Data masking involves replacing sensitive data with fictional or scrambled data. While this could address the CPO's concerns, the development team's need for real data to perform functionality tests might not be met. Data anonymization strikes a balance between privacy and functionality, making it the most suitable option in this scenario.

Data anonymization is the alteration process of personally identifiable information (PII) in a dataset, to protect individual identification. This way the data can be used and still be protected.

Example Code:

<ahref="https://www.company.com/payto.do?routing=00001111&acct=22223334&amount=250">Click here to unsubscribe</a>

This is a XSRF

CSRF or XSRF redirects you to something you didn't intend to go to when clicking a link

With XSRF/CSRF you are forcing the user into performing an action they are already allowed to do. In this case you are tricking the user to click a link forcing them to transfer funds.

A password history policy makes it harder for attackers to reuse stolen credentials.

Domain services, specifically Active Directory (AD) in a Windows environment, provide centralized management and organization of network resources, including computers, users, and groups. It allows for efficient identification and grouping of systems based on various attributes, such as location, role, and service level.

ISO 27001 is an international standard to improve an organization's information security management systems, while NIST CSF helps manage and reduce cybersecurity risks to their networks and data.

High data entropy: In cryptography, entropy is used to produce random numbers, which in turn are used to produce security keys to protect data while it's in storage or in transit. The greater the quality of random number generation (RNG), the greater the quality of random keys produced, and thus the higher the security value of the key

The first step the company should perform to restrict emailing of PHI (Protected Health Information) documents is Classification.

Agile methodology is a way to manage a project by breaking it up into several phases. It involves constant collaboration with stakeholders and continuous improvement at every stage. Once the work begins, teams cycle through a process of planning, executing, and evaluating.

Waterfall - A sequential development process that flows like a waterfall through all phases of a project (analysis, design, development, and testing, for example), with each phase completely wrapping up before the next phase begins.

A TAXII server is a client that exchanges standardized and anonymized cyber threat intelligence among users. It works as a venue for sharing and collecting Indicators of compromise, which have been anonymized to protect privacy.

The GREATEST security concern when outsourcing code development to third-party contractors for an internet-facing application is the possibility of an unknown backdoor being introduced into the code. An unknown backdoor refers to unauthorized access points deliberately inserted into the software without the knowledge or consent of the organization.

FAR - False Acceptance Rate

FRR - False Rejection Rate

NIST - Frameworks

ISO - Standard

Patch should be deployed last in the Production environment.

To ensure that the new backup server rooms are not susceptible to the same vulnerabilities as the existing server room, it's a **good practice to diversify the hardware vendors.** This approach reduces the risk of common vulnerabilities affecting all systems in the same way. Different vendors may use different hardware designs, software stacks, and security configurations, which can provide a level of diversity and defense in depth.

WAF: Web Application Firewall

Broad range of information that is sensitive to a specific organization: Proprietary

Best way to harden cloud-based applications: (Cloud Access Security Broker) CASB & (Next-Generation Secure Web Gateway) NG-SWG

Fingerprint a web server: Use the curl command

Asymmetric encryption: the sender's private key and decrypted with the sender's public key.

Phishing **emails with a word document** attachment typically **will have macros** that can be run for malicious purposes. Macros are scripts that can run whatever you want and however many times you want it to run, it's generally used for automating frequently used tasks.

The most appropriate account type for an application that needs to read and write data to a shared database is a "**Service" account**. Service accounts are used to run specific services or applications in a controlled manner, allowing them to access resources and perform specific actions on behalf of the application or service they represent.

Host1.pcap file the .pcap stands for packet capture so use wireshark

An HVAC (Heating, Ventilation, and Air Conditioning) system can provide both detective and corrective controls for thermal regulation

Don’t Throw Sausage Pizza

Development >> Testing >> Staging >> Production

Dynamic analysis means that the application is tested under "real world" conditions using a staging environment.

A jump server, jump host or jump box is a system on a network used to access and manage devices in a separate security zone. A jump server is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them

Zone transfers = DNSSEC

NGFW = Next generation firewall

The security analyst should perform action D: Utilize behavioral analysis to enable the SIEM’s learning mode. This approach allows the Security Information and Event Management (SIEM) system to learn what is considered normal behavior for each user and thus reduce the number of false positives. It can help in creating a baseline of normal operations and reduce noise.

Third party software vendors are part of the supply chain.

AV = Antivirus

The file was then used by another process to execute a payload.

The concept of connecting a user account across the systems of multiple enterprises is FEDERATION

Geolocation vs. Geofencing: Fencing used for more local restrictions. Geolocation used for an entire country.

A **risk register** is a document that contains ranked and ordered information on the likelihood and potential impact of various risks that may affect business processes and systems. It typically includes information on both threats and vulnerabilities and assesses the risk to the organization. The risk register also highlights the effectiveness of existing controls (mitigating controls) in reducing the impact or likelihood of the identified risks. It serves as a key tool for risk management and helps organizations prioritize and manage risks effectively.

Version control, also known as source control, is the process of tracking and managing changes to files over time

"A secure web gateway (SWG) protects users from web-based threats in addition to applying and enforcing corporate acceptable use policies."

Tokenization is the best approach for storing credit card information securely in a database while allowing for an easy reordering process. Tokenization is a process in which sensitive data, such as credit card numbers, is replaced with a randomly generated token. The actual credit card information is securely stored in a separate, isolated system, often managed by a third-party payment processor.

Annualized Rate of Occurrence (ARO), BEST describes the estimated number of devices to be replaced next year.

Annual Loss Expectancy (ALE), is the expected monetary loss per year due to a risk. This would not be the most appropriate measure for estimating the number of mobile devices to be replaced.

A load balancer can monitor the backend servers and direct traffic to working servers when other servers go offline. It can also maintain session persistence.

A sandbox is a security mechanism that separates running programs and restricts their access to system resources. This can help prevent custom malware from causing harm to the organization’s systems.

Example question:

A company is implementing BYOD and wants to ensure all users have access to the **same cloud-based services. Services = SaaS**

The preparation phase is when the organization is preparing for the attack. Tuning the SIEM is just providing the latest threat information to the system for preparation.

Phases of the Incident Response Plan:

1. Preparation - Preparing for an attack and how to respond

2. Identification - Identifying the threat

3. Containment - Containing the threat

4. Eradication - Removing the threat

5. Recovery - Recovering affected systems

6. Lessons Learned - Evaluating the incident response, see where there can be improvements for a future incident.

Log Collector forwards the logs to a central source

A systems analyst should include the following information in the new digital forensics chain-of-custody form:

The date and time & The provenance of the artifacts

DNS logs can contain a record for every query and response. It can show the IP addresses and domain names that your system should/shouldn't be communicating with, it can reveal malware calling out to its command-and-control server, or data transfers to non-company locations. This is one of the reasons why DNS logs are some of the most valuable logs to import into a SIEM system.

VPC = Virtual Private Cloud

A USB data blocker allows you to plug into Wi-Fi hotspots and USB charging ports safely. These solutions eliminate the risk of infecting your phone, laptop, or tablet with malware, and also prevent hackers from install and running malicious code on your system.

SED = Self Encrypting Drive

The network manager should use an Access Control List (ACL) to control the traffic between the segments. An ACL is a network filter that can be used to control the flow of network traffic based on various criteria, such as the source or destination of the traffic, the type of traffic, or the port number. By configuring an ACL, the network manager can specify which types of traffic are allowed to pass between the network segments and which are not. This will help to prevent unauthorized or malicious traffic from passing between the segments and potentially compromising the network.

Compensating Controls are good against Zero day