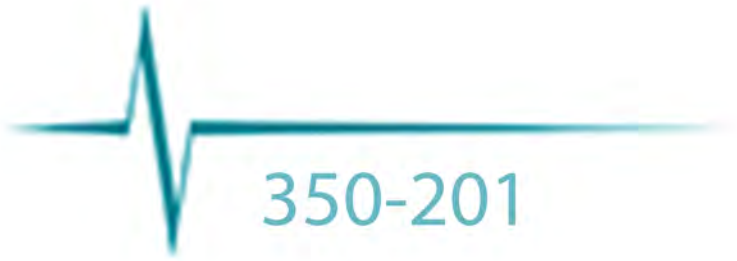
Practice Exam Questions



Performing CyberOps Using Core Security Technologies (CBRCOR)

EXAMKILLER

Help Pass Your Exam At First Try

Cisco

Exam 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

Version: 4.0

[Total Questions: 139]

Question No : 1

Which bash command will print all lines from the “colors.txt” file containing the non case-sensitive pattern “Yellow”?

A. grep -i “yellow” colors.txt
B. locate “yellow” colors.txt
C. locate -i “Yellow” colors.txt
D. grep “Yellow” colors.txt

Answer: A

Question No : 2

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

Question No : 3

A security manager received an email from an anomaly detection service, that one of their contractors has downloaded 50 documents from the company’s confidential document management folder using a company- owned asset al039-ice-4ce687TL0500. A security manager reviewed the content of downloaded documents and noticed that the data affected is from different departments. What are the actions a security manager should take?

A. Measure confidentiality level of downloaded documents.
B. Report to the incident response team.
C. Escalate to contractor’s manager.
D. Communicate with the contractor to identify the motives.

Answer: B

Question No : 4

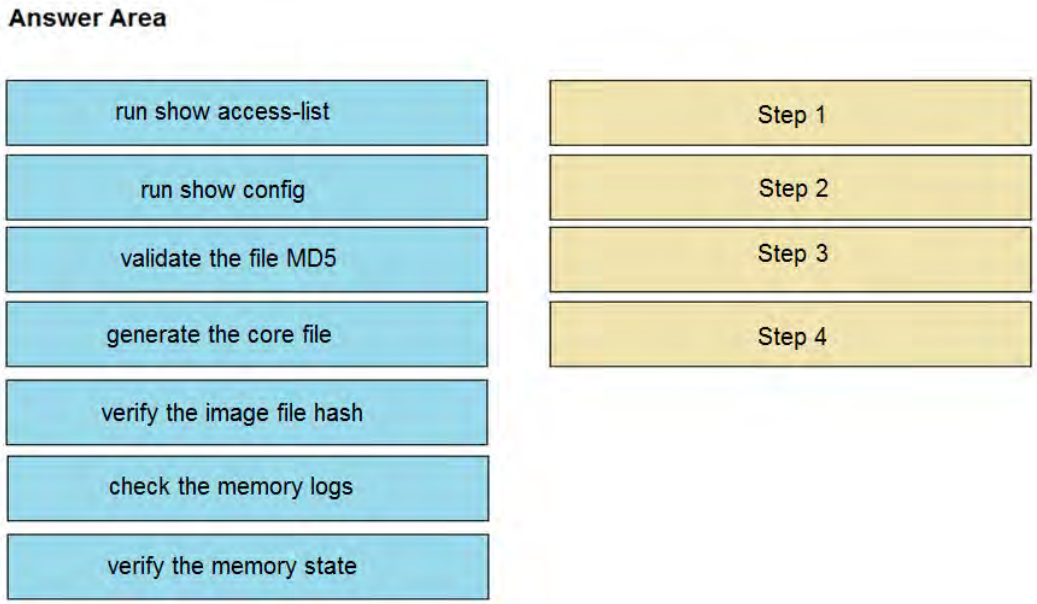
A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format 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

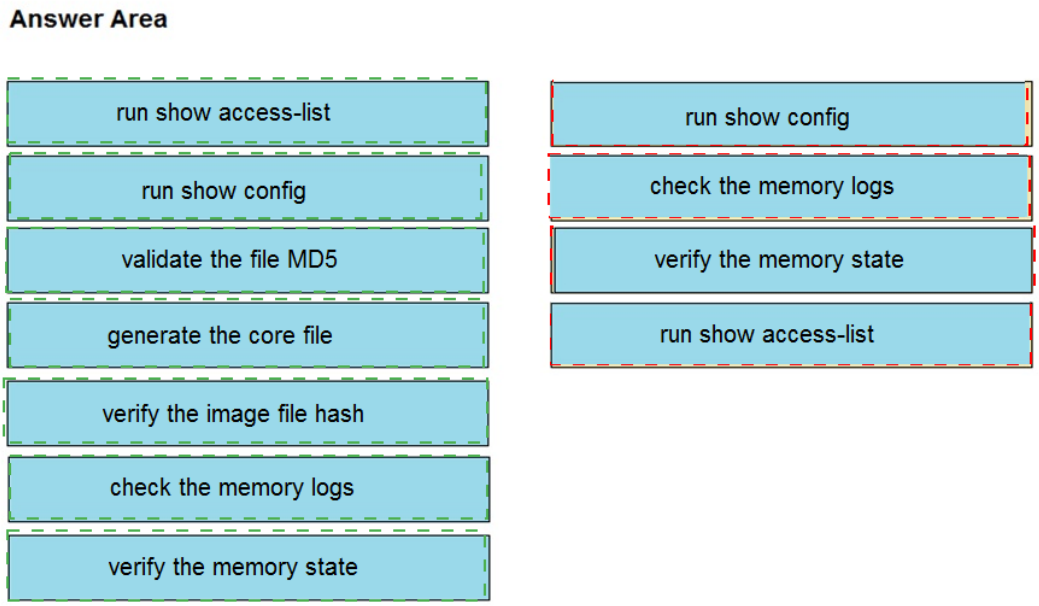
Answer: C

Question No : 5 DRAG DROP

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

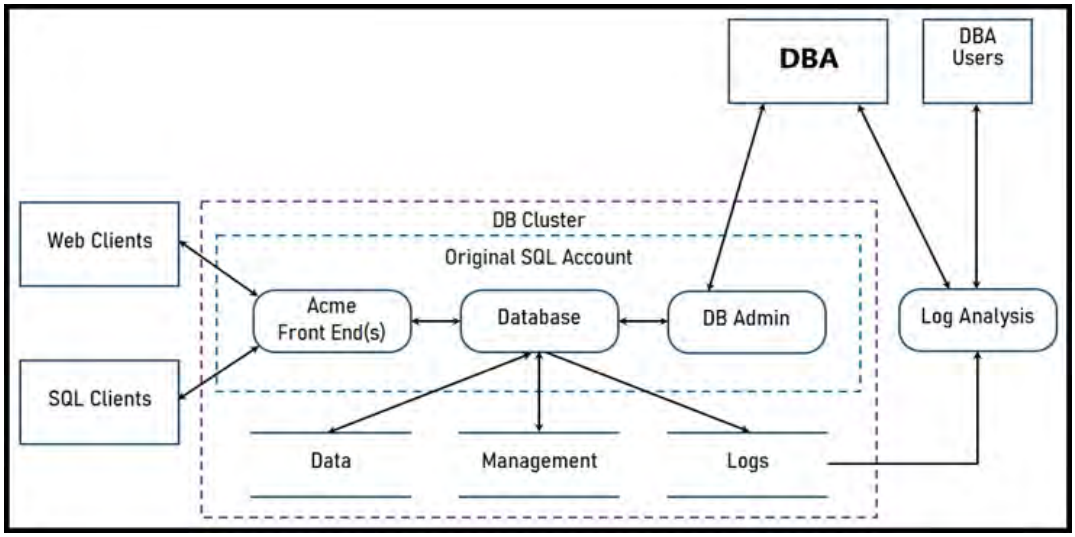


Answer:



Question No : 6

Refer to the exhibit.



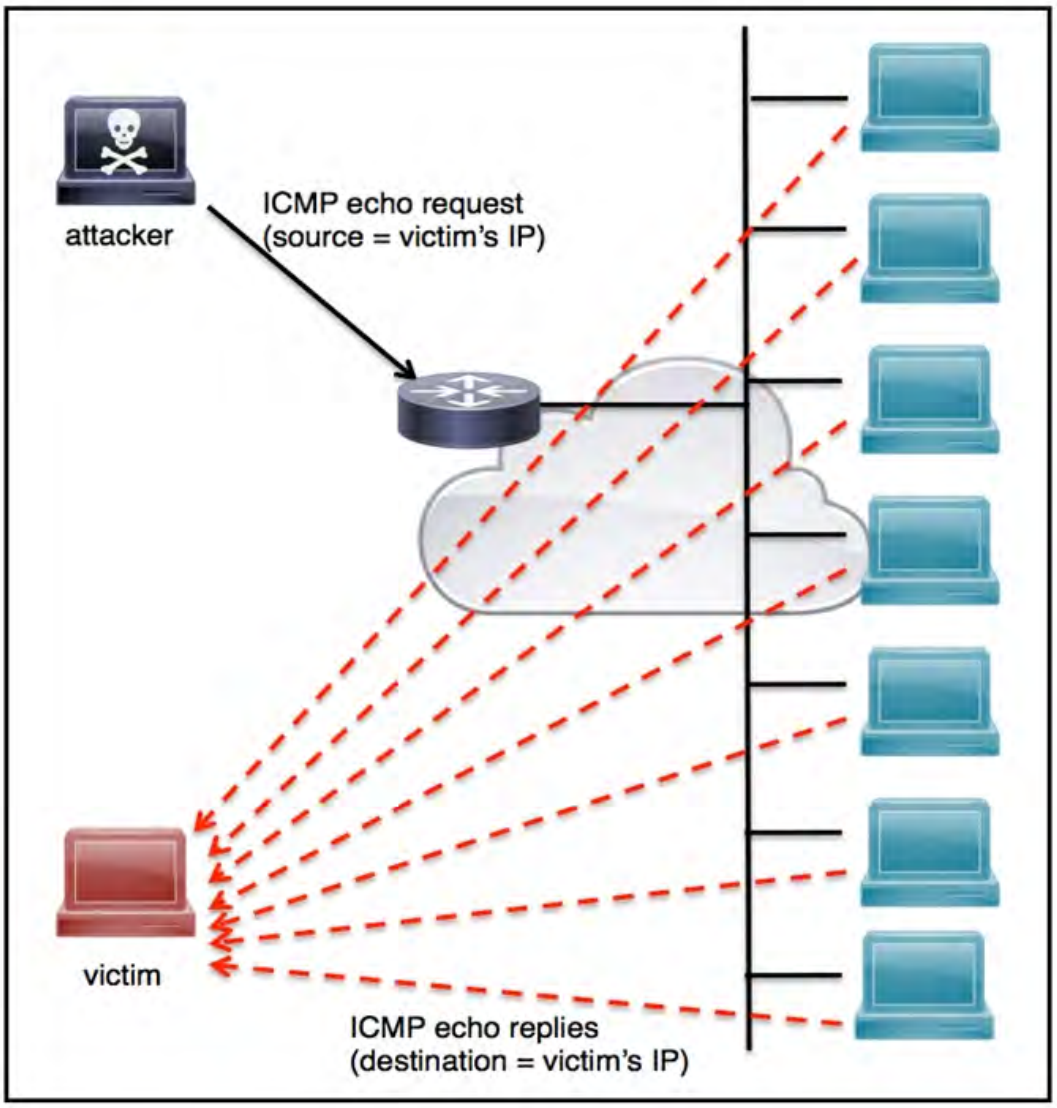
Two types of clients are accessing the front ends and the core database that manages transactions, access control, and atomicity. What is the threat model for the SQL database?

A. An attacker can initiate a DoS attack.
B. An attacker can read or change data.
C. An attacker can transfer data to an external server.
D. An attacker can modify the access logs.

Answer: A

Question No : 7

Refer to the exhibit.



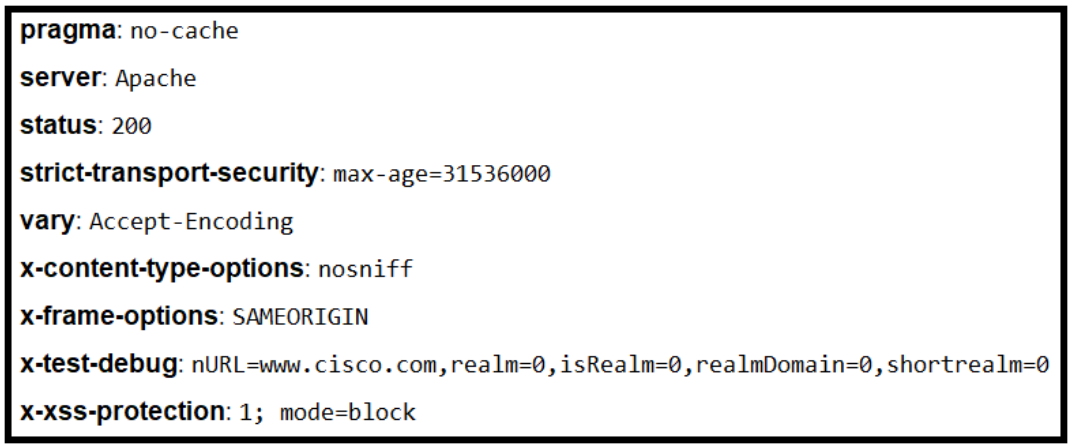
An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action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

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

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

Question No : 8

Refer to the exhibit.



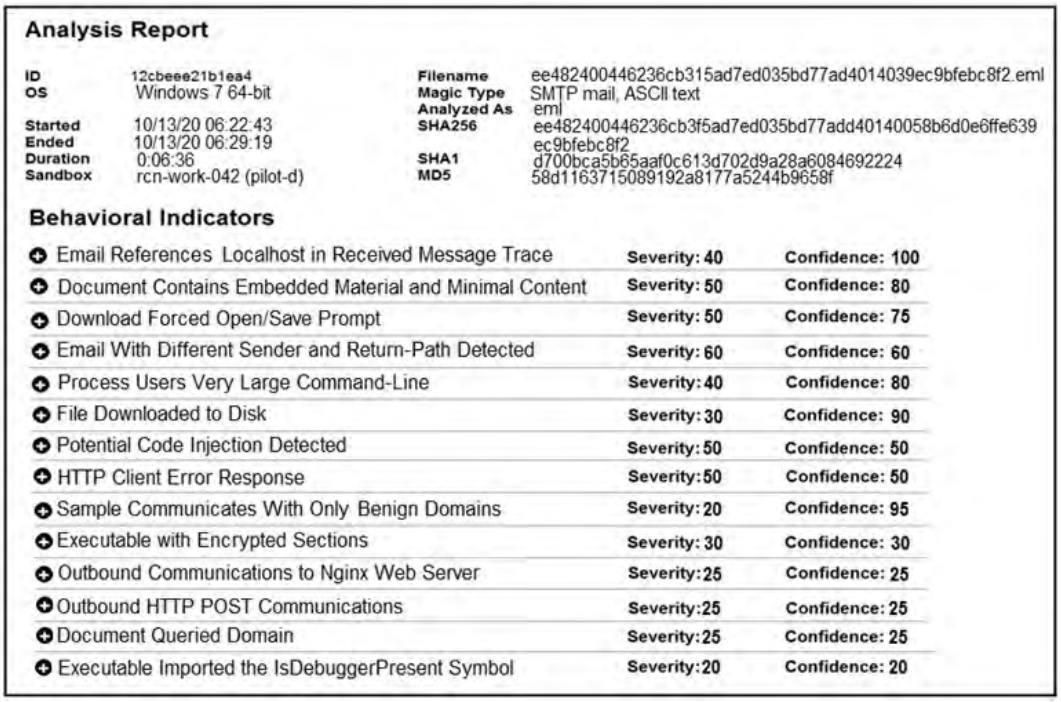
Where is the MIME type that should be followed indicated?

A. x-test-debug
B. strict-transport-security
C. x-xss-protection
D. x-content-type-options

Answer: A

Question No : 9

Refer to the exhibit.



Analysis Report

ID	12cbeee21b1ea4	Filename	ee482400446236cb315ad7ed035bd77ad4014039ec9bfebc8f2.eml
OS	Windows 7 64-bit	Magic Type	SMTP mail, ASCII text
		Analyzed As	eml
Started	10/13/20 06:22:43	SHA256	ee482400446236cb3f5ad7ed035bd77add40140058b6d0e6ffe639ec9bfebc8f2
Ended	10/13/20 06:29:19		
Duration	0:06:36	SHA1	d700bca5b65aaf0c613d702d9a28a6084692224
Sandbox	rcn-work-042 (pilot-d)	MD5	58d1163715089192a8177a5244b9658f

Behavioral Indicators

Email References Localhost in Received Message Trace	Severity: 40	Confidence: 100
Document Contains Embedded Material and Minimal Content	Severity: 50	Confidence: 80
Download Forced Open/Save Prompt	Severity: 50	Confidence: 75
Email With Different Sender and Return-Path Detected	Severity: 60	Confidence: 60
Process Users Very Large Command-Line	Severity: 40	Confidence: 80
File Downloaded to Disk	Severity: 30	Confidence: 90
Potential Code Injection Detected	Severity: 50	Confidence: 50
HTTP Client Error Response	Severity: 50	Confidence: 50
Sample Communicates With Only Benign Domains	Severity: 20	Confidence: 95
Executable with Encrypted Sections	Severity: 30	Confidence: 30
Outbound Communications to Nginx Web Server	Severity: 25	Confidence: 25
Outbound HTTP POST Communications	Severity: 25	Confidence: 25
Document Queried Domain	Severity: 25	Confidence: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20

Cisco Advanced Malware Protection installed on an end-user desktop automatically submitted a low prevalence file to the Threat Grid analysis engine. What should be concluded from this report?

A. Threat scores are high, malicious ransomware has been detected, and files have been modified
B. Threat scores are low, malicious ransomware has been detected, and files have been modified
C. Threat scores are high, malicious activity is detected, but files have not been modified
D. Threat scores are low and no malicious file activity is detected

Answer: B

Question No : 10

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

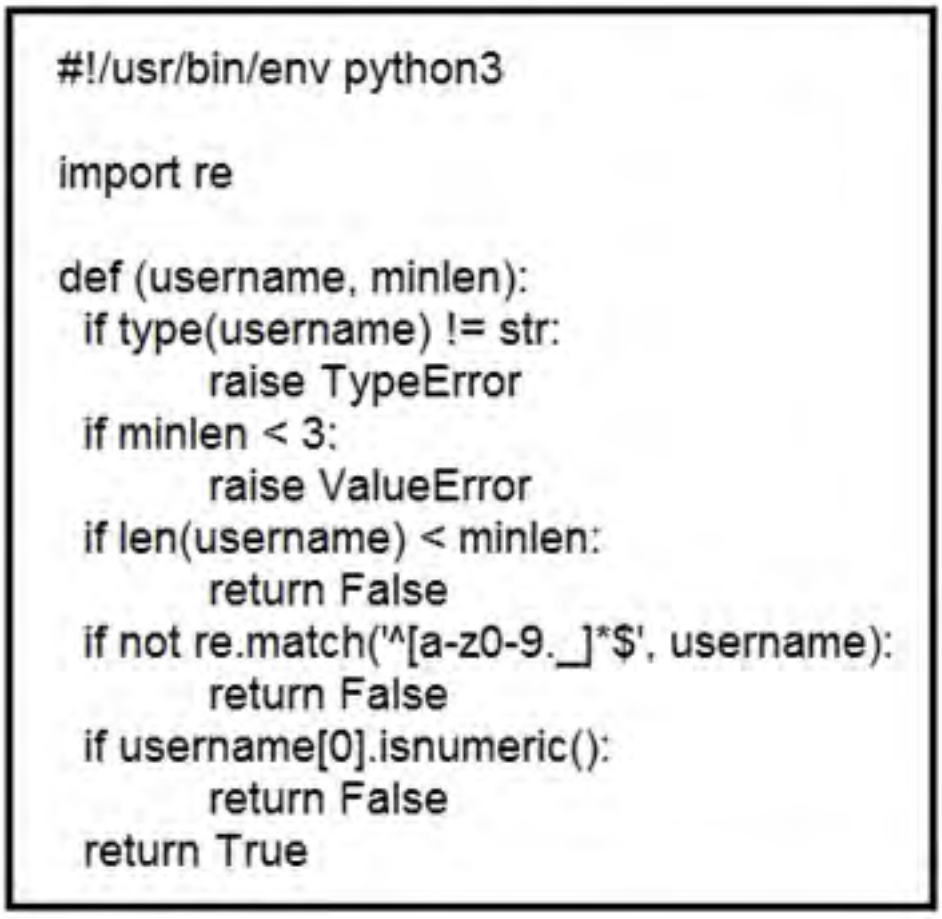
C. Add a confirmation step through which SOAR informs the affected user and asks them to confirm whether they made the attempts

D. Increase incorrect login tries and tune anomalous user behavior not to affect privileged accounts

Answer: B

Question No : 11

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

Question No : 12

The SIEM tool informs a SOC team of a suspicious file. The team initializes the analysis with an automated sandbox tool, sets up a controlled laboratory to examine the malware specimen, and proceeds with behavioral analysis. What is the next step in the malware analysis process?

A. Perform static and dynamic code analysis of the specimen.
B. Unpack the specimen and perform memory forensics.
C. Contain the subnet in which the suspicious file was found.
D. Document findings and clean-up the laboratory.

Answer: B

Question No : 13

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

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

Question No : 14

Refer to the exhibit.

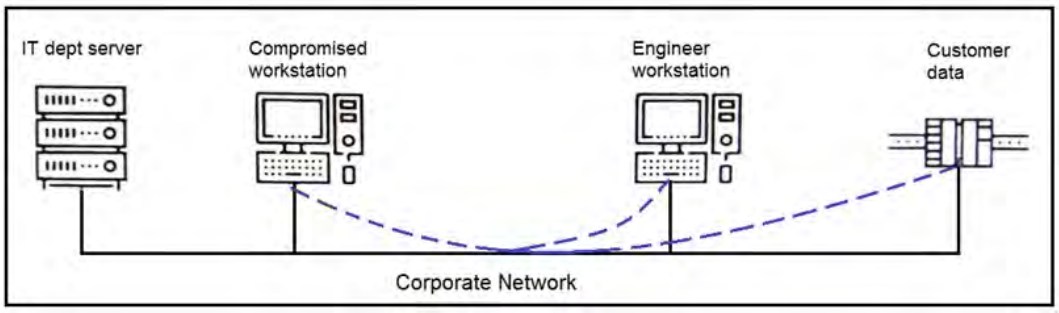
Which data format is being used?

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

Answer: B

Question No : 15

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

Question No : 16

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?

A. x-frame-options

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

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

Question No : 17

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

Question No : 18

Refer to the exhibit.

Distribution Port/ICMP Code	Message	Classification	Application Protocol	Client	Application Risk	Business Relevance	Access Control Rule
80 (http) / tcp	STREAMS_DATA_ON_SYN (129:2:2)	Generic Protocol Command Decode	ICMP	ICMP client	Medium	Medium	rule
80 (http) / tcp	STREAMS_DATA_ON_SYN (129:2:2)	Generic Protocol Command Decode	DNS	DNS client	Very Low	Very High	Default Action
0 (No Code) / icmp	PROTOCOL-ICMP Echo Reply (1:408:8)	Misc Activity	DNS	DNS client	Very Low	Very High	Allow ICMP
54107 / udp	PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt (3:19187:7)	Attempted User Privilege Gain	DNS	DNS client	Very Low	Very High	
49367 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
57477 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
54879 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
60999 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52240 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
54359 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52489 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
60169 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52250 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52485 / up	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
49940 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
57214 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
51608 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52652 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55528 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
61222 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55640 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55991 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	

What is the connection status of the ICMP event?

A. blocked by a configured access policy rule
B. allowed by a configured access policy rule
C. blocked by an intrusion policy rule
D. allowed in the default action

Answer: B

Question No : 19

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.