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

* To proactively monitor, detect, and respond to security threats, managing principal security concerns.

2. What are the three principle components important for Security Operations Management?

* People (skilled analysts and operators)
* Process (defined workflows and playbooks)
* Technology (tools such as SIEM, IDS/IPS, and monitoring platforms)

3. What is 3LD?

* The Third Line of Defense—typically internal audit—providing independent assurance on the effectiveness of governance, risk management, and internal controls.

4. Name the security capabilities / categories that are described in a Security Architecture.

* Identity & Access Management
* Network Security
* Endpoint Security
* Data Protection
* Application Security
* Threat Detection & Response

5. Who are the security capabilities and control measures applied to?

* People, processes, systems, and data across the organization.

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

* The Configuration Management function (often within Change Management).

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

* Data owners, data stewards, compliance officers, IT security teams, and business-unit leaders.

8. Where is threat modelling typically being performed?

* During the design and development phase of systems and applications, often as part of architecture reviews.

9. What are RACIs used for and why?

* To define Roles and Responsibilities (Responsible, Accountable, Consulted, Informed), ensuring clear accountability and communication in processes.

10. What typical activities does the Security Architecture function pursue?

* Developing security design standards
* Performing risk assessments and threat modelling
* Evaluating and selecting security technologies
* Defining security principles and guidelines

11. Why does the security strategy and implementation functions need to work with an organisations Project Office?

* To align security requirements with project timelines, embed security in planning, and avoid late-stage rework.

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

* Providing forensic tools and expertise
* Integrating detection capabilities into systems
* Assisting with malware analysis and remediation planning

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

* Protect (e.g., access control, protective technology)
* Detect (e.g., anomaly detection, continuous monitoring)

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

* Alerting
* Investigation
* Response

15. What components do SIEM systems monitor?

* Logs, network traffic, user activity, system events, and alerts from various security sensors.

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

* Typically three: Tier 1 (alert triage), Tier 2 (incident analysis), Tier 3 (advanced forensics)

17. What are the use case development & lifecycle phases?

* Identification
* Design
* Implementation
* Tuning
* Review

18. What are the 3 basic vulnerability process steps?

* Discovery (scanning)
* Assessment (prioritization)
* Remediation (fix or mitigate)

19. Which information is used for qualifying identified vulnerabilities?

* CVSS scores, asset criticality, exploit availability, business impact, and threat intelligence.

20. How does TVM team collaborate with Threat Intelligence?

* By consuming threat feeds to prioritize vulnerabilities and align remediation with emerging threats.

21. What information should be in a TVM standard?

* Scope and objectives
* Roles & responsibilities
* Scanning frequency and methods
* Risk-rating methodology
* Remediation timelines

22. What accounts should be managed by IAM?

* All user accounts (employees, contractors)
* Service and application accounts
* Privileged/admin accounts

23. Name the Provisioning steps and the key pre-requisite?

* Request → Approval → Creation → Delivery → Review
* Pre-requisite: Defined access policies and role definitions

24. What measure would you take to enhance security of privileged accounts?

* Implement MFA, just-in-time access, session recording, and credential vaulting.

25. What characteristics would an organisation exhibit at an advanced IAM maturity level?

* Automated provisioning/de-provisioning
* Continuous entitlement reviews
* Adaptive access controls
* Integrated identity governance

26. What are the 3 components that make up Threat Management?

* Threat Intelligence
* Threat Detection (monitoring/alerting)
* Threat Response (hunting & remediation)

27. What do you need or needs to be in place for starting threat hunting?

* Access to logs/telemetry
* Threat-intelligence context
* Skilled analysts and analytical tools

28. What is the difference between a red and blue team?

* Red Team simulates adversaries to test defenses
* Blue Team defends, detects, and responds to attacks.

29. What threat intelligence types would you seek and look at in order to get an initial sense of threats your organisation might face?

* Strategic intelligence
* Tactical intelligence
* Operational intelligence
* Technical intelligence (industry-specific reports and IOCs)

30. What application categories could be defined?

* Web applications
* Mobile apps
* APIs
* Cloud-native services
* Embedded systems
* Legacy applications

31. What security challenges would you highlight trying to embed security in an agile development methodology?

* Speed vs. security trade-offs
* Integrating security testing into sprints
* Automating security tooling
* Building a shift-left culture

32. Which application software testing tool would you use in order to identify weaknesses at runtime?

* An IAST (Interactive Application Security Testing) solution
* A RASP (Runtime Application Self-Protection) solution

33. How can you perform SCA on SaaS?

* Use cloud-provider APIs
* Integrate SCA into CI/CD pipelines
* Employ proxy-based scanning of third-party dependencies.

34. Which Incident Response Phase should playbooks be created?

* Preparation

35. Which Incident Response Phase should deal comprehensively with the root causes of an incident?

* Lessons Learned (Post-Incident Review)

36. What are the criticality categories for incidents, and for which would a crisis management team get involved?

* Low, Medium, High, Critical
* Crisis-management team activates on Critical incidents.

37. What mistakes could be made during the response to an incident?

* Poor communication
* Failure to contain the threat
* Lack of coordination
* Skipping root-cause analysis
* Over- or under-escalation

38. What is the main difference between Enterprise Security Architecture and Security Architecture implementation?

* Enterprise Architecture defines high-level principles and design
* Implementation translates those designs into actual controls and deployments.

39. What security architecture means would you employ to get a sense of controls for a specific business solution?

* Solution-architecture review
* Control-mapping frameworks (e.g., SABSA, TOGAF)
* Targeted threat-modelling workshops.

40. What information would you what to have to create a security strategy?

* Business objectives and priorities
* Risk appetite
* Current-state security assessment
* Regulatory requirements
* Threat landscape

41. How can you measure success of security awareness measures?

* Phishing-simulation click rates
* Training completion rates
* Number of user-reported incidents
* Employee survey results

42. What mechanisms and means are available to get visibility and management information security risks across an organisation?

* GRC platforms and risk dashboards
* Continuous monitoring tools
* Security metrics and reporting frameworks

43. What is the key purpose of risk management?

* To identify, assess, and mitigate risks to an acceptable level in line with business objectives.

44. What is a key advantage of defining governance structures?

* Clear accountability, consistent decision-making, and alignment of security with business goals.

45. Mean time to detection is a KPI for which metrics area?

* Incident detection and response performance.