Do you want the “secret sauce" to save your software from cyber attacks.....

@Chidambaram-narayanan

The truth is...

@Chidambaram-narayanan

There is NO silver bullet

@Chidambaram-narayanan

My mission is to help you (and I) grow and learn, every day! My favicons include:

- ✓ Auditing of financial and IT systems
- ✓ Cloud awareness
- ✓ Cybersecurity
- ✓ CISA

@Chidambaram-narayanan

CIS Critical Security Controls v8

CONTROL 01 Inventory and Control of Enterprise Assets	5 Safeguards	IG1 2/5	IG2 4/5	IG3 5/5
CONTROL 02 Inventory and Control of Software Assets	7 Safeguards	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03 Data Protection	14 Safeguards	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software	12 Safeguards	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05 Account Management	6 Safeguards	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06 Access Control Management	8 Safeguards	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07 Continuous Vulnerability Management	7 Safeguards	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08 Audit Log Management	12 Safeguards	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09 Email and Web Browser Protections	7 Safeguards	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10 Malware Defenses	7 Safeguards	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11 Data Recovery	5 Safeguards	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12 Network Infrastructure Management	8 Safeguards	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13 Network Monitoring and Defense	11 Safeguards	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14 Security Awareness and Skills Training	9 Safeguards	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15 Service Provider Management	7 Safeguards	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16 Applications Software Security	14 Safeguards	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17 Incident Response Management	9 Safeguards	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18 Penetration Testing	5 Safeguards	IG1 0/5	IG2 3/5	IG3 5/5

@Chidambaram-narayanan

A

Let’s start where it all begins…

Establish and Maintain an software inventory.

@Chidambaram-narayanan

B

Software inventory template to INCLUDE:

- ✓ Title
- ✓ Publisher
- ✓ Initial install/use date
- ✓ Business purpose for each entry;
- ✓ Uniform Resource Locator (URL),
- ✓ App store(s)
- ✓ Version(s)
- ✓ Deployment mechanism
- ✓ Decommission date.

@Chidambaram-narayanan

C

Ensure authorized software is currently supported

If unsupported:

- ✓ Is it necessary for the fulfillment of the enterprise's mission.
- ✓ If yes, document an exception detailing mitigating controls and residual risk acceptance.

Unsupported + No exception?

- ✓ Document & designate as unauthorized.
- ✓ Review the software list to verify software support at least monthly, or more frequently.

@Chidambaram-narayanan

D

Unauthorized software

- ✓ Discovery tool to identify such software;
- ✓ Perform risk assessment for each unauthorized software;
- ✓ Recommended to remove from use;
- ✓ Review monthly, or more frequently.

@Chidambaram-narayanan

E

Allowlisting of software

- ✓ Identify software and create an allow-listing;
- ✓ Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed.
- ✓ Reassess bi-annually, or more frequently.

@Chidambaram-narayanan

⚠ CAUTION

Merely whitelisting applications is not enough. You also need to whitelist the libraries they call.

It's no secret that cyberattackers love gaining access to script engines such as PowerShell. So scripts need to be regulated as well!

@Chidambaram-narayanan

F

Allow-listing of authorized libraries:

RECAP – A library is

- ✓ Pre-written code used to develop software programs and apps.
- ✓ Designed to assist both the programmer and the programming language compiler in building and executing software.

@Chidambaram-narayanan

F

Allow-listing of authorized libraries:

- ✓ Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process.
- ✓ Block unauthorized libraries from loading into a system process.
- ✓ Reassess bi-annually, or more frequently.

@Chidambaram-narayanan

F

Let’s back it up a bit….

DLL - Dynamic-link library (Microsoft)

- ✓ Shared library concept in Windows & OS/2 Op Sys.
- ✓ File extensions include DLL, OCX, or DRV

SO – Shared Objects (Linux)

- ✓ Same concept as above but in Linux.
- ✓ Shared objects, shared libraries, or shared object libraries.

@Chidambaram-narayanan

G

Allow-listing of scripts

Sure, but what is a script?

A computer language with several commands within a file capable of being executed without being compiled.

Examples of scripting languages include:

- ❑ Perl
- ❑ PHP
- ❑ Python
- ❑ JavaScript

G

Allow-listing of scripts

- ✓ Identify and inventory all scripts that are running on Enterprise Assets.
- ✓ Use technical controls (digital signatures and version control), to ensure that *only authorized scripts*, such as .ps1, .py, etc., files are allowed to execute.
- ✓ Block unauthorized scripts from executing.
- ✓ Reassess bi-annually, or more frequently.

@Chidambaram-narayanan

Let's recap

A. Maintain & manage inventory of software assets;
B. Ensure software is supported by vendors;
C. Utilize software inventory tools;
D. Address unapproved software;
E. Utilize application whitelisting;
F. Implement app whitelisting of libraries;
G. Implement app whitelisting of scripts

@Chidambaram-narayanan

Help my achieve my mission to bring valuable ideas, information & inputs to you.

Like, subscribe, follow (why not all 3?)

Thank you!

@Chidambaram-narayanan