Top 15 Cyber Security Controls

Version 1.0 draft

September 2024

Introduction and FAQ

What is this?

This is a prioritized list of primarily technical cyber security controls that was deduced by analyzing known cyber attacks, that took place over the last decade around the world; attacks which very likely would have been deflected if these controls were in place. This is original research, and it was not derived from any existing framework, guide, etc.

This work began in 2023 out of pure curiosity and a desire to answer a question: "What attack tactics & techniques (T&T's) are the most common *today*, and how does their heatmap look like?" and, subsequently: "What is the minimum number of controls that should be put in place to defend against these T&T's?"

Hundreds of attacks were mapped to MITRE ATT&CK, leading to a map of 500+ mitigation techniques, that were grouped, summarized, and finally compressed to just 15 unique controls. Additional details and notes were added to each control to ensure that critical requirements are not missed.

Is it supposed to replace any of the existing security frameworks?

It's quite the opposite: this list complements existing frameworks (standards, guides) by providing an opportunity to prioritize the implementation of controls according to their importance.

Established frameworks, such as ISO 27001, NIST CSF or CIS Controls, provide a comprehensive approach to managing security in an organization and should be used as main source of knowledge. However, many of these frameworks require a security manager to build a risk register and figure out which risks are more likely and/or more impactful than the others and plan cyber security controls to mitigate them. Unfortunately, without having a bigger picture, this exercise often ends up being an educated guess at best — and reading the tea leaves at worst. As the result, organizations tend to implement complex controls first while missing the basics. This list is supposed to be such 'pocket bigger picture'.

Who can use this and how?

CISO, Head of Security, Security Manager, Consultant — discover security gaps in [your] company in 15 minutes; prioritize controls implementation when using a cyber security framework.

Pentester — focus on the statistically most problematic parts of the attack surface.

Vendor, Sales — leverage real-world data when positioning [your] products/tools before clients.

Is there a list of tools (products) that can be used to close discovered gaps?

There is an accompanying list of vendors and their product available in the project's GitHub repository in a file named **"Val's Top15 - tools.xlsx"** The work on this document is still in progress, but one can get an idea of which products could satisfy the controls' requirements.

I am representing a vendor; how can I add our tool (product) to the list?

Contact me by using GitHub discussions or LinkedIn (please include a note when connecting). If your product satisfies the requirements, it will be added to the list.

I would like to contribute to the project; how can I do that?

Same as above: contact me by using GitHub discussions or LinkedIn.

Where can I find the sources?

Everything is published in the project's GitHub repository.

Some intermediate documents have been redacted to remove (potentially) copyrighted content; they will be released in full upon receiving an authorization from rights holder(s).

Contents

Control #1: Privileged/User Account Management (M1026/1018)

Utilize Privileged/User Account Management solution with continuous audit.

a) Follow the least privilege principle and Just in Time/Just Enough Administration (JIT/JEA) practices.
b) Utilize phish-resistant MFA.
c) Accounts that cannot be protected by MFA must have complex, unique passwords across all systems on the network.
d) Utilize Local Administrator Password Solution (LAPS).
e) Conduct periodic access reviews for human and service (applications) identities

Control #2: Behavior Prevention on Endpoint (M1040)

Utilize anti-malware solution with behaviour analytics.

a) Solution must provide functionality at least equal to Microsoft Defender for Endpoint Attack Surface Reduction (ASR).

Control #3: Operating System Hardening (M1028)

Apply current operation systems hardening best practices.

a) Consider using **CIS Benchmarks**.

Control #4: Network Intrusion Prevention (M1031)

Utilize a Network Intrusion Prevention System.

Note: for cloud-only environments utilize native firewalls where applicable.

a) NIPS should be able to inspect SSL/TLS traffic, recognize known attack/malware traffic patterns, malicious domains and IPs.
b) Segment the network and block unnecessary traffic between segments.
c) Use remote desktop gateways when applicable.

Control #5: Execution Prevention (M1038)

Utilize execution prevention solution.

Note: may be embedded in Control #2: Behavior Prevention on Endpoint

a) Users should not be allowed to run system utilities (Mehta, cmstp, InstallUtil, odbcconf, hh, .cpl files) or scripting interpreters (VB, Python, Powershell) not required by their jobs.
b) Block unknown DLLs.
c) Ensure that accessibility features are protected from change or blocked if not required.

Control #6: User Training (M1017)

Conduct periodic user security awareness training.

a) Select vendors that cover most common attack techniques e.g., spear phishing, MFA bombing, etc.

Control #7: Unused OS Features and Applications (M1042)

Disable or remove applications, services, features and add-ins, that are not explicitly needed.

Note: this control extends Control #2: Operating System Hardening.

Control #8: Filter Web-Based Content (M1021)

Filter web traffic on firewall (proxy) and/or on endpoint.

Note: this functionality may be embedded in solutions for Control #2: Behavior Prevention on Endpoint or Control #4: Network Intrusion Prevention.

Control #9: Filter Email Content (M1054)

Configure email gateway to filter malicious content.

a) Implement Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) to validate incoming emails.
b) Configure Domain-based Message Authentication Reporting and Conformance (DMARC).

Control #10: Encrypt Sensitive Information (M1041)

Encrypt Sensitive Information at rest and in transit.

a) Include sensitive network authentication traffic (Kerberos), audit events traffic (if transferred to a SIEM), emails.
b) Enable Secure Boot and Enable full disk encryption (FDE) while using TPM module where applicable.

Control #11: Vulnerability Scans and Software Updates (M1051)

Conduct regular vulnerability scans of the infrastructure and update software and firmware regularly.

a) Test updates on a small subset of endpoints before wide implementation.

Control #12: Active Directory Hardening (M1015)

Conduct regular AD vulnerability assessments and implement recommended fixes.

a) Block LLMNR and NetBIOS traffic.
b) Enable SMB Signing.

Control #13: Secure Application Development (M1013)

Establish secure software development practices.

a) Conduct application developers-specific training that should include knowledge of OWASP's **Top 10** and **Application Security Verification Standard (ASVS)**.
b) Conduct threat modelling, weakness and vulnerability scans of the source code (SAST), compiled application security testing (DAST), third-party libraries (SCA), used images/containers (e.g., Docker) and Infrastructure-as-Code (IAC) templates.

Control #14: Data Loss Prevention (M1057)

Implement Data Loss Prevention solution.

a) The solution must cover endpoints and locally used media, including USB and other removable devices.
b) Restrict access to online storage (Google Drive, Microsoft OneDrive, Dropbox, etc.)

Control #15: Data Backup (M1053)

Perform regular data backups.

a) Consider following the "3-2-1" backup strategy, which requires storing at least one copy of backups off system in a remote (cloud) location.
b) Encrypt backups by default.
c) Ensure that the backup process cannot overwrite existing remote backups; prefer pulling data instead of pushing it.
d) Include Active Directory backup and/or rollback solutions as a separate option.

Artificial Intelligence usage disclosure

No Artificial Intelligence, LLMs, neural networks and other buzzwords were used during the research process and in the making of this document.

License

Sincerely,
Valeriy 'Val' Shevtsov

Change Log

Date	Version	Change
2024-09-05	1.0 draft	Initial draft; timed to my dad's 0b1000000'th birthday