WARNING

Internal controls inside

@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 Actively manage all software on the network so that only authorized software is installed and can execute.

@Chidambaram-narayanan

Why do we care?

A complete software inventory is the foundation for detecting, preventing & correcting cyber attacks

Need proof? Swipe left

@Chidambaram-narayanan

B

Still asking why?

- ✓ Attackers continuously scan for vulnerable versions of software;
- ✓ Lateral movement across the network;
- ✓ Potential licensing violations;
- ✓ Zero day attacks start here;
- ✓ Shadow networks/ computing;

@Chidambaram-narayanan

C

6 best practices

1. Establish & maintain a software inventory;
2. Ensure authorized software is currently supported;
3. Address unauthorized software;
4. Automated software inventory tools;
5. Allow-listing (whitelist/ blacklist);
6. Allow-list authorized libraries & 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