JASON DION
TRAINING THE CYBER SECURITY WORKFORCE


# Secure Endpoint Management

## THREAT MANAGEMENT

# Secure Endpoint Management

- Hardening System Configurations
- Patch Management
- Compensating Controls
- Group Policies
- Endpoint Security Software

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Hardening System Configurations

- Hardening a system makes it as resistant to attack as possible

- Examples:
  - Disabling unnecessary services
  - Disabling unnecessary ports
  - Verifying secure configurations
  - Centrally controlling device security settings



# Patch Management

- Once a patch is released by the vendor, attackers begin to reverse engineer it
- Organizations must ensure proper patch management to prevent attacks
- Examples:
  - Microsoft System Center Configuration Manager (SCCM)



# Compensating Controls

- If you can't implement a security control, you can compensate for it
- Provides a similar level of security by using an alternate means
- Examples:
  - WannaCry outbreak required disabling SMBv1, but this could break an file share
  - Point-of-Sale or embedded systems can't be updated without possibility of breaking



# Group Policy Objects (GPO)

- Provides admins an efficient way to manage system and security configuration settings across many devices in a network

- Examples:
  - Require the use a firewall on all hosts
  - Mapping to a share drive on login
  - Run scripts at login to verify compliance



# Endpoint Security Software

- Specialized software to enforce the company's security objectives/policies
- This software should report to a centralized management system for cyber security analysts to view and analyze
- Examples:
  - Antivirus or anti-malware
  - Host-based IDS or IPS



# Going the Extra Mile…

- Mandatory Access Control (MAC) sets all security permissions centrally and the users cannot change permissions locally
- Discretionary Access Control (DAC) allows the owners of a file or resource to control the permissions on that resource
- MAC has great security, but is an administration nightmare…only used in very sensitive environments (SE Linux)