ASD ESSENTIAL 8

(Australian Signals Directorate)

SECURITY MADE SIMPLE

The most simple and affordable Security and Compliance Solution

SOC: QRadar

1	**Application whitelisting** of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. **Why:** All non-approved applications (including malicious code) are prevented from executing.	CMT + UEM
2	**Patch applications** e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications. **Why:** Security vulnerabilities in applications can be used to execute malicious code on systems.	CMT + UEM
3	**Patch operating systems.** Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions. **Why:** Security vulnerabilities in operating systems can be used to further the compromise of systems.	CMT + UEM
4	**Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. **Why:** Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.	CMT + iDaaS
5	**User application hardening.** Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers. **Why:** Flash, ads and Java are popular ways to deliver and execute malicious code on systems.	CMT + UEM
6	**Configure Microsoft Office macro settings** to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. **Why:** Microsoft Office macros can be used to deliver and execute malicious code on systems.	CMT
7	**Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository. **Why:** Stronger user authentication makes it harder for adversaries to access sensitive information and systems.	IDaaS
8	**Daily backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes. **Why:** To ensure information can be accessed again following a cyber security incident (e.g. a ransomware incident).	Backup solution & Cloud Apps

Learn about Essential 8 at: **https://asd.gov.au**

Try it for free at: **https://trials.maas360.com**