



Best Practices Guide for Cyber Hygiene

Mission-focused strategies for securing networks against advanced threats

Executive summary

Effective cyber hygiene remains essential for defending networks against advanced persistent threats (APTs), including those leveraging artificial intelligence (AI) for computer network exploitation (CNE). As APTs and cybercriminals increasingly use AI to accelerate and scale various CNE techniques, the frequency and scale of targeting poorly configured and unpatched networks have also increased and will continue to do so. This guide will assist organizations looking to act now and develop plans for long term actions to harden networks against this changing threat landscape.

This guide is informed by NSA's operational experience in defense cyber operations, incident response, and Zero Trust implementation. Critically, these mitigations have been validated against various AI-generated exploitation plans and AI-identified vulnerabilities, proving their resilience in today's AI-enabled threat landscape. This guide emphasizes immediate actions to reduce risk, such as network inventory, multi-factor authentication (MFA), and patching, while building toward implementing Zero Trust practices, such as segmentation and continuous monitoring.

Cyber hygiene involves foundational steps to minimize attack surfaces, detect anomalies, and quickly respond to incidents. Organizations should prioritize Tier 0 activities (e.g., identifying security gaps and implementing common defensive improvements) to achieve quick wins, followed by Tier 1-3 enhancements. These practices align with NIST's [Cybersecurity Framework](#) functions and NSA's [Top Ten Cybersecurity Mitigation Strategies](#), addressing common misconfigurations and weaknesses exploited by adversaries.



Introduction

Adversaries increasingly use AI to automate the intrusion lifecycle, taking advantage of poor cyber hygiene, such as unpatched systems, weak authentication, and misconfigurations. NSA's red, blue, and hunt activities reveal persistent issues, including default configurations, insufficient segmentation, and inadequate monitoring. Network inventory is foundational—understanding what assets exist enables effective risk prioritization and mitigation. This guide prioritizes mitigations ranked by effectiveness against APT tactics, building on [NIST frameworks](#), DoD CIO's [Brilliant at the Basics](#) initiative, and NSA's [Top Ten Cybersecurity Mitigation Strategies](#).

Scope and audience

This guide is tailored for network defenders, cybersecurity teams, and enterprise leaders in the Department of War (DoW), Defense Industrial Base (DIB), and National Security Systems (NSS). It assumes familiarity with basic cybersecurity concepts and focuses on practical, prioritized actions informed by NSA assessments. While applicable broadly, it prioritizes defenses against AI-enhanced threats like automated reconnaissance and living off the land (LOTL) techniques.

The mitigations in the guide will help counter a broad range of exploitation techniques to help minimize mission impacts of network compromises; however, they do not cover every possible attack vector and should not be used as the sole means of hardening networks.

Mitigations

When applying the prioritized mitigations below, adhere to the following key principles: defense-in-depth, assume breach, least privilege, continuous validation, and human oversight of AI tools. The guide has progressive maturity tiers (distinct from NIST CSF Tiers)—each tier builds upon the previous, advancing from immediate risk reduction to sustained resilience. Start by implementing Tier 0 for immediate risk reduction, then progress to higher tiers. See **Appendix C: Aligning with NSA's Top 10 Cybersecurity Mitigation Strategies** for authoritative implementation resources.

Tier 0: Immediate activities to reduce risk

Focus on foundational gaps to halt common exploits and intrusion techniques with these high-impact, low-complexity actions:



1. Identify security gaps

- Establish a complete network inventory (see **Appendix A**) of hardware, software, user accounts, and data flows
 - Map assets to business functions
 - Identify gaps against security baselines
 - Use automated discovery tools to maintain currency
- Defend Privileges and Accounts
 - Implement identity and access management (IdAM)
 - Restrict privileged use;
 - Enforce time-based access
 - Limit IdAM roles
 - Audit accounts
- Segment Networks
 - Use next-generation firewalls to isolate critical systems
 - Consider Virtual Private Cloud (VPC) instances to limit lateral movement between critical services
- Deploy Application-Aware Defenses
 - Monitor and restrict app behavior

2. Validate automated patching and initiate configuration automation

- Update software immediately
- Upgrade software regularly
- Actively manage systems and configurations

3. Implement multi-factor authentication (MFA)

- Enforce phishing-resistant MFA universally
- Transition from basic to advanced MFA

4. Validate security information and event management (SIEM) log ingestion

- Deploy SIEM for easy integration
- Ensure log forwarding

5. Review and eliminate unnecessary network pathways

- Monitor connections between network segments
- Remove unneeded connections

6. Establish user activity baselines and behavioral alerting



- Baseline normal traffic and detect anomalies
- Use auditing tools for privilege abuse detection
- Continuously hunt for intrusions

7. Refine Endpoint Detection and Response (EDR) rules

- Optimize EDR for anomaly detection
- Integrate EDR with hunt operations

8. Implement strict application allowlisting

- Enforce signed software execution policies
- Monitor for abnormal applications, scripts, and living off the land tools

9. Establish and validate incident response (IR) processes and cybersecurity service provider (CSSP) response capabilities

- Create, exercise, and revise recovery plans

Tier 1: Transition and remediation activities

Build on Tier 0 with remediation and automation.

1. Plan and initiate security orchestration, automation, and response (SOAR)

- Identify situations for automated responses
- Test integrations
- Document processes

2. Refine EDR and SIEM

- Ensure comprehensive logging and alerting

3. Validate network segmentation

- Test isolation
- Eliminate shadow IT paths

Tier 2: SOAR development and validation

1. Begin SOAR implementation

- Prioritize automated actions (e.g., quarantine on anomaly detection)

2. Develop and validate responses

- Test in controlled environments

3. Integrate with systems



- Link to SIEM, EDR, and workflows

4. Finalize documentation

- Ensure processes are repeatable
- Ensure human-in-the-loop where appropriate in AI-enabled processes

Tier 3: Adversarial emulation and finalization

1. Plan adversarial emulation

- Prepare for red team exercises

2. Conduct assessments

- Analyze findings
- Remediate gaps via blue teaming

3. Final validation

- Exercise recovery
- Perform continuous hunts

Conclusion

Robust cyber hygiene transforms networks from vulnerable targets to resilient assets. Start with Tier 0 for quick risk reduction, validate through emulation, and integrate AI for enhanced detection. Regular assessments reveal persistent gaps—address them to stay ahead of evolving threats.

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of War, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Questions & Feedback: Defensive_Guidance@nsa.gov; CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov



Appendix A: Technical annex for network inventory

This annex provides technical guidance for the cyber hygiene network inventory. It focuses on creating the network inventory, applying mitigation checklists to each asset in the inventory, and integrating the inventory with AI for threat detection.

Device and network inventory for threat mapping

To counter AI-enabled intrusion attempts, begin by conducting comprehensive inventories. Feed data into AI for pattern recognition and vulnerability suggestions (human validation required).

Table 1: Key Inventory Components

Category	Details
Hardware Devices	Routers, Switches, Firewalls, Servers, Workstations, WAPs, Printers, IoT: Brand, model, firmware, MAC addresses, FQDNs
Software Inventory	OS versions, applications/licenses, firmware
Network Configuration	IPs, subnets, VLANs, firewall rules, routing tables, DNS/DHCP
User/Access	Accounts/roles; exercise accounts (usernames/passwords/status); admin privileges; ACLs
Security Config	AV versions, encryption, VPN, IDS/IPS
Topology	Diagrams; wired/wireless/VPN connections
Ownership/Location	Asset owners; physical locations
Backup/Recovery	Solutions; disaster plans

Employing AI as a defensive tool

Use AI to analyze inventory and logs:

- Input: Complete datasets for better ML results
- Output: Anomaly detection, risk prioritization
- Example: AI flags software with supply chain vulnerabilities, suspicious connections (such as to high-entropy domains based on domain generation algorithms), or privilege abuse patterns
- Best Practice: Combine AI with human hunts; re-assess post-mitigation



Appendix B: Common misconfigurations and mitigations

NSA assessments [highlight recurring issues](#) exploited by APTs. The following table summarizes common misconfigurations and example mitigations to counter.

Table 2: Common misconfigurations and mitigations

Misconfiguration	Description	Mitigation
Default configurations	Default credentials and settings enable unauthorized access	Change defaults; audit permissions
Improper privilege separation	Excessive admin privileges allow rapid lateral movement	Enforce least privilege; use privileged access management (PAM) to grant temporary privileged access, as needed
Insufficient monitoring	Poor sensor configurations miss anomalies	Deploy comprehensive logging; baseline traffic
Lack of segmentation	No boundaries between IT/OT/user networks	Implement firewalls test isolation
Poor patch management	Unpatched systems as entry points	Automate patching; avoid unsupported OS and software
Bypass of access controls	Pass-the-hash/kerberoasting via weak authentication	Enable phishing-resistant MFA; rotate credentials
Weak MFA	Phishing/SIM swap vulnerabilities	Use hardware tokens; block legacy methods
Insufficient access control lists (ACLs)	Overly permissive ACLs allow unauthorized data access and lateral movement	Review and harden ACLs; enforce least privilege on file systems and network resources
Poor credential hygiene	Easily crackable passwords in cleartext	Enforce strong credential policies; monitor for leaks
Unrestricted code execution	Arbitrary post-phishing payloads execute untrusted code	Application allowlisting; signed execution policies



Appendix C: Aligning with NSA's Top 10 Cybersecurity Mitigation Strategies

For support on implementing the tiered mitigations above, the following table identifies relevant strategies from the [NSA's Top Ten Cybersecurity Mitigation Strategies](#). For detailed implementation activities as they pertain to Zero Trust, refer to the [Zero Trust Implementation Guidelines](#) website.

Tier	CSI Activity	Top 10 Cybersecurity Mitigation Strategies
0	Identify security gaps	Defend Privileges and Accounts Actively Manage Systems and Configurations Segment Networks and Deploy Application-Aware Defenses
	Validate automated patching; initiate configuration automation	Update and Upgrade Software Immediately Actively Manage Systems and Configurations
	Implement MFA	Transition to Multi-Factor Authentication
	Validate SIEM log ingestion	Continuously Hunt for Intrusions Integrate Threat Reputation Services
	Review, eliminate unnecessary network pathways	Segment Networks and Deploy Application-Aware Defenses
	Establish user activity baselines, behavioral alerting	Continuously Hunt for Intrusions Integrate Threat Reputation Services
	Refine EDR rules	Continuously Hunt for Intrusions Integrate Threat Reputation Services
	Implement strict application allowlisting	Enforce Signed Software Execution Policies Leverage Hardware Security Features
	Establish, validate IR processes and CSSP response capabilities	Exercise System Recovery Plans
1	SOAR planning, initiation	Continuously Hunt for Intrusions
	Refine EDR, SIEM	Segment Networks and Deploy Application-Aware Defenses
	Validate network segmentation	Integrate Threat Reputation Services
2	Begin SOAR implementation	Continuously Hunt for Intrusions
	Develop, validate responses	
	Integrate with systems	
	Finalize documentation	
	Plan adversarial emulation	
	Conduct assessments	
3	Final validation	Continuously Hunt for Intrusions Exercise System Recovery Plans
	Plan adversarial emulation	
	Conduct assessments	