Cybersecurity Fundamentals

Table of Contents

- Cybersecurity Threats Landscape
- Principles of Information Security
- Risk Management Fundamentals
- Incident Response Policy
- Incident Response Execution
- Disaster Recovery Planning
- Network and System Security
- Remediation
- CIA Triad

Cybersecurity Threats Landscape

- Evolving Ransomware Attacks
- AI Powered Cyber Threats
- Exploitation of Software Vulnerabilities
- Supply Chain Management
- Expanding Attack Surface
- Advanced Persistent Threats

CIA Triad

- Confidentiality
- Integrity
- Availability
- Managed Balance

Principles of Information Security

- Least Privilege and need to know
- Accountability and Non-Repudiation
- Separation of Duties
- Compliance
- Policy Refinement

Risk Management Fundamentals

- Asset Identification and Prioritization
- Threat and Vulnerability Assessment
- Risk Calculation and Analysis
- Risk Treatment and Control
- Continuous Monitoring

Incident Response Policy

- Defined Procedure
- Clear Roles and Responsibilities
- Communication Plan
- Testing/Updates
- Recovery Objectives

Incident Response Execution

- Incident Response Plan
- Monitoring tools
- Forensic Analysis
- Containment
- Recovery
- Document

Disaster Recovery Planning

- Risk Assessment and Business Impact Analysis
- Recovery Objectives (Recovery Time vs. Recovery Point)
- Data Backup and Replication Strategies
- Recovery Site and Infrastructure Planning
- Documentation

Network and System Security

- Access Controls
- Software Version Control
- Firewall and segmentation
- Encrypt data at rest and in transit
- Maintain Audit Logs and Monitor

Remediation

- Prioritize Risk
- Automate updates
- Leverage virtual patching
- Shift Left for Efficiency
- Validate Fix

Questions?