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

* **Aims to manage principal security concerns**

**2.** Which of the following is **NOT** listed as a stakeholder responsible for managing security?

* **Government**

**3.** Which of the following is NOT mentioned as a framework under Operating Model Frameworks, Standards & Tools?

* **TCP/IP**

**4.** Which line of defence is responsible for assessment of compliance & risk management?

* **Second Line – Assessment of compliance & risk management**

**5.** Which of the following is NOT a state in which data needs to be protected?

* **In design**

**11.** Which of the following frameworks are explicitly mentioned under Operating Model Frameworks, Standards & Tools?

* **ISO**
* **NIST**

**14.** Which of the following are lines of defence in the 3 Lines of Defence model?

* **Assessment of compliance & risk management**
* **Audit**

**15.** Which of the following topics are covered in the Recap of Fundamentals section?

* **Threat & Threat Actors**
* **Vulnerabilities and their management**

**16.** Which of the following are states in which data needs to be protected?

* **At rest**
* **In use**
* **In transit**

**17.** Which of the following elements are included in the Focus of Module section?

* **Understand overall scope and demarcations**
* **Understand application of security fundamentals in this context**
* **Understanding People, Processes and Technologies associated with security operations management**

**18.** Which of the following topics are included in the Recap of Fundamentals section?

* **Cryptography**
* **Incident Response**
* **Mobile Solutions**

**19.** What needs to be secured according to the introduction?

* **Data**
* **Users**
* **Network**
* **Infrastructure**

**20.** Which of the following security capability domains are illustrated in the High-Level Security Operation Management View?

* **User Security**
* **Data Security**
* **Infrastructure Security**
* **Network Security**

**21.** Which of the following is NOT a function listed under Enterprise Security Architecture?

* **Cloud Management**

**22.** Which capability focuses on oversight of management, measurement & effectiveness of controls and strategic directions?

* **Cybersecurity Governance**

**23.** In the Cybersecurity Operating Model, the 'operational' group is responsible for which of the following?

* **Day-to-day running of security services**

**24.** Which RACI role owns, approves, and is the final decision-maker for an activity?

* **Accountable**

**25.** Which function deals with secure management of access by users and to resources?

* **Identity and Access Management**

**26.** Which function includes network segmentation, firewalls, and IDS/IPS?

* **Network Security**

**27.** Which function is responsible for vulnerability scanning, assessment, and remediation?

* **Threat & Vulnerability Management**

**28.** Which function deals with managing digital identities and access policies?

* **Identity and Access Management**

**29.** Which process includes classification, discovery, and handling of data?

* **Data Security**

**30.** Which of the following is NOT a typical output of the Security Monitoring function?

* **Documented use cases**

**31.** Which of the following are core components of Enterprise Security Architecture?

* **Application Security**
* **User Security**

**32.** Which responsibilities belong to the Threat & Vulnerability Management function?

* **Remediation**
* **Scanning of networks**

**33.** Which of the following are activities of the Security Monitoring function? (choose two)

* **Tuning of use cases**
* **Onboarding of log feeds**

**34.** Which items are part of the IAM JML process?

* **Joiners**
* **Leavers**

**35.** Which of the following are TYPES of Threat Intelligence?

* **Strategic**
* **Tactical**

**36.** Which of the following are categories of capabilities in the Cybersecurity Operating Model?

* **Non-operational**
* **Oversight through governance**
* **Operational**

**37.** Which of the following are outputs of the Security Architecture function?

* **Security blueprint**
* **Control framework**
* **Maturity roadmaps**

**38.** Which are activities of the Security Strategy and Program Management processes?

* **Organise maturity assessments**
* **Recommend procurement on tenders**
* **Create and implement security improvement programmes**

**39.** Which of the following are key activities of the Infrastructure Security function?

* **Certificate deployment and management**
* **Hardened configuration management**
* **Directory services integration**
* **Mobile & IoT device management**

**40.** Which of the following are phases of the Threat Modelling process?

* **Develop data flow diagram**
* **Identify all system components**
* **Apply selected threat model techniques**
* **Determine and analyse trust boundaries**

**41.** Which of the following is an output of the Security Architecture function?

* **Roadmaps for implementation**

**42.** Which activities are performed by the Security Strategy and Programme Management processes?

* **Organise and perform maturity assessments**
* **Create and implement security improvement programmes**

**43.** What is the main purpose of the HR, Facility & Physical Resource Security function?

* **Establish and maintain security of staff and their work environment**

**44.** Which of the following are processes of the HR, Facility & Physical Resource Security function?

* **Perform background checks**
* **Set up and operate onboarding and offboarding processes**

**45.** Which of the following is NOT listed as an ongoing challenge for security teams?

* **Agricultural supply chain management**

**46.** Which of the following is an activity of the Security Engineering function?

* **Advising on MDM secure configurations**

**47.** Which of the following are concerns of the Security Engineering function?

* **Hardening**
* **Endpoint security**
* **DLP**

**48.** Which of the following are key activities and outputs of the Security Engineering function's Infrastructure Security process?

* **Apply or validate hardened configurations**
* **Creating, reviewing or updating OS security baselines**
* **Validating and managing EDR configuration and status**
* **Advising on MDM secure configurations**

**49.** Which of the following are outputs of the Security Engineering function's Network Security activities?

* **Documented secure rules**
* **White/blacklist documentation**
* **Administrative interaction records**

**50.** Which of the following is NOT an activity of the Security Architecture function?

* **Performing incident forensics**

**51.** Which of the following are processes of the Governance, Strategy & Risk Alignment function?

* **Define, collect and present KPIs**
* **Review and approve strategic decisions**

**52.** Which of the following best describes an output of the Security Strategy and Programme Management function?

* **Security improvement programmes**

**53.** Which of the following are outputs of the HR, Facility & Physical Resource Security function?

* **Physical security metrics reports**
* **Background check results**

**54.** Which function is responsible for creating and communicating security principles & patterns?

* **Security Architecture**

**55.** Which of the following are processes of the Security Architecture function?

* **Assessing security capabilities of the organization**
* **Creating, documenting and communicating security principles and patterns**
* **Analyzing technical and business architectures and specifying security controls**

**56.** Which of the following best describes the role of the Governance, Strategy & Risk Alignment function?

* **Oversee overall security posture and align strategy and risk with organizational expectations**

**57.** Which of the following is NOT a process of the Security Strategy and Programme Management function?

* **Develop incident response playbooks**

**58.** Which of the following are concerns of the Security Engineering function?

* **Hardening**
* **Endpoint security**
* **Proxy Config & Rules**
* **DLP**

**59.** Which of the following are ongoing challenges that security teams need to adapt to?

* **Regulatory landscape changes**
* **New security concepts**

**60.** Which of the following functions is responsible for analyzing technical and business architectures and specifying security controls?

* **Security Architecture**

**61.** What does SIEM stand for?

* **Security Information and Event Management**

**62.** Which of the following are phases in Use Case Development & Lifecycle?

* **Use Case Mobilisation, Operation and Improvement**
* **Use Case Creation, Testing & Deployment**

**63.** How many levels of investigation are there in the Multi-Level Model for Investigations?

* **3**

**64.** Which of the following are key activities and outputs of the Security Monitoring function?

* **Onboarding of log feeds**
* **Tuning of use cases**
* **Qualifying incidents and triaging**

**65.** Which of the following is the first step in the Threat & Vulnerability Management process?

* **IT Asset Management**

**66.** Which of the following are outputs of the Threat & Vulnerability Management function?

* **Progress tracker**
* **Reports**

**67.** Which of the following is NOT a function of the Identity and Access Management service?

* **Configure WAF rules**

**68.** Which of the following are phases in the IAM Fundamental JML process?

* **Leavers**
* **Joiners**
* **Movers**

**69.** Which of the following is a key concern of the IAM function?

* **Directory services**

**70.** Which of the following are supported functions of the IAM/PAM function?

* **Assist with audit queries**
* **Support incident response**

**71.** Which system type manages identities for external customers?

* **CIAM**

**72.** Which of the following are service maturity levels described in the Identity & Access Management section?

* **Advanced**
* **Optimised**
* **Foundation**

**73.** Which of the following best describes the purpose of the 'Provisioning Request' in the high-level IAM process?

* **Initiate identity creation**

**74.** Which of the following are steps in the Incident Management process?

* **Identification**
* **Containment**

**75.** Which of the following is NOT a phase of the Incident Management process?

* **Reporting**

**76.** Which of the following are core phases included in the high-level Incident Management process?

* **Preparation**
* **Eradication**
* **Containment**
* **Identification**

**77.** What does SAST stand for in Application Security?

* **Static Application Security Testing**

**78.** Which of the following are scanning methods in DevSecOps for application security?

* **SAST**
* **DAST**

**79.** Which of the following best describes the purpose of a Web Application Firewall?

* **Protect HTTP/HTTPS traffic at the application layer**

**80.** Which of the following are components of the Application Security Framework?

* **DAST**
* **SAST**
* **Container Vulnerability Scanning**
* **SCA**

**81.** Which function deals with establishing and maintaining security of staff and their work environment?

* **HR, Facility & Physical Resource Security**

**82.** Which function deals with defining and developing security capabilities and assisting in their implementation?

* **Security Architecture**

**83.** Which function organizes and performs maturity assessments and implements security improvement programmes?

* **Security Strategy & Programme Management**

**84.** Which function oversees overall security posture and aligns strategy and risk with organizational expectations?

* **Governance, Strategy & Risk Alignment**

**85.** Which technique lists Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege?

* **STRIDE**

**86.** Which type of threat intelligence focuses on threat information relating to an organization’s industry and business objectives, aimed at a non-technical audience?

* **Strategic**

**87.** Which function devises and performs exploit proof of concept scenarios to test defenses?

* **Advanced Threat Management**

**88.** Which Threat Hunting type is often guided by risk assessment focusing on high-value assets?

* **Situational**

**89.** Which type of threat modelling arranges potential attack vectors in a tree form?

* **Attack Trees**

**90.** Which phase of the Threat Modelling process involves assessing threats and vulnerabilities and devising countermeasures?

* **Perform Threat Analysis**

**91.** Which of the following are types of Threat Intelligence?

* **Strategic**
* **Tactical**

**92.** Which of the following are components of Threat Management?

* **Threat Intelligence**
* **Threat Modelling**

**93.** Which of the following are Threat Hunting tools?

* **SIEM**
* **XDR**

**94.** Which of the following are steps specific to the Threat Modelling process?

* **Identify all system components**
* **Determine and analyse trust boundaries**

**95.** Which of the following are outputs of the Threat Intelligence component?

* **Threat report**
* **Periodic research**

**96.** Which of the following are outputs of the Threat Modelling process?

* **Analysis report**
* **Diagrams and data flow models**
* **Threat description**

**97.** Which of the following are phases of the Threat Hunting process?

* **Review threat landscape and identify specific threats**
* **Formulate a hypothesis to guide threat hunting**
* **Perform the threat hunt**

**98.** Which of the following are outputs of the Advanced Threat Management function?

* **Exploitation report**
* **Honeypots/nets**
* **Adversary TTPs**

**99.** Which of the following are Threat Management components?

* **Threat Intelligence**
* **Threat Modelling**
* **Threat Hunting**
* **Advanced Threat Management**

**100.** Which of the following are activities of the Advanced Threat Management function?

* **Perform system and/or application deep dives**
* **Identify advanced attack scenarios**
* **Devise and perform exploit proof of concepts**
* **Capture adversary TTPs**

**101.** Which of the following is characteristic of the Waterfall software development methodology?

* **Sequential progression through phases with defined stage gates**

**102.** Which of the following is NOT listed as an application category?

* **Virtual Machines**

**103.** In application security, which tool is used for scanning open-source and third-party libraries for known vulnerabilities?

* **SCA**

**104.** Which phase of the Software Development Life Cycle involves creating the system architecture and detailed designs?

* **Design**

**105.** In the Incident Management process, which phase focuses on isolating and stabilizing the affected environment?

* **Containment**

**106.** Which incident severity category corresponds to a major successful ransomware attack with potential existential impact?

* **C1 – Major Incident**

**107.** Which regulation is NOT mentioned under the legal aspects of incident management?

* **ISO 27001**

**108.** What is the primary purpose of a tabletop exercise in incident response?

* **Assign roles and respond to scripted interjections**

**109.** Which of the following is listed as a key mistake in incident response?

* **Failure to report**

**110.** Which case study describes an incident that impacted the Irish Health Service Executive?

* **Conti Cyberattack on Irish HSE**

**111.** Which of the following are characteristics of Software as a Service (SaaS)?

* **Services come as they are**
* **IAM, Data, and BCM are managed by the vendor**

**112.** Which of the following are key concerns of Posture Security Management?

* **Asset inventory and characteristics**
* **Configuration assessment and enforcement**

**113.** Which of these statements about Static Application Security Testing (SAST) are true?

* **Scans uncompiled and compiled code for known vulnerabilities**
* **Integrated into CI/CD pipelines and triggered by code check-in**

**114.** Which phases of the Incident Management process follow containment?

* **Eradication**
* **Lessons Learned**

**115.** Which components are part of a typical DevSecOps architecture?

* **IDE plugins**
* **Build pipeline**

**116.** Which of the following are phases of the Software Development Life Cycle?

* **Planning**
* **Analysis**
* **Design**

**117.** Which of the following are characteristics of the Optimised service maturity level for Application Security?

* **Faster remediation**
* **Security mentality**
* **Advanced level of automation**

**118.** Which of the following are covered by Posture Security Management?

* **Asset inventory and characteristics**
* **Configuration assessment and enforcement**
* **Visibility and compliance dashboards**

**119.** Which of the following legal aspects are referenced in Incident Management?

* **Criminal law (fines and/or imprisonment)**
* **Civil law (compensation)**
* **GDPR**
* **PSD2**

**120.** Which of the following are incident severity categories?

* **C1 – Major Incident**
* **C2 – Significant Incident**
* **C3 – Moderate Incident**
* **C4 – Minor Incident**

**121.** Which Threat Management component is responsible for gathering and compiling information on threat actors and campaigns?

* **Threat Intelligence**

**122.** Which Threat Management component is responsible for modelling threat paths and devising mitigation measures?

* **Threat Modelling**

**123.** Which Threat Hunting type is often guided by risk assessment focusing on high-value assets?

* **Situational**

**124.** Which Advanced Threat Management activity involves deploying honeypots or honeynets?

* **Create, monitor, observe and maintain honeypots/nets**

**125.** Which Threat Intelligence report type is aimed at a non-technical audience and relates to industry-level threats?

* **Strategic**

**126.** In the Threat Hunting process, what is the first step?

* **Review threat landscape and identify specific threat**

**127.** Which of the following is NOT a phase of the Threat Modelling process?

* **Monitor network traffic**

**128.** Which service maturity level for Threat Intelligence is characterized by pro-active and strategic intel gathering?

* **Optimised**

**129.** Which Threat Management component includes advanced adversary deception and disruption services?

* **Advanced Threat Management**

**130.** In the STRIDE threat modelling technique, what does the 'R' represent?

* **Repudiation**

**131.** Which Threat Intelligence report types are aimed primarily at a technical audience?

* **Technical**
* **Tactical**

**132.** Which of the following are outputs of Threat Intelligence activities?

* **Analysis report**
* **Threat mitigation report**

**133.** Which of the following are initial steps in the Threat Hunting process?

* **Review threat landscape and identify specific threat**
* **Formulate a hypothesis to guide threat hunting**

**134.** Which of the following are parts of the Threat Modelling process?

* **Identify all system components**
* **Develop data flow diagram**

**135.** Which of the following are outputs of the Threat Modelling process?

* **Threat description**
* **Diagrams and data flow models**

**136.** Which of the following are components of Threat Management?

* **Threat Intelligence**
* **Threat Hunting**
* **Threat Modelling**

**137.** Which of the following are key concerns listed under Threat Intelligence?

* **Underground intelligence**
* **Vulnerability reports**
* **Threat feeds**

**138.** Which of the following are Threat Hunting types?

* **Unstructured**
* **Situational**
* **Structured**

**139.** Which of the following are listed as Threat Hunting tools?

* **Intelligence Information**
* **SIEM**
* **Security Analytics**
* **XDR**

**140.** Which of the following are steps in the Threat Modelling process?

* **Develop data flow diagram**
* **Apply selected threat model techniques**
* **Validate implemented mitigation measures**
* **Identify all system components**

**141.** Which of the following is NOT an application category mentioned?

* **Virtual machines**

**142.** Which phase of the Software Development Life Cycle involves integrating solution components and validating correctness?

* **Testing & Integration**

**143.** Which statement best describes Agile methodology?

* **Short iterative delivery cycles**

**144.** Which tool scans source code for known vulnerabilities in a static (inside-out) manner?

* **SAST**

**145.** Which method is used for scanning container images and configurations?

* **Container Vulnerability Scanning**

**146.** What SDLC phase comes immediately after Analysis?

* **Design**

**147.** Which application security test is a black-box method performed at runtime?

* **DAST**

**148.** Which testing approach involves manual external security testing by specialized experts?

* **Penetration Testing**

**149.** Which security control protects HTTP/HTTPS traffic at the application layer?

* **WAF**

**150.** What concept refers to integrating security early in the SDLC?

* **Shift Left**

**151.** Which application delivery methodologies are mentioned?

* **Waterfall**
* **Agile**

**152.** Which types of software/services are classified as third-party in the document?

* **COTS**
* **SaaS**

**153.** Which components are part of the Application Security Framework?

* **Container Vulnerability Scanning**
* **DAST**

**154.** Which SDLC phases are correctly paired here?

* **Implementation**
* **Design**

**155.** Which of the following are elements of a DevSecOps architecture?

* **IDE plug-ins**
* **CI/CD pipeline**

**156.** Which of the following are phases of the Software Development Life Cycle?

* **Planning**
* **Analysis**
* **Design**

**157.** Which of the following methods are used for application security testing?

* **SAST**
* **DAST**
* **Container Vulnerability Scanning**

**158.** Which of the following are characteristics of the Optimised service maturity level for Application Security?

* **Faster remediation**
* **Security mentality**
* **Consistent view of risk**

**159.** Which of the following are Application Security Framework components?

* **IDE plug-ins**
* **SAST**
* **DAST**
* **Penetration Testing**

**160.** Which phase of the Incident Management process includes steps to identify and qualify the incident and initiate response?

* **Identification**

**161.** What does the 'Eradication' phase focus on?

* **Eliminating root causes of the incident**

**162.** Which activity is part of the Preparation phase?

* **Create incident response playbooks**

**163.** Which incident severity category corresponds to a minor incident with limited impact?

* **C4 – Minor Incident**

**164.** Which of the following is cited as a key mistake in incident response?

* **Failure to report**

**165.** What deliverable might be created during the Identification phase?

* **Incident notification tracker**

**166.** Which phase involves performing a post-mortem review to identify areas for improvement?

* **Lessons Learned**

**167.** Which legal aspect can involve fines and imprisonment?

* **Criminal law**

**168.** Which case study involved a cyberattack on the Irish Health Service Executive?

* **Conti Cyberattack on Irish HSE**

**169.** Which exercise type involves tabletop interjections and role assignments?

* **Tabletop exercise**

**170.** Which of the following are outputs of the Recovery phase?

* **Restored systems**
* **Operational readiness validation**

**171.** Which of the following are steps in the Containment phase?

* **Identify root sources**
* **Secure areas**

**172.** Which of the following are primary components of a response playbook?

* **Indicators**
* **Stakeholders & RACI**

**173.** Which of the following regulations are mentioned under legal aspects?

* **GDPR**
* **HIQA**

**174.** Which roles are part of the Crisis Response Structure?

* **Crisis Manager**
* **Law Enforcement**

**175.** Which of the following are phases of the Incident Management process?

* **Preparation**
* **Identification**
* **Eradication**

**176.** Which of the following are mistakes cited in Incident Management?

* **Failure to report**
* **No notes taken**
* **Failure to eradicate**

**177.** Which of the following are deliverables of the Preparation phase?

* **Incident management policy**
* **Incident management team org chart**
* **Incident response playbooks**

**178.** Which of the following are incident severity categories?

* **C1 – Major Incident**
* **C2 – Significant Incident**
* **C3 – Moderate Incident**
* **C4 – Minor Incident**

**179.** Which of the following legal aspects/regulations are considered in incident management?

* **Criminal law**
* **Civil law**
* **GDPR**
* **PSD2**

**180.** What is the first step in the Threat & Vulnerability Management process?

* **IT Asset Management**

**181.** In the NIST Cybersecurity Framework, which function focuses on implementing protective measures?

* **Protect**

**182.** Which of the following is NOT a phase of the Software Development Life Cycle (SDLC)?

* **Deployment**

**183.** Which tool performs black-box scanning of running applications to find vulnerabilities?

* **DAST**

**184.** Which ISO 27001 area covers Operations Security?

* **A12**

**185.** In a RACI matrix, who is responsible for executing an activity?

* **Responsible**

**186.** What does PAM stand for in cybersecurity?

* **Privileged Access Management**

**187.** Which incident response phase focuses on restoring systems and services?

* **Recovery**

**188.** What is the name of the process that includes Use Case Identification & Selection, Creation & Testing, and Operation & Improvement in SIEM?

* **Use Case Development & Lifecycle**

**189.** In STRIDE threat modelling, what does the 'D' stand for?

* **Denial of Service**

**190.** Which method scans source code for known vulnerabilities before compilation?

* **SAST**

**191.** Which term describes the initial request and creation of a new digital identity in IAM?

* **Provisioning**

**192.** Which of these is NOT one of the 3 Lines of Defence in security operations?

* **Fourth Line – External auditing**

**193.** Which framework focuses specifically on cloud security best practices?

* **CSA**

**194.** Which of the following is NOT a standard type of Threat Intelligence report?

* **Forensic**

**195.** Which tool analyzes open-source libraries for known vulnerabilities?

* **SCA**

**196.** Which of these is NOT a core concern of Security Monitoring?

* **Email scanning**

**197.** Which NIST CSF function involves detecting anomalies and events?

* **Detect**

**198.** Which ISO 27001 area covers System Acquisition, Development and Maintenance?

* **A14**

**199.** Which document outlines scanning conditions, frequency, and classification criteria for vulnerability management?

* **TVM standard**

**200.** Which of the following are key components of Enterprise Security Architecture?

* **Network Security**
* **Data Security**

**201.** Which of the following are IAM system types?

* **CIAM**
* **PAM**

**202.** Which of the following are phases of the Incident Management process?

* **Identification**
* **Recovery**

**203.** Which of the following are activities of the Security Monitoring function?

* **Onboarding of log feeds**
* **Tuning of use cases**

**204.** Which of the following are roles in a RACI matrix?

* **Responsible**
* **Accountable**

**205.** Which of the following are outputs of the Security Architecture function?

* **Security blueprint**
* **Control framework**

**206.** Which of the following are DevSecOps scan types?

* **SAST**
* **DAST**

**207.** Which of the following are methods of application security testing?

* **DAST**
* **Container Vulnerability Scanning**

**208.** Which of the following are Threat Modelling techniques?

* **STRIDE**
* **Kill Chain**

**209.** Which of the following are components of Operational Monitoring?

* **Log ingestion**
* **SIEM management**

**210.** Which of the following are NIST CSF core functions?

* **Identify**
* **Protect**
* **Detect**

**211.** Which ISO 27001 areas are supported by Security Monitoring?

* **A12 Operations Security**
* **A16 Incident Management**
* **A17 Information Security Continuity**

**212.** Which of the following are phases in the TVM process?

* **Vulnerability Scanning**
* **Vulnerability Classification**
* **Remediation**

**213.** Which of the following are outputs of the Threat & Vulnerability Management function?

* **Reports**
* **Progress tracker**
* **Remediation plan**

**214.** Which of the following are steps in the IAM JML process?

* **Joiners**
* **Movers**
* **Leavers**

**215.** Which of the following are responsibilities of Threat Hunting?

* **Planning and executing hunting campaigns**
* **Identifying specific organizational threats**
* **Collaborating with Incident Response**

**216.** Which of the following are core components of the Enterprise Security Architecture?

* **Network Security**
* **Infrastructure Security**
* **Application Security**
* **Data Security**

**217.** Which of the following are primary concerns of Security Engineering?

* **Hardening**
* **Firewall Config & Rules**
* **DLP**
* **PAM**

**218.** Which of the following are phases of the SIEM Use Case Development & Lifecycle?

* **Identification & Selection**
* **Creation, Testing & Deployment**
* **Mobilisation, Operation & Improvement**
* **Reporting**

**219.** Which of the following are key phases in the Incident Management process?

* **Preparation**
* **Identification**
* **Containment**
* **Eradication**

**220.** Which of these is the primary function of Enterprise Security Architecture?

* **Network Security**

**221.** Which component defines principles and patterns for system and component interactions?

* **Infrastructure Security Architecture**

**222.** Which security principle emphasizes limiting user and system rights to only what is necessary?

* **Least Privilege**

**223.** Which principle focuses on embedding continuous automated checks into security processes?

* **Adopt Zero Trust**

**224.** Under ISO 27001, which control objective covers cryptographic controls?

* **A10 Cryptography**

**225.** Which deliverable translates a cybersecurity strategy into an actionable plan with priorities and resource allocation?

* **Security Roadmap**

**226.** Which NIST Cybersecurity Framework function involves specifying and implementing security controls?

* **Detect**

**227.** Which governance function provides oversight of control effectiveness and strategic direction?

* **Risk Management**

**228.** Which document captures an organization’s security requirements and high-level principles?

* **ESA Documentation**

**229.** Which blueprint component represents logical zones, security capabilities, and flows?

* **Logical Representation**

**230.** Which activity involves developing methodology and tooling requirements for secure software development?

* **Application Security Framework**

**231.** Which ISO 27002 domain covers organization-wide standards for secure data handling?

* **A9 Access Control**

**232.** Which NIST function focuses on restoring and improving security controls after an incident?

* **Recover**

**233.** Which of the following is NOT listed as a security architecture principle in the document?

* **Open Trust by Default**

**234.** Which activity is part of Security Training & Awareness to measure user readiness?

* **Perform phishing exercises**

**235.** Which two are inputs to a security strategy formulation?

* **Cybersecurity risks**
* **Threat landscape**

**236.** Which two outputs result from Enterprise Security Architecture documentation activities?

* **Enterprise security requirements**
* **ESA documentation**

**237.** Which two activities are involved in a security architecture assessment for compliance?

* **Document compliance/non-compliance**
* **Identify alternative controls**

**238.** Which two results are produced when creating a security roadmap?

* **Identified priorities combined with resources**
* **Dedicated workstreams**

**239.** Which two outputs come from security programme Planning & Demand Management?

* **Programme and project status reports**
* **Scheduling and reporting artifacts**

**240.** Which three principles are included in the Security Architecture principles list?

* **CIA (Confidentiality, Integrity, Availability)**
* **Defence in Depth**
* **Automate Security Validation**

**241.** Which three activities are part of Policy Framework development in Strategy Implementation?

* **Draft new or update existing policies**
* **Bring policies through vetting and approval**
* **Create standards and guidelines**

**242.** Which three practices support Cyber Hygiene in Security Training & Awareness?

* **Infusion of good cybersecurity practices**
* **Leveraging proven organizational models**
* **Embedding routines into daily activities**

**243.** Which four activities are key to Security Strategy & Implementation?

* **Establish strategy direction**
* **Creating security roadmap**
* **Develop policy framework**
* **Manage cyber risk**

**244.** Which four outputs are produced by Planning & Demand Management and Risk & Compliance support?

* **Security initiative plans**
* **Programme/project status reports**
* **Scheduling and reporting artifacts**
* **Risk assessment and mitigation tracking**