Enterprise Cybersecurity Architecture Paradigm-Reference Architecture

Enterprise Cybersecurity Architecture attempts to bring order to chaos, control the things it can, while minimizing impact from risks, threats, vulnerabilities, and exposures.

Enterprise Cybersecurity Architecture requires people, process, and technology to guard against risks, threats, vulnerabilities, and exposures.

People are generally the weakest link within an Enterprise Cybersecurity Architecture.

What is Enterprise Cybersecurity Architecture trying to guard against (not an exhaustive list)?

- Espionage
- Insider Threats
- Equipment Theft
- COTS Vulnerabilities
- Social Engineering
- Malware
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges
- APTs

Ensuring risks, threats, and vulnerabilities do not become an exposure.

If threats materialize can they be stopped within the cybersecurity killchain?

Cybersecurity Killchain

1. Reconnaisance
2. Weaponization
3. Delivery
4.Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

Can tooling, incident response, and SOC-Detect, Identify, Respond and Correct? Would anyone know?

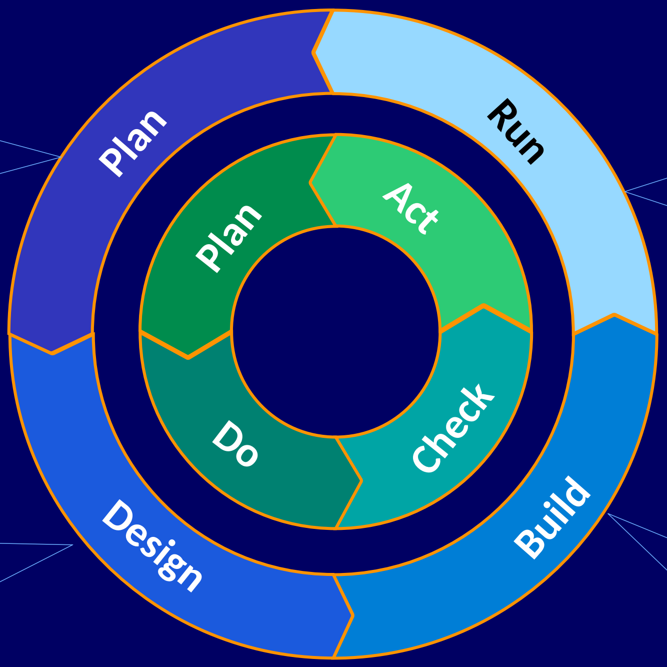
Where do Enterprise Cybersecurity Architecture Expectations Lead (not an exhaustive list)?

- Disaster Recovery
- Business Continuity
- Personnel Security
- Physical Security
- IoT Security
- ICS/SCADA Security
- Application Security
- System Security
- Database Security
- Information Security
- Mobile Security
- Network Security
- Cloud Security
- SecOps

The Expectations of the Enterprise Cybersecurity Architecture Lifecycle

Strategy
Governance
Portfolio Management
Program Management
Project Management
Cost/Benefit Analysis
Value Proposition
Value Chain
Budgets/Forecast
ROI/TCO

Requirements Development
Control Selection
Gap Analysis
Diagrams/Models
Process Development
Secure Design
Risk Assessment
Risk Analysis
Threat Modeling

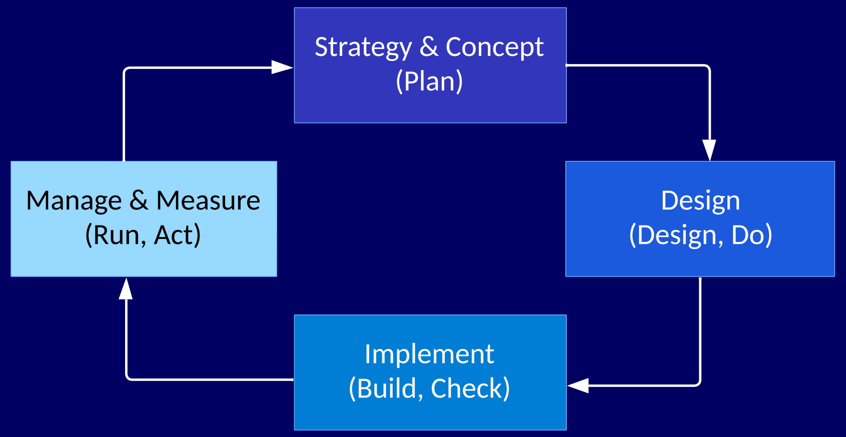


Secure Operations
Continuous Monitoring
Measurements/Metrics
Dashboards
Continuous Improvement
Red/Blue Team Exercises
Tiger Team Exercises
Purple Team Exercises
Threat Intellignce
Incident Response
Decomission

Secure Development
Secure Implementation
Secure Configuration
Secure Deployment
Vulnerability Assessment
SAST/DAST
Pentration Testing

- Cost Efficiency
- Operational Efficiency
- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Auditing
- Non-Repudiation
- Privacy

SABSA Lifecycle



Do you know where you are (current state)?
Do you know where you want to be (target state)?
Do you know how you're going to get there (transition state[s])?
Do you fully understand what you're trying to protect?
Do you have leadership support, the budget and the people to get there?