Session 1:

Introduction and High Level Overview

1. **Aim of Security Operations Management**Coordinate principal security concerns across the enterprise.
2. **Assets to Secure**Networks, infrastructure, data, and users must all be protected.
3. **Protection Contexts**Safeguard assets at rest, in transit, and in use.
4. **Key Stakeholders**Involves users, administrators, business units, and security professionals.
5. **Approaches & Tools**Develop actionable processes, define protection actions, skills, and oversight.
6. **Master Plan Components**Security architecture, action blueprints, and guidance documents.
7. **Frameworks & Standards**Leverage NIST, ISO, TOGAF, MITRE, CSA, COBIT, ITIL, etc.
8. **Three Lines of Defence**

* Controls operation
* Compliance/risk assessment
* Audit.

1. **From Requirements to Architecture**Map business, legal, and policy requirements into security architecture.
2. **Security Best Practices**Adopt ISO 27000 series, NIST guidance, and CSA benchmarks.
3. **Reference Architecture Sample**Illustrates integration of security domains across the enterprise.
4. **Security Operating Model**Governance, architecture, policies, monitoring, incident response, continuous improvement.
5. **Module Focus**Scope, core functions, people, processes, technologies, and IT interfaces.
6. **Recap of Tooling**Penetration testing, malware analysis, and security awareness programs.
7. **Security Operations Objectives**Deliver defined processes, deployed technologies, and competent people.

Session 2:

Cybersecurity Functions

1. **Enterprise Security Architecture**Defines core functions: network, infrastructure, application, data, and user security.
2. **Cyber Defense Function**Monitors and manages controls to support resilience.
3. **Governance Function**Oversees management, measures effectiveness, and sets strategic direction.
4. **Risk Management**Captures and manages organizational risk exposures.
5. **Operational vs Non-Operational**Day-to-day security services vs capability development and awareness.
6. **Enterprise Interfaces**Integrates with HR, Procurement, Change, Audit, Cloud Services, etc.
7. **RACI Role Definitions**Documents responsibilities and communication structures.
8. **Network Security Scope**IDS/IPS, firewalls, WAF, DDoS protection, proxies, segmentation, VPN, NAC.
9. **Network Security Processes**Hardened configs, rule review/approval, SIEM integration, change management.
10. **Infrastructure & App Security**Servers, endpoints, mobile, IoT, platforms, cloud services, SDLC integration.
11. **Infra Security Processes**Configuration hardening, directory integration, PKI, EDR, spam management.
12. **App Security Processes**Requirements compliance, control advisory, SAST, SCA, API/IDE testing.
13. **Identity & Access Management**Secure access for employees, partners, third parties, and guests.
14. **IAM Processes**Joiner/Mover/Leaver lifecycle, group management, recertification, federation.
15. **Data Security**Classification, discovery, handling (at rest/in transit/in use), storage, disposal.
16. **Data Security Processes**DLP, removable device controls, retention, secure disposal.
17. **TVM Function**Scanning, assessment, remediation, threat intelligence, hunting.
18. **TVM Processes**Scanner management, vulnerability analysis, intelligence monitoring, hunting prep.
19. **Security Monitoring**SIEM configuration, alert monitoring, qualification, incident triage.
20. **Incident Response**Investigate, qualify, contain, recover, and improve post-incident.

Session 3:

Security Operations – Core Functions

1. **Operational vs Non-Operational Model**  
   Day-to-day operations vs capability and risk management.
2. **Security Architecture Function**  
   Develops principles, control frameworks, design patterns, blueprints.
3. **Architecture Processes**  
   Capability assessments, principle documentation, maturity analysis, advisory.
4. **Strategy & Implementation**  
   Maturity models, resilience focus, risk and program management.
5. **Strategy Processes**  
   Maturity assessments, improvement programs, policy creation, governance metrics.
6. **HR, Facility & Physical Security**  
   Secures staff and environment pre-/post-hire, health & safety.
7. **Physical Security Processes**  
   Background checks, facility assessments, physical controls, breach handling.
8. **Governance Alignment**  
   Oversees posture, investment priorities, gap analysis, strategic decisions.
9. **Governance Processes**  
   Body establishment, terms of reference, KPI collection, action follow-up.
10. **Cybersecurity Challenges**  
    Evolving threats, cloud adoption, regulatory change, organizational agility.
11. **Core Operational Functions**  
    Governance, architecture, policy, training, network, infra/app security, TVM, monitoring, IR, data mgmt.
12. **Org of Operational Teams**  
    CISO, SecOps lead, Security Engineering, Monitoring, IR, TVM, IAM, Architecture, Strategy.
13. **Security Engineering Scope**  
    Hardening, firewall/proxy/IPS rules, DLP, PKI, PAM, EDR management.
14. **Engineering Outputs**  
    Baselines, hardened configurations, EDR validation, audit reports.
15. **Network Engineering**  
    Review/approve firewall/WAF rules, proxy and IDS/IPS configurations.
16. **Data Engineering**  
    DLP rule creation, removable media restrictions, PKI deployment.
17. **IAM Engineering**  
    Directory group design, federation, PAM system management.
18. **Function Interactions**  
    Supports IR, TVM, Monitoring, InfraOps, AppOps, NetworkOps, Architecture/Risk.
19. **Framework Mapping**  
    Aligns with NIST (Protect/Detect/Respond/Recover), ISO 27001, MITRE ATT&CK.

**Session 4:**

**Operational Monitoring**

1. **Monitoring in Models**SIEM management, log ingestion, use-case development, alert analysis.
2. **Log Ingestion**Onboard feeds from infrastructure and applications into SIEM.
3. **Use-Case Lifecycle**Identify, create, test, deploy, mobilize, report, and improve use cases.
4. **Alert Monitoring**Analyze and qualify alerts, create incidents, triage severity.
5. **Threat & Vulnerability Integration**Ingest TVM scan results and threat intel into monitoring.
6. **KPI & Reporting**Dashboards, regular reports, vendor liaison, platform tuning.
7. **SIEM Architecture**Design for scalable log collection and analysis.
8. **Use-Case Management Details**Requirements definition, data sources, logic, baselines, tuning.
9. **Attack Phases Coverage**Pre-attack (recon/discovery) through post-attack (persistence).
10. **Investigation Model**Tiered analyst levels (L1–L3) and escalation to IR/crisis teams.
11. **Service Improvement**Reduce false positives to focus analysts on high-value tasks.
12. **Service Maturation**Foundation → Advanced → Optimized across scope and automation.
13. **People, Process, Technology Maturity**Progress from initial to optimizing state.
14. **NIST Alignment**Detect (SIEM, analysis, hunting), Respond (IR support), Recover (scope expansion).
15. **ISO 27001 Alignment**Supports controls A12–A18 in the standard.
16. **MITRE ATT&CK Mapping**Monitoring across perimeter, infra, EDR, specialized use cases.
17. **Functional Interactions**Works with IR, TVM, SecEng, InfraOps, AppOps, NetworkOps, Architecture/Risk.
18. **Outsourcing**Monitoring is often partially outsourced.
19. **Continuous Improvement Cycle**Ongoing tuning of technology, people, and processes.

Session 5:

Vulnerability Management

1. **TVM in Models**  
   Scanner management, standards, and integration into operations.
2. **High-Level TVM Process**  
   Asset management → scanning → classification → remediation → reporting.
3. **Scanner Deployment**  
   Set up and maintain vulnerability scanning infrastructure.
4. **TVM Standard**  
   Defines scope, frequency, classification, and remediation criteria.
5. **Scan Scheduling**  
   Regular, discovery, unauthenticated/authenticated scans with notifications.
6. **Result Analysis**  
   Qualify vulnerabilities and produce analysis reports.
7. **Reporting Outputs**  
   Operations, management, and governance-level dashboards and reports.
8. **Remediation Coordination**  
   Engage teams, agree time-bound actions, and track progress.
9. **Compliance Validation**  
   Dashboards and periodic compliance evidence reports.
10. **Threat Hunting Support**  
    Provide ad-hoc scan data to hunting teams.
11. **TVM Architecture**  
    Integrates cloud and on-prem scanning with SIEM.
12. **Cross-Function Interaction**  
    Collaborates with IR, Monitoring, Engineering, Ops, Architecture/Risk, Threat Intel.
13. **Maturity Levels**  
    Foundation, Advanced, Optimized service scope and compliance characteristics.
14. **NIST Alignment**  
    Maps Identify, Detect, Protect, Respond, Recover functions to TVM.
15. **ISO 27001 Alignment**  
    Supports controls A12, A14, A16, A18.
16. **MITRE ATT&CK Mapping**  
    Scanning phases align with Reconnaissance and Discovery tactics.
17. **Session Recap**  
    TVM placement, processes, outputs, architecture, standards, maturity, framework mapping.

Session 6:

Identity and Access Management

1. **IAM in Models**  
   Manages identities and access in both operational and organizational contexts.
2. **General vs Privileged Access**  
   Least-privilege principle; birth rights, role-based, and privileged accounts.
3. **Service Accounts**  
   Best practices for machine-to-machine credentials.
4. **Joiner-Mover-Leaver (JML) Process**  
   Captures the full lifecycle of identities based on HR events.
5. **Affected Capabilities**  
   Central request management, provisioning, HR/payroll integration, communications.
6. **High-Level IAM Flow**  
   Request → identity creation → credential issuance → access configuration.
7. **High-Level PAM Flow**  
   Similar lifecycle for temporary privileged access.
8. **Key Concerns**  
   IAM/PAM systems, directory services, federation, and MFA solutions.
9. **Core IAM Activities**  
   System management, provisioning/deprovisioning, and privilege maintenance.
10. **Directory Management**  
    Group definitions and directory allocations.
11. **Consultancy Role**  
    Design advisory, integration validation, policy compliance checks.
12. **Service Onboarding**  
    Test and validate new services’ integration into IAM/PAM.
13. **Federation & MFA**  
    Configure and manage SSO and MFA integrations.
14. **Documentation Outputs**  
    Standards, procedures, and recertification reports.
15. **PAM Activities**  
    Privileged credential issuance, system maintenance, and audit support.
16. **Functional Interaction**  
    Works with IR, Monitoring, Engineering, Ops, HR, Business, Network Ops, Finance.
17. **IAM Standard Content**  
    Prerequisites, authentication requirements, privileged controls, review cycles.
18. **System Types**  
    Enterprise IAM (EIAM), Customer IAM (CIAM), and Privileged Access Management (PAM).
19. **Service Maturity**  
    Foundation → Advanced → Optimized across technology, people, processes.
20. **Framework Mapping**  
    Aligns NIST (Protect/Respond/Recover) and ISO 27001 controls for IAM/PAM.

Session 7:

Threat Management

1. **Threat Management in Models**  
   Placement of intel, modelling, hunting, and advanced services.
2. **Threat Intelligence**  
   Gather landscape, actor profiles, campaign data, and exploit reports.
3. **Threat Modelling**  
   Analyse exposures, model attack paths, identify/mitigate risks, validate controls.
4. **Threat Hunting**  
   Plan and execute hunts, identify active exploitation, collaborate on remediation.
5. **Advanced Threat Services**  
   Adversary profiling, deception, honeypots/honeynets, red/purple teaming.
6. **Intel Sources**  
   OSINT feeds, vendor advisories, underground forums, research reports.
7. **Intel Processes**  
   Source scanning, threat reporting, mitigation guidance, TTP documentation.
8. **Intel Report Types**  
   Strategic (non-technical), tactical (current threats), technical, operational.
9. **Modelling Steps**  
   Identify components, data flows, trust boundaries, apply STRIDE/attack trees.
10. **Modelling Techniques**  
    STRIDE, attack trees, PASTA, LINDDUN, Kill Chain, Trike, OCTAVE, ATT&CK.
11. **Hunting Process**  
    Define hypothesis, gather/analyze evidence, correlate, report outcomes.
12. **Hunting Types & Tools**  
    Structured (TTPs), unstructured (IOCs), situational; SIEM, XDR, analytics.
13. **Advanced Services**  
    Exploit POCs, honeypots/honeynets, adversary TTP capture, red/purple teaming.
14. **Honeypots/Honeynets**  
    Decoys for adversary observation and analysis.
15. **Service Maturation**  
    Foundation to Optimized for intel, modelling, and hunting capabilities.
16. **NIST Alignment**  
    Identify (intel/model), Detect (hunting), Protect (controls), Respond (IR support).
17. **ISO 27001 Alignment**  
    Covers controls A5–A18 supported by threat management functions.
18. **MITRE ATT&CK Mapping**  
    Align threat functions with adversary tactics & techniques.
19. **Cross-Function Collaboration**  
    Works with IR, SecMon, SecEng, Ops, Architecture/Risk.

Session 8:

Application Security Management

1. **Application Security Scope**  
   Legacy mainframe, desktop, mobile, server, containers, and microservices.
2. **SDLC Phases**  
   Planning, analysis, design, implementation, testing/integration, maintenance with security tasks.
3. **Delivery Models**  
   Waterfall vs Agile (Scrum); both require embedded security.
4. **Waterfall Security Gates**  
   Security requirements at PID, design, implementation, test, and operation.
5. **Agile DevSecOps**  
   “Shift left” security in epics/stories with CI/CD tooling integration.
6. **Third-Party Software**  
   COTS risk assessment, secure configurations, and vendor management.
7. **SaaS Considerations**  
   Vendor-provided IAM, data protection, and business continuity governance.
8. **App Security Framework**  
   IDE plugins, SAST/SCA, DAST, container scans, pen testing, WAF, runtime analysis.
9. **Security Planning**  
   Define privacy, legal, regulatory, and policy requirements.
10. **Security Design**  
    Select controls from architecture, develop blueprints and patterns.
11. **Implementation Support**  
    Configure CI/CD for SAST/SCA/container scans and vet remediation.
12. **Testing Phase**  
    Set up DAST/API tests, analyze findings, support remediation and bug bounties.
13. **Operational Controls**  
    Secure deployments, runtime protections, WAF rule configuration, monitoring.
14. **Secure Coding Practices**  
    Culture building, training, code reviews, tooling, shift-left approach.
15. **SAST**  
    Source-code scanning for OWASP/SANS top flaws, CI/CD integration, FP removal.
16. **SCA**  
    Dependency scanning against vulnerability databases and license checks.
17. **DAST**  
    Black-box testing for runtime vulnerabilities, pipeline integration, remediation feedback.
18. **Container Security**  
    Image/config scanning, CI/CD hooks, modern workload protection.
19. **Penetration Testing**  
    External or bounty-based assessments pre-go-live and periodically.
20. **Posture Management**  
    Cloud asset inventory, config assessment, and policy enforcement in operations.

Session 9:

Incident Management

1. **Incident Phases**  
   Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned.
2. **Preparation Tasks**  
   Policy creation, team structuring, playbook development, training/exercises.
3. **Identification**  
   Define declaration criteria, assess indicators, notify stakeholders, track incidents.
4. **Containment**  
   Isolate affected environments, secure evidence, maintain chain of custody.
5. **Eradication**  
   Eliminate root cause and collaborate with TVM for remediation.
6. **Recovery**  
   Restore systems from clean backups, validate integrity, resume operations.
7. **Lessons Learned**  
   Conduct post-mortems, document findings, implement improvements.
8. **Phase Outputs**  
   Policies, org charts, playbooks, simulation and incident reports.
9. **Incident Severities**  
   C1 (Major) to C4 (Minor) based on impact and risk.
10. **Crisis Response Structure**  
    Roles for Crisis Manager, cyber teams, IT, business, legal, communications, externals.
11. **Playbook Creation**  
    Scenario definitions, indicators, triggers, RACI, processes, tools, and training.
12. **Tabletop Exercises**  
    Role assignments, scripted interjections, decision points, phase walkthroughs.
13. **Common Mistakes**  
    Failures in reporting, documentation, evidence handling, containment, and learning.
14. **Legal Considerations**  
    Criminal/civil liabilities, GDPR, NIS-D, DORA, HIQA, PSD2 compliance.
15. **Case Studies**  
    Ukrainian power grid, NotPetya at Maersk, Conti attack on Irish HSE.
16. **NIST Alignment**  
    Protect (plans/testing), Detect (alerts), Respond (execution/forensics), Recover (plan updates).
17. **ISO 27001 Alignment**  
    Controls A16 (incident) and A17 (continuity), plus compliance (A18).
18. **MITRE ATT&CK Mapping**  
    IR actions mapped to detection, containment, response, and recovery tactics.
19. **Communication Plans**  
    Media, internal, and customer messaging as part of IR.

Session 10:

Security Architecture & Strategy Implementation

1. **Security Architecture Role**  
   Defines principles, control frameworks, patterns, blueprints, and governance.
2. **Enterprise Security Architecture**  
   Covers network, infrastructure, application, data, user, defense, governance, and risk.
3. **Network Architecture**  
   Trust zones, data-flow principles, tech selection, configuration guidelines, metrics.
4. **Infrastructure Architecture**  
   System-interaction principles, logical controls, roadmap, standards, metrics.
5. **Application Architecture**  
   Dev/deploy principles, tooling selection, SDLC integration, and metrics.
6. **Data Architecture**  
   Data-security principles, protection capabilities, end-to-end rules, standards.
7. **User Architecture**  
   User protection layers, privileged-user controls, and standards.
8. **Cyber Defense Architecture**  
   Define defense capabilities, operating model, strategy, and standards.
9. **Architecture Integration**  
   Map security requirements, integrate controls, apply frameworks, evaluate compliance.
10. **Architecture Activities**  
    Document requirements, create ESA, define principles, patterns, standards, governance.
11. **Security Blueprint**  
    Aggregate principles, frameworks, reference architectures, trust zones, processes.
12. **Security Principles**  
    CIA triad, security by design, least privilege, defense in depth, zero trust, automation.
13. **Security Patterns**  
    Infrastructure (auth, placement), network (flows), application (APIs, code security).
14. **Architecture Assessments**  
    Classification, requirement mapping, compliance checks, and exception handling.
15. **Security Strategy Role**  
    Direction-setting using risk, maturity, threat, and business inputs.
16. **Strategic Outputs**  
    Prioritized initiatives with effort estimates and governance/change plans.
17. **Security Roadmap**  
    Actionable plan aligning priorities, resources, progress metrics, and stakeholder buy-in.
18. **Policies & Standards**  
    Policy framework based on ISO 27002 covering policies, standards, and guidelines.
19. **Risk Management**  
    Systematic capture of cyber risks feeding into ERM, guided by NIST RMF.
20. **Training & Awareness**  
    Cyber hygiene, routine practices, and culture building underpinned by policies.