hpt
knowing IT

HSOC
HPT Product

Document

System Hardening Implementation Guide

Steps to help businesses assess their current state, implement remediations, verify outcomes, and maintain continuous monitoring based on the five pillars of "Security by Design"



Prepared by:

HPT Cyber Security Center

November 2026

https://hpt.vn info@hpt.vn

TABLE OF CONTENTS

1. Introduction 1
1.1 Purpose 1
1.2 How to use this document 1
2. Implementation methodology 2
2.1 The four-step cycle 2
2.2 Prioritization principles 2
3. Pillar 1 – Security by design 3
4. Pillar 2 – Secure coding 5
5. Pillar 3 – Least privilege 6
6. Pillar 4 – Defense in depth 8
7. Pillar 5 – 24/7 security monitoring 10
7.1 Criteria to meet 11
7.2 Choosing an operating model 11
8. Phased implementation roadmap 12
9. Maintenance and continuous improvement 14
10. Reference support services 15
10.1 Service groups 15
10.2 Suggestions by scenario 15

1. Introduction

1.1 Purpose

The System Hardening Guidelines set out what an organization needs to do to prevent, detect and limit the impact of known attack techniques. This document turns the Guidelines into **prioritized implementation steps**, helping the organization's IT and information security (IS) teams focus their efforts, verify results and sustain them over time.

For each pillar, the document describes common issues, the steps to take together with the related guideline codes, and the expected outcomes that serve as the basis for verification. Each pillar ends with a section on reference services for organizations that want to add tools, expertise or staff in certain areas.

1.2 How to use this document

- Each implementation step is tagged with a **guideline code** (SD, SC, LP, DD, MN) and the corresponding section of the Guidelines, so the organization can easily cross-check against the checklist in Appendix A.
- **Section 2** describes the overall implementation methodology; **Sections 3 – 7** give detailed guidance for each pillar; **Section 8** arranges the work along a 0–30, 31–90 and 91–180 day roadmap; **Section 9** describes maintenance activities; **Section 10** summarizes support services for reference.
- IT and IS leaders may read Sections 2, 8 and 9; technical teams should read the pillar sections relevant to their own work.

> **Guiding Principles**
>
> The recommendations in this document are product- and vendor-neutral. Each organization selects technologies that fit its infrastructure, scale and compliance requirements.
>
> All changes to production environments should be tested in advance, have a rollback plan, and be approved under the organization's change management process.
>
> This document is classified: **TLP:GREEN**

2. Implementation methodology

2.1 The four-step cycle

Organizations should implement the Guidelines using the cycle below, so that every change is tied to a specific risk and backed by measurable evidence.

Implementation Step	Actions	Expected Outcomes	Guidelines Reference
1. Assess Current State	Build an asset inventory, especially of Internet-facing assets; compare systems against the Appendix A checklist; scan for vulnerabilities and misconfigurations; review service accounts; check for signs of compromise if any is suspected	Gap list by guideline code, prioritized by risk; 0–30 day action list	Appendix A; Section 2.1; MN-16
2. Remediate and Implement	Remediate in order of priority; configure protection layers according to approved baselines; test before applying to production and record changes	Priority items closed; configuration documents, baselines and operating procedures updated	Sections 3 – 6; Section 8.1
3. Verify	Retest remediated findings; conduct penetration testing or exercises to confirm that protection layers break realistic attack chains	Evidence of closed findings; evidence for the checklist and go-live gate	SD-11, SD-12, SC-46, MN-07
4. Monitor and Maintain	24/7 security monitoring; continuous vulnerability and patch management; metrics tracking; post-incident lessons learned	Section 8.2 metrics tracked regularly; use cases and playbooks updated	Section 7; MN-17, MN-18

2.2 Prioritization principles

- **High risk first:** prioritize Internet-facing systems and systems that process sensitive data (Phase 1 of the Guidelines).
- **Reduce risk now, fix root causes later:** apply time-bound compensating controls (access blocking, WAF, virtual patching) while preparing a permanent fix.
- **Every item has an owner:** define a clear owner, deadline and completion criteria.
- **Keep evidence:** retain scan reports, before-and-after configurations and test records to support periodic self-assessments and audits.

3. Pillar 1 – Security by design

Corresponds to Section 3 of the Guidelines. This pillar determines the organization's attack surface: which assets may be exposed to the Internet, whether default configurations are secure, and how quickly vulnerabilities are patched.

Common Issues

- No complete inventory of domains, public IPs, APIs and storage; dev/UAT environments or admin pages remain reachable from the Internet without anyone knowing (SD-16, SD-42, SD-44).
- Each server is configured differently, there is no approved baseline, and configuration drift goes undetected (SD-35, SD-36).
- Patching deadlines in Section 3.8 are not met, especially for actively exploited vulnerabilities and end-of-support components (SD-39 – SD-41).
- No independent security testing before go-live or during infrastructure migration (SD-11, SD-12, SD-14).

Implementation Step	Actions	Guideline Code	Expected Outcomes
Inventory Internet-facing assets	List domains, subdomains, public IPs, open ports, APIs and storage; identify the owner of each asset; remove unnecessary dev/UAT environments, admin pages and API documentation from the Internet	SD-16, SD-42, SD-44; Appendix A.1	Asset inventory with owners; no exposed assets outside the inventory
Standardize configurations against baselines	Build baselines for operating systems, web servers, databases and network devices based on CIS Benchmarks and DISA STIG; apply secure-by-default principles; detect configuration drift regularly	SD-01, SD-35, SD-36, SD-38	Approved baselines; periodic configuration drift reports
Vulnerability and patch management	Scan infrastructure and applications regularly; prioritize by severity, Internet exposure and the known exploited vulnerabilities catalog; patch within the deadlines in Section 3.8; plan replacement of end-of-support components	SD-13, SD-39 – SD-41	Patch deadline compliance metric (Section 8.2); replacement plan for end-of-support components
Security testing before go-live	Test components that are Internet-facing or process sensitive data before they go into operation, when the architecture changes or when infrastructure is migrated; retest after remediation	SD-11, SD-12, SD-14; A.1 item 7	No unresolved Critical/High findings at go-live

Implementation Step	Actions	Guideline Code	Expected Outcomes
Protect public applications and APIs	Place public applications behind a WAF/reverse proxy; configure the API gateway to deny by default and rate-limit per identity; hide API documentation; correlate logs to detect APIs outside the inventory	SD-27, SD-29, SD-30, SD-34; DD-01, DD-02	API inventory; WAF and gateway policies in blocking mode
Review cloud configurations	Check for exposed resources, public buckets, overly broad access permissions and misconfigurations on AWS, Azure and Google Cloud	SD-35, SD-44; LP-44, LP-45	No public resources outside the inventory
Identify compliance requirements	Identify legal and industry regulatory requirements from the system initiation phase (e.g., Circular 12/2022/TT-BTTTT, Circular 09/2020/TT-NHNN, SWIFT CSCF) and the security level of the information system	SD-08	List of compliance requirements applicable to each system

Where to start: reviewing all Internet-facing assets and removing unnecessary components (dev/UAT, admin pages, API documentation, end-of-support components) is the fastest way to close the highest risks of Phase 1.

Reference HPT services: Attack Surface Management (ASM); security configuration assessment; vulnerability scanning and management (VMaaS); patch and compliance management; penetration testing; WAF, API Security; Cloud Security, CSPM; industry- and security-level compliance assessment.

4. Pillar 2 – Secure coding

Corresponds to Section 4 of the Guidelines. The mandatory goals are no remaining SQL injection and no path for an application to create a webshell (SC-01, SC-02). Because source code is often developed by multiple parties over many years, organizations need to verify that the code is actually secure rather than relying on the WAF layer alone.

Common Issues

- Legacy applications build queries by string concatenation in code and stored procedures; internal services (SOAP, internal APIs) have never been tested because they are "not exposed to the Internet" (SC-01, SC-31).
- File upload, data deserialization and framework expression features open a path to webshells (Section 4.5).
- Releases ship continuously, but security testing is done only once a year (SC-45 – SC-47).
- Dependence on third-party developers makes it hard to require and verify compliance (SC-49).

Implementation Step	Actions	Guideline Code	Expected Outcomes
Eliminate SQL injection	Replace string-concatenated queries in code and stored procedures with parameterized queries; include internal services (SOAP, internal APIs) in the review scope, not just Internet-facing components	SC-01, SC-31	No string-concatenated queries remain in reviewed applications
Block webshell creation paths	Control upload functions (validate file types, store outside the web root, disallow execution); review data deserialization and framework expressions	SC-02; Section 4.5	Applications can no longer write and execute arbitrary files
Test according to OWASP	Test web, API and mobile applications against the OWASP Top 10:2025 and OWASP API Security Top 10:2023, focusing on SQL injection, upload, BOLA, SSRF, deserialization and authorization flaws; when a flaw pattern is found, check similar locations; retest after fixes	SC-04 – SC-23, SC-45, SC-46	Test and retest reports; findings tracked until closed
Tie testing to the release cycle	Build security testing into the release process instead of testing only once a year	SC-45, SC-47; SD-11	Security testing is a prerequisite for every major release
Use the WAF as a time-bound compensating layer	Apply virtual patching while code fixes are pending; set a deadline for each rule and track until the code is fixed	SC-03; DD-03	Each virtual patching rule is tied to a finding and a code-fix deadline
Manage third-party developers	Include secure coding requirements in agreements with developers and outsourcing vendors; require testing evidence at acceptance; track vendors' IS risk level	SC-06, SC-49	Security requirements clearly stated when outsourcing; testing evidence at acceptance

Important Note

Under SC-03, WAF and IPS are only time-bound compensating layers. Organizations should use a WAF to reduce risk immediately while fixing the root cause in the source code: an attacker who has already entered the internal network can call back-end services directly without passing through the WAF.

For applications that integrate chatbots or AI assistants, organizations should add controls against prompt injection, data leakage and abuse (outside the scope of Guidelines v1.0, complementing SC-23).

Reference HPT services: Web, API and mobile application penetration testing; continuous penetration testing; WAF as a Service; supply chain security measurement; AI/LLM system and application protection.

5. Pillar 3 – Least privilege

Corresponds to Section 5 of the Guidelines. When an application is exploited, the attacker's code runs under the identity of the service account; tightening the privileges of service accounts and administrator accounts is therefore the most direct way to limit damage.

Common Issues

- No one knows how many service accounts exist, who owns them or what privileges they have; many applications run as LocalSystem, root or sysadmin (LP-09, LP-11).
- Shared administrator passwords; default accounts (sa, SYS, root, Administrator) are still active (LP-28, LP-31, LP-53).
- Administrators access servers directly, without MFA and without session recording (LP-50 – LP-52).
- Concerns that privilege changes will disrupt applications lead to delays.

Implementation Step	Actions	Guideline Code	Expected Outcomes
Inventory service accounts	List service accounts, application pools, database logins, systemd units and Kubernetes service accounts; identify the owner, purpose and current privileges using the template in Appendix D	LP-05, LP-09, LP-11	Service account inventory with owners
Check for signs of abuse before making changes	Before tightening privileges and rotating secrets, check whether service accounts and administrator accounts have been abused; look for persistence mechanisms, unusual connections and signs of lateral movement	LP-18; SD-24	Conclusion on whether or not there are signs of compromise
Reduce service account privileges	Move applications off LocalSystem, root and sysadmin; disable database command execution features; review linked servers/DB links and Kubernetes RBAC per Section 5.4 and Appendix C.5; proceed in order from lowest risk	LP-09 – LP-43; Section 5.6	Excess privileges revoked; each account holds only the privileges it needs
Control privileged accounts	Disable unused default accounts and change passwords of those still in use; eliminate shared administrator passwords; centralize privileged access management with just-in-time (JIT) access and session recording; administer through a jump host	LP-28, LP-31, LP-50, LP-52 – LP-54	No shared passwords remain; administrative sessions are recorded
Deploy phishing-resistant MFA	Apply phishing-resistant MFA to administrative and remote access, then extend it to users; protect against password guessing	LP-51, SC-10; Section 5.2	MFA applied to priority account groups
Reduce cloud privileges	Replace long-lived access keys with managed identities; review storage policies, listing permissions and API client scopes	LP-44 – LP-46	No unnecessary long-lived access keys remain

Implementation Step	Actions	Guideline Code	Expected Outcomes
Monitor account behavior	Alert when a service account logs on interactively, logs on from an unfamiliar machine, spawns a command shell, or when privileged groups change	LP-07, LP-17; UC3, UC16	Corresponding use cases enabled and tested

Where to start: prioritize Internet-facing application chains (Phase 1 of the Guidelines); check for signs of compromise in parallel with the service account review so that already-compromised accounts are not missed. To minimize disruption, change privileges in small batches, test first in a test environment, monitor access error logs after each change and prepare a rollback plan.

Reference HPT services: Configuration security assessment (accounts and permissions); PAM, PAM as a Service; Identity Security – MFA; Threat Hunting, Compromise Assessment; Cloud Security, CSPM; MDR, SOC as a Service 24/7.

6. Pillar 4 – Defense in depth

Corresponds to Section 6 of the Guidelines. Each layer is designed on the assumption that the previous layer has been bypassed; organizations therefore need to deploy all layers and verify that they are truly independent of one another.

Layer (Section 6)	Technical Controls	Actions	Guideline Code
Perimeter and Internet	WAF; DDoS protection; load balancing, reverse proxy	No direct NAT of servers to the Internet; origins accept connections only from the protection layer; WAF and bot management in blocking mode; access logs always enabled	DD-01 – DD-03
Network	NGFW; NAC; NDR	Segment per the table in Section 6.2, with default deny between zones; filter egress traffic through a proxy with an allowlist; control devices joining the user network; detect tunneling and lateral movement	DD-04 – DD-11; UC8
Identity and Access	PAM; MFA	See Section 5 of this document	Section 5 of the Guidelines
Applications and APIs	WAF, API gateway; security testing	See Sections 3 and 4 of this document	Sections 3.6, 4
Servers	EDR/XDR; configuration baselines	EDR on all servers in prevention mode with tamper protection enabled; tune policies so business operations are not affected; enable PowerShell logging and auditd; protect OS credentials; enable host firewalls	DD-12 – DD-17
Data	Database Firewall; data encryption; DLP	Restrict connection sources to databases; monitor high-volume queries and access to sensitive tables; encrypt at rest and in transit with centralized key management; prevent data loss via email, web and endpoints	DD-05, DD-18, DD-21; UC18
Backup and Recovery	3-2-1 backups; immutable copies	Back up following the 3-2-1 rule with an immutable copy; test restores regularly; include attack scenarios against backup infrastructure in the testing scope	DD-19, DD-20
Monitoring and Response	SIEM; EDR; SOAR	See Section 7 of this document	Section 7 of the Guidelines
Verify all layers	Penetration testing; Red Team	Simulate realistic attack chains, from exploiting an Internet-facing application to the core database and backup systems, to verify whether each layer breaks the attack chain	Section 6; MN-07

Additional Note

Email protection (anti-phishing, email-borne malware) is outside the scope of Guidelines v1.0 but is an important complementary layer for the risk of users being deceived described in Section 5.2.

Reference HPT services: NGFW; NAC; DDoS protection; EDR/XDR, MDR; Database Firewall, data encryption, DLP; email protection; Red Team.

7. Pillar 5 – 24/7 security monitoring

Corresponds to Section 7 of the Guidelines. Section 7.1 sets out criteria for organizations to build, select and evaluate monitoring capabilities, whether operated in-house or through an external service.

7.1 Criteria to meet

Requirement in the Guidelines	What the Organization Needs to Do
MN-01: 24/7/365 operation with on-duty analysts	Staff 24/7/365 shifts; every alert is verified and handled by an analyst, not merely forwarded automatically
MN-02, MN-08 – MN-11: log source coverage	Collect logs per the table in Section 7.2 (WAF, servers, API gateway, firewall, EDR, databases, AD/IdP, PAM, VPN, cloud, DNS, proxy); alert when a log source stops sending; track coverage monthly
MN-03: minimum detection use cases	Build and tune use cases from the UC1 – UC19 catalog in Section 7.3, mapped to MITRE ATT&CK and adapted to the organization's systems and business flows
MN-04, Section 7.4: response times	Define acknowledgment, analysis and containment times by severity; measure and report regularly
MN-05: 24/7 escalation chain	Establish a contact and escalation matrix up to authorized decision-makers; periodically verify that contact details remain valid
MN-06: threat intelligence and hunting	Monitor leaked credentials, spoofed domains, data leaks and industry-specific IOCs; conduct regular threat hunting based on new indicators
MN-07: detection and response exercises	Conduct regular exercises (Red Team or attack simulation) to assess detection and response capabilities; update use cases after each exercise
MN-12 – MN-15: containment and playbooks	Pre-approve a list of containment actions (isolating hosts via EDR, blocking IPs and domains, disabling user accounts); build playbooks for key scenarios and automate where appropriate; extend visibility into the internal network layer
Section 7.6: digital forensics and scoping	Prepare capabilities for evidence collection, artifact analysis and root cause and scope determination; plan containment, recovery and lessons learned

7.2 Choosing an operating model

Model	Suitable When	Implementation Notes
In-house	The organization has enough staff for 24/7 shifts and a monitoring platform	Invest in SIEM, SOAR and EDR/XDR platforms; maintain use cases and playbooks and train staff
Outsourced	The organization does not yet have a 24/7 team or needs to meet the Section 7.1 criteria quickly	Evaluate providers against the Section 7.1 criteria; clearly agree on the list of containment actions and the escalation chain
Hybrid	The internal team works business hours and needs after-hours monitoring or specialized capabilities	Assign responsibilities per the RACI table in Section 7.6; agree on shift handover and information sharing

For factories, warehouses and branches with many cameras, sensors and connected devices, organizations should extend monitoring to IoT devices beyond traditional IT infrastructure.

Reference HPT services: SOC as a Service 24/7 (HSOC); MDR; SIEM, XSIAM, SOAR; NDR; Threat Intelligence; Threat Hunting; digital forensics and incident response (DFIR); IoT device monitoring.

8. Phased implementation roadmap

The table below arranges the actions according to the roadmap in Section 8.1 of the Guidelines. The specific order should be adjusted based on the results of the organization's current-state assessment.

Phase	Objective	Actions	Expected Outcomes
Phase 1 **0 - 30 days**	Close the highest risks	• Inventory and remove unnecessary assets from the Internet • Scan for and patch critical vulnerabilities on Internet-facing assets • Check for signs of compromise • Review service accounts; disable database command execution features • Place public applications behind a WAF • Enable EDR in prevention mode on Internet-facing servers and databases • Set up 24/7 monitoring, the escalation chain and the pre-approved containment list	No exposed assets outside the inventory; public applications behind a WAF; critical servers monitored 24/7
Phase 2 **31 - 90 days**	Limit the blast radius	• Network segmentation, egress filtering • Privileged access management; phishing-resistant MFA • Database access control; data encryption • API gateway with default deny • Review cloud configurations and permissions • Containment playbooks; internal network traffic monitoring • Full set of Section 7.3 use cases	An attacker who gains a foothold cannot spread to other zones; privileges are controlled and sessions recorded
Phase 3 **91 - 180 days**	Embed into processes	• Security testing aligned with the release cycle • Continuous attack surface monitoring • Red Team exercises • Threat intelligence • Industry- and security-level compliance assessment • Vendor risk assessment	Security becomes a control gate in the system lifecycle; defensive capability is verified regularly

9. Maintenance and continuous improvement

After completing the phases, the organization sustains the results through the periodic activities below.

Maintenance Requirement	How to Implement
MN-16: self-assessment against Appendix A before go-live and every 6 months	Assess against the Appendix A checklist, combined with scanning and testing to provide evidence for each item; add unmet items to the remediation plan
MN-17: quarterly reporting of Section 8.2 metrics to leadership	Track metrics such as log coverage, time to acknowledge and contain, patch deadline compliance rate and EDR coverage; report trends across quarters
MN-18: update after every incident, review annually	Capture post-incident lessons learned; update use cases and playbooks; adjust the checklist when systems or threats change

10. Reference support services

Organizations can implement everything in this document on their own. Where additional tools, expertise or operations staff are needed, the HPT Cyber Security Center offers the service groups below for reference.

10.1 Service groups

Service Group	Relevant Step	Key Services and Solutions
Assessment and Testing	Current-state assessment; verification	Configuration security assessment; vulnerability scanning; penetration testing; continuous penetration testing; Red Team; industry- and security-level compliance assessment; user awareness assessment
Solutions and Implementation	Remediation and implementation	WAF, API Security; NGFW; NAC; DDoS protection; EDR/XDR; PAM; MFA; Database Firewall; data encryption; DLP; Cloud Security; email protection; AI/LLM application protection; SIEM, XSIAM, SOAR; vulnerability management; attack surface management
Monitoring and Response (HSOC)	Monitoring and maintenance	24/7 IS monitoring (SOC as a Service); MDR; NDR; SOAR; Threat Intelligence; Threat Hunting, Compromise Assessment; digital forensics and incident response (DFIR); managed vulnerability management, patching, WAF, PAM and cloud security services; IoT monitoring; supply chain security measurement

10.2 Suggestions by scenario

Organization's Situation	Services to Consider
Unsure where systems stand relative to the Guidelines	Current-state assessment against the Appendix A checklist: configuration assessment, vulnerability scanning and ASM
Suspected compromise; unusual signs observed but not yet confirmed	Compromise Assessment; if an incident is confirmed, move to DFIR
Active incident	DFIR: containment, investigation, scoping and recovery support
About to expose a new application to the Internet	Penetration testing and review of the Appendix A.1 checklist before go-live
Continuous application releases, several versions per month	Continuous penetration testing
Application has vulnerabilities but code cannot be fixed in time	WAF as a Service (time-bound virtual patching) alongside a code-fix plan
No 24/7 security staff	SOC as a Service 24/7; MDR
SIEM already in place but too many alerts and slow handling	Use case tuning; SOAR; hybrid monitoring model

Organization's Situation	Services to Consider
Many shared administrator accounts, no session recording	PAM combined with phishing-resistant MFA
Migrating systems to the cloud	Cloud Security, CSPM; retest before go-live on the new infrastructure (SD-14)
Want to know whether defenses can withstand a targeted attack	Red Team
Regulatory compliance requirements	Industry compliance assessment (Circular 09/2020/TT-NHNN, SWIFT CSCF, Circular 12/2022/TT-BTTTT); security-level information system consulting
Factories and warehouses with many IoT devices	IoT device monitoring

Contact

HPT Cyber Security | Email: hsoc@hpt.vn

Contact:

Head Office
Lot E2a-3, D1 St., Saigon High Tech Park, Tang Nhon Phu Ward, HCMC, Vietnam
Tel: +(84 28) 38 266 206 | **Email:** info@hpt.vn
Website: https://hpt.vn

HPT Vietnam Corporation

HPT Customer Service Center
37 Nguyen Truong To St, Xom Chieu Ward, HCMC, Vietnam
Tel: +(84 28) 38 266 206 | **Hotline:** 18006686

Hanoi Branch
10th Floor, Viet Tower, No. 1 Thai Ha St, Dong Da Ward, Hanoi, Vietnam
Tel: +(84 28) 38 266 206