The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0

Cybersecurity Domains

Security Architecture
- Data Leakage Prevention
- DDoS Prevention
- Patch Management
- Baseline Configuration
- Endpoint Hygiene
- Data Protection
- Network Design
- Secure System Build
- Certificate Management (Internal & External)
- Container Security
- Cloud Security
- Cryptography
  - Encryption Standards
- Access Control
- Federated Identity
- MFA & SSO
- Identity Management
- Privileged Access Management
- Identity & Access Management
- Security Engineering
- Key and Secret Management
  - Vaulting
  - HSM

Frameworks and Standards
- CIS Top 20 Controls / CIS Benchmarks
- NIST Cybersecurity Framework
- ISO 27001 27017 27018
- OWASP Top 10 (WebApp & API)
- MITRE ATT&CK Framework

Career Development
- Certifications
- Training
- Conferences
- Coaches and Role Models
- Peer Groups
- Self Study

Physical Security
- IoT Security

Security Operation
- Threat Hunting
- Vulnerability Management
- SOAR
- SIEM
- Active Defense
- Security Operation Centers
- Incident Response
  - Detection
  - Breach Notification
  - Containment
  - Blue Team
  - Investigation
  - Eradication
  - Breach Notification
  - Forensics
  - Red Team

User Education
- Training (new skills)
- Awareness (reinforcement)
- Cyber security table-top excersice

Threat Intelligence
- External
- Internal
- Contextual
- IOCs
- Intel. Sharing

Application Security
- CI/CD integration
- "Shift Left"
- Security UX
- S-SDLC
- Security QA
- API Security
- SAST
- Open Source Scan
- Source Code Scan
- Data-Flow Diagram

Risk Assessment
- Vulnerability scan
- Assets Inventory
- 4th Party Risk
- 3rd Party Risk
- Infrastructure (Network and Systems)
- Penetration test
- Social Engeering
- Risk Monitoring Services (Risk score)
- DAST
- Application Pen Tests

Enterprise Risk Management
- Risk Treatment Actions
- Risk Acceptance Statement
- Cyber Insurance
- 1. Process Owners
- Lines of Defense
- 2. Risk Mgmt Group
- BCP/DR Plan
- Risk Register
- 3. Audit
- Risk Appetite
- Crisis Management
- SOC1/SOC2
- ISMS

Governance
- Laws and Regulations
  - PCI
  - HIPAA
  - Industry Specific
  - GDPR
  - Central Government
  - GLBA
  - Regional
  - CCPA
  - NYS-DFS 23 NYCRR 500
- Executive Management Involvement
  - Risk Informed
- Company's Written Policies
  - Reports and Scorecards
  - KPI / KRI
  - Internal Policy
  - Standard
  - Guideline
  - Procedure
  - Compliance & Enforcement