JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Eradication and Recovery

CYBER INCIDENT RESPONSE

Eradication and Recovery

- Remove any artifacts of the incident
- Restore the network to full functionality
- Correct any security deficiencies
- Remove malicious code, sanitize compromised media, and fix any of the affected user accounts

What Recovery is Not…

- Not a rebuilding of the entire network…
- Not a full redesign of the system…
- Not a reason to buy all new equipment…

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Reconstruction and Reimaging

- Once an attacker touches your system, consider it compromised
- Reconstruct or reimage the system from a known good backup
- Consider the root cause of the incident so that the system isn't susceptible to the same attack vector again

Patching

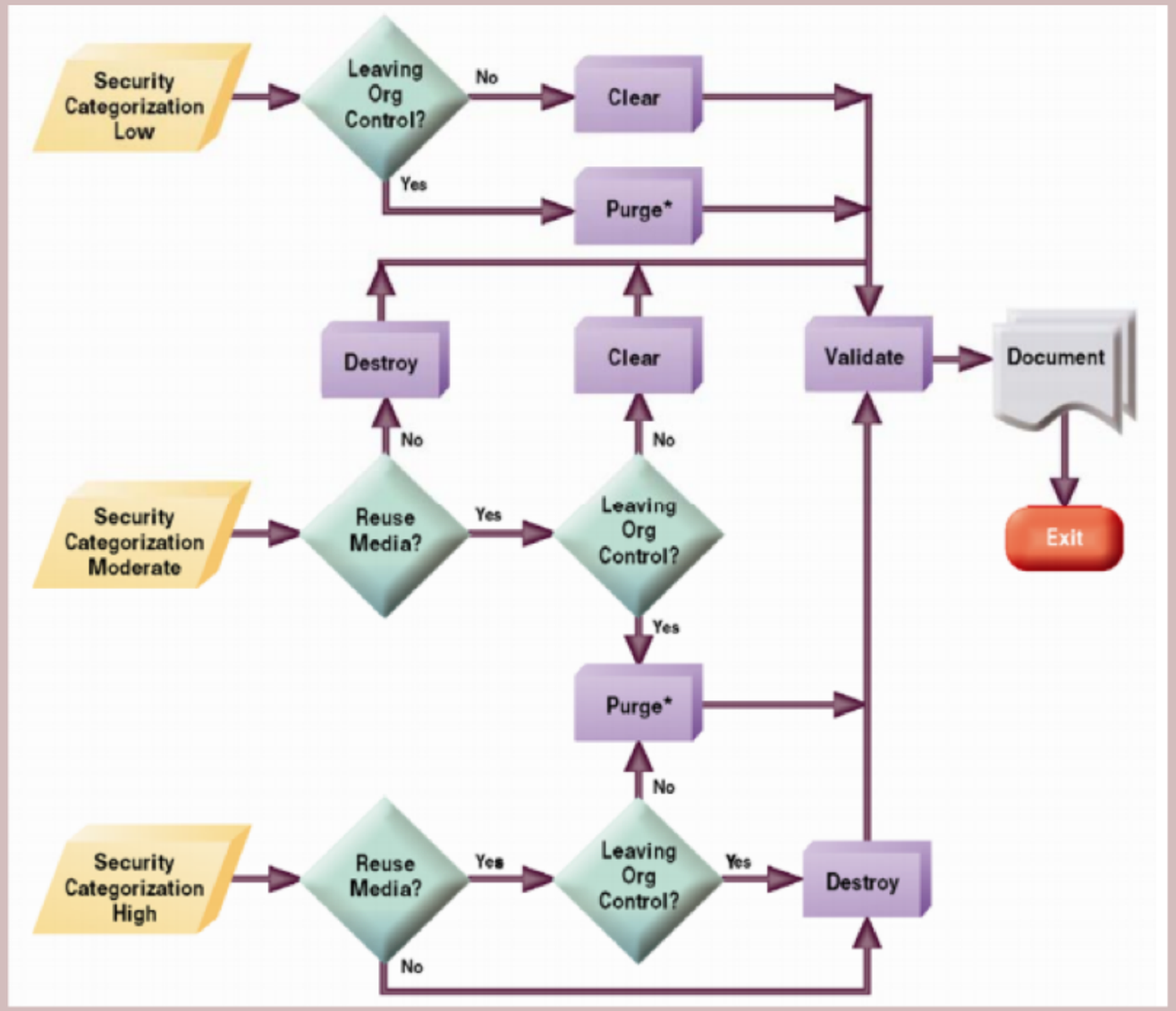
- Patch any systems that may be vulnerable to the same attack vector
- This is a good time to rescan and patch ALL of your systems…

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Sanitization and Disposal

- Clear
  - Logical techniques used to sanitize data (reset to factory state or overwriting a disk with all 0s)
- Purge
  - Physical or logical techniques to make data recovery from a disk infeasible using newest techniques (degaussing or overwrite 0s 35x)
- Destroy
  - Data recovery infeasible and disk drive unusable for storage (melting, incinerating, destroying)

Sanitization and Disposal



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Validation Effort

- Only authorized user accounts exist on each system in the network
- Verify permission assigned to each user
- Verify all systems are logging correctly
- Verify vulnerability scans on all systems are routinely conducted