CSO/CISO/BISO/TISO/ISO-Cybersecurity Operations Concerns

Cybersecurity Operations

Cybersecurity Services Catalog

Vulnerability Management
- Penetration Testing
- Vulnerability Assessment
- Static Analysis Security Testing (SAST)
- Red/Blue Team Testing
- Dynamic Analysis Security Testing (DAST)

eMail Security
- Antimalware
- Phishing Mitigation
- SPAM Filtering
- Safe Links

Denial of Service Mitigation
- Economic DoS Mitigation
- DDoS Mitigation

Application Gateways
- Web Application Firewall
- SOA/XML Gateway
- API Gateway

Identity and Access Management
- Directory Services
- Federated Services
- Single Sign-On
  - OAuth
  - Open ID
  - SAML
- Password Reset
  - Self-Service Password Reset
  - Help Desk
- Passwordless
  - Passkeys
- Multi-Factor Authentication
  - Soft Token
  - Hard Token
  - Authenticator Applications
- Access Control
  - Rule-Based Access
  - Attribute-Based Access
  - Role-Based Access
  - Risk-Based Access
- Biometrics
  - Finger/Palm Print
  - Iris/Facial Scan
  - Key Stroke Recognition
  - Voice Recognition

Security Incident and Event Monitoring (SIEM)

Security Orchestration, Automation, Response (SOAR)

Endpoint Protection/Endpoint Detection & Response (EPP/EDR)
- Antispyware
- Software Firewall
- Malware Behavioral Analysis
- User Behavioral Analysis
- Whole Disk Encryption
- File Integrity Monitoring
- Host Intrusion Detection/Prevention
- Trusted Platform Module
- Antimalware/Anti-Virus
- Safe Boot/BIOS Integrity

Artifical Intelligence
- LLM/SLM
- Deep Learning
- Machine Learning
  - Supervised
  - Unsupervised

Cryptography
- Asymmetric Algorithms
- Hashing Algorithms
- Encryption at Rest
- Quantum Algorithms
- Symmetric Algorithms
- Public Key Infrastructure
- Encryption in Transit
  - Virtual Private Networks (VPN)
  - IPSec
  - TLS
- Certificate Authority
  - Internal CA
    - Device Certificates
    - User Certificates
  - Public Trusted CA
    - Extended Validated Certificates
- Hardware Security Modules
  - Trusted Platform Modules

Malware Behavioral Analysis

Mobile Data Management (MDM)

File Security/Activity Monitoring

File Integrity Monitoring

TLS Decryption

Cloud Access Security Broker (CASB)

User Behavioral Analysis

Network Detection and Response (NDR)

Data Leakage/Data Loss Protection (DLP)

Cloud Financial Operations

Asset Management

Incident Detection

Security Analysis
- Lateral Movement Analysis
- NetFlow Analysis
- Malware Behavioral Analysis
- IoCs
- User Behavioral Analysis
  - Systems Accessed
  - Authentication and File Access
  - Locations and Time of Day/Night

Threat Intelligence
- Threat Intelligence Feeds
  - Indusrty IoCs
  - Threat Notifications
- ISAC Membership
  - Indusrty IoCs
  - Indusrty Attack Trends
  - Threat Intelligence Sharing
  - Industry Attack Vector Identification

Policy Violations
- Shadow IT
- Shadow API
- Shadow AI

Detect and Analyze Phase
- Incident Identification
- Incident Classification

Third-Party Notification Monitoring

Fraud Monitoring

Alert Monitoring

Threat Hunting
- Insider Threat Analysis
- Deep Dive Analysis
- IoC Analysis
- Lateral Movement Analysis
- User Behavioral Analysis

Incident Response

Investigations

Forensic Analysis
- Chain of Custody
  - Evidence Collection
  - Evidence Preservation
- Third-Party Retainer
  - Incident Timeline
  - Forensic Data Collection
  - Threat Elimination Attestation

Law Enforcement Engagement
- International
  - Interpol
- Federal
  - FBI
  - DHS
  - US Secret Service
- State
  - Local

Legal Engagement
- Client Attorney Privilege
  - Discovery
    - eDiscovery
  - Litigation Hold
- Criminal Prosecution
  - Employee
  - Third-Party
- Attorney Work Product Doctrine
  - Warrants
  - Subpoenas
  - Search Orders
- Tort/Civil Litigation
  - Class Action Lawsuits
  - Identity Theft and Credit Monitoring

Breach Notification
- Vendor/Supplier Notifications
- Client Notifications
- Consumer Notifications
- Cyber Insurance Notifications
- Public Relations
  - Social Media Release
  - Press Release
- Regulator Notifications
  - Federal Agencies
  - State Agencies
  - Federal AG
  - State AG

Standard Operating Procedures
- Playbooks
- Runbooks

Crisis Communication
- War Room
- Call Tree
- Executive Communications
- Board Communications

Continuous Improvement
- Red/Blue Team Testing
- Lessons Learned
- Purple Team Testing
- Tabletop Exercises
- Capability Gap Assessment
  - Skill Gap Asessment
  - Tooling Gap Assessment

Preparation

Detect and Analyze

Containment

Eradicate

Recover

Report

Remediate