rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. An error in the correlation rules triggered multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alerts.

Correct Answer: A

QUESTION 280
A company suspects that some corporate accounts were compromised. The number of suspicious logins from locations not recognized by the users is increasing. Employees who travel need their accounts protected without the risk of blocking legitimate login requests that may be made over new sign-in properties. Which of the following security controls can be implemented?

A. Enforce MFA when an account request reaches a risk threshold.
B. implement geofenoing to only allow access from headquarters
C. Enforce time-based login requests trial align with business hours
D. Shift the access control scheme to a discretionary access control

Correct Answer: A

QUESTION 281
Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

A. Privileged access management
B. SSO
C. RADIUS
D. Attribute-based access control

Correct Answer: A

QUESTION 282
A company's cybersecurity department is looking for a new solution to maintain high availability. Which of the following can be utilized to build a solution? (Select Two)

A. A stateful inspection
B. IP hashes
C. A round robin
D. A VLAN
E. A DMZ

Correct Answer: DE

QUESTION 283
A major clothing company recently lost a large amount of proprietary information The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

A. Configure DLP solutions
B. Disable peer-to-peer sharing.
C. Enable role-based access controls
D. Mandate job rotation.
E. Implement content filters

Correct Answer: A

QUESTION 284
A penetration tester successfully gained access to a company's network The investigating analyst determines malicious traffic connected through the WAP despite filtering rules being in place. Logging in to the connected switch, the analyst sees the following m the ARP table:

```
10.10.0.33    a9:60:21:db:a9:83
10.10.0.97    50:4f:b1:55:ab:5d
10.10.0.70    10:b6:a8:1c:0a:33
10.10.0.51    50:4f:b1:55:ab:5d
10.10.0.42    d5:7d:fa:14:a5:46
```

Which of the following did the penetration tester MOST likely use?

A. ARP poisoning
B. MAC cloning
C. Man in the middle
D. Evil twin

Correct Answer: C

QUESTION 285
Joe, a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective. Joe ran a set of commands and received the following output:

```
Domain Name: COMPTIA.ORG
Registry Domain ID: 1234554321
Registrar Server: whois.networksolutions.com
Updated Date: 2018-12-01T05:08:11Z
Creation Date: 1998-02-26T05:00:00Z
Registrar Registration Expiration Date: 2021-02-25T05:00:00Z
Registrar: NETWORK SOLUTIONS, LLC
Registrar IANA ID: 2
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: YourBusiness Corporation
Registrant Organization: YourBusiness Corporation
Registrant Street: 500 Pennsylvania Ave
Registrant City: Downers Grove
Registrant State: IL
Registrant Postal Code: 11105
Registrant Country: US
Registrant Phone: 1 800 555 5555
Registrant Fax: 1 800 555 5556
Registrant Email: info@comptia.org
Admin:  Jason Doe
Admin Organization: CompTIA
```

Which of the following can be determined about the organization's public presence and security

posture? (Select TWO).

A. Joe used Who is to produce this output.
B. Joe used cURL to produce this output.
C. Joe used Wireshark to produce this output
D. The organization has adequate information available in public registration.
E. The organization has too much information available in public registration.
F. The organization has too little information available in public registration

Correct Answer: AD

QUESTION 286
Which two features are available only in next-generation firewalls? (Choose two)

A. deep packet inspection
B. packet filtering
C. application awareness
D. stateful inspection
E. virtual private network

Correct Answer: DE

QUESTION 287
An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would BEST support the new office?

A. Always On
B. Remote access
C. Site-to-site
D. Full tunnel

Correct Answer: B

QUESTION 288
A security proposal was set up to track requests for remote access by creating a baseline of the users' common sign-in properties. When a baseline deviation is detected, an Iv1FA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?

A. Context-aware authentication
B. Simultaneous authentication of equals
C. Extensive authentication protocol
D. Agentless network access control

Correct Answer: B

QUESTION 289
A security an analyst needs to implement security features across smartphones. laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?

A. Enforcing encryption
B. Deploying GPOs
C. Removing administrative permissions
D. Applying MDM software

Correct Answer: D

QUESTION 290
Which of the following is a difference between a DRP and a BCP?

A. A BCP keeps operations running during a disaster while a DRP does not.
B. A BCP prepares for any operational interruption while a DRP prepares for natural disasters
C. A BCP is a technical response to disasters while a DRP is operational.
D. A BCP Is formally written and approved while a DRP is not.

Correct Answer: B

QUESTION 291
A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

A. Dumpster diving
B. Shoulder surfing
C. Information elicitation
D. Credential harvesting

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