IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **CAS-005**

Title : CompTIA SecurityX Certification Exam

Version : DEMO

1.A security analyst discovered requests associated with IP addresses known for born legitimate 3nd bot-related traffic.
Which of the following should the analyst use to determine whether the requests are malicious?
A. User-agent string
B. Byte length of the request
C. Web application headers
D. HTML encoding field
Answer: A
Explanation:
The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.
Why Use User-Agent String?
Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.
Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.
Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.
Other options provide useful information but may not be as effective for initial determination of the nature of the request:
B. Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.
C. Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.
D. HTML encoding field: This is not typically used for identifying the nature of the request.
References:
CompTIA SecurityX Study Guide
"User-Agent Analysis for Security," OWASP
NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

2.A user reports application access issues to the help desk.
The help desk reviews the logs for the user

Time	Internal IP	Public IP	IP geolocation	Application	Action
8:47 p.m.	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Human resources system	Allow
8:49 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 p.m.	192.168.1.5	104.18.16.29	Toronto	Human resources system	Deny

Which of the following is most likely The reason for the issue?
A. The user inadvertently tripped the impossible travel security rule in the SSO system.
B. A threat actor has compromised the user's account and attempted to lop, m
C. The user is not allowed to access the human resources system outside of business hours
D. The user did not attempt to connect from an approved subnet
Answer: A

Explanation:
Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.
Analysis of Logs:
At 8:47 p.m., the user accessed a VPN from Toronto.
At 8:48 p.m., the user accessed email from Los Angeles.
At 8:48 p.m., the user accessed the human resources system from Los Angeles.
At 8:49 p.m., the user accessed email again from Los Angeles.
At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.
These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-63B, "Digital Identity Guidelines"
"Impossible Travel Detection," Microsoft Documentation

3.A company wants to invest in research capabilities with the goal to operationalize the research output. Which of the following is the best option for a security architect to recommend?
A. Dark web monitoring
B. Threat intelligence platform
C. Honeypots
D. Continuous adversary emulation
Answer: B
Explanation:
Investing in a threat intelligence platform is the best option for a company looking to operationalize research output. A threat intelligence platform helps in collecting, processing, and analyzing threat data to provide actionable insights. These platforms integrate data from various sources, including dark web monitoring, honeypots, and other security tools, to offer a comprehensive view of the threat landscape.
Why a Threat Intelligence Platform?
Data Integration: It consolidates data from multiple sources, including dark web monitoring and honeypots, making it easier to analyze and derive actionable insights.
Actionable Insights: Provides real-time alerts and reports on potential threats, helping the organization take proactive measures.
Operational Efficiency: Streamlines the process of threat detection and response, allowing the security team to focus on critical issues.
Research and Development: Facilitates the operationalization of research output by providing a platform for continuous monitoring and analysis of emerging threats.
Other options, while valuable, do not offer the same level of integration and operationalization capabilities:
A. Dark web monitoring: Useful for specific threat intelligence but lacks comprehensive

operationalization.
C. Honeypots: Effective for detecting and analyzing specific attack vectors but not for broader threat intelligence.
D. Continuous adversary emulation: Important for testing defenses but not for integrating and operationalizing threat intelligence.
References:
CompTIA SecurityX Study Guide
"Threat Intelligence Platforms," Gartner Research
NIST Special Publication 800-150, "Guide to Cyber Threat Information Sharing"

4.A security configure is building a solution to disable weak CBC configuration for remote access connections lo Linux systems.
Which of the following should the security engineer modify?
A. The /etc/openssl.conf file, updating the virtual site parameter
B. The /etc/nsswith.conf file, updating the name server
C. The /etc/hosts file, updating the IP parameter
D. The /etc/etc/sshd, configure file updating the ciphers
Answer: D
Explanation:
The sshd_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed.
By editing the /etc/ssh/sshd_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the SSH server does not use insecure encryption methods.
References:
CompTIA Security+ Study Guide
OpenSSH manual pages (man sshd_config)
CIS Benchmarks for Linux

5.A software company deployed a new application based on its internal code repository Several customers are reporting anti-malware alerts on workstations used to test the application.
Which of the following is the most likely cause of the alerts?
A. Misconfigured code commit
B. Unsecure bundled libraries
C. Invalid code signing certificate
D. Data leakage
Answer: B
Explanation:
The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third-party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.

Why Unsecure Bundled Libraries?
Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.
Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.
Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.
Other options, while relevant, are less likely to cause widespread anti-malware alerts:
A. Misconfigured code commit: Could lead to issues but less likely to trigger anti-malware alerts.
C. Invalid code signing certificate: Would lead to trust issues but not typically anti-malware alerts.
D. Data leakage: Relevant for privacy concerns but not directly related to anti-malware alerts.
References:
CompTIA SecurityX Study Guide
"Securing Open Source Libraries," OWASP
"Managing Third-Party Software Security Risks," Gartner Research