Cybersecurity Architecture Roadmap

Version 2.1 – April 2019 © Adrian Grigorof

Currently implemented
2019 implementation
2020 implementation
Not on the roadmap

NIST Risk Management Framework – SP 800-18

Categorize System | Select Controls | Implement Controls | Assess Controls | Authorize System | Monitor Controls

Information Security Office

- Incident Response and Recovery
- Asset Management
- Vulnerability Management
- SIEM & Analytics
- Penetration Testing / Red Teaming
- eDiscovery / Forensics
- Threat Hunting
- Configuration Management
- Patch Management
- Security Governance
- Awareness and Training
- Security Architecture
- Risk Assessments / Compliance
- Supply Chain Risk Management

MSSPs

- Managed NAC
- Managed SIEM
- Managed Firewalls/IDS/IPS/Web Filtering
- Managed IPS/IDS
- eDiscovery / Forensics Retainer
- Threat Hunting
- Managed Detection and Response

Clients

On-premises & Mobile

Managed Clients

Endpoint Protection (EP)
Endpoint Encryption (EE)
Endpoint DLP
Endpoint DR
Device Authentication
VPN Client

CASB
MDM
NAC
MFA

Hybrid Infrastructure

	On-premises	IoT Operational Technologies	3rd Party Hosting Private Cloud	Public Cloud	Software as a Service (SaaS)
Extranet / DMZ	Firewall IPS Web Filtering Edge DLP Antimalware SSL Decryption WAF FIM EDR	Firewall IPS WAF	Firewall EP WAF DLP FIM	Firewall IPS Cloud DLP WAF	Email Antimalware SSO MFA CASB
Endpoints	Firewall EP DLP EDR FIM DB Encryption	Firewall EP FIM	Firewall EP EDR FIM DB Encryption	EP EDR FIM DB Encryption Application Segmentation	
LAN / WLAN	NAC ACLs Wireless IDS NMS	NAC ACLs Wireless IDS NMS	ACLs		

Privileged Access Management (PAM)
Identity and Access Management (IDAM) / IDAM Governance
Log Collection / Monitoring / Baselining
Vulnerability / Patch Management / Backup and Disaster Recovery / PKI / Key Management
Asset Management

Identify

- Governance
- Risk Assessments
- Compliance
- Configuration Management
- Vulnerability Scanning
- Penetration Testing
- Asset Management

Protect

- Firewalls / ACLs
- Remote Access (VPN)
- Endpoint Protection (EP)
- Email Antimalware
- Intrusion Prevention (IPS)
- Web Filtering
- Identity and Access Management (IDAM)
  - Single Sign-On (SSO)
  - Multi-Factor Authentication (MFA)
  - Privileged Access Management (PAM)
  - IDAM Governance
- Network Access Control (NAC)
- Mobile Device Management (MDM)
- Endpoint Encryption (EE)
- Database Audit Monitoring
- Device Authentication
- Web Application Firewall (WAF)
- Database Encryption
- Cloud Access Security Broker (CASB)
- Application Segmentation
- Public Key Infrastructure (PKI)
- Key Management
- DDoS Protection
- Application Whitelisting

Security Controls vs NIST Cybersecurity Framework

Detect

- SIEM & Analytics
- Intrusion Detection (IDS/IPS)
- Vulnerability Scanning
- Wireless IDS
- Endpoint EDR / HIDS
- Endpoint DLP
- Edge DLP
- Edge Antimalware
- SSL Decryption
- NMS
- File Integrity Monitoring (FIM)
- Baselining
- Threat Hunting
- Threat Intelligence Feeds
- Deception / Honeypots
- Code Analysis

Respond

- Incident Response and Recovery
- Endpoint Detection and Response
- eDiscovery / Forensics

Recover

- Disaster Recovery Planning
- Incident Response and Recovery

NIST SP 800-53 - Security and Privacy Controls for. Federal Information Systems and Organizations