



Vulnerability, Patch & Availability Management



Vulnerability Management

This refers to the cyclical practice of identifying, categorizing and mitigating vulnerabilities



Patch Management

This covers the lifecycle of reviewing and applying patches to systems.



Vulnerability Management Threats

- Zero day vulnerabilities
- Workarounds (temporary fixes)



Patch Management Threats

- Patch failure
- Poor patch testing (time pressure)



Vulnerability Management Tools

- Intel from external sources
- Good communication plan



Patch Management Tools

- Multiple environments for testing
- Effective roll back procedures
- Virtual patching



Availability Management

Concerned primarily with uptime and also disaster recovery procedures.



Availability Management Threats

- Application failure
- DDoS attacks
- Misconfiguration
- Power failure
- Natural disasters



Availability Management Tools

- Load balancing
- Redundancy
- Backups
- Backup sites

