



Vendor: CompTIA

Exam Code: CAS-005

Exam Name: CompTIA SecurityX Certification Exam

Version: DEMO

QUESTION 1

A company hosts a platform-as-a-service solution with a web-based front end, through which customers interact with data sets. A security administrator needs to deploy controls to prevent application-focused attacks. Which of the following most directly supports the administrator's objective?

- A. improving security dashboard visualization on SIEM
- B. Rotating API access and authorization keys every two months
- C. Implementing application load balancing and cross-region availability
- D. Creating WAF policies for relevant programming languages

Answer: D

Explanation:

A Web Application Firewall (WAF) provides specific protection against application-focused attacks (such as SQL injection, cross-site scripting, etc.) by analyzing and filtering HTTP requests. Creating WAF policies tailored to the application's programming languages will directly support the security administrator's objective of preventing application-specific attacks.

QUESTION 2

A security analyst is reviewing the following log:

Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

Which of the following possible events should the security analyst investigate further?

- A. A macro that was prevented from running
- B. A text file containing passwords that were leaked
- C. A malicious file that was run in this environment
- D. A PDF that exposed sensitive information improperly

Answer: C

Explanation:

The **dll file** with a **10 MB size** is allowed to be executed in the **c:\temp** directory. Since **DLL (Dynamic Link Library) files** are often associated with executable code and can be used for malicious purposes, this **should be investigated further**. The fact that it is allowed to run raises suspicion, and the location of the file (**temp directory**) is commonly used by malware for executing unauthorized processes.

QUESTION 3

A systems administrator wants to use existing resources to automate reporting from disparate security appliances that do not currently communicate. Which of the following is the best way to meet this objective?

- A. Configuring an API Integration to aggregate the different data sets
- B. Combining back-end application storage into a single, relational database
- C. Purchasing and deploying commercial off the shelf aggregation software
- D. Migrating application usage logs to on-premises storage

Answer: A

Explanation:

Configuring an API integration is the best way to automate reporting from disparate security appliances. APIs allow for the integration of data from different sources, enabling automated aggregation and reporting without the need to invest in new tools or migrate data manually. This solution leverages existing resources and allows the systems to communicate effectively.

QUESTION 4

A developer needs to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module. Which of the following is the most appropriate technique?

- A. Key splitting
- B. Key escrow
- C. Key rotation
- D. Key encryption
- E. Key stretching

Answer: E

Explanation:

Key stretching enhances the security of stored passwords by applying computationally intensive algorithms (e.g., bcrypt, PBKDF2) to make brute-force attacks more difficult, without replacing the underlying crypto-module.

QUESTION 5

A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	190ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

Which of the following should the company implement to best resolve the issue?

- A. IDS
- B. CDN
- C. WAF
- D. NAC

Answer: B

Explanation:

To improve global response times (e.g. India/Australia seeing multi-second load times) and offload traffic from your origin web servers, deploying a Content Delivery Network is the most effective solution.

QUESTION 6

A security officer received several complaints from users about excessive MFA push notifications at night. The security team investigates and suspects malicious activities regarding user account authentication. Which of the following is the best way for the security officer to restrict MFA notifications?

- A. Provisioning FIDO2 devices
- B. Deploying a text message based on MFA
- C. Enabling OTP via email
- D. Configuring prompt-driven MFA

Answer: D

Explanation:

Prompt-driven MFA means that MFA prompts are triggered only when there is suspicious activity or a specific need for authentication, rather than being sent regularly. This approach would reduce the excessive notifications while still ensuring security, addressing the user's complaints effectively.

QUESTION 7

A security professional is investigating a trend in vulnerability findings for newly deployed cloud systems. Given the following output:

Date	IP address	System name	Finding	Criticality rating
10/13/2023	10.123.34.98	System1	OpenSSL version 1.01	Medium
10/13/2023	10.3.114.72	System6	OpenSSL version 1.01	Medium
10/13/2023	10.12.134.45	System12	Java 11 runtime environment found	Medium
10/13/2023	10.68.65.11	System36	OpenSSL version 1.01	Medium
10/13/2023	10.23.74.9	System37	Java 11 runtime environment found	Medium
10/13/2023	10.13.124.3	System45	OpenSSL version 1.01	Medium

Which of the following actions would address the root cause of this issue?

- A. Automating the patching system to update base Images
- B. Recompiling the affected programs with the most current patches
- C. Disabling unused/unneeded ports on all servers
- D. Deploying a WAF with virtual patching upstream of the affected systems

Answer: A

Explanation:

The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.

Automating the patching system to update base images: Automating the patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.

QUESTION 8

Which of the following best describes the challenges associated with widespread adoption of homomorphic encryption techniques?

- A. Incomplete mathematical primitives
- B. No use cases to drive adoption
- C. Quantum computers not yet capable
- D. Insufficient coprocessor support

Answer: D

Explanation:

Fully homomorphic encryption schemes impose massive computational overhead, and without specialized hardware accelerators or co-processors to offload the heavy integer and polynomial arithmetic, performance remains prohibitive for broad deployment.

QUESTION 9

After some employees are caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

- A. Improve firewall rules to avoid access to those platforms
- B. Implement a cloud access security broker
- C. Create SIEM rules to raise alerts for access to those platforms
- D. Deploy an internet proxy that filters certain domains

Answer: B

Explanation:

A CASB provides visibility and control over sanctioned and unsanctioned cloud services. By sitting between users and cloud providers, it can block or quarantine uploads to personal storage accounts in real time, preventing data exfiltration at the cloud access layer rather than relying solely on detection after the fact.

QUESTION 10

An organization wants to create a threat model to identify vulnerabilities in its infrastructure. Which of the following, should be prioritized first?

- A. External-facing Infrastructure with known exploited vulnerabilities
- B. Internal infrastructure with high-severity and Known exploited vulnerabilities
- C. External facing Infrastructure with a low risk score and no known exploited vulnerabilities
- D. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource

Answer: A

Explanation:

External-facing infrastructure with known exploited vulnerabilities poses the highest immediate risk, as it is directly accessible to attackers and already associated with active threats. This should be the **top priority** in any threat modeling effort.

QUESTION 11

A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

- A. Ability to obtain components during wartime
- B. Fragility and other availability attacks
- C. Physical Implants and tampering
- D. Non-conformance to accepted manufacturing standards

Answer: C

Explanation:

The allow list for specific countries of origin as a risk mitigation indicates that the central bank is focused on preventing physical implants and tampering in hardware. This is a form of supply chain attack where malicious actors may insert malicious hardware components into devices, leading to potential compromises in security. By restricting the countries of origin, the bank is likely aiming to prevent such vulnerabilities.

QUESTION 12

A company's security team is notified about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best allows the company to identify third-party vulnerabilities in the future?

- A. Using IaC to include the newest dependencies
- B. Creating a bug bounty program
- C. Implementing a continuous security assessment program
- D. Integrating a SAST tool as part of the pipeline

Answer: D

Explanation:

Software Composition Analysis (SCA) tools scan for known vulnerabilities in third-party libraries and dependencies. Integrating an SCA tool into the development pipeline enables automatic identification of such vulnerabilities early in the development lifecycle.

QUESTION 13

While reviewing recent incident reports a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter. Which of the following best describes this type of correlation?

- A. Spear-phishing campaign
- B. Threat modeling
- C. Red team assessment
- D. Attack pattern analysis

Answer: D

Explanation:

Attack pattern analysis involves identifying recurring techniques or behaviors used by threat actors - such as impersonating a recruiter - to correlate incidents and uncover broader campaigns. The security officer is recognizing a consistent method across multiple reports, which defines this as attack pattern analysis.

QUESTION 14

During a security assessment using an EDR solution, a security engineer generates the following report about the assets in the system:

Device	Type	EDR status
LN002	Linux SE	Enabled (unmanaged)
0WIN23	Windows 7	Enabled
0WIN29	Windows 10	Enabled (bypass)
MAC005	Mac OS	Enabled

After five days, the EDR console reports a blocked infection on the host 0WIN23 by a remote access Trojan. Which of the following most likely enabled the attempted infection?

- A. 0W1N23 uses a legacy version of Windows that is not supported by the EDR
- B. LN002 was not supported by the EDR solution and propagates the RAT
- C. The EDR has an unknown vulnerability that was exploited by the attacker
- D. 0W1N29 spreads the malware through other hosts in the network

Answer: D

Explanation:

The key clue is the "Enabled (bypass)" status on 0WIN29. That means the EDR agent was running but being bypassed, effectively allowing malicious code to execute unchecked. An attacker could exploit that bypass to install the RAT on 0WIN29, and then attempt lateral movement to 0WIN23. 0WIN23's EDR then detected and blocked the inbound infection, but the initial foothold was enabled by the vulnerability in the 0WIN29 deployment.

QUESTION 15

Emails that the marketing department is sending to customers are going to the customers' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated. Which of the following should the security team update in order to fix this issue? (Choose three.)

- A. DMARC
- B. SPF
- C. DKIM
- D. DNSSEC
- E. SASC
- F. SAN
- G. SOA

H. MX

Answer: ABC

Explanation:

To prevent emails from being marked as spam, several DNS records related to email authentication need to be properly configured and updated when there are changes to the email server's certificates:

DMARC (Domain-based Message Authentication, Reporting & Conformance): DMARC records help email servers determine how to handle messages that fail SPF or DKIM checks, improving email deliverability and reducing the likelihood of emails being marked as spam.

SPF (Sender Policy Framework): SPF records specify which mail servers are authorized to send email on behalf of your domain. Updating the SPF record ensures that the new email server is recognized as an authorized sender.

QUESTION 16

Users are experiencing a variety of issues when trying to access corporate resources. Examples include:

- Connectivity issues between local computers and file servers within branch offices
- Inability to download corporate applications on mobile endpoints while working remotely
- Certificate errors when accessing internal web applications

Which of the following actions are the most relevant when troubleshooting the reported issues? (Choose two.)

- A. Review VPN throughput
- B. Check IPS rules
- C. Restore static content on lite CDN.
- D. Enable secure authentication using NAC
- E. Implement advanced WAF rules.
- F. Validate MDM asset compliance

Answer: AF

Explanation:

Review VPN throughput helps identify remote access issues, such as slow or failed application downloads.

Validate MDM asset compliance ensures mobile devices meet security requirements, which can affect access to apps and certificates.

QUESTION 17

A software engineer is creating a CI/CD pipeline to support the development of a web application. The DevSecOps team is required to identify syntax errors. Which of the following is the most relevant to the DevSecOps team's task?

- A. Static application security testing
- B. Software composition analysis
- C. Runtime application self-protection
- D. Web application vulnerability scanning

Answer: A

Explanation:

Static Application Security Testing (SAST) analyzes source code, bytecode, or binaries without executing the program, making it highly relevant for identifying syntax errors during the development process. This approach is ideal for the DevSecOps team's task of identifying errors before deployment.

QUESTION 18

An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry. Which of the following should the security analyst use to perform threat modeling?

- A. ATT&CK
- B. OWASP
- C. CAPEC
- D. STRIDE

Answer: A

Explanation:

The MITRE ATT&CK framework provides a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs) that can be used for threat modeling. It helps identify gaps in detection capabilities by mapping real-world attack behaviors specific to the industry, making it the most relevant for the task.

QUESTION 19

A security analyst detected unusual network traffic related to program updating processes. The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing valid binaries but with different hashes. Which of the following solutions would most likely prevent this situation from reoccurring?

- A. Improving patching processes
- B. Implementing digital signature
- C. Performing manual updates via USB ports
- D. Allowing only dies from internal sources

Answer: B

Explanation:

Digital signatures ensure the integrity and authenticity of binaries. If binaries are tampered with or replaced by malicious versions, signature verification will fail. This would prevent malicious files with the same name but different hashes from executing, thereby mitigating such attacks.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14