Correct Answer: D

QUESTION 292
An organization is having difficulty correlating events from its individual AV. EDR. DLP. SWG. WAF. MOM. HIPS, and CASB systems. Which of the following is the BEST way to improve the situation?

A. Remove expensive systems that generate few alerts.
B. Modify the systems to alert only on critical issues.
C. Utilize a SIEM to centralize togs and dashboards.
D. Implement a new syslog/NetFlow appliance.

Correct Answer: C

QUESTION 293
A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted. Which of the following resiliency techniques was applied to the network to prevent this attack?

A. NIC Teaming
B. Port mirroring
C. Defense in depth
D. High availability
E. Geographic dispersal

Correct Answer: C

QUESTION 294
A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of the following should the manager request to complete the assessment?

A. A service-level agreement
B. A business partnership agreement
C. A SOC 2 Type 2 report
D. A memorandum of understanding

Correct Answer: A

QUESTION 295
During an incident, an EDR system detects an increase in the number of encrypted outbound connections from multiple hosts. A firewall is also reporting an increase in outbound connections that use random high ports. An analyst plans to review the correlated logs to find the source of the incident. Which of the following tools will BEST assist the analyst?

A. A vulnerability scanner
B. A NGFW
C. The Windows Event Viewer
D. A SIEM

Correct Answer: D

Explanation:
Reviewing logs > SIEM, NGFW, or Event Viewer Multiple hosts > SIEM, or NGFW if reviewing traffic to and from certain hosts. Firewall logs would likely be routed to the SIEM though.

QUESTION 296
Which of the following is an example of risk avoidance?

A. Installing security updates directly in production to expedite vulnerability fixes
B. Buying insurance to prepare for financial loss associated with exploits
C. Not installing new software to prevent compatibility errors
D. Not taking preventive measures to stop the theft of equipment

Correct Answer: C

QUESTION 297
Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).

A. Production
B. Test
C. Research and development
D. PoC
E. UAT
F. SDLC

Correct Answer: BE

QUESTION 298
A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would BEST meet the architect's objectives?

A. Trusted Platform Module
B. IaaS
C. HSMaaS
D. PaaS
E. Key Management Service

Correct Answer: A

QUESTION 299
An attack relies on an end user visiting a website the end user would typically visit, however, the site is compromised and uses vulnerabilities in the end users browser to deploy malicious software. Which of the blowing types of attack does this describe?

A. Smishing
B. Whaling
C. Watering hole

D. Phishing

Correct Answer: B

QUESTION 300
A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution. In order to restrict PHI documents, which of the following should be performed FIRST?

A. Retention
B. Governance
C. Classification
D. Change management

Correct Answer: A
Explanation:
In these cases, secure PHI retention is absolutely necessary. The Centers for Medicare & Medicaid Services (CMS) requires that hospitals keep their records for five years at a minimum , with a six year PHI retention requirement for critical access hospitals.

QUESTION 301
A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral

Correct Answer: C

QUESTION 302
A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

A. Snapshot
B. Differential
C. Full
D. Tape

Correct Answer: B
Explanation:
https://aceits.net/types-of-backup-and-what-data-should-be-backed-up/

QUESTION 303
Which of the following corporate policies is used to help prevent employee fraud and to detect

system log modifications or other malicious activity based on tenure?

A. Background checks
B. Mandatory vacation
C. Social media analysis
D. Separation of duties

Correct Answer: B

QUESTION 304
A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

A. Create a new network for the mobile devices and block the communication to the internal network and servers
B. Use a captive portal for user authentication.
C. Authenticate users using OAuth for more resiliency
D. Implement SSO and allow communication to the internal network
E. Use the existing network and allow communication to the internal network and servers.
F. Use a new and updated RADIUS server to maintain the best solution

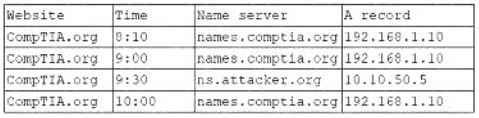
Correct Answer: BC

QUESTION 305
A company is considering transitioning to the cloud. The company employs individuals from various locations around the world The company does not want to increase its on-premises infrastructure blueprint and only wants to pay for additional compute power required. Which of the following solutions would BEST meet the needs of the company?

A. Private cloud
B. Hybrid environment
C. Managed security service provider
D. Hot backup site

Correct Answer: B

QUESTION 306
A customer has reported that an organization's website displayed an image of a smiley (ace rather than the expected web page for a short time two days earlier. A security analyst reviews log tries and sees the following around the lime of the incident:



Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?

A. Invalid trust chain
B. Domain hijacking
C. DNS poisoning
D. URL redirection

Correct Answer: C

QUESTION 307
Which of the following will Increase cryptographic security?

A. High data entropy
B. Algorithms that require less computing power
C. Longer key longevity
D. Hashing

Correct Answer: C

QUESTION 308
An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

A. SIEM
B. SOAR
C. EDR
D. CASB

Correct Answer: B
Explanation:
Why is SOAR used? To synchronize tools, accelerate response times, reduce alert fatigue , and compensate for the skill shortage gap. To collaborate with other analysts during investigations. To analyze workload, organize an analyst's tasks, and allow teams to respond using their own processes.

EDR
The Endpoint Detection and Response Solutions (EDR) market is defined as solutions that record and store endpoint -system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore ...

QUESTION 309
A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?

A. SaaS
B. IaaS
C. PaaS
D. SDN

Correct Answer: A

QUESTION 310
An organization has implemented a two-step verification process to protect user access to data that 6 stored in the could Each employee now uses an email address of mobile number a code to access the data. Which of the following authentication methods did the organization implement?