COALITION INCIDENT RESPONSE

General Security Recommendations

BEST PRACTICES

Account Controls

- Implement multi-factor authentication (MFA) on any/all systems where it is supported
  - Email
  - Remote Connections
  - Citrix
  - VPN
- Inform users never to use the same password for business accounts and personal accounts
- Implement a password manager to enforce stronger passwords
- Do not re-use passwords between user accounts
- Reset user passwords to be 16+ characters, allow any characters and force block password reuse
- Create admin accounts separate from the normal user account. For example, instead of granting **john@fakedomain.com** domain admin access, create an account named **john.admin@fakedomain.com** for auditing purposes.

Security Hygiene Routines

- Ensure all anti-virus databases are up to date
- Perform vulnerability assessments and penetration tests against your environment
- Be diligent in patching all systems in the environment
- Implement cloud backups for all critical data
- Test all software before pushing to workstations
- Perform system upgrades as soon as support reaches end of life

Network Controls

- Block access on the firewall from unknown IPs or IP ranges

Windows Controls

- Block PowerShell on user end points / Windows machines
- Block executables from running in Temp locations
- Restrict run for auto-run registry key to block all or specific programs from running
- Disable SMBv1 across the environment
- Implement LAPS (Local Administrator Password Solution)
- Review Active Directory accounts and remove any stale accounts

COALITION INCIDENT RESPONSE

General Security Recommendations *contd.*

TOOLS, TRAINING, AND INSTRUCTION

Netwrix: AD account audits and alerts

- netwrix.com

LAPS: Microsoft's Local Administrator Password Solution

- Local Administrator Password Solution (LAPS)
- Local Administrator Password Solution

Disable SMBv1

- Disable SMB v1 in Managed Environments with Group Policy

Software Restriction

- Use Software Restriction Policies to block viruses and malware

Firewall Tips

- Poking Holes in the Firewall: Egress Testing with AllPorts.Exposed

Multi-Factor Authentication

- Duo.com (one of many MFA solutions for cross platform 2FA)
- Google Authenticator and other free solutions are available: google.com/landing/2step

Service to securely send sensitive data to recipient

- OneTimeSecret.com

DNS layer security

- umbrella.cisco.com