



















































What is the primary purpose of internal compliance reporting?

Overall explanation

OBJ: 5.3 - The primary purpose of internal compliance reporting is to provide updates on compliance status, identify potential issues, and inform the organization's management about its adherence to regulatory requirements and policies. Internal compliance reporting provides information about what exists to a company's managers.  It doesn't involve requesting information. Internal compliance reporting is for the use of the company itself and is not meant to be shown to third party auditors. External compliance reporting would provide information to third party auditors. Internal compliance reporting is not intended for public disclosure; it is focused on internal communications within the organization.

**To provide compliance updates to the organization's management**

Which of the following statements BEST explains the importance of employee retention in securing an organization?

**Employee retention helps to maintain institutional knowledge and expertise in managing security automation.**

OBJ: 4.7 - Employee retention means that the organization can retain experienced staff who have gained valuable institutional knowledge and expertise in managing security automation and orchestration. This accumulated knowledge helps ensure the smooth functioning and effective utilization of these processes. There is no evidence that retaining employees has an impact on avoiding social engineering attacks. Employee retention provides institutional knowledge which makes managing security automation easier. High employee retention means that employees have been with the organization for a longer time, and they would have had more exposure and experience with the automated security processes. This can lead to a deeper understanding, which in turn can improve response times in handling security incidents. Employee retention is not directly related to the need for automation and orchestration. Regardless of the employee retention rate, the benefits of automation and orchestration in secure operations remain valid.

**In Dion Training's data management framework, Scherazade determines the why and how data will be collected. She then directs Sahra what should be done with the data that is collected. Which of the following BEST describes the roles that Scherazade and Sahra have?**

**The data controller and the data processor.**

OBJ: 5.4 - Scherazade is the data controller because the data controller determines how and why the data is collected and used. Sahra is the data processor because the data processor follows the data controller's directions for using the data that is collected. The data owner is the person who is ultimately responsible for the confidentiality, integrity, and availability of the data.  The data custodian handles the management of the system used to store and collect the data. The data owner is the person who is ultimately responsible for the confidentiality, integrity, and availability of the data.

As a security analyst, you are investigating a suspicious file activity incident. While examining metadata associated with different files, which of the following pieces of information is NOT typically presented in metadata?

OBJ: 4.9 - Metadata does NOT normally include the file's extension. The name of the user who created the file is often included as part of the file's metadata. This is crucial information during an investigation of unauthorized file access or alteration. File size is a common piece of metadata. This could potentially be useful in an investigation if, for example, a file's size significantly changes without a clear reason. Date and time of last modification is an integral part of metadata. This can help establish timelines of activity and identify any unexpected changes, which is crucial during an investigation.

You were recently hired by a large software company that specializes in developing mobile applications. After receiving your username and password, you are required to provide a fingerprint scan using a biometric reader to gain access to the company's development environment. Which type of multi-factor authentication (MFA) factor does the biometric reader represent?

OBJ: 4.6 - The MFA factor being used in the scenario is Something you are. Biometric authentication, such as a fingerprint scan, falls under the category of Something you are. Biometric factors use unique physical characteristics or behavioral traits of an individual for authentication, making them a strong and convenient form of MFA. Something you know refers to authentication factors that involve knowledge of a specific piece of information, such as a password or PIN. In the scenario, the employee is not providing any information to authenticate, but rather using a fingerprint scan, which is a biometric factor. Somewhere you are is a location-based authentication. It is a type of contextual authentication that considers the user's geographic location as an additional factor. Something you have refers to authentication factors that involve possessing a physical object or token, such as a smart card, security token, or mobile device. In the scenario, the employee is not using any physical object or token, but rather a biometric scan (fingerprint).

Which of the following is NOT true about the importance of Security Information and Event Management (SIEM)?

**SIEM systems can aid in the procurement and asset management of secure software systems.**

OBJ: 4.4 - SIEM systems are not primarily used for software procurement or asset management. Their primary purpose is to provide real-time analysis of security alerts and to offer a holistic view of an organization's security scenario. They are not involved in tasks such as procurement and management of hardware. SIEM systems can indeed create and maintain a record of an organization's IT equipment as a part of their comprehensive data collection. One of the critical roles of SIEM is the real-time monitoring and analysis of security alerts across an organization's network. SIEM systems collect and aggregate log data from an array of sources within an organization’s IT infrastructure, providing a centralized view of the security landscape.

Dion Training has implemented fixes for buffer overflow vulnerabilities in their application. To validate the effectiveness of their remediation efforts, which approach should be considered?

**Contracting a cybersecurity firm for targeted vulnerability assessments.**

OBJ: 4.3 - A specialized assessment by a third-party can evaluate specific fixes, such as those for buffer overflows, ensuring they've been effectively addressed. While threat intelligence is valuable, it isn't a direct method to validate remediation of specific vulnerabilities. Training is essential but does not directly measure the effectiveness of applied fixes for existing vulnerabilities. Performance metrics might indicate system health, but they do not directly review the remediation of buffer overflow issues.

Which of the following data considerations pertains to data that is currently being processed by a computer?

Overall explanation

OBJ: 3.3 - Data in Use refers to active data which is currently being processed or manipulated by a computer. Data at Rest indicates data that is not currently being processed or moved, typically stored data. While Data in Transit involves data movement, it doesn’t specifically refer to data being processed by a computer. Data Sovereignty governs the jurisdiction and legalities of data based on its geographical location, not its active usage.

What is the main danger that comes from Shadow IT?

OBJ: 2.1 - Shadow IT is a type of threat actor that is the result of unauthorized or unapproved IT systems or devices within an organization.  Shadow IT can introduce security risks because the unauthorized system or device may provide attackers with a way to gain access to an otherwise secure system. In most cases, the unapproved system or device will not create any disruption to the services. The unapproved system or device will only lead to data losses if a threat actor can use it to gain access and then leverage the access to exfiltrate data.  Therefore, data losses aren't the main danger. An unapproved system or device will only lead to financial losses if a threat actor can use it to gain access and then leverage the access to create financial losses.  Therefore, financial losses aren't the main danger – a larger attack vector

In a business process analysis (BPA), which factor encompasses the human resources and additional support needed to carry out a mission essential function?

**Staff**

OBJ: 5.3 - Staff is a component of a BPA identifies the personnel and various supports that are essential for the execution of a critical function. Though process flow describes the operational steps in detail, it does not specifically focus on the personnel and support resources. Outputs concern the data or products generated by the function, not the resources that support the function. Inputs define the required information for a process and the implications of their timing, not the human and support resources.

Dion Training Solutions recently experienced a cyberattack that resulted in significant data loss and financial implications. In an effort to protect against future financial consequences, the company decides to explore measures that could help mitigate these risks. Which action is Dion Training Solutions likely to take?

Dion Training Solutions recently experienced a cyberattack that resulted in significant data loss and financial implications. In an effort to protect against future financial consequences, the company decides to explore measures that could help mitigate these risks. Which action is Dion Training Solutions likely to take?   
**Purchase cyber liability insurance**

OBJ: 4.3 - Cyber liability insurance is designed to offset costs involved with recovering from a cyber breach or similar events. This will financially safeguard Dion Training Solutions against potential repercussions of future cyber incidents. While encryption can secure data and prevent unauthorized access, it doesn't offer financial coverage against cyber breaches. While IDS can alert and help prevent unauthorized access, it does not provide financial protection against the consequences of cyberattacks. Migration might enhance security, but it doesn't shield the company from the financial implications of a cyberattack.

Which of the following BEST describes the data owner's role in an organization's data governance framework?

OBJ: 5.1 - The owner's role is accountable for the data's security and compliance with the organization's strategic objectives. Outlines the purposes, conditions, and methods of personal data processing to comply with GDPR pertain to the controller role, not the owner. While the owner is responsible for the level of security, the actual implementation of encryption is usually handled by IT or security teams.  Providing detailed recommendations on specific security controls to be included in the ISMS is typically associated with specialized committees or the ISO/IEC 27002 standard, not directly with the owner.

An organization is looking to protect sensitive financial data stored in spreadsheets. Which of the following methods would be the MOST effective in ensuring the data's confidentiality and integrity?

**Data encryption and digital watermarking**

OBJ: 3.3 - Data encryption and digital watermarking the spreadsheet ensures unauthorized parties cannot view its content, and digital watermarking embeds a hidden mark to track and verify the document's authenticity and integrity. While version control and backup are crucial for maintaining data history and recovery, neither directly ensures the spreadsheet's confidentiality or verifies its integrity. While network monitoring and firewall protect against unauthorized access and attacks, they don't directly ensure the confidentiality or integrity of specific spreadsheet data. Password protection restricts access, and read-only access prevents modifications, but neither ensures data confidentiality from unauthorized decryption or verifies its integrity against all forms of tampering.

Tara, a database specialist, is planning out the way in which data will be stored. She has decided to substitute the sensitive data with non-sensitive representations. The sensitive data and non-sensitive representation will be stored in a separate database. Which data security technique is likely being used?

**Tokenization**

OBJ: 3.3 - Tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token. The token and the data it substitutes are stored in a secure database. If the original data is needed, it can be accessed using the token and querying the database. The token will be a different size and have a different structure than the original data so the token can’t be used to decipher the original data. Hashing is the process of converting an input of any length into a fixed size string of text, using a mathematical function. The process explained above doesn't indicate that a mathematical function is being used. Non-human readable data refers to a form of data that needs a computer or special software to interpret. In the case above both sets of data are human readable. Obfuscation is the hiding or camouflaging of information to prevent access to it. Obfuscation doesn't involve an additional database of linked sensitive and non-sensitive data.

Which attribute of a threat actor refers to their ability to develop unique exploit techniques and tools?

**Capability**

OBJ: 2.1 - Capability pertains to a threat actor's proficiency in devising new exploit techniques and tools. It can range from using commonly found attack tools to creating zero-day exploits in various systems. Those with the highest capabilities can even deploy non-cyber tools, such as political or military assets. Sophistication relates to the level of intricacy and advancement of a threat actor's methods and tools, but does not directly address their skill in crafting novel exploits. While funding can boost a threat actor's capabilities by providing them the means to acquire resources, it doesn't specifically denote their expertise in developing unique exploits. While resources can aid in bolstering a threat actor's capabilities, this term primarily refers to the tools and personnel that a threat actor can access or utilize.

Which of the following BEST describes the significance of key length in encryption standards?

**It sets a minimum for key length**

OBJ: 1.4 - Key length in encryption determines the minimum length that an encryption key can be to ensure a strong level of security. While length will impact the key's complexity, the key length doesn't set other factors beyond the minimum length.

You are a security analyst at Dion Training and you are investigating a security breach that occurred on one of your web servers. You find out that an attacker was able to exploit a vulnerability in the web application and gain access to the server. You also find out that the hacker used a tool that she obtained on a website. The tool automated the exploitation process. What type of threat actor are you most likely dealing with?

**Unskilled attacker**

OBJ: 2.1 - An unskilled attacker is one that lacks technical expertise or sophistication. Unskilled attacker often use a tool that automate the exploitation process, requiring minimal user input, such as a script or an exploit kit. A nation-state threat actor is one that represents the interests of a sovereign country. A nation-state threat actor may use a tool that automates the exploitation process and requires minimal user input, but these types of tools are often easy to detect. Non-state actors are much more likely to use more advanced or customized tools which are much harder to detect. Organized crime is a group of individuals that operates in a coordinated and structured manner to engage in illegal activities for profit or power. Organized crime may use a tool that automates the exploitation process and requires minimal user input, but they have the funding and expertise to use more sophisticated or targeted tools which are less likely to be detected. A hacktivist is one that uses cyberattacks to express dissent or support for a cause or movement. A hacktivist may use a tool that automates the exploitation process and requires minimal user input, but they may also use more creative or symbolic tools depending on their message.

Geneve has a well paid job with the government of Arus and has authorized access to sensitive data. She thinks the government is corrupt. Recently, she has been approached by an agent for the country of Erastein. The agent offers to pay her a lot of money to exfiltrate data from her government. She was told that Erastein will be negotiating a treaty with Arus and the documents will help Erastein get land they have long wanted. Which of the following BEST describes Geneve's motivation for the data exfiltration?

OBJ: 2.1 - Political motivations are based on an attacker's view that an organization's actions are unjust or contrary to the attacker's political beliefs.  In this case, Geneve's view that the government is corrupt allows her to justify her actions.   Service disruption is the act of interrupting or degrading the availability or performance of a system or network. An insider threat actor may conduct service disruption as part of their cyberattacks, but it doesn't usually achieve their goals. There is no indication that Geneve wants to disrupt service in this scenario. Financial gain is the motivation that drives a threat actor to conduct cyberattacks for profit. An insider threat actor may be motivated by financial gain, and usually target financial institutions, businesses, or individuals for fraud, theft, ransomware, etc. In this case, Geneve is well paid, so financial gain is less likely to be a motivation for her actions Espionage is the act of obtaining secret or confidential information without the permission of the holder of the information. An attacker may use espionage to support their other motivations, such as sabotage, cyberwarfare, revenge, blackmail, etc. While the government of Erastein is interested in gaining a competitive advantage, Geneve is motivated by her perception that the government is corrupt

**Which of the following procedures outline the steps for controlling alterations to IT systems within an organization?**

**Change management**

OBJ: 5.1 - The change management procedure outlines the steps and guidelines for managing changes to IT systems within an organization. It includes processes for requesting, evaluating, approving, implementing, and reviewing changes to minimize the risk of disruptions and ensure that changes are carried out in a controlled and coordinated manner. Onboarding and Offboarding involves the processes and tasks related to welcoming new employees (onboarding) and handling the departure of employees (offboarding) within an organization. While important for managing personnel transitions, it is not directly related to changes in IT systems. Incident response procedure defines the steps for detecting, analyzing, responding to, and recovering from cybersecurity incidents and data breaches. While essential for handling security incidents, it is not directly related to managing changes to IT systems. Playbooks are comprehensive sets of instructions that outline predefined responses to specific situations or events. They are often used in incident response and cybersecurity for guiding actions during security incidents. While valuable for incident management, playbooks are not specifically related to managing changes in IT systems.

Kelly Financial Solutions processes thousands of credit card transactions daily. To enhance security, the IT department wants to ensure that sensitive data, such as credit card numbers, remains protected even while being actively processed in the system's memory. Which technology would be MOST effective in safeguarding data-in-use in this scenario?

**Homomorphic encryption**

OBJ: 3.3 - Homomorphic encryption allows data to be processed without being decrypted, effectively securing data-in-use. Computations can be performed on the encrypted data directly, and the results, when decrypted, match as if the operations were done on the plaintext. A VPN encrypts network traffic between two points, ensuring data-in-transit security. It doesn't focus on safeguarding data actively being processed in a system's memory. DLP solutions monitor and control data transfers, helping to prevent data breaches. However, they don't provide specific protection for data being actively processed in memory. While FDE is effective for protecting data at rest, especially on hard drives or SSDs, it doesn't specifically secure data-in-use.

Which of the following statements BEST explains the importance of package monitoring in the context of vulnerability management?

**It helps identify and address vulnerabilities in software packages.**

OBJ: 4.3 - Package monitoring involves keeping track of software package versions and security patches, which helps identify potential vulnerabilities and ensures that appropriate actions are taken to mitigate risks. By promptly addressing vulnerabilities, organizations can reduce the risk of potential exploits and maintain a more secure environment. The purpose of package monitoring which is keeping track of software package versions and security patches, not tracking software package dependencies. Tracking the physical location and status of hardware packages, is not the intended purpose of package monitoring. While updating software packages is essential for performance and functionality, package monitoring, in the context of vulnerability management, is not focused on general updates.

Which of the following statements BEST explains the importance of automating user provisioning?

**It ensures timely access to resources and enhances productivity.**

OBJ: 4.7 - Automated user provisioning helps in granting immediate access rights, reducing waiting times and hence improving productivity. While automation can help in provisioning, authentication remains a separate and crucial component of system security. Automated user provisioning, when done correctly, actually enhances security by ensuring standardized and consistent provisioning processes. While automation reduces human intervention, oversight and management are still needed, especially for exceptions and audits.

Among the following who is MOST likely to make unauthorized copies of sensitive data they were initially granted access to for a specific project?

**Contractor**

OBJ: 2.1 - While a contractor is not a full-time employee, they may have legitimate access to certain systems or data, making them a potential internal threat actor if they misuse this access. An activist group might have political or social motivations, but they don't inherently have permissions on the target system unless specified otherwise. An external threat actor does not have authorized access to the system and might employ methods like malware or social engineering to breach security. An employee typically has broader and more regular access to the company's systems, not just specific project-based access.

Which of the following email security techniques specifically utilizes email certificates to authenticate and safeguard email content?

**S/MIME**

OBJ: 2.2 - S/MIME (Secure Multipart Internet Message Extensions) leverages email certificates to both sign and encrypt email content, ensuring both authenticity and confidentiality. Transport Layer Security primarily encrypts the communication path between servers, but it doesn't use individual email certificates for signing and encrypting content within the email. Domain-based Message Authentication, Reporting & Conformance (DMARC) focuses primarily on the authenticity of the domain from which emails originate, rather than on using certificates to sign and encrypt the email content itself. Sender Policy Framework verifies the legitimacy of the sender's IP against a list of approved IPs for the domain, but doesn't use email certificates for content encryption or signature.

Which of the following statements BEST explains the importance of E-discovery in incident response?

**E-discovery involves examining drives to find data that is electronically stored to use them for evidence.**

OBJ: 4.8 - E-discovery is an essential component of incident response and primarily relates to the collection and handling of electronic data. It is designed to be used as evidence in legal cases and includes in its scope anything that is stored electronically - emails, documents, databases, presentation files, voicemails, video/audio files, social media posts, and more. Although the process of preserving evidence is essential during an incident response phase, it is principally linked to the Preservation phase and not specifically E-discovery. While identifying and recognizing threats or breaches is critical, it principally manifests in the Detection and Analysis phase, not E-discovery. Documenting the details of an incident, its impacts, and potential remedies typically occurs during the reporting phase, and not in the process of E-discovery

What is the primary responsibility of a data custodian in the realm of data governance?

**Enforces security controls for the safe transport and storage of data.**

OBJ: 5.1 - The custodian ensures that data is managed securely in line with the guidelines provided by the data owner and controller. Developing and overseeing the execution of the organization's IT strategy is generally done by IT leadership or the governance board, rather than the custodian. The responsibility of data classification usually lies with the data owner. How personal data should be processed and for what purposes are decisions typically made by the controller, not the custodian.

Which of the following terms is used to describe a situation where a security system or tool incorrectly flags an action or event as malicious or harmful, even though it's actually benign?

**False positive**

OBJ: 4.3. - A false positive occurs when a security measure mistakenly identifies a legitimate action as malicious or a threat, potentially leading to unnecessary corrective actions or alerts. A false negative arises when a security system fails to detect a genuine threat or malicious action, allowing potentially harmful activities to continue without intervention. Penetration testing is a simulated cyber-attack against a system to identify exploitable vulnerabilities, using both automated tools and manual techniques. Package monitoring involves keeping track of software packages for updates or changes, ensuring they're secure and don't contain vulnerabilities, crucial in environments with many dependencies.

**A healthcare organization wants to ensure that patient medical records, which include personal information and health histories, are kept confidential when transmitted between facilities. Which of the following techniques would be the MOST effective in safeguarding this data during transmission?**

**Secure file transfer protocol (SFTP)**

OBJ: 3.3 - SFTP provides secure data transfer, end-to-end encryption. While tokenization can replace sensitive data elements with non-sensitive equivalents, it is typically used for data at rest, not for data in transit. Data masking changes the data to protect its content, but when transmitting actual medical records, the true data needs to reach the other facility. Full disk encryption protects data at rest, not data in transit.

Which of the following network designs involves using air-gapping, disconnecting cables, or locking devices to prevent unauthorized access or interference?

**Physical isolation**

OBJ: 3.1 - Physical isolation is a network design that involves using air-gapping, disconnecting cables, or locking devices to prevent unauthorized access or interference. It can offer benefits such as security, privacy, and reliability. Logical segmentation is a network design that involves dividing a network into smaller segments to improve performance and security, not using air-gapping, disconnecting cables, or locking devices. Software-defined networking (SDN) is a network technology that involves dynamically configuring and managing network devices and services through software, not using air-gapping, disconnecting cables, or locking devices. Decentralized is a network design that involves distributing the control and authority among multiple nodes or entities, not using air-gapping, disconnecting cables, or locking devices.

**Kelly Innovations LLC has observed that their network devices are receiving communication requests that require secure and private interactions, originating from unidentified sources. The IT department hasn’t identified similar requests on other parts of the network. Which would be the MOST secure method to ensure private communication among these devices?**

OBJ: 3.2 - TLS protocol is designed to provide privacy and data integrity between two communicating applications. It's notably used for web browsers and other applications that require data to be securely exchanged over a network, thus suitable for such a situation. A jump server is used as an intermediary for managing devices in a separate security zone but is not particularly utilized for ensuring secure, private communications between devices. A NGFW is an integrated network platform that includes standard firewall capabilities and other network device filtering functionalities, but it's not specifically used to ensure secure, private communications between devices. Sensors monitor and collect data from the environment. However, they don't provide secure and private communications between devices.

Which of the following BEST describes the action taken when a file is quarantined during an alert response?

**Access to the original file is denied to the user.**

OBJ: 4.4 - When a file is quarantined, it is isolated, ensuring the user, or possibly any user, cannot access it. This can be achieved by encrypting the file or moving it to a designated quarantine zone in the file system. While quarantine can be a preliminary step before deciding to delete a file, they are not synonymous. Quarantine involves isolating the file without removing it completely. Quarantining specifically targets the suspicious or malicious file, not all files in its directory. While some quarantined files may be analyzed further, quarantine in itself doesn't imply immediate forwarding to another platform.

Which of the following is a hardware vulnerability that relates to using devices or components that are no longer supported by the manufacturer, possibly leading to unpatched security risks?

OBJ: 2.3 - End-of-life refers to hardware that is no longer supported by the manufacturer, often leading to unpatched and exploitable vulnerabilities. Legacy hardware denotes older systems or components still in use, which can be vulnerable, but doesn’t necessarily mean they are unsupported or at their end-of-life. Supply Chain vulnerabilities refer to vulnerabilities in the supply chain related to third-party service providers, not to using unsupported hardware components.Firmware vulnerabilities are related to the permanent software programmed into the read-only memory, not the discontinued support of hardware components.

Which of the following statements BEST explains the importance of considering single points of failure?

**Mitigating single points of failure is crucial to maintain the availability and reliability of automated security operations.**

OBJ: 4.7 - Single points of failure can lead to system outages and compromise the availability and reliability of automated security operations. By identifying and mitigating these single points of failure, organizations can enhance the resilience of their automated systems, ensuring continuous and reliable security operations.  Single points of failure are vulnerabilities that can disrupt the entire system if they fail, and their existence has nothing to do with whether human decision-making is replaced or not. Single points of failure can exist in both traditional and automated security models. They are a concern in any system where the failure of a critical component could lead to widespread disruption or compromise. The concept of single points of failure is about identifying critical components or processes that, if disrupted, can cause the entire system to fail. It is not about centralizing control for better orchestration.

**Which aspect of security alerting and monitoring is focused on ensuring that specific software solutions, such as databases or CRM tools, are functioning securely and are not compromised by external threats?**

**Applications Monitoring**

OBJ: 4.4 - Applications monitoring zeroes in on specific software solutions, evaluating their performance, security, and ensuring that they operate without vulnerabilities or external compromises. Reporting involves creating summaries or detailed insights about monitoring results but doesn't specify what component (system, application, or infrastructure) is being observed. Infrastructure monitoring is more about observing the overall health and security of foundational IT structures, like servers and networks, which provide the base for both systems and applications. While systems do support and host applications, systems monitoring primarily emphasizes the security and functionality of the hardware and its core services.

**Which of the following is a form of obfuscation where data strings are replaced with a single character like an X or a \* but the structure of the data string remains the same?**

**Data Masking**

OBJ: 3.3 - Data masking is an obfuscation type which redacts the data by substituting the data with a character like an X or a \*. The structure of the string is not changed so, for example, a 10 digit phone number would appear with 10 Xs. In Stagenography, data is embedded in a picture or some other source. In Tokenization, the data is replaced with a token which has a different structure.  The token is used to point to the data. Key stretching is not a data obfuscation technique. It is a technique used to protect passwords.

Oliver travels frequently for work. His organization wants to implement an additional authentication method that considers his geographic location before granting access to sensitive systems. Which factor of multifactor authentication is the organization planning to use?

**Somewhere you are**

Which of the following tools is MOST known for agentless security monitoring/alerting?

**Security Information and Event Management (SIEM)**

OBJ: 4.4 - SIEM tools are essential for consolidating and analyzing logs and alerts from various sources within an environment. These tools are known for their agentless capabilities, where they can collect and process logs without needing a dedicated agent on the source system, providing flexibility in diverse infrastructure setups While an IDS can detect malicious activities, it typically requires agents or sensors to capture traffic or system activities A WAF is designed to filter and monitor HTTP traffic to and from a web application, preventing web-based attacks. It doesn't specifically provide agentless monitoring/alerting at a better capacity of the options that are available. Antivirus software is geared towards detecting and removing malicious software from a system and typically requires an agent for operation.

As organizations grow and expand their digital operations, how can automation and orchestration assist in maintaining security posture?

**Enables consistent security standards during scaling.**

OBJ: 4.7 - Automation and orchestration ensure that as new systems and services are added, they adhere to established security baselines, ensuring uniformity. Automation and orchestration are digital-centric tools and don't promote a shift away from digital operations. While automation can streamline data operations, its primary role isn't to promote data decentralization. While automation assists in many tasks, so far it has not negated the crucial role of human judgment and expertise in security operations.

**Which of the following terms specifically represents the target duration for recovering IT and business operations after a disruptive event?**

**RTO**

OBJ: 5.2 - RTO (Recovery time objective) sets the goal for the time taken to recover business operations after an outage, essential for continuity planning. BCP (Business continuity planning) is the overarching process that includes recovery time objectives, but it is not a time-specific recovery target. MTTR (Mean time to repair) is the average repair time for a failed system or component, not the timeframe for full business recovery. RPO (Recovery point objective) assesses the maximum tolerable data age for recovery purposes, unrelated to the duration for restoring operations.

At Dion Training, promoting security awareness is paramount. To fortify organizational data protection, what should Dion Training do to uphold and enhance password management best practices?

**Instruct users to create strong, unique passwords for each account.**

OBJ: 5.6 - Encouraging employees to keep their passwords confidential and use strong, unique passwords for each account is a crucial aspect of password management best practices. This practice enhances security awareness by promoting secure password habits. Reusing passwords is a bad practice, so it should be avoided Letting users create unique long, strong passwords that they can remember is a better practice. In the past, aging rules were seen as a useful way to improve password management.  However, in current NIST guidelines, aging rules are seen as counter-productive. Users are more likely to write down and reuse passwords when they are forced to change passwords frequently. Letting users create long, strong passwords that they can remember is a better practice. In the past, complexity rules were seen as a useful way to improve password management.  However, in current NIST guidelines, complexity rules are seen as counter-productive. Users are more likely to write down complex passwords because they are difficult to remember. Letting users create long, strong passwords that they can remember is a better practice.

Dark Sky Technologies has hired a vendor to develop a custom software solution for their accounting department. They need a document that provides detailed instructions and requirements for the software development project that will include features the software should have, when the work must finished, and other essential details. Which document would best meet Dark Sky's needs?

**SOW**

OBJ: 5.3 - A Work Order (WO) or Statement of Work (SOW) is the correct document for the ABC Company's needs. It provides detailed instructions and requirements for specific tasks or projects to be carried out by a vendor, making it suitable for the software development project. A Service-level Agreement (SLA) typically outlines specific performance metrics, service levels, and responsibilities for ongoing services, but it does not provide detailed instructions and requirements for specific tasks or projects like software development. A Master Service Agreement (MSA) establishes the overall framework for a long-term business relationship between an organization and a vendor. While it may touch on project details, it does not provide the detailed instructions and requirements needed for a specific software development project. A Business Partners Agreement (BPA) is a type of agreement that outlines the terms and conditions of a partnership between two organizations, not the specific instructions and requirements for a particular project.

**After a security audit, Kelly Innovations LLC decided to dispose of several old storage drives containing sensitive data. They wish to employ a method that ensures the data on these drives is completely unrecoverable. Sasha suggests hitting the drives with a hammer. Given that this is not the most effective solution, which of the following is the BEST method to use?**

**Pulverizing with industrial machinery**

OBJ: 4.1 - While simply hitting a hard drive with a hammer might damage it, a significant amount of data can still be recoverable. Industrial machinery is designed to destroy drives thoroughly, leaving no data intact. Incineration can be effective, but using municipal incinerators might leave some remnants of the drives, making this method less secure. Degaussing method exposes hard disks to powerful electromagnets, disrupting data storage patterns. However, not all types of drives, like SSDs and optical media, can be degaussed, limiting its applicability. While shredding can be an effective method, reducing drives or paper to 12mm strips (Level 1) might still leave data recoverable. More thorough shredding or additional measures would be required for complete data destruction.

In the realm of systems and data management, who is primarily responsible for determining the classification of data and ensuring it aligns with organizational policies?

OBJ 5.1 - A data owner is typically an individual or a functional role within an organization that is responsible for the data's classification, and ensuring it is in line with the organization's security policy. Data processors process data on behalf of the data controller and don't decide on data classifications.  A data controller determines the purposes and means of processing personal data, but the classification and alignment with organizational policies is typically under the purview of the data owner. End users access and use the data but do not typically have responsibilities for classifying it or ensuring its alignment with organizational policies

Which of the following cryptographic techniques uses the same key for both encryption and decryption processes, making it essential that the key remains secret and is shared securely among the involved parties?

OBJ: 2.5 - AES (Advanced Encryption Standard) is a symmetric encryption algorithm where the same key is used for both the encryption and decryption processes. RSA (Rivest–Shamir–Adleman) is an asymmetric encryption technique that involves two distinct keys - one private and one public, not using the same key for encryption and decryption. In ECC (Elliptic Curve Cryptography), public and private key pairs are generated based on elliptic curve mathematics. The public key is used for encryption, and the corresponding private key is used for decryption. Diffie-Hellman is an asymmetric key exchange method used to securely exchange cryptographic keys over a public channel, not a symmetric encryption method.