1. **What is the basic aim of Security Operations Management?**

* Manage principal security concerns and protecting:
  + Networks
  + Infrastructure
  + Data
  + Users

1. **What are the 3 principal components important for Security Operations Management?**

* People
* Processes
* Technologies

1. **What is 3LD?**

* Three Lines of Defence:
  + - * **First Line**: Security controls and their operation (Architecture & Operation)
      * **Second Line**: Assessment of Compliance & Risk Management
      * **Third Line**: Audit

1. **Name the security capabilities/categories described in a Security Architecture.**
   * + Network Security
     + Infrastructure Security
     + Data Security
     + User Security
     + Cyber Defence
     + Application Security
2. **Who are the security capabilities and control measures applied to?**

* Employees
* Contractors
* Partners
* Customers
* Devices
* Locations
* Off-site archives

1. **What function deals with ensuring configuration baselines are applied appropriately?**

* Infrastructure Security

1. **Who in an organisation has a keen interest in data security?**

* CIO/CISO
* Incident Management Team Coordinator
* Security Operations Lead
* Business Manager
* Media and Public Relations Manager
* Managed Service Provider (MSP)

1. **Where is threat modelling typically being performed?**

* Threat & Vulnerability Management (TVM) function

1. **What are racis used for and why?**

Racis are used to define roles and responsibilities for various activities.

For each task they help to identify who is:

* Responsible
* Accountable
* Consulted
* Informed
* Ensures clear communication and accountability

1. **What typical activities does the Security Architecture function pursue?**

* **Planning and designing:**
  + Developing security frameworks and architectural blueprints
  + Identifying areas requiring enhanced protection
* **Risk assessment:**
  + Evaluating vulnerabilities in the system
  + Implementing strategies to mitigate identified risks
* **Implementation:**
  + Deploying security controls like firewalls, intrusion detection systems, and encryption
* **Compliance:**
  + Ensuring alignment with industry standards and regulations
* **Monitoring and maintenance:**
  + Continuously reviewing and updating security measures to adapt to new threats

1. **Why does the security strategy and implementation functions need to work with an organization’s Project Office?**

* **Alignment with organizational goals:**
* Embedding security measures into the design of projects from the outset
* **Resource allocation:**
* Identifying and securing resources to implement security solutions effectively
* **Risk mitigation:**
* Proactively addressing potential risks during project planning and execution
* **Streamlined processes:**
* Ensuring efficient communication and integration between project development and security teams

1. **What interactions has a security engineering team with the incident response team?**

* **Detection:**
* Engineers set up monitoring tools to detect anomalies or threats in real-time
* **Response planning:**
* Collaboratively develop comprehensive incident response strategies
* **Forensic analysis:**
* Provide technical expertise to investigate attack vectors and vulnerabilities
* **Post-incident review:**
* Analyze lessons learned to strengthen future defences and update security controls

1. **Which areas does security engineering activities cover in the NIST CSF?**

* **Identify:**
* Activities include asset management and risk assessment
* **Protect:**
* Implementation of access controls, encryption, and security training
* **Detect:**
* Setting up monitoring systems for threat detection
* **Respond:**
* Developing and executing incident response plans
* **Recover:**
* Designing recovery plans to ensure business continuity and improve resilience

`

1. **What are the 3 main core areas of security monitoring function concerns?**

* **Threat Detection:**
  + Identifying potential security threats, such as unauthorized access or malware
* **Incident Response:**
  + Ensuring timely and effective responses to detected security incidents
* **Compliance Monitoring:**
  + Verifying adherence to regulatory and organizational security policies

1. **What components do SIEM systems monitor?**

* **Network Devices:**
  + Firewalls, routers, and switches
* **Servers:**
  + Operating systems and applications
* **Endpoints:**
  + Laptops, desktops, and mobile devices
* **Applications:**
  + Web servers, databases, and cloud services
* **Logs:**
  + System, application, and security logs for event correlation
* **User Activity:**
  + Monitoring user behaviour to detect anomalies

1. **How many levels of investigation usually exist in security monitoring?**

* **Level 1:** **Initial triage and analysis of alerts to filter out false positives**
* **Level 2:** **In-depth investigation of confirmed incidents to determine the scope and impact**
* **Level 3:** **Advanced analysis, including forensic investigations and root cause analysis**

1. **What are the use case development and lifecycle phases?**

* **Identification:**
  + Define the problem or scenario to address
* **Development:**
  + Create detailed use case descriptions and workflows
* **Implementation:**
  + Deploy the use case in the relevant system or environment
* **Testing:**
  + Validate the use case against expected outcomes
* **Optimization:**
  + Refine the use case based on feedback and performance
* **Maintenance:**
  + Continuously monitor and update the use case to adapt to evolving requirements