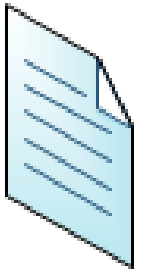
سبر 1213
Network Defense

Lecture #8 Part 1
Using Risk Management Tools

Risk Assessments

- Documenting the assessment

- Results valuable
  - Help organization evaluate threats and vulnerabilities
  - Should be protected
  - Only accessible to management and security professionals



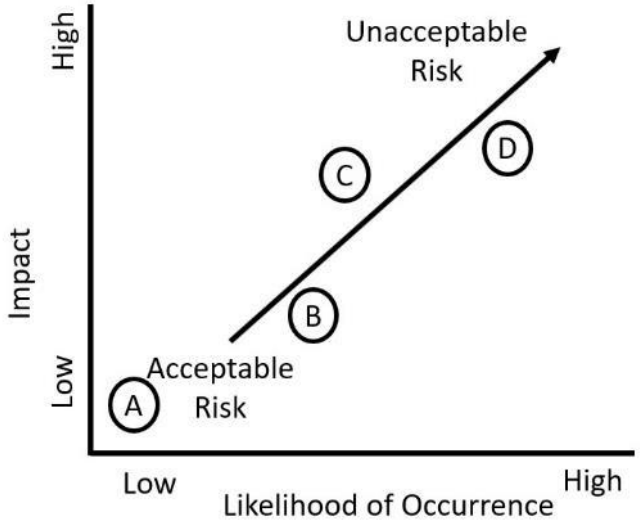
Risk Register

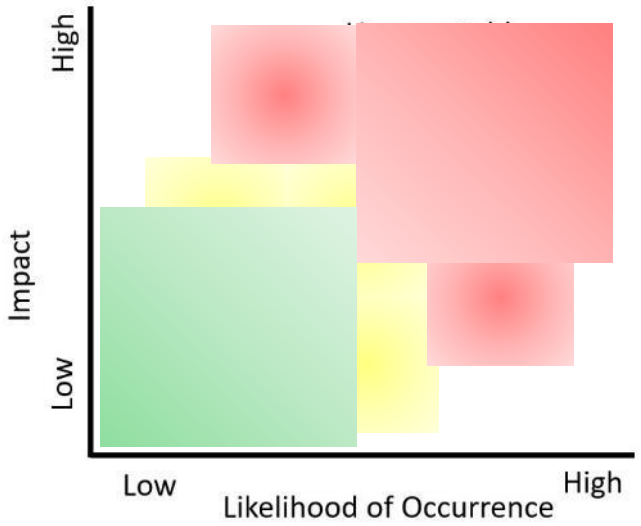
- A record of information on identified risks
- A repository of information on risks
- Often recorded in a table

- Category
- Specific risk
- Likelihood
- Impact
- Risk score
- Security controls
- Contingencies
- Risk score (with controls)
- Action assigned to
- Action deadline

Risk Matrix Versus Heat Map

- Risk matrix
  - Plots risks onto graph or chart





- Heat map
  - Uses colors such as green and red

Supply Chain Assessment

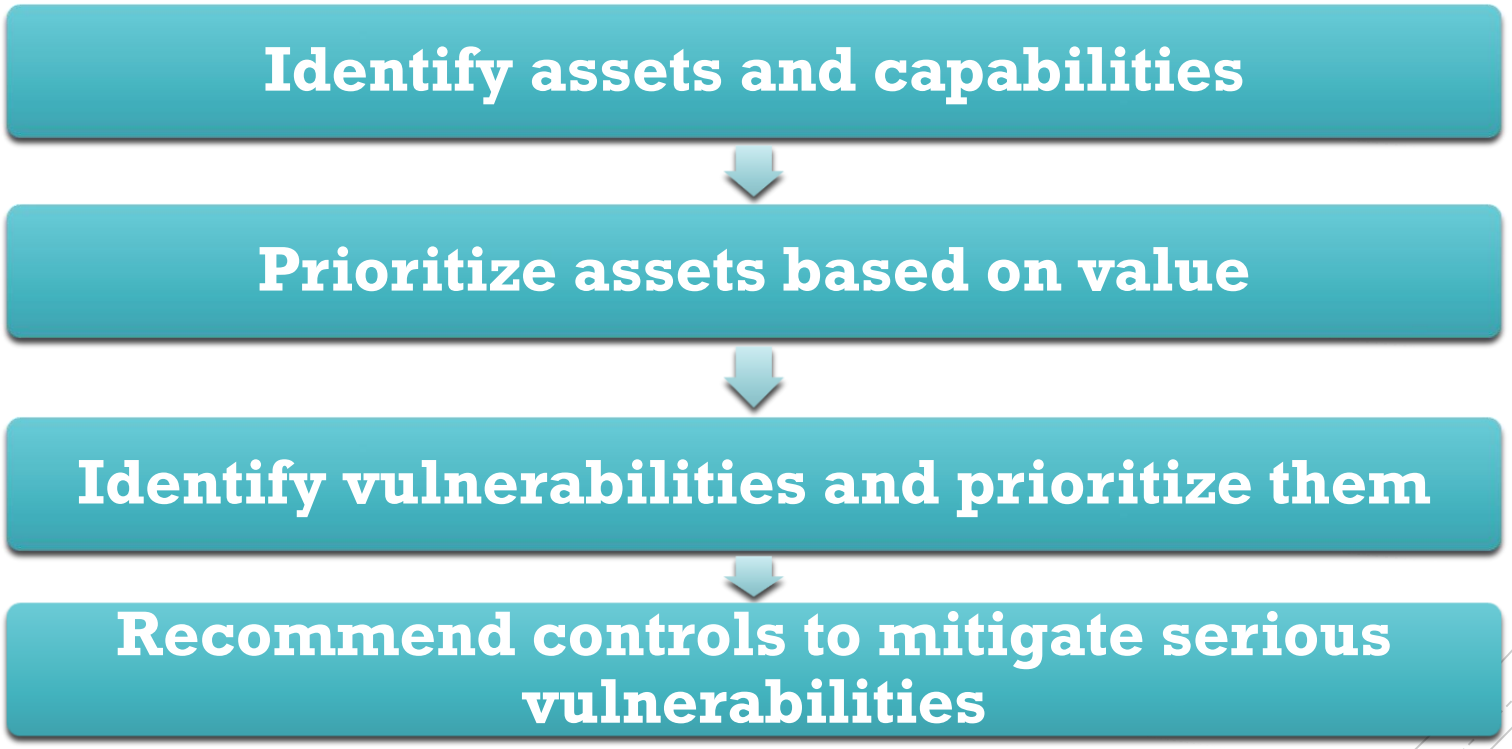
- Supply chain
  - Materials
  - All the processes required to create and distribute a product
- Assessment evaluates these elements
  - Identifies risks such as single point of failure

Risk Management

- Threat Hunting
  - gathering data on the threat through threat intelligence
  - internal sources (device logs, IDS alerts, and data)
  - external sources
  - Threat feeds
  - Adversary tactics, techniques, and procedures (TTPs)

Checking for Vulnerabilities

- Determines the security posture of a system
- Identifies vulnerabilities and weaknesses



Checking for Vulnerabilities

- Password cracker
  - Attempts to discover passwords

MD5 Hash:
161ebd7d45089b3446ee4e0d86dbcf92

Password: P@ssw0rd

  - Offline password cracker
  - Online password cracker

Checking for Vulnerabilities

- Network scanner
  - Nmap, Netcat, Nessus
  - Ping scan
  - Arp ping scan
  - Syn stealth scan
  - Service scan
  - OS detection

Network Scanners

- Network scanner
  - Arp ping scan
  - Syn stealth scan
  - Port scan
  - Service scan
  - OS detection

Vulnerability Scanning

- Identify vulnerabilities and misconfigurations
  - Open ports
  - Weak passwords
  - Default accounts
  - Sensitive data
  - Security and configuration errors

Vulnerability Scanning

- Passively test security controls
  - Does not exploit vulnerabilities
- Identify lack of security controls
  - Systems without patches
  - Systems without antivirus software

Vulnerability Scanning

- False positive
  - Scan detected a vulnerability
  - But the vulnerability doesn't actually exist
- False negative
  - Vulnerability exists
  - But the scan did not detect it