

CISO MindMap 2025

What do Security Professionals Really do?

Managing Security Projects
Business Case Development
Alignment with IT Projects
Balancing budget for People, Training, and Tools/Technology/Hardware, travel, conferences
Communicating and reporting
CapEx and OpEx considerations
Technology prioritization
Secure redundant & under utilized tools
Recruiting, performance and retention
Staff turnover prevention
Balance FTE and contractors
Staff training and skills update

Acquisition Risk Assessment
Network/Application/Cloud Integration Cost
IAM integration
Security tools rationalization
Multi-Cloud architecture
Strategy and Guidelines
Cloud Security Posture Management (CSPM)
Ownership/Liability/Incidents
Vendor's Financial Strength
SLAs
Infrastructure Audit
Disaster Recovery Business
Proof of Application Security
Data ownership, compliance
Integration of Identity Management/Access/SSO
SaaS Policy and Guidelines
Cloud log integration/APIs
Virtualized security appliances
Cloud-native access security
Container-to-container communication security
Service mesh, micro services
Serviceless computing security
Technology advancements

Cloud Computing
Cloud log integration/APIs
Virtualized security appliances
Cloud-native access security
Container-to-container communication security
Service mesh, micro services
Serviceless computing security
Technology advancements

Mobile Technologies
Lost/Stolen devices
BYOD and MDM (Mobile Device Management)
Mobile Apps Inventory
MIDN: Spoofing/Phishing
Business Partnerships
Agility, Business Continuity and Disaster Recovery
Oversight industry trends (e.g. ML, Threats, etc.)
Evaluating Emerging Technologies (Quantum, Crypto, GenAI, etc.)
IoT Frameworks
Hardware/Devices security features
IoT Communications Protocols
Device Identity, Auth and Integrity
Over the Air updates
Track and Trace
Condition Based Monitoring
Contextual Experience
Smart Grid
Smart Cities / Communities
Others
IoT SaaS Platforms
Augmented and Virtual Reality
Drones
Edge Computing

IoT
Track and Trace
Condition Based Monitoring
Contextual Experience
Smart Grid
Smart Cities / Communities
Others
IoT SaaS Platforms
Augmented and Virtual Reality
Drones
Edge Computing

Artificial Intelligence and Generative AI (GenAI)
AI Governance, Policies, Transparency
LLMs, Chatbots, Agents, RAG
Safe and ethical uses of GenAI
Secure AI/GenAI models
Protecting Intellectual Property
Identify GenAI plausible use cases
Securing training and test data
Advanced attacks
AI enabled security tools, threat detection
Train Infedex teams on AI technologies
NIST AI Risk Mgmt Framework
Use of GenAI in risk assessment
AI/GenAI: Testing tools
OWASP Top 10 LLM and GenAI risk

Project Delivery Lifecycle
Embedding security in Project Requirements
Threat modeling and Design reviews
Security Testing
Certification and Accreditation
Traditional Network Segmentation
Micro segmentation strategy
Application protection
Defense-in-depth
Remote Access
Encryption Technologies
Backup/Replication/Multiple Sites
Cloud/Hybrid/Multiple Cloud Vendors
Software Defined Networking
Network Function Virtualization
Zero trust models and roadmap
SASE/SSSE strategies, vendors
Overlay networks, secure enclaves

Security Architecture
Traditional Network Segmentation
Micro segmentation strategy
Application protection
Defense-in-depth
Remote Access
Encryption Technologies
Backup/Replication/Multiple Sites
Cloud/Hybrid/Multiple Cloud Vendors
Software Defined Networking
Network Function Virtualization
Zero trust models and roadmap
SASE/SSSE strategies, vendors
Overlay networks, secure enclaves

Compliance and Audits
GDPR, GDSB & other data privacy laws
ISO
HIPAA and HITRUST
Regular Audits
SSAE 16
NIST SP 800-53
CMMC
HITRUST
SOC2
SEC notification requirements
Other compliance needs

Legal
Data Discovery and Data Ownership
Vendor Contracts
Investigations/Forensics
Attorney-Client Privilege
Data Retention and Destruction
Physical Security
Vulnerability Management
Ongoing risk assessment/pen testing
Code Review, SAST
Use of Risk Assessment Methodology and Framework
Policies and Procedures
Threats and Incident Awareness
Data Discovery
Data Classification
Access Control
Data Loss Prevention - DLP
Customer and Partner Access
Encryption/Keying
Monitoring and Alerting
Industrial Control Systems
Operational Technologies
PLCs
SCADA
HMIs
Third party risk management (TPRM) automation
Cyber Risk Quantification (CRQ)
Maximize Controlled Risk Register
Loss, Fraud prevention

Risk Management
Physical Security
Vulnerability Management
Ongoing risk assessment/pen testing
Code Review, SAST
Use of Risk Assessment Methodology and Framework
Policies and Procedures
Threats and Incident Awareness
Data Discovery
Data Classification
Access Control
Data Loss Prevention - DLP
Customer and Partner Access
Encryption/Keying
Monitoring and Alerting
Industrial Control Systems
Operational Technologies
PLCs
SCADA
HMIs
Third party risk management (TPRM) automation
Cyber Risk Quantification (CRQ)
Maximize Controlled Risk Register
Loss, Fraud prevention

Last update: March 31, 2025
Expiration date: September 30, 2026
Twitter: @rafeeq_rehman
Downloads: <http://rafeeqrehman.com>

InfoSec Professionals Responsibilities

Security Operations
Threat Prevention (NIST CSF Identify & Protect)
Asset Management
Network/Application/Firmware
Vulnerability Management
Security
Operating Systems
Network Devices
Applications
Databases
Code Review
Physical Security
Cloud/Containerization testing
Mobile Devices & Apps
Containers
Attack surface management
IAM
Identify (periodic or continuous)
Classify
Risk Based Approach
Prioritize (e.g. use of EPSS)
Mitigation (P, verify, false positive)
Sanitize
Application Security
Application Development
Secure Code
Secure Code Review
Application Vulnerability Testing
Change Control
File Integrity Monitoring
Risk Application Firewall
Integration to SIEM and Incident Response
Inventory open source components
Source code supply chain security
API Security
Network API and API
Identity Management
DLP
Anti Malware, Anti-spoof
Threat/Control/Filtering
DNS security filtering
Patching
Cloud Protection
Hardware gateways
Desktop security
Encryption, SSL, PII
Security Health Checks
Public address reputation
Security checks
Awareness training
Threat Detection (NIST CSF Detect)
Log Analysis/Correlation/SIEM
Alerting (SOC/PS, FIM, WAF, Anti Malware, etc.)
Network analysis
DLP
Threat hunting and insider threat
MISP integration
Threat Detection (periodic assessment)
Gap assessment
Promotion to IR plan
SOC Operations
SOC Structure Mgmt
SOC Staff continuous training
Shift management
SOC procedures
SOC Metrics and Reports
SOC and NCC integration
SOC Tech stack management
SOC DR exercise
Personnel on-call tasks
Long term trend analysis
Integrate new data
Insecure data areas
Unstructured data from IoT
Data Development
Machine Learning
Self Development
Understand Algorithm Biases
Autonomous
AI/ML
Drones
Medical Devices
Industrial Control Systems (ICS)
Switch at track
Data entry
De-Op integration
Prepare for unplanned work
Use of AI, Sensor and Data Analytics
Use of computer vision in physical security
Log anomaly detection
ML model training, retraining
Red team/blue team exercises
Integrate threat intelligence platform (TIP)
Detection technologies for breach detection
Full packet inspection
Detect misconfigurations
Integrate cloud based tools

Identity Management
Identity Credentialing
User provisioning and identity life cycle management
Single Sign On (SSO, Singleflight sign on)
Directory Synchronization, Cloud Identity, Local ID stores
Federation, SAML, Shibboleth
2-Factor (Multi-Factor) Authentication - MFA, C
Automated Approvals
Role-Based Access Control (RBAC)
Common identity, Economics and Mobile Apps
Personalized user interface
UI Process Integration
Integrating cloud-based identities
IoT service identities
IAM SaaS solutions
Unified identity profiles
Voice signatures
Face recognition
Passport-less authentication
IAM with Zero Trust technologies
Privileged Access Management (PAM)
Use of public identity (OAuth, OpenID, etc.)
Digital Certificates
API authentication and secrets management

Governance
Strategy and business alignment
Security policies, standards
Legal, regulatory and contract
NIST - relevant NIST standards
SOC
COSSO
COBIT
ITIL
FAIR
FISMA
CMMC
Visibility across multiple frameworks
Roles and Responsibilities (RACI charts)
Data Ownership, sharing, and data privacy
Confidential Management
Metrics and Reporting
Executive Metrics
Operational Metrics
Validating effectiveness of metrics
IT, OT, IOT/IIoT Convergence
Options for cooperative SOC, collaborative intranet
Tools and network considerations
Establishing control effectiveness
Maintaining a readiness plan for 1-5 years
Board oversight and board presentations
Aligning with Corporate Objectives
Continuous Mgmt Updates, metrics
Integration, grow and take
Corporate policies, picking battles carefully
Innovation and Value Creation
Expectations Management
Proactive program risk reduction
BSGS

Security Team Branding
Enable Secure Application access
Secure expanded attack surface
Security of sensitive data movement from home
Zero trust access to applications
Automate patching
Secure DevOps, DevSecOps
Embedding security tools in CI/CD pipelines
Automate threat hunting
Automate risk scoring
Automate asset inventory
Secure infrastructure as code
Automate API inventory
Automate risk register
Automate security metrics
Automate incident response where applicable
Automate compliance checks

Automation and Analytics
Automate patching
Secure DevOps, DevSecOps
Embedding security tools in CI/CD pipelines
Automate threat hunting
Automate risk scoring
Automate asset inventory
Secure infrastructure as code
Automate API inventory
Automate risk register
Automate security metrics
Automate incident response where applicable
Automate compliance checks

Remote Work
Enable Secure Application access
Secure expanded attack surface
Security of sensitive data movement from home
Zero trust access to applications

Incident Management (NIST CSF Respond & Recover)
Create adequate incident response capability
Incident Response Playbooks
Incident Response Assessment
Forensic Investigation
Data Breach Preparation
Update and Test Incident Response Plan
Set Leadership Expectations
Foster and IR Partner relations
Advisable Logging
Search exercises (e.g. simulated)
First responders training
IS Playbook testing
Media Relations
Business Continuity Planning
Recovery
Identify critical systems
Perform ransomware BIA
Uniform ransomware BIA
Develop ransomware strategy
Secure adequate backups
Periodic backup test
Offline backup in case backup is compromised
Implement machine integrity checking
Automation and SOAR
Supply chain incident mgmt
Data inventory of software components
Integrate into vulnerability mgmt
Integrate into SOC and risk mgmt process
Managing relationships with the environment
Cyber Risk Insurance

Focus Areas for 2025-26

1. It is time for securing GenAI
2. Consolidate and rationalize security tools
3. Identify and manage security debt
4. Ransomware and Cyber resilience
5. Create meaningful metrics
6. Improve Cyber Hygiene

© Copyright 2012-2025 - Rafeeq Rehman