Group Policy Phases

Phase 1: Initial Setup and lock out
- Changed default admins and disables them
- Windows Defender
- Group Policy Update Time

Phase 2: Domain Security
- Polices
- Windows Update Settings
- Firewall

PHASE 1:

1. **Computer Config**
    a. **Policies**
        i. **Windows Settings**
            1. **Security Settings**
                a. **Local Policies**
                    i. **Security Options**
                        1. Accounts Administrator | Disabled
                        2. Accounts Microsoft accounts | Users can’t add or log on
                        3. Accounts Guest account | Disabled
                        4. Accounts limit local account | Enabled
                        5. Accounts Rename Administrator account | OldAdm1n
                        6. Accounts Rename Guest account | BadGuest
                        7. Network Access Do not allow anonymous enumeration * | Enabled
                        8. Network Access Let everyone permissions | Disabled
                        9. User Account Control : Switch to secure desktop
        ii. **Administrative Template**
            1. **Windows Components**
                a. **Windows Defender**
                    i. Allow antimalware service to remain running | Enabled
                    ii. Allow antimalware service to startup with normal | Enabled
                    iii. Configure local administrator merge behavior | Disabled
                    iv. Turn off routine remediation | Disabled
                    v. Turn off Windows Defender | Disabled
                    vi. Exclusions
                        1. Set all to disabled
                    vii. MAPS
                        1. Configure local settings override | Disabled
                        2. Join MAPS | Enable -> Advanced MAPS
                        3. Send file samples | Send safe samples

viii. **Network Inspection System**
   1. Specify Additional definitions | Disabled
   2. Turn on definition retirement | Enabled
   3. Turn on protocol recognition | Enabled

ix. **Quarantine**
   1. Configure local settings | Disabled
   2. Configure removal of items | Disabled

x. **Real-Time Protection**
   1. Configure local setting * | Disabled
   2. Monitor file and program activity | Enabled
   3. Scan all downloaded files and attachments | Enabled
   4. Turn off real-time | Disabled
   5. Turn on behavior monitoring | Enabled
   6. Turn on process scanning | Enabled
   7. Turn on raw volume | Enabled

xi. **Remediation**
   1. Configure local setting | Disabled
   2. Run Scheduled full scan | Every Day
   3. Specify the time of day | 0

xii. **Reporting**
   1. Leave alone

xiii. **Scan**
   1. Check for the latest virus | Enabled
   2. Turn on Heuristic | Enabled
   3. Allow users to pause scan | Disabled (Possibly enabled)
   4. Configure local setting * | Disable
   5. Scan * | Enabled

xiv. **Signature Updates**
   1. Allow definition updates * | Enabled
   2. Allow notifications to disable definitions | Enabled
   3. Allow real-time updates | Enabled

4. Check for latest virus and spyware definition on startup | Enabled
5. Define file shares | Disabled
6. Initiate definition update on startup | Enabled

xv. Threats

1. Specify threat alert level | Enabled everything to 2

2. System

a. Group Policy

i. Set Group Policy refresh interval (computers and domain controllers | 10 Minute Refresh with 1 minute random

Phase 2

2. Computer Config

a. Policies

i. Administrative Template

1. Windows Components

a. Windows Defender

i. Scan

1. Specify day of the week | Everyday
2. Specify the interval | 1
3. Specify the maximum depth | 3
4. Specify the maximum CPU | disabled
5. Specify maximum size of archive | Disabled
6. Specify the scan type | Enabled Full system scan
7. Specify the time for scan | Disabled
8. Start the scheduled scan | Disabled
9. Turn on catch-up * scan | Enabled
10. Turn on email scanning | Enabled
11. Turn on removal of item | Disabled
12. Turn on reparse point | Enabled

b. Windows Powershell

i. Turn on script execution | Allow local script and remote signed

c. Security Center

i. Turn on | Enabled

ii. Windows Settings

1. Security Settings

a. Account Policies

i. Password

1. Minimum age | 0 days
2. Minimum length | 12 characters

ii. Lockout

1. Lockout duration | 10 Minutes
2. Lockout threshold | 3 Minutes
3. Reset Counter | 10 Minutes

b. Local policies

i. Audit Policies

1. Audit logon events | success and failure
2. Audit privilege use | success and failure
3. Audit account management | success and failure
4. Audit logon events | success and failure
5. Audit policy change | success and failure

ii. User Rights Assignment

1. Access Credential Manager | Deny all
2. Access this computer from the network (Do by account, takes more time but is more secure)
3. Act as part of OS | Deny all
4. Add workstations to domain | Domain Admins
5. Allow log on locally | Domain Admins, Domain Users Administrators
6. Allow log on through Remote Desktop services | Domain Admins and Remote Desktop Users
7. Change system time | Domain Admins
8. Change time zone | Domain Admins

iii. Security Options

1. Domain Member: Digitally encrypt when possible | Enabled

2. Domain Member require strong session key | Enabled
3. Interactive Logon: Machine inactivity limit
4. Interactive Logon: Number of previous logon | 1
5. Interactive Logon: Message text | Authorized users only
6. Interactive Logon: Message title | Offical Notice
7. Microsoft network client digitally sign (if server agrees) | Enabled
8. Microsoft network client send unencrypted password | Disabled
9. Microsoft network server digitally sign (if client agrees) | Enabled
10. User Account Control: Admin approval mode for built-in | Enabled
11. User Account Control: Allow UIAccess applications | Disabled
12. User Account Control: Behavior of elevation prompt | credentials secure desktop
13. User Account Control: Behavior of elevation prompt (users) | credential secure desktop.
14. User Account Control: Detect application installations | Enabled

c. System Services

i. Windows Defender * | Automatic
ii. Windows Firewall | Automatic

d. Windows Firewall

i. Turn all profiles on to block inbound and outbound
    1. Display notification | Yes
    2. Apply local firewall rules | Yes
    3. Apply local connection security rules | Yes

e. Windows Remote Shell

i. Allow remote shell | Deny

f. Windows Update

i. Allow automatic update | Enabled
ii. Configure automatic update | 3 , Everyday @ 3
iii. Specify intranet Microsoft update | Disabled