Security baseline (Sept2019Update) for Windows 10 v1903 and Windows Server v1903

We are updating our Windows 10 v1903 and Windows Server v1903 security configuration baseline recommendations to address some issues:

* The first and most important change is that we are removing the Computer Configuration setting, “Enable svchost.exe mitigation options” (in System\Service Control Manager Settings\Security Settings) from the Windows 10 and Windows Server baselines at this time because of reports that in its current implementation it causes more compatibility issues than we had anticipated.
* We have also adjusted a few auditing settings in the Domain Controller baseline to align more closely with recommendations in the [Windows 10 and Windows Server 2016 security auditing and monitoring reference](https://www.microsoft.com/en-us/download/details.aspx?id=52630) document (also reflected [here](https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings)).

We have also added a Baseline-ADImport.ps1 PowerShell script to import all the baseline’s GPOs into Active Directory Group Policy, and improved other scripts, including preventing the local-policy script from running on Domain Controllers.