Defense in Depth

Table of Contents

- Definition
- Layered Security
- Operational Controls
- Technical Controls
- Personnel Controls
- Increasing Risk
- Reducing Success
- Real World Examples
- Common Attacks

Definition

- Assume Breach Mentality
- Integrate People, Process, Technology
- Continuous adaptation
- Attack Surfaces
- Networks, Ends, Applications, Data

Layered Security

- User Security Measures
- Perimeter Security Measures
- Network Security Measures
- Host Based Firewall
- Data Security Measures

Operational Controls

- Strategy Execution
- Performance Metrics
- Corrective Actions
- Shorter Time Horizons
- Subsystem/Functional level

Technical Controls

- Systems over People
- Automation
- Compliment not Antagonize
- Firewalls, Encryption, Access Control, EDR, IDS/IPS, VAS

Personnel Controls

- Background screening and Vetting
- Least Privilege
- Security Training
- Oversight
- Accountability

Increasing Risk

- Deception Operations
- Active Defense and Counterattack
- Threat Intelligence Sharing
- Offensive AI/ML
- Aggressive Legal Pursuit

Reducing Success

- SOC Visibility Triad (Logs, Traffic, Ends)
- Risk Adaptive Approach
- Accelerated Incident Response
- Network Segmentation
- Zero Trust Model

Common Attacks

- Malware
- Phishing
- DDOS
- MITM
- SQL Injection

Real World Examples

- BitCoin 2020
- Johnson Controls 2023
- MGM 2023
- Kyivstar 2023
- Rapid Reset 2023

Questions?