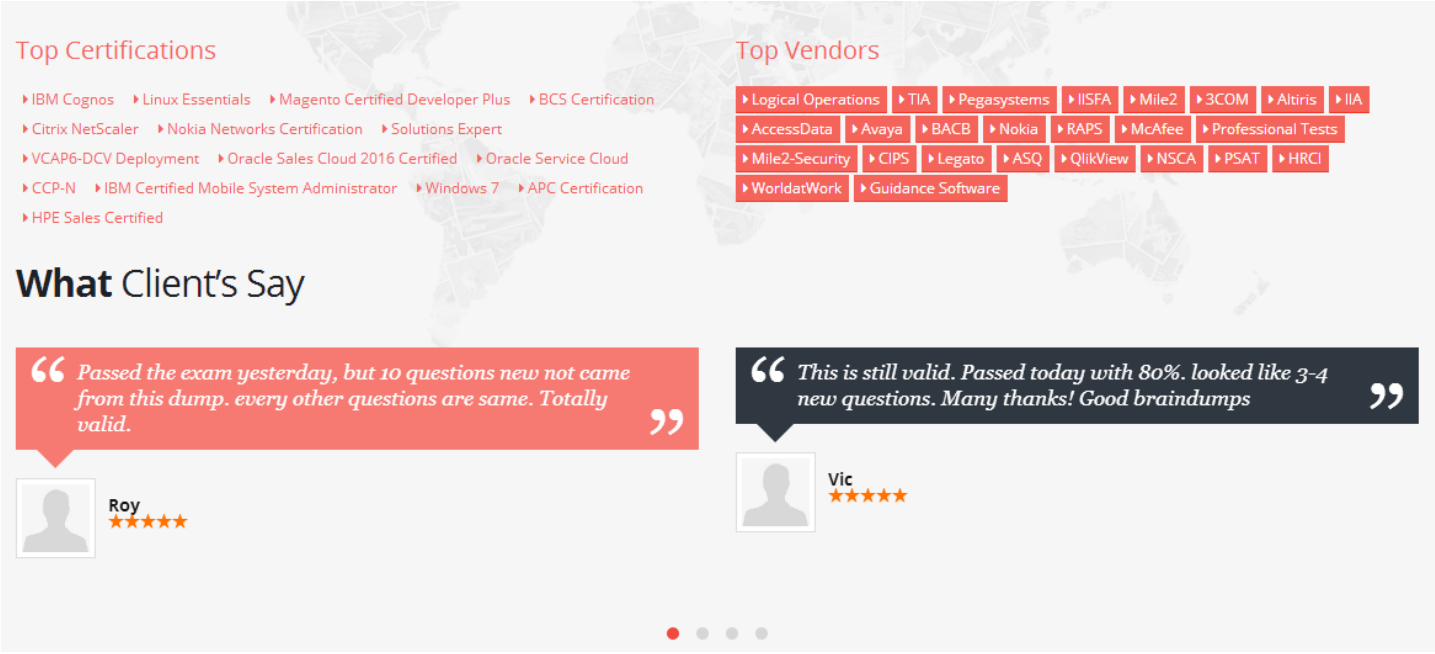
Lead2passExam



http://www.lead2passexam.com/

Available Exam Cram and Valid Dumps - Lead2Pass Exam

Exam : **CS0-002**

Title : CompTIA Cybersecurity Analyst (CySA+) Certification Exam

Vendor : CompTIA

Version : DEMO

NO.1 A Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software. Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?

A. EDR

B. Port security

C. NAC

D. Segmentation

Answer: A

Explanation:

EDR stands for endpoint detection and response, which is a type of security solution that monitors and protects all devices that are connected to a network, such as laptops and mobile phones. EDR can help to ensure that all devices are patched and running some sort of protection against malicious software by providing continuous visibility, threat detection, incident response, and remediation capabilities. EDR can also help to enforce security policies and compliance requirements across all devices .

NO.2 A security analyst is running a tool against an executable of an unknown source. The Input supplied by the tool to the executable program and the output from the executable are shown below:

Input supplied by tool	Output from executable
asdfnerlajnvjanjkdfnvkjanakjdv	asdfnerlajnvjanjkdfnvkjanakjdv
klrejfkalsdjfklasdjffjladsf892	klrejfkalsdjfklasdjffjladsf892
ADSFQEDVASDASDFASDF;ADSFASDWDF	command not found
qscTRGvcaDFcaDCasDC23rdcasdfAS	qscTRGvcaDFcaDCasDC23rdcasdfAS
lqkejfc934cjcjvsad:cmaoiwefasd	lqkejfc934cjcjvsad:cmaoiwefasd

Which of the following should the analyst report after viewing this Information?

A. The toot caused a buffer overflow in the executable's memory

B. Input can be crafted to trigger an Infection attack in the executable

C. The executable attempted to execute a malicious command

D. A dynamic library that is needed by the executable a missing

Answer: A

Explanation:

A buffer overflow is a type of attack that exploits a vulnerability in an application or program that does not properly check the size or boundaries of an input. A buffer overflow occurs when an attacker supplies more data than the buffer can hold, causing the excess data to overwrite adjacent memory locations. This can result in unpredictable behavior, such as crashes, errors, data corruption, or execution of malicious code2 The tool that the analyst ran against the executable supplied an input that was too long for the buffer allocated by the executable. This caused a buffer overflow in the executable's memory, as indicated by the error message "Segmentation fault (core dumped)".

NO.3 A security analyst reviews SIEM logs and discovers the following error event:

```
ERROR Event ID 4
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server
DBASVRR4$. The target name used was GC/PDC1DC.Domain57/Administrator. This
indicates that the target server failed to decrypt the ticket provided by
the client. Check if there are identically named server accounts in these
two domains, or use the fully qualified name to identify the server.
```

Which of the following environments does the analyst need to examine to continue troubleshooting the event?

A. Windows domain controller

B. SQL server

C. DNS server

D. WAF appliance

E. Proxy server

Answer: A

Explanation:

A Windows domain controller is a server that manages authentication and authorization for users and computers in a Windows domain. A Windows domain controller uses Active Directory Domain Services (AD DS) to store information about users, groups, computers, policies, and other objects in a domain. A Windows domain controller can generate event logs that record various activities and events related to security, system, application, etc. The event log shown in the question indicates that it was generated by a Windows domain controller with an IP address of 10.0.0.1 and a hostname of DC01.

NO.4 An analyst determines a security incident has occurred Which of the following is the most appropnate NEXT step in an incident response plan?

A. Consult the disaster recovery plan

B. Consult the malware analysis process

C. Consult the data classification process

D. Consult the communications plan

Answer: D

Explanation:

A communications plan is a document that outlines who should be notified and how during an incident response. It can also specify the roles and responsibilities of the incident response team members, the escalation procedures, and the communication channels. Consulting the communications plan is the most appropriate next step in an incident response plan after determining a security incident has occurred. Consulting the malware analysis process, the disaster recovery plan, or the data classification process may be relevant at later stages of the incident response, but not as the next step. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NO.5 During an Incident, it Is determined that a customer database containing email addresses, first names, and last names was exfiltrated. Which ot the following should the security analyst do NEXT?

A. Encrypt the database with available tools.

B. Email the customers to inform them of the breach.

C. Follow the incident communications process.

D. Consult with the legal department for regulatory impact.

Answer: C
Explanation:
An incident communications process is a set of procedures that defines how to communicate with internal and external stakeholders during and after an incident, such as customers, employees, management, regulators and media. An incident communications process can help to provide accurate, timely and consistent information about the incident, its impact and the actions taken to resolve it. An incident communications process can also help to maintain trust and reputation, comply with legal obligations and prevent misinformation or confusion3 .

NO.6 A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:

From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	sara.ellis@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	jason.lee@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

Which of the following technologies would MOST likely be used to prevent this phishing attempt?
A. DNSSEC
B. S/IMAP
C. STP
D. DMARC
Answer: D
Explanation:
DMARC stands for Domain-based Message Authentication, Reporting and Conformance. It is an email authentication protocol that helps prevent spoofing and phishing attacks by verifying that the sender's domain matches the domain in the email header. DMARC also provides a way for domain owners to specify how receivers should handle unauthenticated messages from their domain1

NO.7 A digital forensics investigator works from duplicate images to preserve the integrity of the original evidence. Which of the following types of media are most volatile and should be preserved? (Select two).
A. Packet decoding
B. SSD storage
C. Memory cache

D. Registry file
E. Temporary filesystems
F. Swap volume
Answer: C,F
Explanation:
Memory cache and swap volume are types of media that are most volatile and should be preserved during a digital forensics investigation. Volatile media are those that store data temporarily and lose their contents when the power is turned off or interrupted. Memory cache is a small and fast memory that stores frequently used data or instructions for faster access by the processor. Swap volume is a part of the hard disk that is used as an extension of the memory when the memory is full or low .

NO.8 An organization has specific technical nsk mitigation configurations that must be implemented before a new server can be approved for production Several critical servers were recently deployed with the antivirus missing unnecessary ports disabled and insufficient password complexity Which of the following should the analyst recommend to prevent a recurrence of this risk exposure?
A. Perform automated security controls testing of expected configurations pnor to production
B. Perform an Nmap scan on all devices before they are released to production
C. Perform password-cracking attempts on all devices going into production
D. Perform antivirus scans on all devices before they are approved for production
Answer: A
Explanation:
Automated security controls testing is a method that uses tools or scripts to verify that the security controls of a system or device are configured correctly and comply with the organization's policies and standards. Performing automated security controls testing of expected configurations prior to production would help prevent a recurrence of the risk exposure caused by missing antivirus, unnecessary ports enabled, and insufficient password complexity. Performing password-cracking attempts, Nmap scans, or antivirus scans on all devices before they are released to production are other methods that can help detect some security issues, but they are not as comprehensive or efficient as automated security controls testing. Reference:
https://www.nist.gov/system/files/documents/2017/04/28/sp800-115.pdf

NO.9 A risk assessment concludes that the perimeter network has the highest potential for compromise by an attacker, and it is labeled as a critical risk environment. Which of the following is a valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques?
A. A control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment
B. A control that demonstrates that all systems authenticate using the approved authentication method
C. A control that demonstrates that the network security policy is reviewed and updated yearly
D. A control that demonstrates that access to a system is only allowed by using SSH
Answer: A
Explanation:

A valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques is a control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment. This control can help ensure that the firewall rules are configured correctly and securely, and that they do not allow unnecessary or unauthorized access to the perimeter network. The other options are not compensating controls or do not address the risk of active reconnaissance. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/compensating-controls

NO.10 Which of the following is the greatest security concern regarding ICS?

A. The systems are oftentimes air gapped, leading to fileless malware attacks.

B. The systems are configured for automatic updates, leading to device failure.

C. Issues on the systems cannot be reversed without rebuilding the systems.

D. The involved systems are generally hard to identify.

Answer: C

Explanation:

Industrial control systems (ICS) are systems that monitor and control physical processes, such as power generation, water treatment, manufacturing, and transportation. ICS are often critical for public safety and national security, and therefore a prime target for cyberattacks. One of the greatest security concerns regarding ICS is that issues on the systems cannot be reversed without rebuilding the systems. This means that any damage or disruption caused by an attack can have long-lasting and catastrophic consequences for the physical infrastructure and human lives. The other options are not true or not specific to ICS. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 13; https://www.us-cert.gov/ics/What-are-Industrial-Control-Systems

NO.11 A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

A. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud.

B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.

C. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.

D. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.

Answer: A

Explanation:

"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services." https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solution/ CASB stands for Cloud Access Security Broker, which is a solution that monitors and controls the access and usage of cloud services by an organization's users. DLP stands for Data Loss Prevention, which is a solution that prevents unauthorized disclosure or leakage of sensitive data. Utilizing the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud is the best recommendation for a security

analyst to mitigate the threat of financial data leakage into the cloud, because it would prevent users from uploading or transferring financial information to cloud services that are not authorized or secure. Utilizing the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises, not utilizing the CASB solution for this purpose but adding DLP on premises for data in motion or data at rest are other possible recommendations, but they are not as effective or relevant as utilizing the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud. Reference: https://www.csoonline.com/article/3200344/what-is-a-casb-and-why-do-you-need-one.html

NO.12 Wncn ol the following provides an automated approach 10 checking a system configuration?

A. SOAR

B. SCAP

C. Scripting

D. OVAL

E. CI/CD

Answer: B

Explanation:

SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications that allows automated configuration and vulnerability management of systems. SCAP provides an automated approach to checking a system configuration by using standardized expressions and formats to evaluate the system's compliance with predefined policies or benchmarks. CI/CD, OVAL, scripting, or SOAR are other terms related to automation or security, but they do not provide an automated approach to checking a system configuration. Reference: https://csrc.nist.gov/projects/security-content-automation-protocol

NO.13 An organization has the following risk mitigation policy:

Risks with a probability of 95% or greater will be addressed before all others regardless of the impact.

All other prioritization will be based on risk value.

The organization has identified the following risks:

Risk	Probability	Impact
A	95%	$110,000
B	99%	$100,000
C	50%	$120,000
D	90%	$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. D, A, C, B

B. A, B, D, C

C. A, B, C, D

D. D, A, B, C

Answer: A

Explanation:

According to the risk mitigation policy, risks with a probability of 95% or greater will be addressed first, regardless of the impact. Therefore, risk D is the highest priority, as it has a probability of 95%

and an impact of $100,000. The next priority is risk A, which has a probability of 90% and an impact of $200,000. The remaining risks will be prioritized based on their risk value, which is calculated by multiplying the probability and the impact. Risk C has a risk value of $40,000 (80% x $50,000), while risk B has a risk value of $30,000 (60% x $50,000). Therefore, risk C is higher priority than risk B.

NO.14 An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised Which of the following should Ihe analyst do FIRST?

A. Isolate the container from production using a predefined policy template

B. Contact law enforcement to report the incident

C. Perform threat hunting in other areas of the cloud infrastructure

D. Perform a root cause analysis on the container and the service logs

Answer: A

Explanation:

The analyst should isolate the container from production using a predefined policy template first. Isolating the container is a containment measure that can help prevent the spread of the compromise to other containers or systems in the cloud infrastructure. Containment is an important step in the incident response process, as it can limit the impact and damage of an incident. Using a predefined policy template can help automate and standardize the isolation process, ensuring that it is done quickly and consistently1.

NO.15 A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?

A. Software assurance

B. Change management

C. Anti-tamper

D. CI/CD

Answer: C

Explanation:

Anti-tamper is a process that protects a system or device from unauthorized changes or modifications. It can also log and report any attempts to alter the system or device. The company is using anti-tamper to ensure the appliance is not altered from its original configured state. CI/CD, software assurance, and change management are not processes that specifically deal with unauthorized changes. Reference: https://www.acq.osd.mil/se/briefs/16943-DoD-AT-Overview-Brief.pdf

NO.16 An analyst reviews the most recent vulnerability management report and notices a firewall with 99.98% required uptime is reporting different firmware versions on scans than were reported in previous scans. The vendor released new firewall firmware a few months ago. Which of the following will the analyst most likely do next given the requirements?

A. Request to route traffic through a secondary firewall

B. Perform a credentialed scan

C. Request an exception to the uptime policy.

D. Check for change tickets.

Answer: D

Explanation:

The analyst should check for change tickets as the next step, given that the firewall is reporting different firmware versions on scans than were reported in previous scans. Change tickets are records of any authorized changes made to a system or a network, such as updating firmware, installing patches, or modifying configurations. Checking for change tickets can help verify if the firmware change was intentional and approved, or if it was unauthorized or malicious.

NO.17 Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?

A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from nonauthorized access.

B. Build the chain-of-custody document, noting the media model, serial number, size, vendor, date, and time of acquisition.

C. Execute the command #dd if-/dev/sda of=/dev/sdc bs=512 to clone the evidence data to external media to prevent any further change.

D. Perform a disk sanitization using the command #dd if=/dev/zero of=/dev/sdc bs=1M over the media that will receive a copy of the collected data.

Answer: B

Explanation:

Building the chain-of-custody document is the procedure that must be completed first for this type of evidence acquisition. The chain-of-custody document is a record that tracks the handling and custody of digital evidence from the time it is collected until it is presented in court. The chain-of-custody document should include information such as the media model, serial number, size, vendor, date, and time of acquisition, as well as the names and signatures of the persons who handled, transferred, or examined the evidence. The chain-of-custody document helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1.

NO.18 A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

A. detection and prevention capabilities to improve.

B. the time spent by analysts on each of the incidents.

C. possible evidence that is missing during forensic analysis.

D. which analysts require more training.

E. which systems were exploited more frequently.

Answer: A

Explanation:

A Diamond Model analysis of an incident is a framework that identifies the four essential features of an attack: adversary, capability, infrastructure, and victim1 By analyzing these features and their relationships, a security analyst can gain insights into the attack's objectives, methods, sources, and

targets. A potential benefit of this activity is that it can identify detection and prevention capabilities to improve, such as gaps in security controls, indicators of compromise, or mitigation strategies2

NO.19 An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

A. SCADA

B. Modbus

C. CAN bus

D. IoT

Answer: C

Explanation:

The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.

CAN bus stands for Controller Area Network bus, which is a communication protocol that allows different devices and components in a vehicle to communicate and exchange data. The vulnerability within the new fleet of vehicles is most likely targeting the CAN bus, because it could allow an attacker to manipulate or disrupt the operation of the vehicle. SCADA, Modbus, and IoT are other terms related to communication protocols or systems, but they are not specific to vehicles.

Reference: https://www.csoonline.com/article/3218104/what-is-a-can-bus-and-how-can-it-be-hacked.html

NO.20 A security team has begun updating the risk management plan, incident response plan, and system security plan to ensure compliance with security review guidelines. Which of the following can be executed by internal managers to simulate and validate the proposed changes?

A. Peer review

B. Control assessment

C. Internal management review

D. Tabletop exercise

Answer: D

Explanation:

According to the CompTIA CySA+ Certification Exam (CS0-002) study guide, a tabletop exercise can be executed by internal managers to simulate and validate changes to the risk management plan, incident response plan, and system security plan. In a tabletop exercise, participants discuss and work through a simulated scenario, usually in a classroom or conference room setting, to evaluate their readiness and understanding of the proposed changes. This type of exercise can help to identify any potential issues or gaps in the proposed changes and can provide valuable insights for refining and improving the plans.

NO.21 An employee contacts the SOC to report a high-severity bug that was identified in a new, internally developed web application, which went live in production last week. The SOC staff did not receive contact details or escalation procedures to follow. Which of the following stages of the SDLC process was overlooked?

A. Implementation and integration
B. Input validation
C. Planning
D. Operations and maintenance
Answer: C
Explanation:
The planning stage of the SDLC process is when the project scope, objectives, requirements, risks, and deliverables are defined and agreed upon by all stakeholders. This stage also involves creating a project plan that outlines the tasks, resources, schedule, budget, and communication channels for the project.
The planning stage is crucial for ensuring that the project is aligned with the business goals and customer needs, and that the project team has a clear vision and direction for the development process. By overlooking this stage, the SOC staff did not receive contact details or escalation procedures to follow in case of a high-severity bug, which could have serious consequences for the security and functionality of the web application.

NO.22 A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?
A. Static analysis
B. Packet inspection
C. Web-application vulnerability scan
D. Penetration test
Answer: A
Explanation:
Static analysis is a method of analyzing software code without executing it, by using tools or techniques that check for syntax errors, logic errors, vulnerabilities, coding standards, and other quality issues. Static analysis can help software developers to correct the error-handling capabilities of an application before pushing it to production, as it can detect potential errors and bugs at an early stage of development. A web-application vulnerability scan (A) is a method of testing web applications for security flaws by simulating attacks and analyzing responses. It can be useful for finding vulnerabilities in web applications, but not for validating the error-handling capabilities of an application. A packet inspection is a method of monitoring network traffic by examining the data packets that are sent and received over a network. It can be useful for detecting malicious or unauthorized activity on a network, but not for validating the error-handling capabilities of an application. A penetration test (D) is a method of evaluating the security of a system or network by simulating real-world attacks and exploiting vulnerabilities. It can be useful for assessing the overall security posture of a system or network, but not for validating the error-handling capabilities of an application.

NO.23 A company notices unknown devices connecting to the internal network and would like to implement a solution to block all non-corporate managed machines. Which of the following solutions would be best to accomplish this goal?
A. WPA2 for W1F1 networks
B. RADIUS with challenge/response

C. NAC with 802.1X implementation
D. Extensible Authentication Protocol
Answer: C
Explanation:
This solution is the best to accomplish the goal of blocking all non-corporate managed machines from connecting to the internal network. NAC stands for network access control, which is a method of enforcing policies and rules on network devices based on their identity, role, location, and other attributes. 802.1X is a standard for port-based network access control, which authenticates devices before granting them access to a network port or wireless access point.

NO.24 During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the next step the analyst should take?
A. Only allow binaries on the approve list to execute.
B. Use file integrity monitoring to validate the digital signature
C. Run an antivirus against the binaries to check for malware.
D. Validate the binaries' hashes from a trusted source.
Answer: D
Explanation:
Validating the binaries' hashes from a trusted source is the next step the analyst should take after discovering some binaries that are exhibiting abnormal behaviors and finding unexpected content in their strings. A hash is a fixed-length value that uniquely represents the contents of a file or message. By comparing the hashes of the binaries on the compromised machine with the hashes of the original or legitimate binaries from a trusted source, such as the software vendor or repository, the analyst can determine whether the binaries have been modified or replaced by malicious code. If the hashes do not match, it indicates that the binaries have been tampered with and may contain malware.

NO.25 A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst should take in this situation?
A. Develop a new signature to block the indicators of compromise.
B. Develop a new signature to alert on the indicators of compromise.
C. Develop a query to search for the indicators of compromise.
D. Develop a dashboard to track the indicators of compromise.
Answer: C
Explanation:
Developing a query to search for the indicators of compromise is the first action the analyst should take in this situation. Indicators of compromise (IOCs) are pieces of information that suggest a system or network has been compromised by an attacker. IOCs can include IP addresses, domain names, file hashes, URLs, or other artifacts that are associated with malicious activity. Developing a query to search for IOCs can help to identify any potential incidents or threats in the environment and initiate further investigation or response .

NO.26 An organization has the following policy statements:
* All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.

* AM network activity will be logged and monitored.
* Confidential data will be tagged and tracked
* Confidential data must never be transmitted in an unencrypted form.
* Confidential data must never be stored on an unencrypted mobile device.

Which of the following is the organization enforcing?

A. Data management, policy

B. Encryption policy

C. Acceptable use policy

D. Data privacy policy

Answer: D

Explanation:

Data privacy policy is the organization's policy that defines how it collects, uses, stores, and shares personal data of its customers, employees, or other stakeholders. Data privacy policy also covers how the organization complies with relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). The policy statements listed in the question are examples of data privacy policy provisions that aim to protect the confidentiality, integrity, and availability of personal data.