CERTSHOP

CompTIA® CySA+ - Quiz Questions with Answers

1.0 Security Operations

1.

Acme Inc. is considering using federated identities within their corporate network. Which of the following are common entities involved in federated identities?

Select all that apply.

- **IDP**
- **Consumer**
- SASE
- SPF
- Supplicant

Three key roles when using federated identities are:

- *IDP (identity provider): Provides identities, makes identity-related assertions to relying parties, and releases identity-related information to relying parties*
- *RP (relying party) or service provider (SP): Provides services to federation members and securely handles user and IDP data*
- *Consumer: The user of services that may make decisions about identity attributes and provide information to validate identity claims made to an IDP*

SASE (secure access service edge or secure access secure edge; pronounced "sassy") is a network architecture that combines SD-WAN (Software-Defined Wide Area Networking) and security functions with a focus on endpoint and network layer security that are intended to meet the needs of modern decentralized networks (as opposed to centralized, data center-based networks).

SPF (sender policy framework) is an authentication standard designed to improve email security.

In 802.1X, the software agent running on the device requesting access is known as supplicant software.

2.

Acme Inc. wants to enable third party developers to interface with their web application. Which of the following technologies should they use to offer developers the MOST flexibility?

API

SNMP

Plug-in

Honeypot

Correct answer: API

An API (Application Programming Interface) is a programmatic interface to a system that helps enable automation and system integrations.

SNMP (Simple Network Management Protocol) is a protocol commonly used for monitoring network infrastructure.

A plug-in is a program that runs inside of another program.

A honeypot is a system that is intentionally vulnerable to exploits, and it is designed to lure attackers.

3.

Which of the following is an example of an open source threat intelligence source?

Social media

Server logs

Firewall logs

APTs

Correct answer: Social media

Open source threat intelligence refers to information about threats that come from sources that are available to the general public. Social media, websites, and the dark web are examples of open source threat intelligence sources.

An APT (Advanced Persistent Threat) is a type of sophisticated threat actor.

Server logs and firewall logs are not typically available to the general public.

4.

Which of the following is NOT an example of an on-premises security solution?

VPC

IDS

IPS

Firewall

Correct answer: VPC

A VPC (Virtual Private Cloud) is an environment in a public cloud that is semi-isolated from the rest of the infrastructure. Typically, this isolation is achieved by placing the VPC in a private subnet. VPCs may also include additional security controls. A VPC is inherently part of cloud infrastructure, not on-premises infrastructure.

A firewall, IPS (Intrusion Prevention System), and IDS (Intrusion Detection System) appliance are all examples of hardware security devices that could be deployed on-premises.

5.

What Linux command provides information about process run times, CPU utilization, and memory consumption?

ps

df

ping

Sysinternals

Correct answer: ps

The Linux ps command provides information on Linux processes such as when they started, their CPU and memory consumption, and the process (command) that initiated them. Users can add additional flags to modify the output of the ps command. Here is an example output from the "ps aux" command on a Linux system:

```
root@server:~# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  2.2 167892 10508 ?        Ss   Nov11   2:03 /sbin/init
root           2  0.0  0.0      0     0 ?        S    Nov11   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Nov11   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Nov11   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   Nov11   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   Nov11   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   Nov11   0:00 [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   Nov11   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        S    Nov11   0:00 [rcu_tasks_rude_]
root          12  0.0  0.0      0     0 ?        S    Nov11   0:00 [rcu_tasks_trace]
root          13  0.0  0.0      0     0 ?        S    Nov11   0:48 [ksoftirqd/0]
```

The Linux df command provides information on disk utilization. Users can add additional flags to modify the output of the df command.

The ping command is used to test connectivity between network devices.

Sysinternals is a suite of Windows system resource monitoring tools.

6.

What Linux command MOST likely produced this output?

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  2.2 167892 10508 ?        Ss   Nov11   2:03 /sbin/init
root           2  0.0  0.0      0     0 ?        S    Nov11   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Nov11   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Nov11   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   Nov11   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   Nov11   0:00 [netns]
```

ps aux

strings root

md5sum --all

nmap -sV localhost

Correct answer: ps aux

The Linux ps command provides information on Linux processes such as when they started, their CPU and memory consumption, and the process (command) that initiated them. Users can add additional flags to modify the output of the ps command. The example output in the question is from the "ps aux" command on a Linux system.

The strings command is a Linux utility commonly used to extract plaintext data in binary files.

md5sum is a Linux utility that generates MD5 sums based on a file that is provided as input. The output of the command is "<md5 hash value> <file name>", where <md5 hash value> is the MD5 hash and <file name> is the name of the input file.

nmap is a popular open-source port scanning utility that supports a variety of flags that modify it's behavior.

7.

Acme Inc. uses 25 different SaaS and web applications. Acme Inc. employees are struggling to maintain all the different accounts required for these services and complaining of password fatigue. What technology would BEST help Acme Inc. address this problem?

SSO

FISMA

Webhook

PKI

Correct answer: SSO

SSO (Single Sign-On) enables users to authenticate one time with one set of credentials to access multiple systems. SSO reduces password fatigue, limits the risk of password reuse since users aren't creating multiple accounts, reduces the risk of credential exposure on third-party sites since the third-party site does not store the credentials, and requires users to remember fewer passwords, which can reduce support calls and password resets.

FISMA (Federal Information Security Management Act) applies to government agencies and organizations acting on their behalf. FISMA has various security requirements including requiring a vulnerability management program.

A webhook is a type of software integration that involves one application or service triggering an action in another application or service using a web request.

PKI (Public Key Infrastructure) is an asymmetric encryption framework that enables authentication, data confidentiality, and data integrity. Common use cases for PKI include code signing, encrypting data in transit, and generating SSL (Secure Sockets Layer) certificates for websites.

8.

New Org LLC. is a newly-formed business. Charlie, the CISO, is responsible for chartering New Org LLC.'s cybersecurity program. Which of the following is NOT one of the three key objectives of a cybersecurity program?

Encryption

Confidentiality

Integrity

Availability

Correct answer: Encryption

Confidentiality, Integrity, and Availability, also known as the CIA triad, are the three key objectives of modern cybersecurity programs.

Encryption can help enable these objectives, but is not a primary objective itself.

9.

When executed from a PowerShell prompt on a Windows 11 computer, what will the PowerShell code below do?

Write-Host "I am a CySA+ candidate!"

Print the text *"I am a CySA+ candidate!"* in the PowerShell window

Generate an error due to the unescaped "!" character

Create an empty .ps1 file

Create a .ps1 file with the Read-Host command appended to the first line

---

Correct answer: Print the text "I am a CySA+ candidate!" in the PowerShell window

CySA+ candidates should be familiar with basic PowerShell and Python code. The code in the question would print the text "I am a CySA+ candidate!" in the PowerShell window. It is valid PowerShell code, so it would not create an error. It also does not have any directives or cmdlets to create files, so it would not create any additional files. The "exit" command is used to close a PowerShell window and it is not present in the code sample.

10.

Which of the following are examples of CHD?

Select all that apply.

- **Cardholder name**
- **Primary credit card account number**
- Prescription refill date
- PCI DSS
- PII
- Preexisting conditions

CHD (cardholder data) refers to credit card information, such as primary credit card account numbers, cardholder name, and credit card expiration date. CHD data is sometimes called PCI (Payment Card Industry) data because of its relevance to PCI DSS (Payment Card Industry Data Security Standard).

PII (personally identifiable information) is a different type of sensitive data.

Prescription refill date and preexisting conditions are not cardholder data.

11.

Which of the following is NOT the responsibility of a certificate authority in the PKI certificate issuance process?

Verifying requestor identity

Generating certificates

Storing certificates

Signing certificates

Correct answer: Verifying requestor identity

A CA (Certificate Authority) is a major component of PKI (Public Key Infrastructure). A CA is responsible for certificate generation, storage, and signing.

An RA (Registration Authority) is responsible for the verification of the identity of certificate requestors.

12.

An API server provides users with access to resources after they are authenticated using the OAuth 2.0 protocol. The users in this scenario are which of the four parties involved in OAuth flows?

Resource Owners

Clients

Resource Servers

Authorization Servers

Correct answer: Resource Owners

There are four parties in OAuth flows. They are:

- *Clients: Applications used by end users*
- *Resource Owners: End users*
- *Resource Servers: Servers from a service resource owners want applications to use*
- *Authorization Servers: Servers from the identity provider*

The users consuming the APIs in this example are resource owners.

13.

802.1X is typically used to implement what?

NAC

SNMP

DKIM

VDI

Correct answer: NAC

802.1X is an authentication protocol typically used to implement NAC (Network Access Control).

DKIM (DomainKeys Identified Mail) is a protocol that enables organizations to include content in email messages that can verify an email message was sent from a specific domain.

VDI (Virtual Desktop Infrastructure) is a form of virtualization that provides access to desktop operating systems by streaming them from centralized hardware.

SNMP (Simple Network Management Protocol) is a protocol typically used for monitoring and managing network devices.

14.

What does this Linux command do?

grep -i exam cysa.log

Search the file "cysa.log" for the text "exam"

Italicize all instances of the word "exam" in the file "cysa.log"

Copy the contents of the file "cysa.log" to a new file named "exam"

Copy the contents of the file "exam" to a new file named "cysa.log"

Correct answer: Search the file "cysa.log" for the text "exam"

The grep command is used to search files for patterns and return content that matches. The grep command supports different flags that modify its behavior. For example, the -i flag makes a grep search case insensitive (case sensitive is the default behavior).

15.

Which of the following is the BEST example of a vulnerability?

A webserver affected by CVE-2014-0160

A script kiddie

An insider threat

A darknet

Correct answer: A webserver affected by CVE-2014-0160

A vulnerability is a weakness in a system or process that could allow an exploit or attack. CVE-2014-0160 (the Heartbleed bug) is a common vulnerability.

A script kiddie and an insider threat are both threat actors that might exploit a vulnerability.

A darknet is a pool of unused IP addresses that are monitored to detect potential attackers and identify malicious patterns.

16.

Yuri, a software developer at Acme Inc., installs and activates a widget in their Integrated Development Environment (IDE) that performs static code analysis to detect potential security issues in their code. This is an example of what type of tool integration?

Plug-in

Webhook

API

Honeypot

Correct answer: Plug-in

A plug-in is a program that runs inside of another program.

A webhook is a type of software integration that involves one application or service triggering an action in another application or service using a web request.

An API (Application Programming Interface) is a programmatic interface to a system that helps enable automation and system integrations.

A honeypot is a system that is intentionally vulnerable to exploits, and it is designed to lure attackers.

17.

Quinn, a security engineer at Acme Inc., is tasked with evaluating different tools to replace a legacy antivirus program for Windows endpoints. The business requirements call for threat detection, behavioral analysis, and alert notifications.

Which category of security tools is MOST likely to meet the requirements?

EDR

CRL

WAF

SPF

Correct answer: EDR

EDR (Endpoint Detection and Response) tools are a category of security tools focused on detecting and responding to threats on endpoints such as personal computers. EDR solutions typically include threat detection, behavioral analysis, alert notification, and threat neutralization features.

A CRL (Certificate Revocation List) is a list of certificates a CA has invalidated or canceled.

A WAF (Web Application Firewall) is a special firewall intended for use with web applications.

SPF (Sender Policy Framework) is an authentication standard designed to improve email security.

18.

Acme Inc. security contractors are conducting a penetration test on an Acme Inc. datacenter. This is an example of what type of security control?

Operational

Technical

Application

Configuration

Correct answer: Operational

Operational security controls are procedures and practices that improve security posture. Examples of operational controls include running penetration tests, reverse engineering, and security awareness training.

Technical controls are the different applications, systems, devices, and configurations that help enforce security policies and improve security posture.

19.

SSL inspection would be MOST USEFUL for which of the following use cases?

Reading HTTPS traffic

Password cracking

Time synchronization

Password hashing

Correct answer: Reading HTTPS traffic

Modern HTTPS traffic is encrypted using TLS (Transport Layer Security). This encryption creates a challenge for organizations that want to inspect traffic. Without the ability to decrypt the traffic, the data payloads are illegible. SSL (Secure Sockets Layer) inspection solves this problem by terminating SSL/TLS connections at an inspection appliance and passing the traffic to/from the source/destination. With the SSL inspection appliance (which can be a security device such as a firewall or intrusion prevention system) able to decrypt the traffic, organizations can now monitor and inspect traffic.

NTP (Network Time Protocol) servers are typically used for time synchronization.

Password hashing and password cracking are not standard SSL inspection use cases.

20.

On a Linux system, a file "test.log" contains the the text "I will pass the CySA+ exam" on a single line. There are no other contents in the file. Assuming the user has permission to read the file and is in the same directory as "test.log", which of these grep commands would return a match?

Select all that apply.

grep -i cysa test.log

grep -ni cysa test.log

grep + test.log

grep cysa test.log

The grep command is used to search files for patterns and return content that matches. The grep command supports different flags that modify its behavior. For example, the -i flag makes a grep search case insensitive (case sensitive is the default behavior).

- *"grep -i cysa test.log" will match because the -i flag makes the search case-insensitive and "cysa" will match "CySA"*
- *"grep -ni cysa test.log" will work the same as "grep -i cysa test.log" except it will include a line number in the output*
- *"grep + test.log" will match because "+" has an exact match in the file*

"grep cysa test.log" will not match because grep is case-sensitive by default and there is no exact match for "cysa".

21.

TTP are based on the tactics, techniques, and procedures of what type of threat actor?

APT

Script kiddies

OSINT

Honeypot

Correct answer: APT

APTs (Advanced Persistent Threats) are sophisticated threat actors that carry out complex attacks. TTP (Tactics, Techniques, and Procedures) are derived by studying APT behavior.

Script kiddies are a type of threat actor, but they're not the basis for TTP. Script kiddies are unsophisticated and typically depend on readily available tools and low-complexity attacks.

OSINT (Open Source Intelligence) is not a type of threat actor.

A honeypot is a system that is intentionally vulnerable to exploits and is designed to lure attackers.

22.

Which of the following is an example of CHD?

Primary account number

127.0.0.1:8080

HKU

sysLocation

Correct answer: Primary account number

CHD (Cardholder Data) refers to credit card information such as primary credit card account numbers, cardholder name, and credit card expiration date. CHD data is sometimes called

PCI (Payment Card Industry) data because of it's relevance to PCI DSS (Payment Card Industry Data Security Standard).

127.0.0.1:8080 is an IPv4 loopback address (127.0.0.1) and port number (8080) combination.

HKEY_USERS (HKU) is a Windows registry root key. Information underneath this root key is related to user accounts on the system.

sysLocation is a value commonly associated with SNMP (Simple Network Management Protocol) monitoring that contains information about a system's location.

23.

Dani, a security engineer at Acme Inc., is creating a system hardening checklist for servers the organization maintains. Which of the following should Dani include in the checklist?

Restrict administrative access

Disable disk encryption

Enable the guest account

Disable secure boot

Correct answer: Restrict administrative access

Restricting administrative access is a common hardening technique that helps enforce the principle of least privilege.

Secure boot and disk encryption can help improve security, so disabling them is not typically a recommended step for system hardening.

Enabling a guest account on a Windows server allows "guests" to access the system. This increases security risk and is typically not a recommended step for system hardening,

24.

Which of the following is one of the "three As" in AAA?

Accounting

Access

Administration

Adversary

Correct answer: Accounting

The "three As" in AAA are:

- *Authentication, which deals with verifying identities*
- *Authorization, which deals with allowing or disallowing an identity access to resources*
- *Accounting, which deals with monitoring and logging*

25.

Acme Inc. is using the AAA framework as part of a new network design. Lucian, a network architect at Acme Inc., is tasked with designing all the components related to accounting.

Which of the following is MOST likely to be part of Lucian's task?

Defining default log levels

Choosing an identity provider

Configuring OAuth

Financial reporting

Correct answer: Defining default log levels

AAA is a framework for controlling and managing access to resources such as networks and computers. The "three As" in AAA are:

- *Authentication, which deals with verifying identities*
- *Authorization, which deals with allowing or disallowing an identity access to resources*
- *Accounting, which deals with monitoring and logging*

Since Lucian is responsible for accounting, setting default log levels is most likely to become their responsibility.

Financial reporting would be the responsibility of accounting (in a different context) and finance departments.

Choosing an identity provider is an authentication related task. OAuth is an authorization standard.

26.

A misconfigured application on a server deployed in a small lab network created a huge spike in network traffic and caused performance issues across the entire network. This is an example of what type of network issue?

Bandwidth consumption

Beaconing

Social engineering

Phishing

Correct answer: Bandwidth consumption

Bandwidth consumption issues occur when a significant amount of network bandwidth is consumed and business functions are disrupted or service outages occur as a result. Common causes of bandwidth consumption issues include malicious activity, misconfigurations, and traffic spikes.

Beaconing is a type of network traffic that enables operators of botnets or other malware that uses a command and control model to detect if they have compromised a system, check system status, or perform malicious activity such as running unauthorized commands.

Social engineering is a type of attack that involves influencing human behavior to compromise information or systems. Phishing is a common example of social engineering.

27.

Assume http://malicoussite.example.com is a site hosting malware and safesite.example.net is a legitimate website. The HTML code below is a simple example of what technique?

https://safesite.example.net

Obfuscated link

Honeypot

Script kiddie

MQTT

Correct answer: Obfuscated link

Obfuscated links are links that hide their destination from users. For example, a shortened URL that redirects to a malicious webpage is an example of an obfuscated link. The HTML code above displays the text "https://safesite.example.net" but actually links to the malicious site "http://malicioussite.example.com".

A honeypot is a system that is intentionally vulnerable to exploits and is designed to lure attackers.

A script kiddie is a type of threat actor.

MQTT (Message Queuing Telemetry Transport) is a network protocol.

28.

Alex, a systems engineer at Acme Inc., wants to bundle an application into a portable lightweight package with the smallest attack surface practical. Which of the following options should Alex use?

Containerization

Virtual machines

VLANs

SSO

Correct answer: Containerization

Containerization is a form of application-level virtualization that enables an application and its dependencies to be bundled into portable containers that can run on different operating systems as long as they support a compatible container engine.

Virtual machines include a full operating system, are typically larger than containers, and typically have more dependencies.

VLANs (Virtual Local Area Networks) are logical networks that can provide logical network segmentation to separate portions of a network. VLANs are typically implemented using a router or managed switch that supports VLAN tagging.

SSO (Single Sign-On) enables users to authenticate one time with one set of credentials to access multiple systems.

29.

Luka, a security architect at Acme Inc., wants to create a darknet to monitor threat actor behavior. Luka purchased a /30 pool of public IPv4 addresses and is actively monitoring the addresses.

What type of workloads should Luka deploy to the IPv4 addresses to complete the darknet?

None

Containerized workloads

Vulnerable virtual machines

Honeypots

Correct answer: None

A darknet is a pool of unused IP addresses that are monitored to detect potential attackers and identify malicious patterns. By definition, the IP addresses should remain unused. Deploying workloads such as honeypots would transform the darknet into a honeynet.

30.

What type of information can be found in AbuseIPDB?

Potentially malicious IP addresses

Revoked SSL certificates

Trusted certificate authorities

Detailed logs of network traffic for a Linux mail server

Correct answer: Potentially malicious IP addresses

AbuseIPDB is an online database that enables users to check if an IP address, domain, or network has been reported as engaging in abusive behavior. There are other comparable online tools available, but AbuseIPDB is specifically called out on the CySA+ exam objectives and CySA+ candidates should be familiar with this online tool.

31.

Application logs show that a user logged in from Canada on Nov 11, 2024 at 11:11:11 p.m. UTC and then logged in again from England on Nov 11, 2024 at 11:21:21 p.m UTC. This is an example of what type of abnormal account activity?

Impossible travel

Duplicate existence

Recursive logins

Duplicate identity

Correct answer: Impossible travel

Impossible travel is a form of abnormal user activity. Impossible travel occurs when a user is recorded logging in from different geographical locations within a timeframe that would be impossible for a human. In this example, it's not possible for a human to travel from Canada to England in ten minutes.

Duplicate existence, recursive logins, and duplicate identity are incorrect. They are not standard forms of abnormal account activity.

32.

Alex is a security administrator at Acme Inc. tasked with reviewing the logs from several systems involved in a security incident. Alex notices that timestamps do not align across different system logs, even after accounting for different timezones. Which of the following could BEST explain why the log timestamps are not properly aligned across systems?

Improper NTP configuration

Using HTTP instead of HTTPS

Improper log levels

Using MQTT instead of MQTTS

Correct answer: Improper NTP configuration

NTP (Network Time Protocol) is a network protocol used to synchronize time across systems. NTP servers enable multiple client systems to synchronize their time with an authoritiative source and help keep timestamps in sync throughout a network.

Log levels would not directly impact timestamps.

Using the HTTP(S) and MQTT(S) protocols would not directly impact timestamps.

33.

Which of the following is an example of a knowledge factor in authentication?

Password

Fingerprint

Smartcard

Authenticator application

Correct answer: Password

Common authentication factors include:

- *Knowledge factors - "something you know," e.g., a password*
- *Possession factors - "something you have," e.g., a smartcard or authenticator application*
- *Biometric factors - "something you are," e.g., a fingerprint*
- *Location factors - "where you are," e.g., accessing a system from a specific location*

Authentication factors can be combined to improve security. MFA (Multifactor Authentication) combines two or more different authentication factors in the authentication process.

34.

Port security is MOST commonly associated with which unique identifier on a device?

MAC address

Serial number

UUID

FQDN

Correct answer: MAC address

Port security is an access control that limits network access based on MAC (Media Access Control) addresses.

While a serial number, FQDN (Fully Qualified Domain Name), or UUID (Universal Unique Identifier) can be useful identifiers in different contexts, MAC addresses are typically the basis of port security.

35.

Which aspect of the AAA framework focuses on monitoring and logging?

Accounting

Access

Alerting

Authorization

Correct answer: Accounting

AAA is a framework for controlling and managing access to resources such as networks and computers. The "three As" in AAA are:

- *Authentication, which deals with verifying identities*
- *Authorization, which deals with allowing or disallowing an identity access to resources*
- *Accounting, which deals with monitoring and logging*

36.

An Acme Inc. security policy requires that all PowerShell scripts downloaded from the Internet are signed by a trusted publisher.

Which execution policies are compliant with this policy?

Select the option that includes ALL PowerShell execution policies that permit remote scripts to run ONLY if they are signed by a trusted publisher.

AllSigned and RemoteSigned

AllSigned and Restricted

RemoteSigned and Bypass

AllSigned

Correct answer: AllSigned and RemoteSigned

PowerShell execution policies determine what type of PowerShell scripts are allowed to run on a system. The five different execution policies, from most to least restrictive are:

1. *Restricted: No PowerShell scripts can execute*
2. *AllSigned: Allows the execution of scripts that have a trusted signature*
3. *RemoteSigned: Allows the execution of any locally created scripts but requires external scripts to have a trusted signature*
4. *Unrestricted: Allows the execution of any scripts, but prompts for confirmation if when external scripts are executed*
5. *Bypass: Allows the execution of any scripts*

Restricted is not compliant because it does not allow the execution of signed scripts.

Unrestricted and bypass are not compliant because they do not require signatures on remote scripts.

AllSigned and RemoteSigned both enforce the requirement for signatures on remote scripts.

37.

Acme Inc. purchased and actively monitors a pool of public IPv4 addresses. Acme Inc. has not deployed any workloads that use the IP addresses and only uses the monitoring data to identify potential attack patterns. This is an example of what type of active defense?

Darknet

Honeypot

Dark web

Honeynet

Correct answer: Darknet

A darknet is a pool of unused IP addresses that are monitored to detect potential attackers and identify malicious patterns.

A honeypot is a system that is intentionally vulnerable to exploits and is designed to lure attackers.

A honeynet is a network of honeypots.

The dark web is a portion of the internet that typically requires a Tor web browser to access.

38.

Taylor, a security administrator at Acme Inc., is attempting to find specific messages in a /var/log/cysa/ directory that include the string "Auth". Taylor wants to use grep to search files in /var/log/cysa/ and all the directories under it recursively. Which command should Taylor use?

grep -r Auth /var/log/cysa/

grep -i Auth /var/log/cysa/

grep -n auth /var/log/

grep -e /var/

Correct answer: grep -r Auth /var/log/cysa/

The grep command is used to search files for patterns and return content that matches. The grep command supports different flags that modify its behavior. For example, the -i flag makes a grep search case insensitive (case sensitive is the default behavior).

Other common grep flags include:

- *"-c" counts how many matches there are for a specific pattern*
- *"-n" shows the line and line number for a match*
- *"-v" shows all lines that are not a match*
- *"-r" reads files under a directory recursively*
- *"-e" searches a specified pattern(s)*

The -r flag is what Taylor needs in this case.

39.

notskrnl.exe, smss.exe, and winlogon.exe are all examples of what category of software?

System processes

Firewalls

IPS/IDS

File managers

Correct answer: System processes

System processes perform core operating system functions. notskrnl.exe (Core NT Kernel Process), smss.exe (Session Manager), and winlogon.exe (Logon Process) are all examples of system processes on a Windows operating system. They are not firewalls, IPS/IDS (Intrusion Prevention System/Intrusion Detection System), or file managers.

40.

What are the three key objectives of cybersecurity programs?

Confidentiality, integrity, and availability

Encryption, networking, and threat detection

Risk mitigation, vulnerability management, and encryption

Confidentiality, privacy, and risk mitigation

Correct answer: Confidentiality, integrity, and availability

Confidentiality, Integrity, and Availability, also known as the CIA triad, are the three key objectives of modern cybersecurity programs.

The other answers include topics that are important to cybersecurity but are not the three key objectives CySA+ candidates should know for the exam.

41.

Jie, a security analyst at Acme Inc., is looking for security configuration benchmarks for Windows 11 computers. What source is MOST likely to have the information Jie needs?

CIS website

Fast-flux DNS

NIST SP 800-88 documentation

Cyber Kill Chain

Correct answer: CIS website

CIS (The Center for Internet Security) is a nonprofit organization that focuses on security best practices. CIS maintains and provides security configuration benchmarks and hardening guides for different operating systems, including Windows 11 and multiple Linux distributions.

Fast-flux DNS is when an attacker associates many IP addresses with a domain and quickly changes them.

NIST SP 800-88 defines three main types of media sanitization.

Lockheed Martin's Cyber Kill Chain is an attack framework.

42.

Which grep flag is used to return all the lines that do NOT match the string specified?

-v

-r

-i

-n

Correct answer: -v

The grep command is used to search files for patterns and return content that matches. The grep command supports different flags that modify its behavior. For example, the -i flag makes a grep search case insensitive (case sensitive is the default behavior).

Other common grep flags include:

- *"-c" counts how many matches there are for a specific pattern*
- *"-n" shows the line and line number for a match*
- *"-v" shows all lines that are not a match*
- *"-r" reads files under a directory recursively*
- *"-e" searches a specified pattern(s)*

43.

Which of the following is a valid logging BEST practice?

Logs should be protected from changes

Organizations should always use the highest logging level

Logs should only be transported via MQTTS

Organizations should always use the lowest logging level

Correct answer: Logs should be protected from changes

Log records should be immutable so they provide an accurate and reliable record of what actually occurred. Protecting log records from changes is an important part of maintaining their integrity.

There is no one-size-fits-all standard for the right logging level for an organization. Organizations should choose the logging level that balances capturing information, avoiding "floods" of data that are not useful, and storage.

MQTTS is a network protocol that devices may use to transmit data, but it is not a best practice to use MQTTS only for log transmission.

44.

Which of the following statements about OpenID is FALSE?

It supports authorization

It supports authentication

It is a federated identity technology.

Replay attacks are a potienal security risk when using OpenID

Correct answer: OpenID

OpenID is a federated identity technology that supports authentication. OpenID does not support authorization. Potential security risks related to OpenID include redirect manipulation, phishing, and replay attacks.

45.

Yuri, a security analyst at Acme Inc., needs to select a hashing algorithm to validate the integrity of a file after it is downloaded. Which of the following is an example of a hashing algorithm?

MD5

ChaCha20

RC4

3DES

Correct answer: MD5

Hashes are one-directional functions that enable data of an arbitrary size to be transformed into a fixed size. Strong hash functions greatly reduce or reasonably eliminate the chance of a duplicate hash being generated unless two files are the same. SHA256 and MD5 are examples of hashing algorithms.

The other algorithms are symmetric key algorithms.

46.

Amal logs into a banking website with a username, password, and code from an authenticator app. Which authentication factors did Amal use?

Knowledge and possession

Knowledge only

Possession and location

Possession only

Correct answer: Knowledge and possession

Common authentication factors include:

- *Knowledge factors - "something you know," e.g., a password*
- *Possession factors - "something you have," e.g., a smartcard or authenticator application*
- *Biometric factors - "something you are," e.g., a fingerprint*
- *Location factors - "where you are," e.g., accessing a system from a specific location*

Authentication factors can be combined to improve security. MFA (Multifactor Authentication) combines two or more different authentication factors in the authentication process.

47.

Amal is a security engineer at Acme Inc. Amal is helping the IT team develop a logging strategy for a new network. Which of the following should Amal recommend be incorporated into the logging strategy?

Send logs to a central location for storage, analysis, and reporting

Avoid using NTP for time synchronization, use RTC instead

Set all log levels to Emergencies

Set all log levels to Critical

Correct answer: Send logs to a central location for storage, analysis, and reporting

Logs should be sent to a central location to help streamline storage, analysis, and reporting. Centralization makes it easier for administrators to work with logs and add context to security incidents that impact multiple systems.

NTP (Network Time Protocol) is a network protocol used to synchronize time across systems. NTP servers enable multiple client systems to synchronize their time with an authoritative source and help keep timestamps in sync throughout a network. NTP would be useful for time synchronization in the new network.

There is no one-size-fits-all standard for the right logging level for an organization. Organizations should choose the logging level that balances capturing information, avoiding "floods" of data that are not useful, and storage. Nothing in the question tells us Emergencies or Critical are the right log levels in this case.

48.

How many authentication factors are TYPICALLY used with passwordless authentication?

One

Five

Three

Zero

Correct answer: One

Passwordless authentication typically uses one authentication factor such as a USB token.

49.

What cybersecurity objective deals with preventing unauthorized access to sensitive data?

Confidentiality

Integrity

Availability

Privacy

Correct answer: Confidentiality

Confidentiality, Integrity, and Availability, also known as the CIA triad, are the three key objectives of modern cybersecurity programs.

Confidentiality deals with preventing unauthorized access to sensitive data.

Integrity deals with ensuring data and systems are free from unauthorized modifications.

Availability deals with ensuring data and systems remain accessible to authorized users.

Privacy focuses on protecting how organizations share data related to individuals.

50.

Acme Inc. is considering using OpenID for identity services as part of an upcoming project. Which of the following statements about OpenID is TRUE?

OpenID supports authentication

OpenID supports authorization

OpenID is immune to replay attacks

OpenID is immune to redirect manipulation

Correct answer: OpenID supports authentication

OpenID is a federated identity technology that supports authentication. OpenID does not support authorization. Potential security risks related to OpenID include redirect manipulation, phishing, and replay attacks.

51.

EDR is BEST described as a modern replacement for what type of technology?

Antivirus

SSL

WAF

Relational database

Correct answer: Antivirus

EDR (Endpoint Detection and Response) tools are a category of security tools focused on detecting and responding to threats on endpoints such as personal computers. EDR solutions typically include threat detection, behavioral analysis, alert notification, and threat neutralization features. They can be described as modern replacements for traditional antivirus programs.

An EDR is not a viable replacement for SSL (or TLS), a WAF (Web Application Firewall), or a relational database.

52.

Which of the following is TRUE about JSON formatting?

It uses curly brackets to structure data

It uses dotted-decimal notation to structure data

It uses angle brackets to structure data

It does NOT support key:value pairs natively

Correct answer:

JSON (JavaScript Object Notation) is a data format that uses key:value pairs and curly brackets {} to structure data.

```
{
 "org": "CompTIA",
 "exam": "CySA+"
}
```

is an example of data using a JSON format.

53.

Acme Inc. has an office near the ocean. The high humidity in the area contributed to a premature server failure that caused a database to go offline for six hours. The threat in this scenario is an example of which of the four threat categories identified by NIST?

Structural

Adversarial

Accidental

Environmental

Correct answer: Structural

NIST (The National Institute of Standards and Technology) identifies four categories of threats. They are:

- *Adversarial threats that try to intentionally harm an organization*
- *Accidental threats which can occur when individuals make a mistake*
- *Structural threats which can occur when equipment, resources, software, or infrastructure fail or are depleted*
- *Environmental threats that stem from disasters (e.g., hurricanes, fires, or power outages)*

While the humidity contributed to the failure, this was not an environmental threat as it did not stem from a disaster. It was a structural threat as a piece of equipment failed.

54.

The Acme Inc. QA team load tests a web application deployed on a public cloud platform once every month. The testing is typically done during off-peak hours to avoid service disruptions. Due to a misconfiguration in the DevOps pipeline, some of the automated load tests during normal business hours and created significant performance degradation because Acme Inc.'s backbone router could not support all the traffic.

Which type of network issue BEST describes this problem?

Bandwidth consumption

Beaconing

Fuzzing

Network loop

Correct answer: Bandwidth consumption

Bandwidth consumption issues occur when a significant amount of network bandwidth is consumed and business functions are disrupted or service outages occur as a result. Common causes of bandwidth consumption issues include malicious activity, misconfigurations, and traffic spikes.

Beaconing is a type of network traffic that enables operators of botnets or other malware that use a command and control model to detect if they have compromised a system, check system status, or perform malicious activity such as running unauthorized commands.

Fuzz testing, also known as fuzzing, is a form of testing where invalid or random data is sent to an application to see how it responds. Fuzz tests are typically automated and useful for uncovering issues like poor error handling and memory leaks.

A network loop is a misconfiguration in network connection that can lead to rapid bandwidth consumption.

55.

Acme Inc. is considering the pros and cons of threat intelligence sharing. Which of the following is NOT common use of threat intelligence sharing?

For improving confidentiality

As a part of monitoring and detection

For vulnerability management

As a part of risk management

Correct answer: For improving confidentiality

Threat intelligence sharing plays an important role in overall cybersecurity. There are five areas for the use of threat intelligence sharing that CySA+ candidates should be familiar with. They are:

- *As a part of incident response*
- *For vulnerability management*
- *As a part of risk management*
- *To inform and influence security engineering*
- *As a part of monitoring and detection*

While threat intelligence sharing may indirectly improve confidentiality by helping an organization learn of new threats or techniques, it is not a direct use like the other answers.

56.

Information from what source would be MOST likely indicate that impossible travel may have occurred?

Authentication logs

DNS logs

NTP server

ISACs

Correct answer: Authentication logs

Impossible travel is a form of abnormal user activity. Impossible travel occurs when a user is recorded logging in from different geographical locations within a timeframe that would be impossible for a human. In this example, it's not possible for a human to travel from Canada to England in ten minutes. An authentication log would contain this sort of login information.

DNS (Domain Name System) logs would contain information related to DNS lookups.

NTP (Network Time Protocol) servers are used for time synchronization.

ISACs (Information Sharing and Analysis Centers) are organizations that help other organizations share and learn about threat information and can provide helpful cybersecurity tools and assistance.

57.

How many standard Cisco log levels are there?

8

7

21

11

Correct answer: 8

The eight standard Cisco log levels are:

- *Level 0- Emergencies*
- *Level 1- Alerts*
- *Level 2- Critical*
- *Level 3- Errors*
- *Level 4- Warning*
- *Level 5- Notifications*
- *Level 6- Information*
- *Level 7- Debugging*

The higher the log level number, the more information is included in the associated logs. Each higher-numbered log level includes the log messages from the lower-numbered levels. For example, Alerts (Level 1) include more log messages than Emergencies (Level 0) because Alerts include Level 1 and Level 0 messages.

58.

A disgruntled Acme Inc. employee deploys connects an unauthorized smart camera to a corporate network using an 802.11ax connection. This unauthorized device is an example of what?

Wireless rouge

Wired rouge

Beacon

NAC

Correct answer: Wireless rouge

A wired rouge is an unauthorized wired device that is connected to a network. Wired rouges can be created resulting from mistakes by legitimate users (e.g., an employee connecting a test device) or threat actors with malicious intent (like the scenario in this question). A wireless rouge is similar, but uses a wireless connection. 802.11ax is a type of WiFi, therefore the camera is a wireless rouge.

Beacon is not correct. Beaconing is a type of network traffic that enables operators of botnets or other malware that use a command and control model to detect if they have compromised a system, check system status, or perform malicious activity such as running unauthorized commands.

NAC (Network Access Control) is a way to restrict or allow network access.

59.

The file cysa.log on a Linux server contains the following three lines of text:

EXAM

exam

eXaM

Assuming it is executed from the same directory as the cysa.log file, what is the expected output of the command below?

grep EXAM cysa.log

EXAM

EXAM

exam

eXaM

An error message

No output

Correct answer: EXAM

Without the -i flag, grep does case-sensitive pattern matching. Therefore, the command "grep EXAM cysa.log" would match one line and return the output "EXAM". It would not throw an error in the situation described in the question.

60.

Which of the following is an example of a hashing algorithm?

SHA256

AES

Blowfish

RC4

Correct answer: SHA256

Hashes are one-directional functions that enable data of an arbitrary size to be transformed into a fixed size. Strong hash functions greatly reduce or reasonably eliminate the chance of a duplicate hash being generated unless two files are the same. SHA256 is a popular example of a hashing algorithm.

The other answers are examples of symmetric key algorithms.

61.

Which of the following Cisco log level would include the most information in the associated logs?

Information

Alert

Warning

Emergencies

Correct answer: Information

The eight standard Cisco log levels are:

- *Level 0- Emergencies*
- *Level 1- Alerts*
- *Level 2- Critical*
- *Level 3- Errors*
- *Level 4- Warning*
- *Level 5- Notifications*
- *Level 6- Information*
- *Level 7- Debugging*

The higher the log level number, the more information is included in the associated logs. Each higher-numbered log level includes the log messages from the lower-numbered levels. For example, Alerts (Level 1) include more log messages than Emergencies (Level 0) because Alerts include Level 1 and Level 0 messages.

Of the answers below, Information has the highest number log level, and, therefore, it is the correct answer.

62.

Ira, a security engineer at Acme Inc., is tasked with finding a security solution that can enforce security policies when a user accesses cloud resources. Which of the following solutions is the BEST fit for this high-level requirement?

CASB

NTP

PHI

VDI

Correct answer: CASB

CASBs (Cloud Access Security Brokers) provide policy-enforcement checkpoints that can help enable secure access to cloud resources. CASBs can be deployed on-premises or in the cloud.

NTP (Network Time Protocol) is a network protocol used to synchronize time across systems. NTP servers enable multiple client systems to synchronize their time with an authoritative source and help keep timestamps in sync throughout a network.

PHI (Personal Health Information) is a category of personal information related to healthcare.

VDI (Virtual Desktop Infrastructure) is a form of virtualization that provides access to desktop operating systems by streaming them from centralized hardware.

63.

A threat actor compromised a database that includes primary credit card account numbers for Acme Inc. customers. Compliance with which standard will LIKELY be impacted by this security incident?

PCI DSS

CHD

OSS TMM

OWASP

Correct answer: PCI DSS

CHD (Cardholder Data), is not a standard, it is a data classification that refers to credit card information such as primary credit card account numbers, cardholder name, and credit card expiration date. CHD data is sometimes called PCI (Payment Card Industry) data because of its relevance to PCI DSS (Payment Card Industry Data Security Standard).

OSS TMM (Open Source Security Testing Methodology Manual) is a resource published by the Institute for Security and Open Methodologies that provides guidance related to security testing with a focus on communications, human interactions, and physical locations

OWASP (Open Worldwide Application Security Project) is an organization focused on web application security.

64.

OpenIOC is used for what purpose?

Standardizing how threat intelligence is shared

Organizing penetration tests

Programmatically cracking salted passwords

Creating rainbow tables

Correct answer: Standardizing how threat information is shared

OpenIOC is an XML-based schema for formatting messages with indicators of compromise.

The other options are not use cases for OpenIOC.

65.

Tristan, a security analyst at Acme Inc., configures a security appliance to send a web request that triggers a vulnerability scan on a server once a new vulnerability is reported. This is an example of what type of integration?

Webhook

Plug-in

Honeypot

CWE

Correct answer: Webhook

A webhook is a type of software integration that involves one application or service triggering an action in another application or service using a web request.

A plug-in is a program that runs inside of another program.

A honeypot is a system that is intentionally vulnerable to exploits, and it is designed to lure attackers.

CWEs (Common Weakness Enumerations) are standard types and descriptions of common software security issues.

66.

To better understand a recent malware infection at Acme Inc., Kiran, a security analyst, attempts to reverse engineer the malware in a sandbox environment. This is an example of what type of security control?

Operational

Technical

Intelligence-driven

Competitive

Correct answer: Operational

Operational security controls are procedures and practices that improve security posture. Reverse engineering is an example of an operational control.

Technical controls are the different applications, systems, devices, and configurations that help enforce security policies and improve security posture.

"Intelligence-driven" and "competitive" are not standard names for types of security controls.

67.

Which flag is used to make nmap run a stealth scan?

-sS

--stealth

-T --stealth

-T5

Correct answer: -sS

nmap is a popular open-source network scanning utility. It supports multiple flags that change its behavior. The --sS flag causes nmap to run a stealth scan. The -Tx (where x is a number from 0–5) is nmaps timing flag. --stealth is not a valid nmap flag.

68.

Which of these devices should be placed in a screened subnet?

Web server

Accountant's laptop

Air-gapped system

EDR

Correct answer: Web server

A screened subnet is a special portion of the network intended for devices that need to receive connections from an untrusted network like the public Internet. A screened subnet provides isolation from a more secure internal network while still placing devices behind a firewall. Web servers and email servers are often placed in a screened subnet.

An air-gapped system is typically completely disconnected from any network.

An account's laptop would not typically direct connections from the outside world in the same way a web server or email server would.

EDR (Endpoint Detection and Response) tools are a category of security tools focused on detecting and responding to threats on endpoints such as personal computers. EDR solutions typically include threat detection, behavioral analysis, alert notification, and threat neutralization features.

69.

What can a CA use to invalidate a certificate before the certificate's expiration date?

CRL

CASB

HKU

VPC

Correct answer: CRL

A CRL (Certificate Revocation List) is a list of certificates a CA has invalidated or canceled. Adding a certificate to a CRL enables a CA (Certificate Authority) to flag it as invalid. For example, a CA may add a compromised or weak certificate to a CRL before the certificate's expiration date.

CASBs (Cloud Access Security Brokers) provide policy-enforcement checkpoints that can help enable secure access to cloud resources. CASBs can be deployed on-premises or in the cloud.

HKU (HKEY_USERS) is a Windows registry root key. The information underneath this root key is related to user accounts on the system.

A VPC (Virtual Private Cloud) is an environment in a public cloud that is semi-isolated from the rest of the infrastructure. Typically, this isolation is achieved by placing the VPC in a private subnet. VPCs may also include additional security controls.

70.

A recent security breach lead to the randomized usernames and salted passwords of multiple Acme Inc. customers being compromised. Based on the information given, was any CHD compromised. If so, what pieces of data were CHD?

No

Yes, randomized usernames are CHD

Yes, salted passwords are CHD

Yes, salted passwords and randomized usernames are CHD

Correct answer: No

CHD (Cardholder Data) refers to credit card information such as primary credit card account numbers, cardholder name, and credit card expiration date.

CHD data is sometimes called PCI (Payment Card Industry) data because of its relevance to PCI DSS (Payment Card Industry Data Security Standard).

71.

Kai, a business analyst at Acme Inc., is creating a wiki page that details the stages of the threat intelligence cycle and activities that occur during each stage. Which of the following is a stage in the threat intelligence cycle?

Threat data analysis

DevSecOps integration

Post-incident analysis

Eradication

Correct answer: Threat data analysis

The intelligence cycle includes five stages. They are:

1. *Requirements gathering: In this stage, organizations assess past threats, what information could have mitigated past threats, what controls and processes could improve security posture, and define requirements.*
2. *Threat data collection: In this stage, organizations collect threat intelligence data related to their requirements.*
3. *Threat data analysis: In this stage, organizations analyze the data collected in the threat data collection stage.*
4. *Threat intelligence dissemination: In this stage, teams share information with stakeholders such as leadership and security operations.*
5. *Gathering feedback: In this stage, organizations collect feedback on the process to enable continuous improvement.*

72.

Which of the following combinations represents ONLY ONE TYPE of authentication factor?

Smartcard and a code from an authenticator app

PIN number and fingerprint

Password and smartcard

PIN number and a code from an authenticator app

Correct answer: Smartcard and a code from an authenticator app

Common authentication factors include:

- *Knowledge factors - "something you know," e.g., a password*
- *Possession factors - "something you have," e.g., a smartcard or authenticator application*
- *Biometric factors - "something you are," e.g., a fingerprint*
- *Location factors - "where you are," e.g., accessing a system from a specific location*

Smartcard and a code from an authenticator app are both possession factors.

All the other answers contain two different types of factors.

73.

Kim, a security engineer at Acme Inc., deploys updated EDR software to endpoints across the network and configures the EDRs to quarantine software that behaves suspiciously. This is an example of what type of security control?

Technical

Operational

Authentication

Heuristic

Correct answer: Technical

Technical controls are the different applications, systems, devices, and configurations that help enforce security policies and improve security posture.

EDR (Endpoint Detection and Response) tools are a category of security tools focused on detecting and responding to threats on endpoints such as personal computers. EDR solutions typically include threat detection, behavioral analysis, alert notification, and threat neutralization features. Deploying an EDR is an example of a technical security control.

Operational security controls are procedures and practices that improve security posture.

"Authentication" and "heuristic" are not standard names for types of security controls.

74.

Which of the following are examples of forms of active monitoring?

Select all that apply.

- **iPerf**
- **Pings**
- Network taps
- Port mirroring

Active monitoring involves reaching out to systems and proactively capturing data. Pings (e.g., using the "ping" command) are a common form of active monitoring to detect the up/down status of a system. iPerf is a tool that actively measures bandwidth capacity.

Network taps and port mirroring are forms of passive monitoring that do not proactively poll systems — they simply enable traffic to be captured and analyzed.

75.

Alex, a systems administrator at Acme Inc. just ran the command "file /tmp/suspect" to check the file type of "/tmp/suspect". This is the output of the command:

/tmp/suspect: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=088134fc01cb0bfe457089a149f370231ab912c1, for GNU/Linux 3.2.0, stripped

When Alex attempts to read the file with a text editor, there are many non-printable characters displayed. What command would BEST help Alex read any plaintext in the file?

strings

nano

vi

vim

Correct answer: strings

Based on the output of the file command, this is a binary file (it is the binary for the Linux "w" utility). The Linux "strings" command searches files for human-readable text strings. It is typically used to extract human-readable text from binary files (such as complied programs).

The other answers are popular Linux text editors.

76.

Which of the following are stages of the threat intelligence cycle?

Select all that apply.

Threat data analysis

Gathering feedback

Requirements gathering

Lessons learned

Root cause analysis

Retrospective

The threat intelligence cycle includes five stages:

- *Requirements gathering: In this stage, organizations assess past threats, what information could have mitigated past threats, what controls and processes could improve security posture, and define requirements.*
- *Threat data collection: In this stage, organizations collect threat intelligence data related to their requirements.*
- *Threat data analysis: In this stage, organizations analyze the data collected in the threat data collection stage.*
- *Threat intelligence dissemination: In this stage, teams share information with stakeholders such as leadership and security operations.*
- *Gathering feedback: In this stage, organizations collect feedback on the process to enable continuous improvement.*

Lessons learned, root cause analysis, and retrospectives are common practices in cybersecurity and software development, but they are not specific threat intelligence cycle stages.

77.

Acme Inc. is using OAuth to provide identity services for a web application. Which of the following OAuth parties corresponds to the web application in this scenario?

Client

Resource Owner

Access Server

Authorization Server

Correct answer: Client

There are four parties in OAuth flows. They are:

- *Clients - Applications used by end users*
- *Resource Owners - End users*
- *Resource Servers - Servers from a service resource owners want applications to use*
- *Authorization Servers - Servers from the identity provider*

78.

Dana, a security analyst at Acme Inc., is reviewing network traffic and notices an unusual amount of peer-to-peer traffic on one of the VLANs. This is a potential example of what?

IOC

DLP

CWE

PHI

Correct answer: IOC

An IOC (Indicator of Compromise) is data that implies a system or network may have been compromised. Common IOC examples include logins from dormant user accounts, unexpected configuration file changes, unusual network activity, and unexpected services running on a system. Irregular peer-to-peer traffic is a common potential IOC that could suggest the presence of a threat actor or malware.

DLP (Data Loss Prevention) is a category of security technologies designed to prevent data exfiltration and data loss.

CWEs (Common Weakness Enumerations) are standard types and descriptions of common software security issues.

PHI (Personal Health Information) is a category of personal information related to healthcare.

79.

The combination of a vulnerability an organization has and the threats that could exploit it equal what?

Risk

Mitigation factor

IOC

OSINT

Correct answer: Risk

Risk = threat × vulnerability is a common way to express the idea that an organization's risk is a combination of the threats it faces and its vulnerabilities.

Mitigation factor is not a standard term. Mitigations in general reduce risk.

An IOC (Indicator of Compromise) is data that implies a system or network may have been compromised. Common IOC examples include logins from dormant user accounts, unexpected configuration file changes, unusual network activity, and unexpected services running on a system.

OSINT (Open Source Intelligence) is data collected and analyzed from publicly available sources such as websites, social media, and WHOIS records.

80.

Hao, an employee at Acme Inc., uses their Google identity to access websites and services with different identity management systems that are not hosted by Google. This is an example of what type of technology?

Federation

Passwordless

Serverless

Identity enumeration

Correct answer: Federation

Federation is an identity management process that enables an identity and associated information to be used across different identity management systems. Using a Google, GitHub, Microsoft, or LinkedIn identity to log in to services hosted by other third-party entities is a common example of federation.

Passwordless authentication involves authenticating without a password. Typically, passwordless authentication uses a single factor that is considered more secure than traditional passwords.

Serverless computing is a form of computing where functions are executed as they are called and the underlying server infrastructure is abstracted away from the user. AWS Lambda, Google App Engine, and Azure Functions are examples of serverless computing. Serverless computing is sometimes called FaaS (Function as a Service).

Identity enumeration is incorrect. In general, enumeration is a way threat actors capture information about a target or from a system.

81.

Acme Inc. operates a corporate datacenter with multiple servers. An air conditioner failure caused a database server to overheat and lose the last two hour's worth of data. The threat in this scenario is an example of which of the four threat categories identified by NIST?

Structural

Temperature

Adversarial

Accidental

Correct answer: Structural

NIST (The National Institute of Standards and Technology) identifies four categories of threats. They are:

- *Adversarial threats that try to intentionally harm an organization*
- *Accidental threats which can occur when individuals make a mistake*
- *Structural threats which can occur when equipment, resources, software, or infrastructure fail or are depleted*
- *Environmental threats that stem from disasters (e.g., hurricanes, fires, or power outages)*

Loss of data from an air conditioner failing is an example of a structural threat.

Temperature is not one of the four threat categories identified by NIST.

82.

Taylor, a security administrator at Acme Inc., is attempting to find specific messages in a "cysa.log" file that include the string "Auth" or the string "Denied". Taylor is at a Bash shell prompt in the same directory as the cysa.log file. Which command should Taylor run to see results that include the string "Auth" or the string "Denied"?

grep -e Auth -e Denied cysa.log

grep -k Auth -2 Denied cysa.log

grep -k Auth Denied cysa.log

grep Auth Denied cysa.log

Correct answer: grep -e Auth -e Denied cysa.log

The grep command is used to search files for patterns and return content that matches. The grep command supports different flags that modify its behavior. For example, the -i flag makes a grep search case insensitive (case sensitive is the default behavior).

Other common grep flags include:

- *"-c" counts how many matches there are for a specific pattern*
- *"-n" shows the line and line number for a match*
- *"-v" shows all lines that are not a match*
- *"-r" reads files under a directory recursively*
- *"-e" searches a specified pattern(s)*

-k is not a valid grep flag. Specifying the patterns without the -e flag would create an error for the second pattern ("Denied") as grep would treat it as a file to search for the first pattern ("Auth").

83.

Mahan, a network administrator at Acme Inc., wants to limit network access to trusted MAC addresses. What access control should Mahan use?

Port security

VDI

NTP

Protocol analysis

Correct answer: Port security

Port security is an access control that limits network access based on MAC (Media Access Control) addresses.

VDI (Virtual Desktop Infrastructure) is a form of virtualization that provides access to desktop operating systems by streaming them from centralized hardware.

NTP (Network Time Protocol) is a network protocol used to synchronize time across systems. NTP servers enable multiple client systems to synchronize their time with an authoritative source and help keep timestamps in sync throughout a network.

A protocol analyzer is a tool for granular analysis of network traffic. Protocol analysis is not correct.

84.

An API server is provides users with access to resources after they are authenticated using the OAuth 2.0 protocol. The API server in this scenario is which of the four parties involved in OAuth flows?

Resource Server

Resource Owner

Client

Authorization Server

Correct answer: Resource Server

There are four parties in OAuth flows. They are:

- *Clients - Applications used by end users*
- *Resource Owners - End users*
- *Resource Servers - Servers from a service resource owners want applications to use*
- *Authorization Servers - Servers from the identity provider*

An API (Application Programming Interface) server is a simple example of a Resource Server for OAuth flows.

85.

Acme Inc. uses centralized server hardware to stream Windows desktop operating system access over the network for employees to use. What type of virtualization is this?

VDI

VPC

VPN

VLAN

Correct answer: VDI

VDI (Virtual Desktop Infrastructure) is a form of virtualization that provides access to desktop operating systems by streaming them from centralized hardware.

A VPC (Virtual Private Cloud) is an environment in a public cloud that is semi-isolated from the rest of the infrastructure. Typically, this isolation is achieved by placing the VPC in a private subnet. VPCs may also include additional security controls.

A VPN (Virtual Private Network) provides an encrypted tunnel over an insecure network to secure communications and connect networks and endpoints.

VLANs (Virtual Local Area Networks) are logical networks that can provide logical network segmentation to separate portions of a network. VLANs are typically implemented using a router or managed switch that supports VLAN tagging.

86.

The Acme Inc. development team is launching a project to build a new app using serverless architecture. Which of the following services or tools will be MOST useful in building the app?

Lambda

Wireshark

Snapdragon

Bastion host

Correct answer: Lambda

Serverless computing is a form of computing where functions are executed as they are called and the underlying server infrastructure is abstracted away from the user. AWS Lambda, Google App Engine, and Azure Functions are examples of serverless computing. Serverless computing is sometimes called FaaS (Function as a Service).

Wireshark is a network analyzer and packet capture utility that would not directly help build a serverless application.

Snapdragon is a type of processor.

A bastion host is a type of computer that is used to provide access from one network to another.

87.

Which of the following is an example of a location factor in authentication?

User location

Password

Smartcard

Authenticator application

Correct answer: User location

Common authentication factors include:

- *Knowledge factors - "something you know," e.g., a password*
- *Possession factors - "something you have," e.g., a smartcard or authenticator application*
- *Biometric factors - "something you are," e.g., a fingerprint*
- *Location factors - "where you are," e.g., accessing a system from a specific location*

Authentication factors can be combined to improve security. MFA (Multifactor Authentication) combines two or more different authentication factors in the authentication process.

88.

Kalani, a security engineer at Acme Inc., is ranking risks on a 0-100 scale based on a variety of factors related to the threats. This is an example of what type of risk assessment?

Quantitative

Qualitative

Mathematic

Baselined

Correct answer: Quantitative

Risk assessments that are based on numerical values are typically described as quantitative risk assessments.

Qualitative risk assessment is a form of risk assessment that describes risk without numerically assessing or ranking it. Using a risk matrix to categorize risks as "low," "medium," or "high" is an example of qualitative risk assessment.

Mathematic and baselined are not common names for risk assessment types.

89.

Dani, a network architect at Acme Inc., is using 802.1X as part of the design for a new branch office. Which of the following statements about 802.1X are TRUE?

Select all that apply.

It is a type of out-of-band NAC

It is an agent-based NAC implementation

It is a type of in-band NAC

It is an agentless NAC implementation

Agent-based NAC (network access control) solutions require that devices run special software to communicate with the authenticating service. NAC implementations using the 802.1X use an agent-based model. Agentless NAC does not require special software.

In-band NAC refers to approaches to NAC in which a NAC appliance sits inline between devices requesting access and the network resources that can be accessed. Out-of-band NAC solutions use authentication servers that are not inline between devices requesting access and the network resources that can be accessed. 802.1X uses an out-of-band approach to NAC.

90.

A smart fridge vendor added a hidden security feature that records all the conversations of their users and parses the recorded text for trade secrets and confidential information they can use to increase profits.

Which category of threat actor BEST describes the smart fridge vendor?

Supply chain

Technology exploiting

Organized crime

Insider threat

Correct answer: Supply chain

There are multiple different threat actor types CySA+ candidates should be familiar with, including:

- *Nation-state: These threat actors are backed by a country's government, are highly sophisticated, and have many resources.*
- *Organized crime: These threat actors are typically focused on organized attacks with a financial motive. In recent years, ransomware attacks have been a common attack used by organized crime threat actors.*
- *Hacktivists: These threat actors are motivated by a political or philosophical ideology.*
- *Script kiddies: These threat actors are unsophisticated and typically depend on readily available tools and low-complexity attacks.*
- *Insider threats: These threat actors come from within an organization. They are particularly risky because insiders often already have access to systems.*
- *Supply chain: These threat actors are part of hardware or software supply chains or directly attack hardware or software supply chains to compromise systems and data.*

The smart fridge vendor in the example is a supply chain threat actor because they supply equipment to end users and leveraged that supply chain for malicious reasons.

91.

Yuri, a system administrator at Acme Inc., wants to check if an operating system .iso file is legitimate. Which of the following techniques should Yuri use?

Compare the file's SHA256 hash to a known legitimate copy

Run the "file" command against the local copy of the .iso file

Run the "file" command against a remote copy of the .iso file

Use DMARC to compare the two files

Correct answer: Compare the file's hash to a known legitimate copy

File hashes provide users with a way to determine if two files are the same. Hashes are one-directional functions that enable data of an arbitrary size to be transformed into a fixed size. Strong hash functions greatly reduce or reasonably eliminate the chance of a duplicate hash being generated unless two files are the same. SHA256 is a popular example of a hashing algorithm.

The "file" command is used to detect a file's category (such as binary or ASCII text). It would not help directly confirm if the .iso file in the example is legitimate.

DMARC (Domain-Based Message Authentication, Reporting, and Conformance) is an email security option that uses DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) to authenticate messages and enable users to determine if a message should be accepted.

92.

The Acme Inc. security operations team has completed the analysis of threat intelligence information. They are now distributing reports to management and IT on their findings. What stage of the threat intelligence cycle is in progress?

Threat intelligence dissemination

SecOps planning

Continuous DevSecOps deployment

Requirements gathering

Correct answer: Threat intelligence dissemination

The intelligence cycle includes five stages. They are:

1. *Requirements gathering: In this stage, organizations assess past threats, what information could have mitigated past threats, what controls and processes could improve security posture, and define requirements.*
2. *Threat data collection: In this stage, organizations collect threat intelligence data related to their requirements.*
3. *Threat data analysis: In this stage, organizations analyze the data collected in the threat data collection stage.*
4. *Threat intelligence dissemination: In this stage, teams share information with stakeholders such as leadership and security operations.*
5. *Gathering feedback: In this stage, organizations collect feedback on the process to enable continuous improvement.*

The security operations team is sharing information they have analyzed. Therefore, they are in the threat intelligence dissemination stage.

SecOps planning, and continuous DevSecOps deployment are incorrect answers based on other lifecycle processes such as the SDLC (Software Development Lifecycle).

93.

What type of application and service monitoring would likely use ping?

Up/down monitoring

Transactional logging

Application and service logging

SNMP monitoring

Correct answer: Up/down monitoring

There are several forms of application and service monitoring CySA+ candidates should be familiar with, including:

- *Up/down monitoring - Determines if a service is running at all*
- *Performance monitoring - Determines if speed and responses are working as expected*
- *Transactional logging - Records activity such as steps the users take in an application*
- *Application and service logging - Records logs about service or application status and functions*

ping is a common command used to verify network connectivity between hosts and is one method that can be used to check up/down status of a service.

SNMP (Simple Network Management Protocol) is a protocol that is typically used to monitor network devices and could also be used as part of up/down monitoring.

94.

Hao is a security engineer at Acme, Inc. Cruz is tasked with deploying a secure computer terminal that is physically segmented from the corporate network. How can Hao BEST complete this task?

Implement an air gap

Place the terminal in a VPC

Create a VLAN for the terminal

Create a point-to-point VPN

Correct answer: Implement an air gap

An air gap physically separates systems from other systems or networks. An air gap is a type of physical segmentation. The other answers VPC (Virtual Private Cloud), VLAN (Virtual Local Area Network), and VPN (Virtual Private Network) are forms of logical segmentation or isolation.

95.

Rosario, a junior software engineer at Acme Inc., deploys a script that makes sensitive company data public. The intent of the script was to perform a data backup and Rosario did not intend to leak the data. The leaked data gives Acme Inc.'s competition details about Acme Inc.'s proprietary business process. The threat in this scenario is an example of which of the four threat categories identified by NIST?

Accidental

Human-made

Environmental

Adversarial

Correct answer: Accidental

NIST (The National Institute of Standards and Technology) identifies four categories of threats. They are:

- *Adversarial threats that try to intentionally harm an organization*
- *Accidental threats which can occur when individuals make a mistake*
- *Structural threats which can occur when equipment, resources, software, or infrastructure fail or are depleted*
- *Environmental threats that stem from disasters (e.g., hurricanes, fires, or power outages)*

While many threats are human-made threats, "human-made" is not one of the four threat categories identified by NIST.

96.

Which of the following techniques provides physical segmentation?

Air gap

VPC

VLAN

VPN

Correct answer: Air gap

An air gap physically separates systems from other systems or networks. An air gap is a type of physical segmentation.

VPC (Virtual Private Cloud), VPN (Virtual Private Network), and VLAN (Virtual Local Area Network) are all examples of logical isolation.

97.

Acme Inc. network architecture is designed so that functionality such as SD-WAN, CASB, antimalware tools, and firewall as a service are deployed in a converged fashion to provide tight security controls at the network and endpoint layer for their highly decentralized network. What type of network architecture does Acme Inc. use?

SASE

Passwordless

PAM

Serverless computing

Correct answer: SASE

SASE (Secure Access Service Edge or Secure Access Secure Edge, pronounced "sassy") is a network architecture that combines SD-WAN (Software-Defined Wide Area Networking) and security functions with a focus on endpoint and network layer security that are intended to meet the needs of modern decentralized networks (as opposed to centralized, datacenter-based networks).

Passwordless authentication involves authenticating without a password. Typically, passwordless authentication uses a single factor that is considered more secure than traditional passwords.

PAM (Privileged Access Management) is the set of technologies and practices involved in securing and managing accounts, access, and permissions for systems and entities throughout an organization. PAM helps organizations enforce the principle of least privilege to limit access to what is required to accomplish legitimate tasks.

Serverless computing is a form of computing where functions are executed as they are called and the underlying server infrastructure is abstracted away from the user. AWS Lambda, Google App Engine, and Azure Functions are examples of serverless computing. Serverless computing is sometimes called FaaS (Function as a Service).

98.

Which of the following is a federated identity technology that supports authentication but does NOT support authorization?

OpenID

SAML

NTP

SD-WAN

Correct answer: OpenID

OpenID is a federated identity technology that supports authentication. OpenID does not support authorization.

SAML (Security Assertion Markup Language) is a federated identity technology that supports authentication and authorization. Enterprise-grade authentication and authorization implementations in organizations that use Linux is a typical use case for SAML.

NTP (Network Time Protocol) is a protocol for synchronizing time with a server or pool of servers. NTP helps devices on a network maintain synchronized time settings and timestamps.

SD-WAN (software-defined wide area networking) is a form of SDN (Software-Defined Networking) focused on WAN (Wide Area Network) traffic.

99.

Acme Inc. deployed multiple web servers and cloud workloads with the sole purpose of exposing fake targets to attackers and slow down malicious network scans. This is an example of what threat hunting technique?

Tarpit

Warm servers

Cluster defense

Swampping

Correct answer: Tarpit

A tarpit is an active defense technique that exposes fake targets to slow down and confuse attackers.

The other responses are not standard threat hunting techniques.