JASON DION
TRAINING THE CYBER SECURITY WORKFORCE


# Implementing and Testing

## VULNERABILITY MANAGEMENT

# Implementing and Testing a Solution

- Vulnerability analysts don't implement the fixes
- Their role is to find the issues and pass them to the system administrators to fix
- Fixes may not be quick, often they require approval from the Change Control Board
- Fixes should be tested in a lab environment prior to rolling it out to the enterprise

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Coordinating Your Efforts

- Vulnerability Analysts view fixes as the highest priority…
- Not everyone in the organization does…
- You need to coordinate with others to get these vulnerabilities remediated
- Service degradation, promises to customers, and IT governance can slow down your efforts



# Service Degradation

- Vulnerability scanning places a resource tax upon the network and its servers when scans are conducted
- Scans can risk disrupting business functions
- Overcoming objections:
  - Consider different scanning times (non-peak hours)
  - Change scanning settings to lower intensity modes



# Promises to Customers

- MOUs and SLAs have specific uptime, performance, and other requirements that the organization must meet
- Scans can risk disrupting business functions
- Overcoming objections:
  - Ensure the cybersecurity team is involved in the drafting of the MOUs and SLAs
  - Discuss appropriate times and scope for scans

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# IT Governance

- Can create hurdles in getting approval to implement changes
- Fixes can risk disrupting business functions
- Overcoming objections:
  - Work within the organization policies when possible to get resources and support
  - Utilize the Emergency Change Control Board when critical fixed must be implemented quickly