

- A. MOU
- B. MTTR
- C. SLA
- D. NDA

Correct Answer: C

Explanation:

Service level agreement (SLA). An SLA is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.

QUESTION 115

A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, "Special privileges assigned to new login." Several of these messages did not have a valid logon associated with the user before these privileges were assigned. Which of the following attacks is MOST likely being detected?

- A. Pass-the-hash
- B. Buffer overflow
- C. Cross-site scripting
- D. Session replay

Correct Answer: A

Explanation:

<https://www.beyondtrust.com/resources/glossary/pass-the-hash-ptb-attack>

QUESTION 116

A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?

- A. Checksums
- B. Watermarks
- C. Oder of volatility
- D. A log analysis
- E. A right-to-audit clause

Correct Answer: D

Explanation:

<https://www.sumologic.com/glossary/log-analysis/>

"While companies can operate private clouds, forensics in a public cloud are complicated by the right to audit permitted to you by your service level agreement (SLA) with the cloud provider."

QUESTION 117

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

- A. An incident response plan
- B. A communications plan
- C. A disaster recovery plan
- D. A business continuity plan

Correct Answer: D

Explanation:

Business continuity may be defined as "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident", [1] and business continuity planning [2][3] (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company. [4] In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery. [5] Business continuity is the intended outcome of proper execution of both business continuity planning and disaster recovery.

QUESTION 118

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data.

Correct Answer: B

QUESTION 119

The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

- A. Updating the playbooks with better decision points
- B. Dividing the network into trusted and untrusted zones
- C. Providing additional end-user training on acceptable use
- D. Implementing manual quarantining of infected hosts

Correct Answer: A

QUESTION 120

A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text()='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
...
```

Which of the following can the security analyst conclude?

- A. A replay attack is being conducted against the application.
- B. An injection attack is being conducted against a user authentication system.
- C. A service account password may have been changed, resulting in continuous failed logins within the application.
- D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Correct Answer: C

QUESTION 121

A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

- A. IPSec
- B. Always On
- C. Split tunneling
- D. L2TP

Correct Answer: B

QUESTION 122

A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create consultant accounts for each region, each configured with push MFA notifications.
- B. Create one global administrator account and enforce Kerberos authentication
- C. Create different accounts for each region. limit their logon times, and alert on risky logins
- D. Create a guest account for each region. remember the last ten passwords, and block password reuse

Correct Answer: C

Explanation:

<https://www.crowdstrike.com/blog/service-accounts-performing-interactive-logins/>

QUESTION 123

A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

Correct Answer: C

Explanation:

A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies

[JK0-022 Exam Dumps JK0-022 PDF Dumps JK0-022 VCE Dumps JK0-022 Q&As](#)

<https://www.ensurepass.com/JK0-022.html>

QUESTION 124

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

- A. `hping3 -s comptia.org -p 80`
- B. `nc -l -v comptia.org -p 80`
- C. `nmap comptia.org -p 80 -sV`
- D. `nslookup -port=80 comptia.org`

Correct Answer: C

Explanation:

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

QUESTION 125

An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

- A. Incident response
- B. Communications
- C. Disaster recovery
- D. Data retention

Correct Answer: C

QUESTION 126

A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

- A. A packet capture
- B. A user behavior analysis
- C. Threat hunting
- D. Credentialed vulnerability scanning

Correct Answer: C

Explanation:

<https://www.comptia.org/blog/your-next-move-threat-hunter#:~:text=Threat%20hunters%20are%20IT%20professionals%20who%20proactively%20find,that%20might%20evade%20the%20security%20operations%20center%20%28SOC%29.>

QUESTION 127

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

Correct Answer: C

Explanation:

Separation of duties - is a means of establishing checks and balances against the possibility that critical system or procedures can be compromised by insider threats. Duties and responsibilities should be divided among individuals to prevent ethical conflicts or abuse of powers.

QUESTION 128

The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

- A. Limit the use of third-party libraries.
- B. Prevent data exposure queries.
- C. Obfuscate the source code.
- D. Submit the application to QA before releasing it.

Correct Answer: D

QUESTION 129

A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

- A. Open the document on an air-gapped network
- B. View the document's metadata for origin clues
- C. Search for matching file hashes on malware websites
- D. Detonate the document in an analysis sandbox

Correct Answer: D

QUESTION 130

An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

- A. Date of birth
- B. Fingerprints
- C. PIN
- D. TPM

Correct Answer: B

QUESTION 131

Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log in to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)