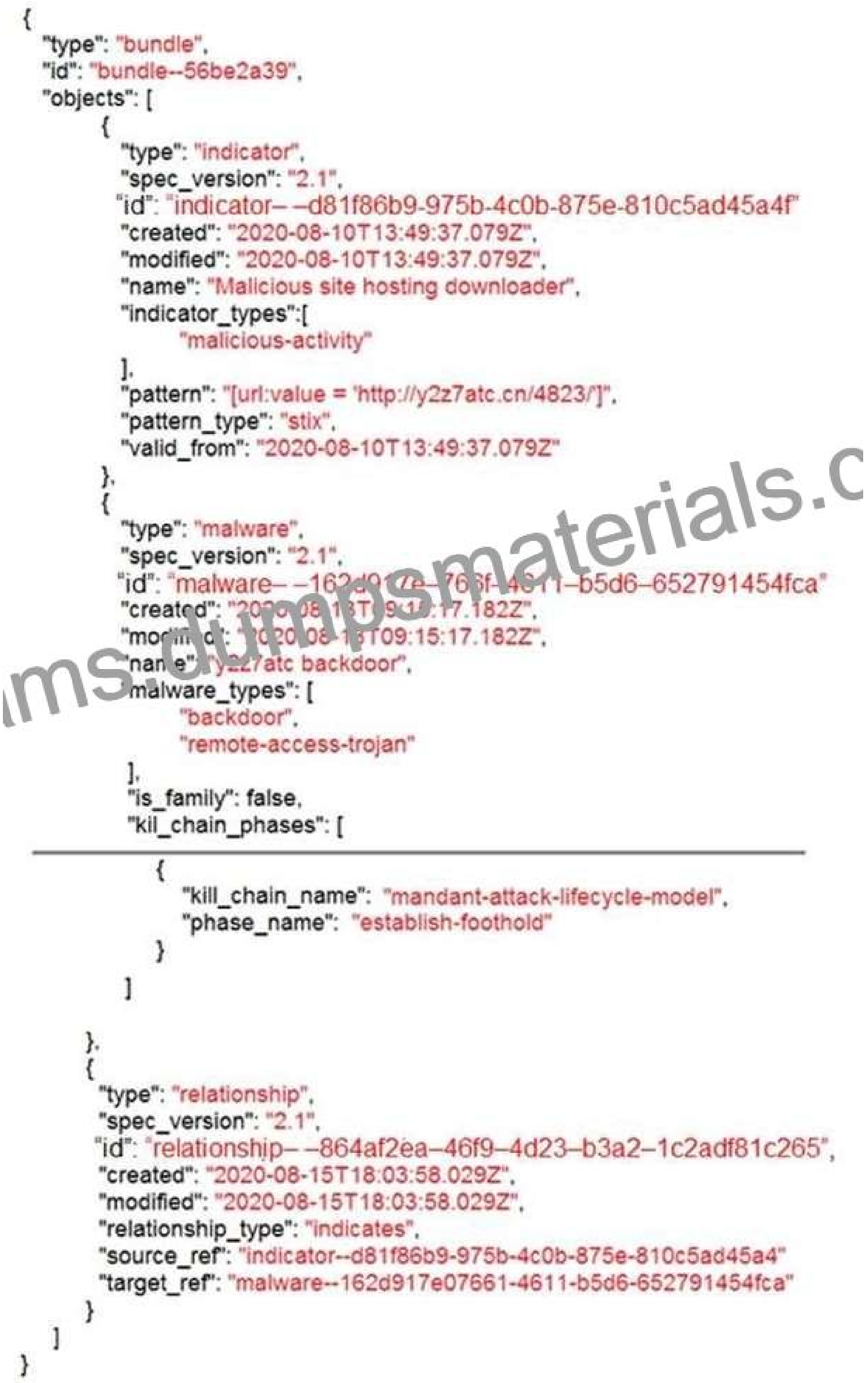
```
TCP    192.168.1.8:54580          vk-in-f108:imaps              ESTABLISHED
TCP    192.168.1.8:54583          132.245.61.50:https           ESTABLISHED
TCP    192.168.1.8:54916          bay405-m:https                ESTABLISHED
TCP    192.168.1.8:54978          vu-in-f188:5228               ESTABLISHED
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?

* packet sniffer
* malware analysis
* SIEM
* firewall manager

NEW QUESTION 56

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



```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
      {
        "type": "indicator",
        "spec_version": "2.1",
       "id": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4f"
        "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--162d917e-766f-4611-b5d6-652791454fca"
        "created": "2020-08-18T09:15:17.182Z",
        "modified": "2020-08-18T09:15:17.182Z",
        "name": "y2z7atc backdoor",
        "malware_types": [
              "backdoor",
              "remote-access-trojan"
        ],
        "is_family": false,
        "kil_chain_phases": [
            {
              "kill_chain_name": "mandant-attack-lifecycle-model",
              "phase_name": "establish-foothold"
            }
        ]

     },
     {
       "type": "relationship",
       "spec_version": "2.1",
      "id": "relationship--864af2ea-46f9-4d23-b3a2-1c2adf81c265",
       "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"
     }
   ]
}
```

* website redirecting traffic to ransomware server
* website hosting malware to download files
* web server vulnerability exploited by malware
* cross-site scripting vulnerability to backdoor server

NEW QUESTION 57

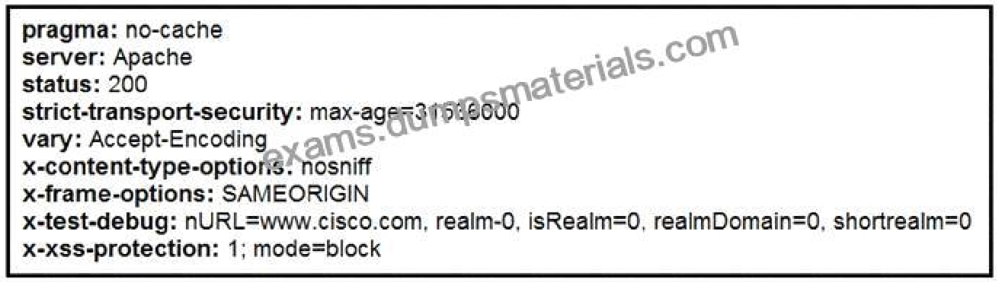
Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?
* customer data

- internal database
- internal cloud
- Internet

Threat intelligence tools primarily search the Internet to identify potential malicious IP addresses, domain names, and URLs. They scour various online sources, including databases of known threats, security forums, and other cyber threat intelligence feeds to gather information. This data is then used to update their internal databases and protect against known and emerging threats.

NEW QUESTION 58

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, realmDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Where does it signify that a page will be stopped from loading when a scripting attack is detected?

- x-frame-options
- x-content-type-options
- x-xss-protection
- x-test-debug

The HTTP response header that signifies a page will be stopped from loading when a scripting attack is detected is the x-xss-protection header. When configured with the value &#8220;1; mode=block&#8221;, it instructs the browser to block the entire page from loading if a cross-site scripting (XSS) attack is detected, rather than attempting to sanitize the potentially malicious script. This header is a browser-side measure to prevent the execution of scripts if an XSS attack is suspected.

The other headers listed serve different purposes:

* x-frame-options: Controls whether a browser should be allowed to render a page in a <frame>, <iframe>, <embed>, or <object>.

* x-content-type-options: Prevents the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.

* x-test-debug: This is not a standard response header and does not relate to XSS protection.

It&#8217;s important to configure web servers and applications with the appropriate security headers to mitigate various types of web-based attacks.

NEW QUESTION 59

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

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

* by entities that issue the payment cards or that perform support issuing services
* post-authorization by non-issuing entities if the data is encrypted and securely stored
* by issuers and issuer processors if there is a legitimate reason

NEW QUESTION 60

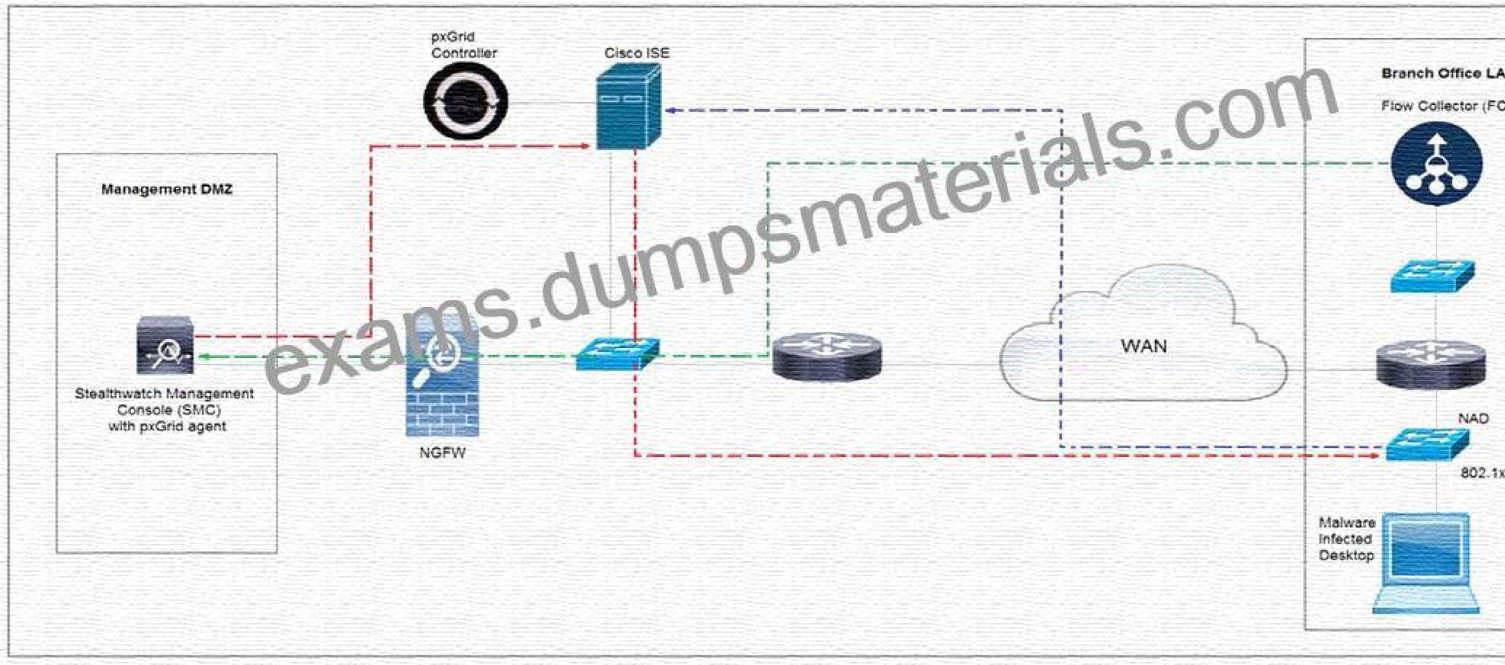
A SOC analyst detected a ransomware outbreak in the organization coming from a malicious email attachment. Affected parties are notified, and the incident response team is assigned to the case. According to the NIST incident response handbook, what is the next step in handling the incident?

* Eradicate malicious software from the infected machines.
* Collect evidence and maintain a chain-of-custody during further analysis.
* Perform a vulnerability assessment to find existing vulnerabilities.
* Create a follow-up report based on the incident documentation.

According to the NIST incident response handbook, after detecting a ransomware outbreak and notifying the affected parties, the next step is to eradicate the malicious software from the infected machines. This involves removing the ransomware and any associated malware to prevent further encryption or spread of the infection3

NEW QUESTION 61

Refer to the exhibit.



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 method was used to signal ISE to quarantine the endpoints?

* SNMP
* syslog
* REST API
* pxGrid

In the context of Cisco Secure Network Analytics (formerly known as Stealthwatch) and ISE (Identity Services Engine), pxGrid

(Platform Exchange Grid) is used for sharing context-aware information across different security tools toenable rapid threat containment. When a malware-infected endpoint is detected, Cisco Secure Network Analytics can communicate with ISE using pxGrid to signal the need for quarantine.

This allows ISE to place the infected endpoint into a designated quarantine VLAN using an Adaptive Network Control policy, effectively isolating the threat and preventing it from spreading through the network.

References:

* Cisco&#8217;s guide on pxGrid

* Cisco&#8217;s solution overview on Rapid Threat Containment

NEW QUESTION 62

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

* Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.
* Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.
* Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.
* Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.

NEW QUESTION 63

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?

* DLP for data in motion
* DLP for removable data
* DLP for data in use
* DLP for data at rest

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

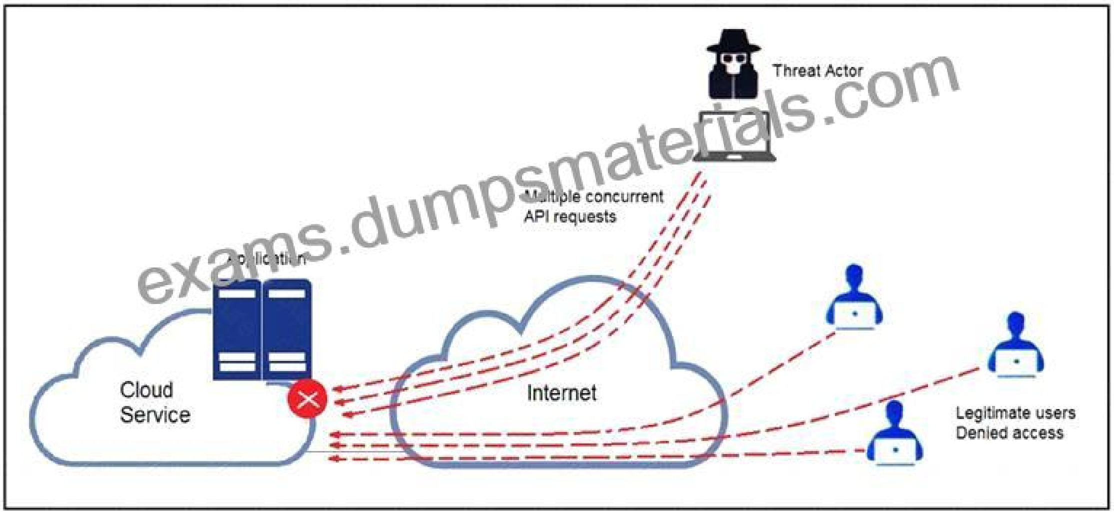
NEW QUESTION 64

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?

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

NEW QUESTION 65

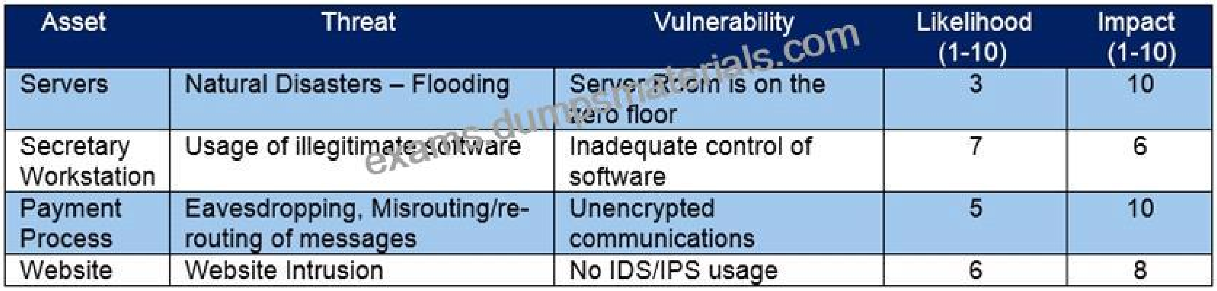
Refer to the exhibit.


Threat Actor
Multiple concurrent API requests
Application
Cloud Service
Internet
Legitimate users Denied access

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

NEW QUESTION 66

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?
* servers
* website
* payment process
* secretary workstation

NEW QUESTION 67

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?
* Run the sudo sysdiagnose command
* Run the sh command
* Run the w command
* Run the who command

NEW QUESTION 68

A security engineer discovers that a spreadsheet containing confidential information for nine of their employees was fraudulently posted on a competitor&#8217;s website. The spreadsheet contains names, salaries, and social security numbers. What is the next step the engineer should take in this investigation?
* Determine if there is internal knowledge of this incident.
* Check incoming and outgoing communications to identify spoofed emails.
* Disconnect the network from Internet access to stop the phishing threats and regain control.
* Engage the legal department to explore action against the competitor that posted the spreadsheet.

NEW QUESTION 69

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?
* Identify the business applications running on the assets
* Update software to patch third-party software
* Validate CSRF by executing exploits within Metasploit
* Fix applications according to the risk scores

The Cisco 350-201 exam consists of 90-110 questions and has a duration of 120 minutes. 350-201 exam tests the candidate's knowledge of Cisco security technologies, including network security, cloud security, endpoint protection, threat intelligence, and incident response. 350-201 exam is available in English and Japanese and can be taken at authorized testing centers or online.

Achieve the 350-201 Exam Best Results with Help from Cisco Certified Experts:
https://www.dumpsmaterials.com/350-201-real-torrent.html]