Vendor: CompTIA

Exam Code:CAS-005

Exam Name: CompTIA SecurityX Exam

Version: Demo

QUESTION 1

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

Correct Answer: B

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website\\'s performance. A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.

B. CDN (Content Delivery Network): A CDN stores copies of the website\\'s content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user

experience globally.

C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency. D. NAC (Network Access Control): NAC solutions control access

to network resources but are not designed to address web performance issues. Implementing a CDN is the best solution to resolve the performance issues observed in the log output.

References:

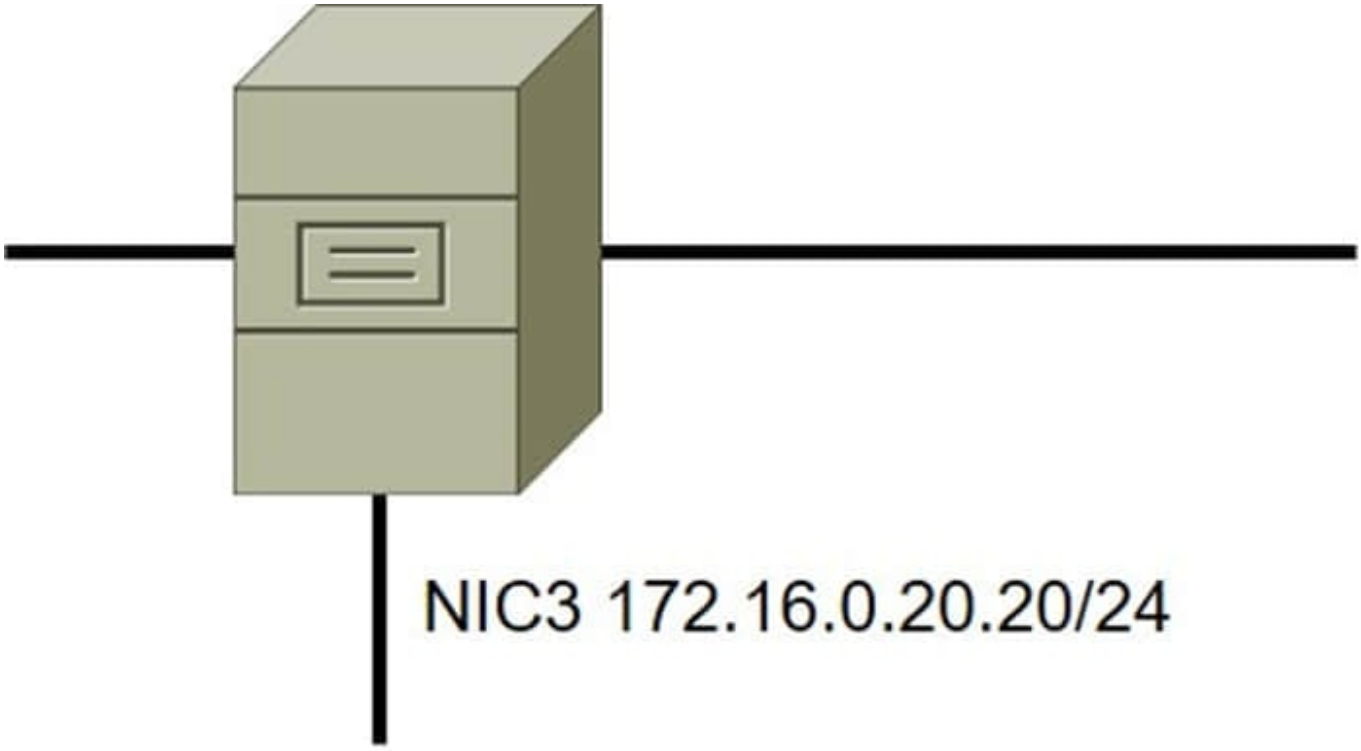
CompTIA Security+ Study Guide

"CDN: Content Delivery Networks Explained" by Akamai Technologies NIST SP 800-44, "Guidelines on Securing Public Web Servers"

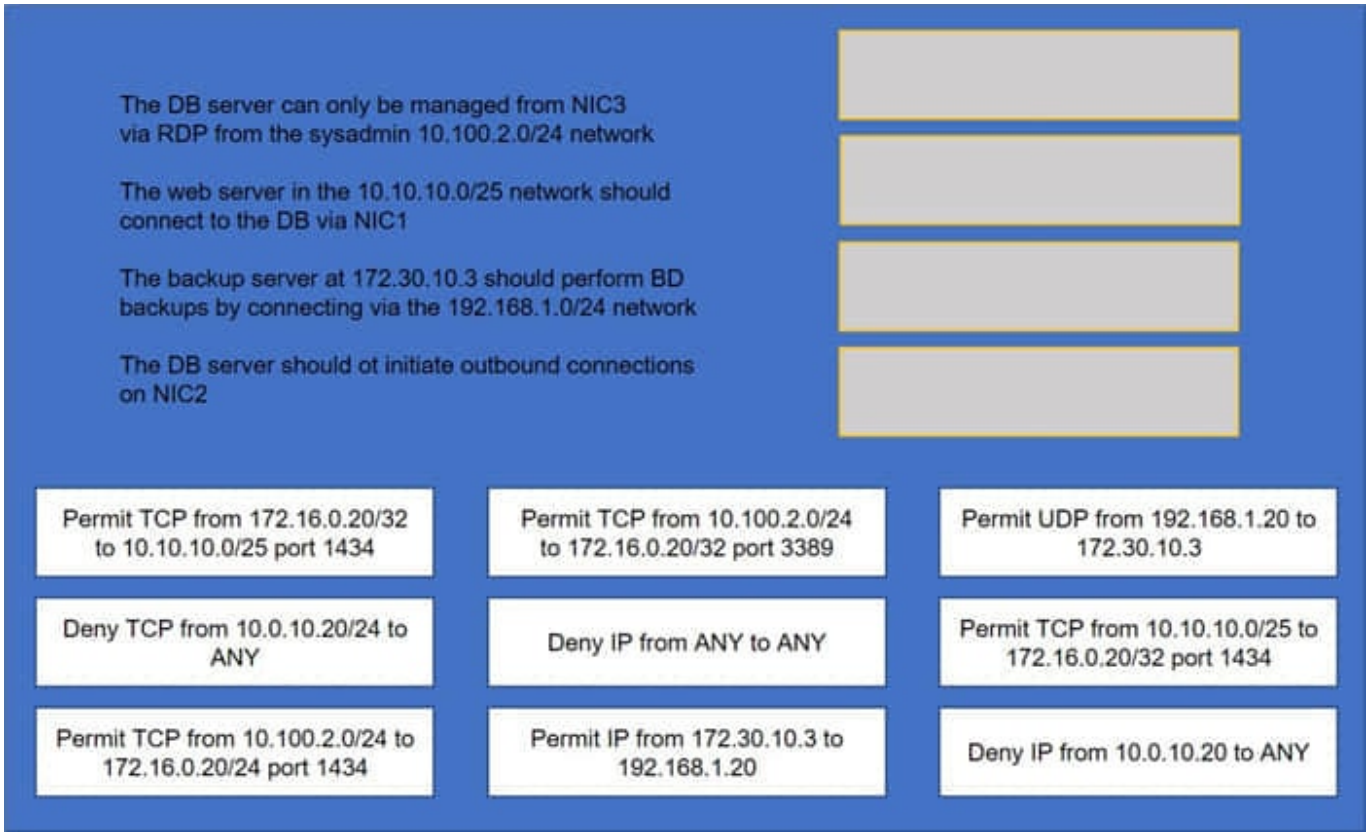
QUESTION 2

DRAG DROP

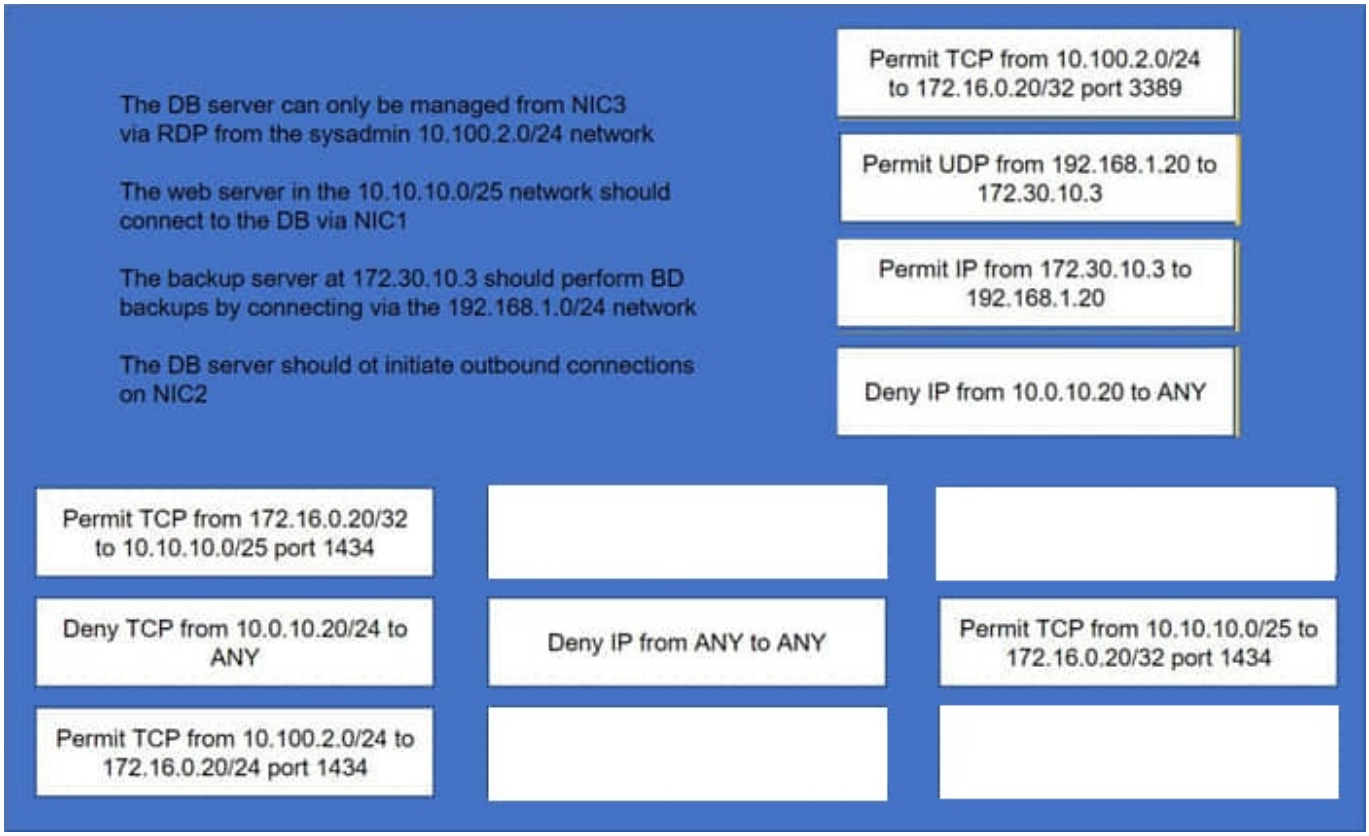
A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.



Select and Place:



Correct Answer:



QUESTION 3

A junior security researcher has identified a buffer overflow vulnerability leading to remote code execution in a former employer\\'s software. The security researcher asks for the manager\\'s advice on the vulnerability submission process. Which of the following is the best advice the current manager can provide the security researcher?

A. Collect proof that the exploit works in order to expedite the process.

B. Publish proof-of-concept exploit code on a personal blog.

C. Recommend legal consultation about the process.

D. Visit a bug bounty website for the latest information.

Correct Answer: C

Legal consultation is crucial before proceeding with any vulnerability disclosure process, especially when dealing with vulnerabilities found in former employers\\' software. It ensures that the researcher adheres to legal and ethical standards, protects their rights, and avoids potential legal risks associated with disclosure. Therefore, advising the security researcher to seek legal consultation is the most prudent course of action in this situation.

QUESTION 4

A security engineer evaluates the overall security of a custom mobile gaming application and notices that developers are bringing in a large number of open-source packages without appropriate patch management. Which of the following would the engineer most likely recommend for uncovering known vulnerabilities in the packages?

A. Leverage an exploitation framework to uncover vulnerabilities.

B. Use fuzz testing to uncover potential vulnerabilities in the application.

C. Utilize a software composition analysis tool to report known vulnerabilities.

D. Reverse engineer the application to look for vulnerable code paths.

E. Analyze the use of an HTTP intercepting proxy to dynamically uncover issues.

Correct Answer: C

QUESTION 5

A security engineer wants to reduce the attack surface of a public-facing containerized application

Which of the following will best reduce the application\\'s privilege escalation attack surface?

A. Implementing the following commands in the Dockerfile: RUN echo user:x:1000:1000iuser:/home/user:/dew/null > /ete/passwd

B. Installing an EDR on the container\\'s host with reporting configured to log to a centralized SIFM and Implementing the following alerting rules TF PBOCESS_USEB=rooC ALERT_TYPE=critical

C. Designing a muiticontainer solution, with one set of containers that runs the mam application, and another set oi containers that perform automatic remediation by replacing compromised containers or disabling compromised accounts

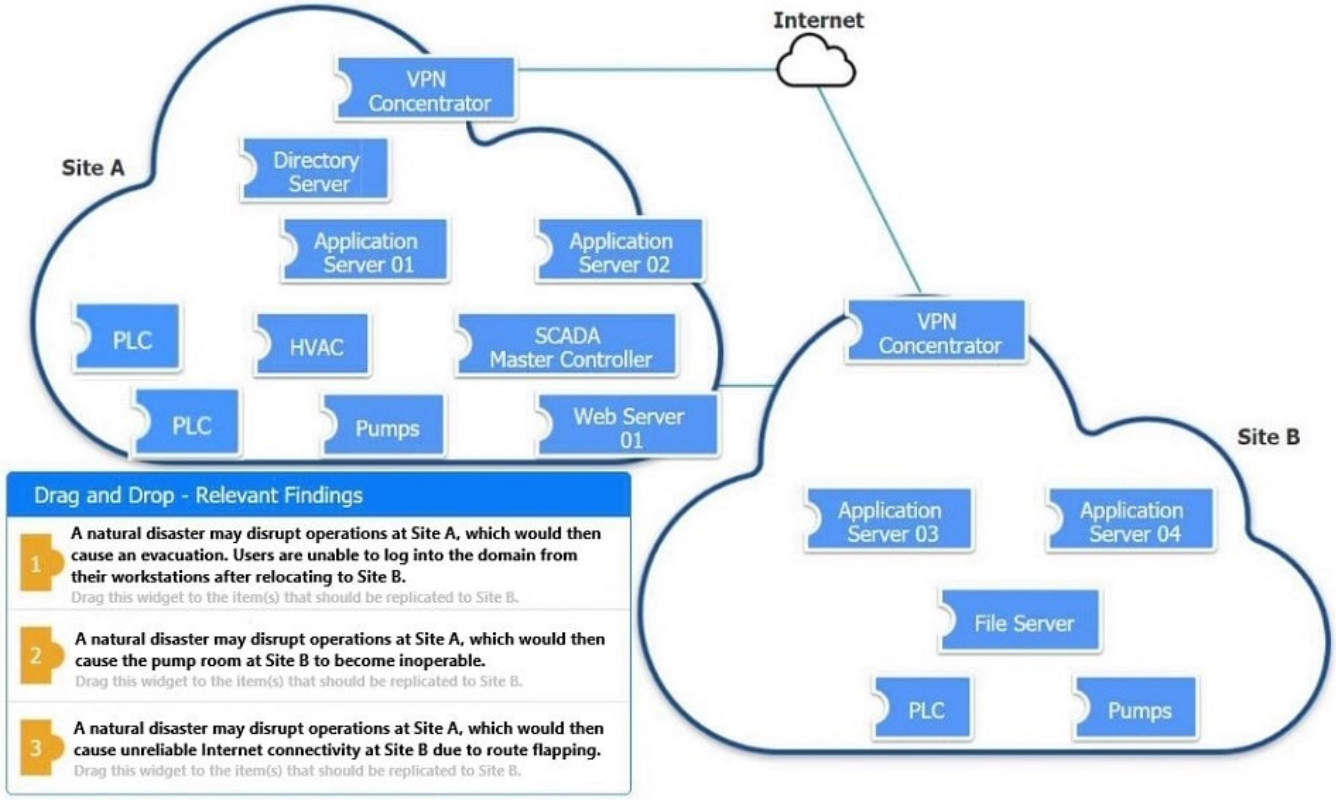
D. Running the container in an isolated network and placing a load balancer in a public- facing network. Adding the following ACL to the load balancer: PZRKZI HTTES from 0-0.0.0.0/0 pert 443

Correct Answer: A

Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of privilege escalation attacks because even if an attacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access. A. Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges. B. Installing an EDR on the container\\'s host: While useful for detecting threats, this does not reduce the privilege escalation attack surface within the containerized application. C. Designing a multi-container solution: While beneficial for modularity and remediation, it does not specifically address privilege escalation. D. Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface. References: CompTIA Security+ Study Guide Docker documentation on security best practices NIST SP 800-190, "Application Container Security Guide"

QUESTION 6

DRAG DROP



An organization is planning for disaster recovery and continuity of operations.

INSTRUCTIONS

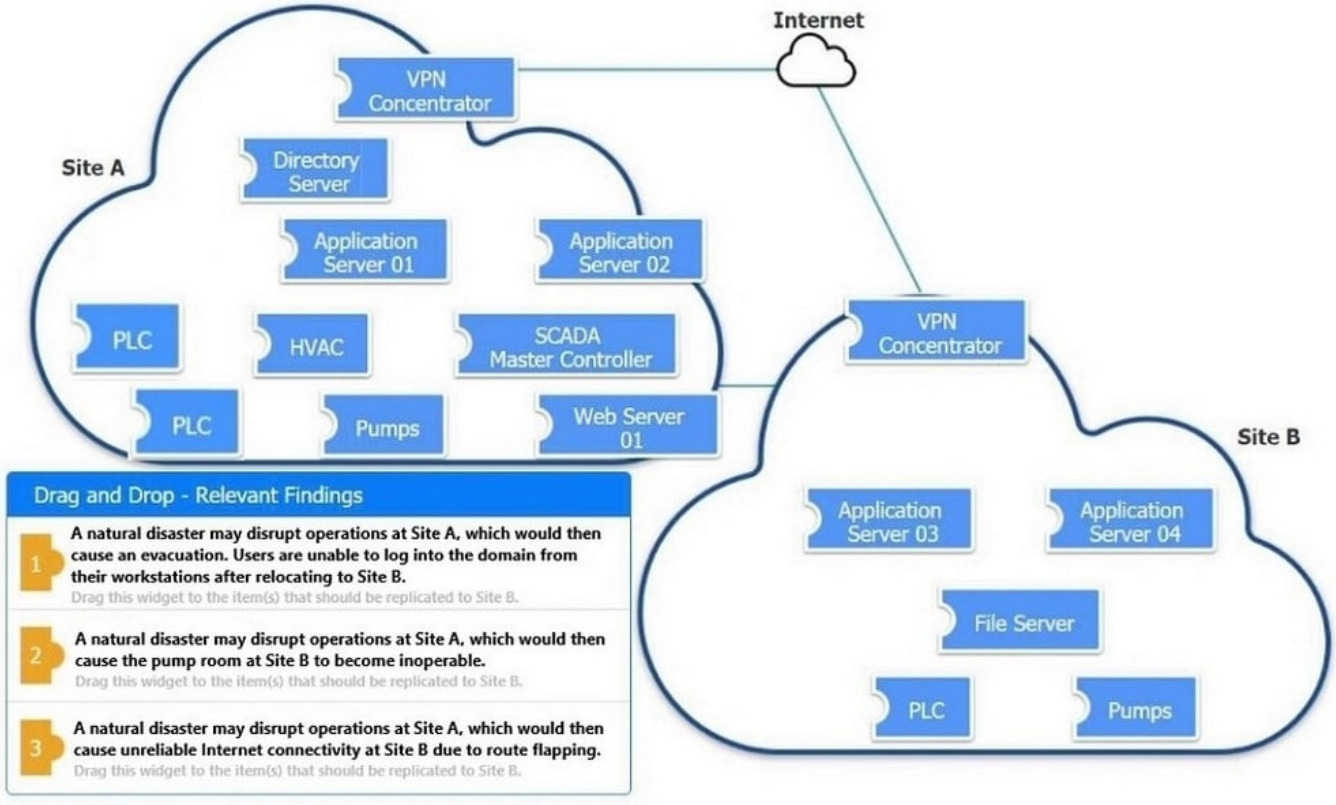
Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

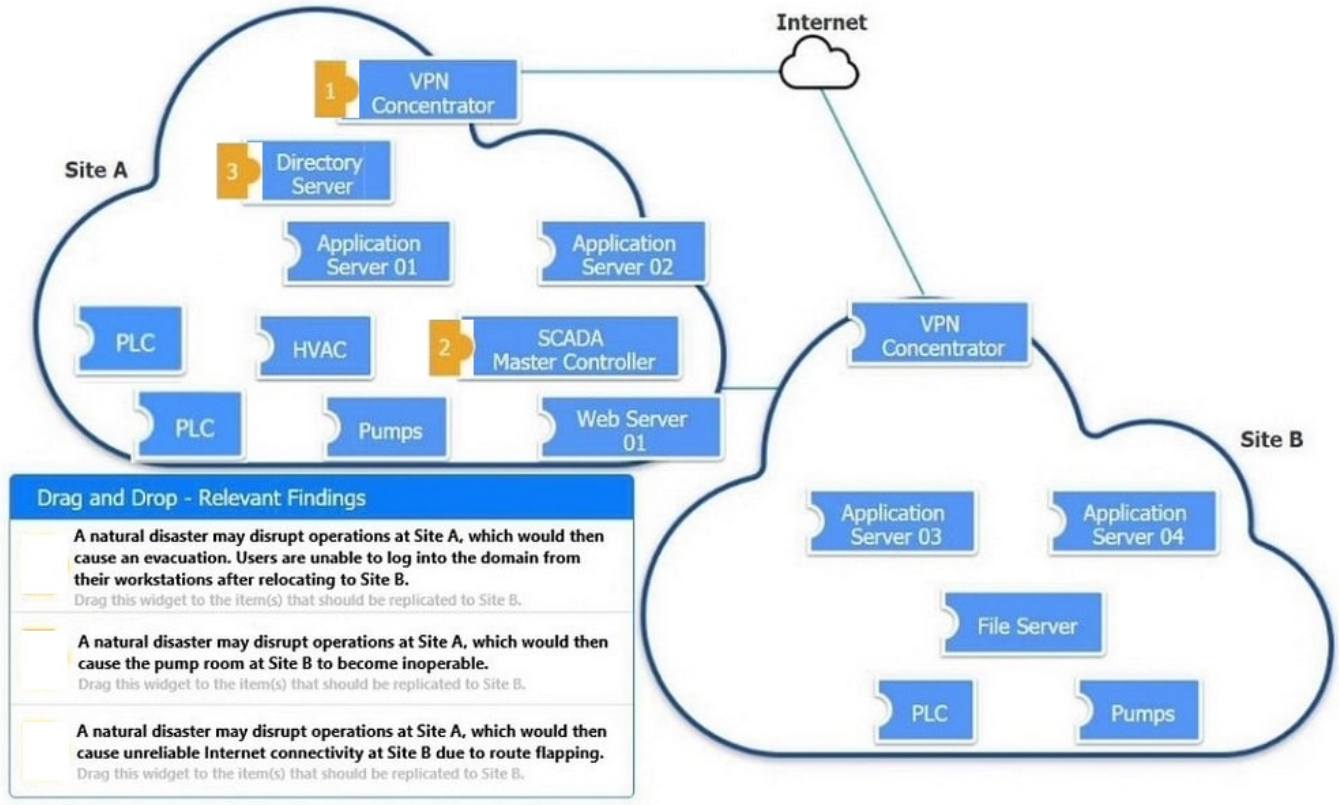
Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simul-ation, please click the Reset All button.

Select and Place:



Correct Answer:



QUESTION 7

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

Correct Answer: B

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"

QUESTION 8

A company\\'s SICM Is continuously reporting false positives and false negatives The security operations team has Implemented configuration changes to troubleshoot possible reporting errors

Which of the following sources of information best supports the required analysts process? (Select two).

A. Third-party reports and logs

B. Trends

C. Dashboards

D. Alert failures

E. Network traffic summaries

F. Manual review processes

Correct Answer: AB

When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:

A. Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader perspective on potential threats. These sources often contain valuable

insights and context that can help correlate events more accurately, reducing the likelihood of false positives and false negatives. B. Trends: Analyzing trends over time can help in understanding patterns and anomalies in the data. By

observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine-tuning

the SIEM configurations to better detect true positives and reduce false alerts.

Other options such as dashboards, alert failures, network traffic summaries, and manual review processes are also useful but are more operational rather than foundational for understanding the root causes of reporting errors in SIEM

configurations.

References:

CompTIA SecurityX Study Guide: Emphasizes the importance of leveraging external threat intelligence and historical trends for accurate threat detection. NIST Special Publication 800-92, "Guide to Computer Security Log Management":

Highlights best practices for log management, including the use of third-party sources and trend analysis to improve incident detection. "Security Information and Event Management (SIEM) Implementation" by David Miller: Discusses the use

of external intelligence and trends to enhance SIEM accuracy.

QUESTION 9

SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from company\\'s privileged network.

The company\\'s hardening guidelines indicate the following:

There should be one primary server or service per device.

Only default ports should be used.

Non-secure protocols should be disabled.

INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

The primary server or service of the device (Note that each IP should by associated with one service/port only)

The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

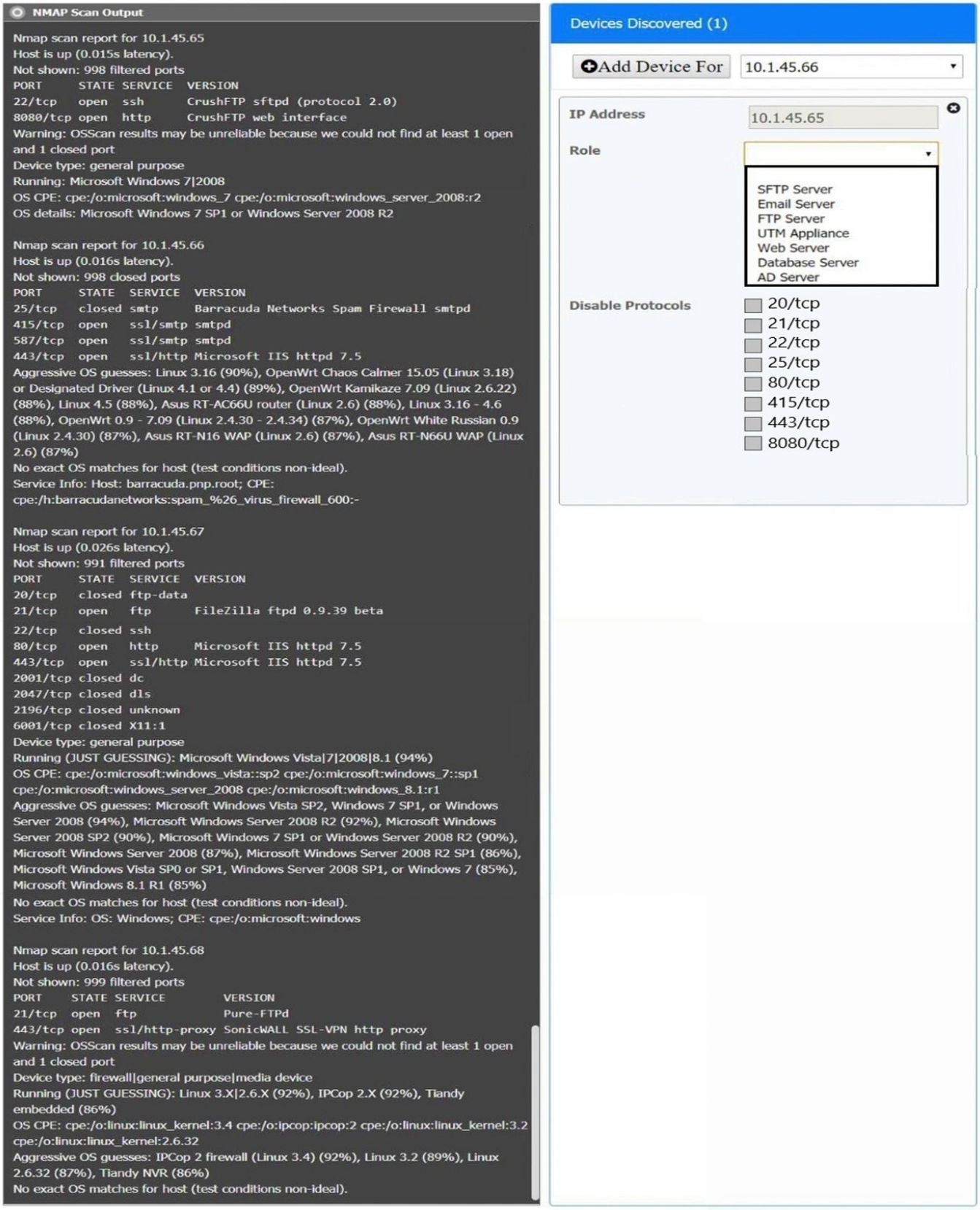
NMAP Scan Output

```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT     STATE  SERVICE  VERSION
25/tcp   closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp  open   ssl/smtp smtpd
587/tcp  open   ssl/smtp smtpd
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE  VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp   closed ssh
80/tcp   open   http     Microsoft IIS httpd 7.5
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE         VERSION
21/tcp  open  ftp             Pure-FTPd
443/tcp open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```

Devices Discovered (0)

Add Device For

10.1.45.65
10.1.45.66
10.1.45.67
10.1.45.68



A. See the complete solution below in Explanation.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

10.1.45.65 SFTP Server Disable 8080

10.1.45.66 Email Server Disable 415 and 443

10.1.45.67 Web Server Disable 21, 80

10.1.45.68 UTM Appliance Disable 21

QUESTION 10

Which of the following is the security engineer most likely doing?

Account	Host	Log-in date	Local log-in time	Office location
Sales_1	PC-18	4/16	9:05 a.m.	USA
Sales_1	PC-18	4/17	9:10 a.m.	USA
Sales_1	PC-10	4/18	9:08 a.m.	USA
Sales_1	PC-10	4/19	9:01 a.m.	USA
Sales_1	PC-64	4/21	8:58 a.m.	UK

A. Assessing log in activities using geolocation to tune impossible Travel rate alerts

B. Reporting on remote log-in activities to track team metrics

C. Threat hunting for suspicious activity from an insider threat

D. Baselining user behavior to support advanced analytics

Correct Answer: A

In the given scenario, the security engineer is likely examining login activities and their associated geolocations. This type of analysis is aimed at identifying unusual login patterns that might indicate an impossible travel scenario. An impossible travel scenario is when a single user account logs in from geographically distant locations in a short time, which is physically impossible. By assessing login activities using geolocation, the engineer can tune alerts to identify and respond to potential security breaches more effectively.

QUESTION 11

An organization developed a containerized application. The organization wants to run the application in the cloud and automatically scale it based on demand. The security operations team would like to use container orchestration but does not want to assume patching responsibilities. Which of the following service models best meets these

requirements?

A. PaaS

B. SaaS

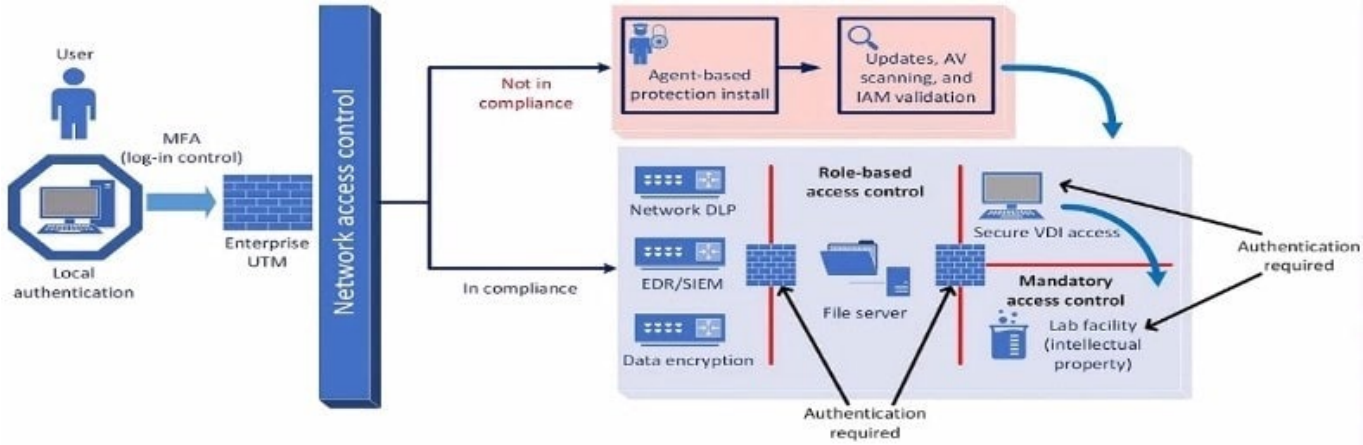
C. IaaS

D. MaaS

Correct Answer: A

QUESTION 12

A company plans to implement a research facility with Intellectual property data that should be protected The following is the security diagram proposed by the security architect



Which of the following security architect models is illustrated by the diagram?

A. Identity and access management model

B. Agent based security model

C. Perimeter protection security model

D. Zero Trust security model

Correct Answer: D

The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is a security framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before

gaining access to resources.

Key Characteristics of Zero Trust in the Diagram:

Role-based Access Control: Ensures that users have access only to the resources necessary for their role.

Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.

Network Access Control: Ensures that devices meet security standards before accessing the network.

Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.

This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.

References:

CompTIA SecurityX Study Guide

NIST Special Publication 800-207, "Zero Trust Architecture" "Implementing a Zero Trust Architecture," Forrester Research