AISA

Essential 8 and the software supply chain

Paul McCarty - Founder SecureStack
paulm@securestack.com

AUSTRALIAN CYBER CONFERENCE 2022

SecureStack CEO

STARTUPS | DEVSECOPS | SNOWBOARDING

BOEING
NASA JPL
JOHN DEERE
Queensland Government
Regence
U.S.ARMY

What does Essential 8 have going for it?

- Easy to understand
- Describes controls that can be used anywhere
- Good penetration into mainstream
- Multiple maturity levels

What does Essential 8 NOT do very well?

- Reads as an enterprise Windows & desktop framework
- Not very inclusive
- Seems genuinely ignorant of the rest of IT

THE ESSENTIAL 8

- Application Control
- Patch Applications
- Configure Microsoft Office Macro Setting
- User Application Hardening
- Restrict administrative privileges
- Patch Operating Systems
- Multi-factor authentication
- Regular Backups

THE ESSENTIAL 8

Application Control

Patch Applications

Configure Microsoft Office Macro Setting

User Application Hardening

Restrict administrative privileges

Patch Operating Systems

Multi-factor authentication

Regular Backups

APPLICATION CONTROL

Microsoft

SDLC
Sofware Development Life Cycle

Control what binaries are allowed to run on Windows Desktop

Define what applications can run in the users browser via CSP, SRI, etc

PATCH APPLICATIONS

Microsoft

SDLC
Sofware Development Life Cycle

Make sure that desktop applications are up to date

Make sure that all application components are up to date & all CI/CD envs are up to date

CONFIGURE MICROSOFT OFFICE MACRO SETTING

Microsoft

Disable Microsoft Office macros

Yeah, naw.

USER APPLICATION HARDENING

Microsoft

Stop using browser technology from 2004

Encryption, TLS 1.3, HSTS, client side hardening, CSP, WAF, CDN, secure frameworks

RESTRICT ADMINISTRATIVE PRIVILEGES

Microsoft

SDLC
Sofware Development Life Cycle

Don’t use admin, don’t run apps as admin

Separate dev, staging, prod. Least permissions for CI/CD and app, no IAM *.*

PATCH OPERATING SYSTEMS

Microsoft

SDLC
Sofware Development Life Cycle

Patch the Windows OS

Scan for out of date packages. Current container images, CI/CD environments, don't use pinned versions

MFA

Microsoft

SDLC
Sofware Development Life Cycle

Users use MFA to log into apps, SaaS tools

Same same

REGULAR BACKUPS

Microsoft

SDLC
Sofware Development Life Cycle

Backups of important data, software, creds, and configurations stored centrally

Backups of all source code, creds, configurations stored centrally

https://github.com/SecureStackCo/Essential8-SDLC

Essential 8 mapping to ISM mapped to SDLC

Mitigation Strategy	Maturity Level Two	Maturity Level Three	SDLC
Application control	0843, 1490, 1657, 1660, 1661	0843, 1490, 1656, 1657, 1658, 1544, 1659, 1582, 1660, 1661, 1662, 1663	1536, 1757
Patch applications	1690, 1691, 1693, 1698, 1699, 1700, 1704	1690, 1691, 1692, 1693, 1698, 1699, 1700, 1704, 0304	0380, 0402, 0938, 1467, 1483, 1754

Paul McCarty

@eastsidemccarty

paulm@securestack.com

Continuous compliance-as-a-Service