hpt knowing IT

HSOC

HPT Product

Tài liệu

Hướng dẫn thực hiện Gia cố hệ thống

Các bước giúp doanh nghiệp đánh giá hiện trạng, khắc phục, kiểm chứng và giám sát liên tục theo 5 trụ cột Security by Design



Thực hiện bởi:

Trung tâm Điều hành An ninh mạng HPT

Tháng 11/2026

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

MỤC LỤC

1. Giới thiệu 1
1.1 Mục đích 1
1.2 Cách sử dụng tài liệu 1
2. Phương pháp triển khai 2
2.1 Vòng lặp bốn bước 2
2.2 Nguyên tắc ưu tiên 2
3. Trụ cột 1 – Security by Design 3
4. Trụ cột 2 – Lập trình an toàn 5
5. Trụ cột 3 – Least Privilege 7
6. Trụ cột 4 – Defense in Depth 8
7. Trụ cột 5 – Giám sát an ninh 24/7 10
7.1 Các tiêu chí cần đáp ứng 10
7.2 Lựa chọn mô hình vận hành 11
8. Lộ trình triển khai theo giai đoạn 12
9. Duy trì và cải tiến liên tục 13
10. Dịch vụ hỗ trợ tham khảo 14
10.1 Các nhóm dịch vụ 14
10.2 Gợi ý theo tình huống 14

1. Giới thiệu

1.1 Mục đích

Hướng dẫn gia cố hệ thống nêu những gì một tổ chức cần làm để phòng ngừa, phát hiện và hạn chế tác động của các kỹ thuật tấn công đã biết. Tài liệu này cụ thể hóa hướng dẫn thành **các bước thực hiện có thứ tự ưu tiên**, giúp đội ngũ CNTT và ATTT của tổ chức triển khai đúng trọng tâm, kiểm chứng được kết quả và duy trì bền vững.

Với mỗi trụ cột, tài liệu nêu các vấn đề thường gặp, các bước cần thực hiện kèm mã hướng dẫn liên quan và kết quả cần đạt để làm căn cứ kiểm chứng. Cuối mỗi trụ cột có phần dịch vụ tham khảo, dành cho trường hợp tổ chức muốn bổ sung công cụ, chuyên môn hoặc nhân sự ở một số hạng mục.

1.2 Cách sử dụng tài liệu

- Mỗi bước thực hiện được gắn với **mã hướng dẫn** (SD, SC, LP, DD, MN) và mục tương ứng trong hướng dẫn, để tổ chức dễ đối chiếu với checklist tại Phụ lục A.
- **Mục 2** mô tả phương pháp triển khai chung; **Mục 3 – 7** hướng dẫn chi tiết từng trụ cột; **Mục 8** sắp xếp công việc theo lộ trình 0–30, 31–90 và 91–180 ngày; **Mục 9** nêu các hoạt động duy trì; **Mục 10** tổng hợp dịch vụ hỗ trợ để tham khảo.
- Lãnh đạo CNTT, ATTT có thể đọc Mục 2, 8 và 9; đội kỹ thuật đọc các mục trụ cột liên quan đến phần việc của mình.

> **Nguyên tắc áp dụng**
>
> Các khuyến nghị trong tài liệu không phụ thuộc sản phẩm hay nhà cung cấp. Tổ chức lựa chọn công nghệ phù hợp với hạ tầng, quy mô và yêu cầu tuân thủ của mình.
>
> Mọi thay đổi trên môi trường vận hành nên được thử nghiệm trước, có phương án khôi phục và được phê duyệt theo quy trình quản lý thay đổi của tổ chức.
>
> Tài liệu được phân loại: **TLP:GREEN**

2. Phương pháp triển khai

2.1 Vòng lặp bốn bước

Tổ chức nên triển khai Hướng dẫn theo vòng lặp dưới đây, để mỗi thay đổi gắn với một rủi ro cụ thể và có bằng chứng đo được.

Bước thực hiện	Việc cần làm	Kết quả cần đạt	Mã hướng dẫn
1. Đánh giá hiện trạng	Lập danh mục tài sản, đặc biệt là tài sản hướng Internet; đối chiếu hệ thống với checklist Phụ lục A; dò quét lỗ hổng và cấu hình; rà soát tài khoản dịch vụ; kiểm tra dấu hiệu xâm nhập nếu có nghi ngờ	Danh sách khoảng cách theo mã hướng dẫn, xếp ưu tiên theo rủi ro; danh sách việc cần làm 0–30 ngày	Phụ lục A; Mục 2.1; MN-16
2. Khắc phục và triển khai	Khắc phục theo thứ tự ưu tiên; cấu hình các lớp bảo vệ theo baseline đã phê duyệt; thử nghiệm trước khi áp dụng trên môi trường vận hành và ghi nhận thay đổi	Các hạng mục ưu tiên được đóng; tài liệu cấu hình, baseline, quy trình vận hành được cập nhật	Mục 3 – 6; Mục 8.1
3. Kiểm chứng	Tái kiểm tra các lỗi đã khắc phục; kiểm thử xâm nhập hoặc diễn tập để xác nhận các lớp bảo vệ cắt được chuỗi tấn công thực tế	Bằng chứng đóng lỗi; bằng chứng cho checklist và cổng go-live	SD-11, SD-12, SC-46, MN-07
4. Giám sát và duy trì	Giám sát an ninh 24/7; quản lý lỗ hổng, bản vá liên tục; theo dõi chỉ số; rút kinh nghiệm sau sự cố	Chỉ số Mục 8.2 được theo dõi định kỳ; use case, playbook được cập nhật	Mục 7; MN-17, MN-18

2.2 Nguyên tắc ưu tiên

- **Rủi ro cao làm trước:** ưu tiên hệ thống hướng Internet và hệ thống xử lý dữ liệu nhạy cảm (Giai đoạn 1 của Hướng dẫn).
- **Giảm rủi ro ngay, khắc phục tận gốc sau:** áp dụng biện pháp bù đắp có thời hạn (chặn truy cập, WAF, vá ảo) trong lúc chuẩn bị khắc phục triệt để.
- **Mỗi hạng mục có đầu mối:** xác định người phụ trách, thời hạn và tiêu chí hoàn thành rõ ràng.
- **Lưu bằng chứng:** giữ lại báo cáo quét, cấu hình trước và sau thay đổi, biên bản kiểm thử để phục vụ tự đánh giá định kỳ và kiểm toán.

3. Trụ cột 1 – Security by Design

Tương ứng Mục 3 của Hướng dẫn. Đây là trụ cột quyết định bề mặt tấn công của tổ chức: tài sản nào được phép lộ ra Internet, cấu hình mặc định có an toàn không, lỗ hổng được vá trong bao lâu.

Vấn đề thường gặp

- Không có danh mục đầy đủ tên miền, IP public, API, kho lưu trữ; môi trường dev/UAT hoặc trang quản trị vẫn truy cập được từ Internet mà không ai biết (SD-16, SD-42, SD-44).
- Mỗi máy chủ cấu hình một kiểu, chưa có baseline được phê duyệt, không phát hiện được lệch cấu hình (SD-35, SD-36).
- Không đáp ứng được thời hạn vá tại Mục 3.8, nhất là với lỗ hổng đang bị khai thác thực tế và thành phần hết hỗ trợ (SD-39 – SD-41).
- Chưa có kiểm thử bảo mật độc lập trước go-live hoặc khi chuyển đổi hạ tầng (SD-11, SD-12, SD-14).

Bước thực hiện	Việc cần làm	Kết quả cần đạt	Mã hướng dẫn
Lập danh mục tài sản hướng Internet	Liệt kê tên miền, subdomain, IP public, cổng mở, API, kho lưu trữ; xác định chủ sở hữu từng tài sản; gỡ môi trường dev/UAT, trang quản trị, tài liệu API không cần thiết khỏi Internet	Danh mục tài sản có chủ sở hữu; không còn tài sản lộ ngoài danh mục	SD-16, SD-42, SD-44; Phụ lục A.1
Chuẩn hóa cấu hình theo baseline	Xây dựng baseline cho hệ điều hành, máy chủ web, CSDL, thiết bị mạng dựa trên CIS Benchmarks, DISA STIG; áp dụng nguyên tắc mặc định an toàn; định kỳ phát hiện lệch cấu hình	Baseline được phê duyệt; báo cáo lệch cấu hình định kỳ	SD-01, SD-35, SD-36, SD-38
Quản lý lỗ hổng và bản vá	Quét định kỳ hạ tầng và ứng dụng; xếp ưu tiên theo mức độ, theo tài sản hướng Internet và danh mục lỗ hổng đang bị khai thác; vá trong thời hạn tại Mục 3.8; lập kế hoạch thay thế thành phần hết hỗ trợ	Chỉ số tuân thủ thời hạn vá (Mục 8.2); kế hoạch thay thế thành phần hết hỗ trợ	SD-13, SD-39 – SD-41
Kiểm thử bảo mật trước go-live	Kiểm thử thành phần hướng Internet hoặc xử lý dữ liệu nhạy cảm trước khi vận hành, khi thay đổi kiến trúc hoặc chuyển đổi hạ tầng; tái kiểm thử sau khắc phục	Không còn lỗi mức Nghiêm trọng/Cao chưa xử lý khi go-live	SD-11, SD-12, SD-14; A.1 mục 7
Bảo vệ ứng dụng và API công khai	Đặt ứng dụng public sau WAF/reverse proxy; API gateway mặc định từ chối, giới hạn tần suất theo danh tính; ẩn tài liệu API; đối chiếu log để phát hiện API ngoài danh mục	Danh mục API; chính sách WAF, gateway ở chế độ chặn	SD-27, SD-29, SD-30, SD-34; DD-01, DD-02
Rà soát cấu hình cloud	Kiểm tra tài nguyên phơi lộ, bucket công khai, quyền truy cập quá rộng, lệch cấu hình trên AWS, Azure, Google Cloud	Không còn tài nguyên công khai ngoài danh mục	SD-35, SD-44; LP-44, LP-45

Bước thực hiện	Việc cần làm	Kết quả cần đạt	Mã hướng dẫn
Xác định yêu cầu tuân thủ	Xác định yêu cầu pháp lý, quy định ngành ngay từ giai đoạn khởi tạo hệ thống (ví dụ Thông tư 12/2022/TT-BTTTT, Thông tư 09/2020/TT-NHNN, SWIFT CSCF) và cấp độ của hệ thống thông tin	Danh sách yêu cầu tuân thủ áp dụng cho từng hệ thống	SD-08

Gợi ý bắt đầu: rà soát toàn bộ tài sản hướng Internet và gỡ các thành phần không cần thiết (dev/UAT, trang quản trị, tài liệu API, thành phần hết hỗ trợ) là cách nhanh nhất để đóng các rủi ro cao nhất của Giai đoạn 1.

Dịch vụ HPT tham khảo:

- Quản lý bề mặt tấn công (ASM)
- Đánh giá an toàn cấu hình bảo mật; dò quét và quản lý lỗ hổng (VMaaS)
- Quản lý bản vá và tuân thủ; kiểm thử xâm nhập
- WAF, API Security; Cloud Security, CSPM
- Đánh giá tuân thủ theo ngành, theo cấp độ

4. Trụ cột 2 – Lập trình an toàn

Tương ứng Mục 4 của Hướng dẫn. Mục tiêu bắt buộc là không còn SQL injection và không còn đường tạo webshell từ ứng dụng (SC-01, SC-02). Vì mã nguồn thường do nhiều bên phát triển qua nhiều năm, tổ chức cần kiểm chứng mã đã thực sự an toàn thay vì chỉ dựa vào lớp WAF.

Vấn đề thường gặp

- Ứng dụng cũ có câu truy vấn ghép chuỗi trong mã và stored procedure; dịch vụ nội bộ (SOAP, API nội bộ) chưa từng được kiểm thử vì "không ra Internet" (SC-01, SC-31).
- Chức năng upload, giải tuần tự dữ liệu, biểu thức của framework tạo đường cho webshell (Mục 4.5).
- Phát hành phiên bản liên tục nhưng kiểm thử bảo mật chỉ làm một lần mỗi năm (SC-45 – SC-47).
- Phụ thuộc nhà phát triển bên thứ ba, khó yêu cầu và kiểm chứng tuân thủ (SC-49).

Bước thực hiện	Việc cần làm	Kết quả cần đạt	Mã hướng dẫn
Loại bỏ SQL injection	Thay câu truy vấn ghép chuỗi trong mã và stored procedure bằng truy vấn tham số hóa; đưa cả dịch vụ nội bộ (SOAP, API nội bộ) vào phạm vi rà soát, không chỉ thành phần hướng Internet	Không còn truy vấn ghép chuỗi trong các ứng dụng đã rà soát	SC-01, SC-31
Chặn đường tạo webshell	Kiểm soát chức năng upload (kiểm tra loại tệp, lưu ngoài thư mục web, không cho phép thực thi); rà soát giải tuần tự dữ liệu và biểu thức của framework	Ứng dụng không còn khả năng ghi và thực thi tệp tùy ý	SC-02; Mục 4.5
Kiểm thử theo OWASP	Kiểm thử ứng dụng web, API, mobile theo OWASP Top 10:2025 và OWASP API Security Top 10:2023, tập trung vào SQL injection, upload, BOLA, SSRF, giải tuần tự, lỗi phân quyền; khi phát hiện một mẫu lỗi, rà các vị trí tương tự; tái kiểm thử sau khi sửa	Báo cáo kiểm thử và tái kiểm thử; lỗi được theo dõi đến khi đóng	SC-04 – SC-23, SC-45, SC-46
Gắn kiểm thử với nhịp phát hành	Đưa kiểm thử bảo mật vào quy trình phát hành, thay vì chỉ kiểm thử một lần mỗi năm	Kiểm thử bảo mật là điều kiện trước mỗi đợt phát hành quan trọng	SC-45, SC-47; SD-11
Dùng WAF làm lớp bù đắp có thời hạn	Áp dụng vá ảo (virtual patching) trong lúc chờ sửa mã; đặt thời hạn cho từng quy tắc và theo dõi đến khi mã được sửa	Mỗi quy tắc vá ảo gắn với một lỗi và thời hạn sửa mã	SC-03; DD-03
Quản lý nhà phát triển bên thứ ba	Đưa yêu cầu lập trình an toàn vào thỏa thuận với nhà phát triển, đơn vị gia công; yêu cầu bằng chứng kiểm thử khi nghiệm thu; theo dõi mức độ rủi ro ATTT của nhà cung cấp	Yêu cầu bảo mật được nêu rõ khi thuê ngoài; bằng chứng kiểm thử khi nghiệm thu	SC-06, SC-49

> **Lưu ý quan trọng**
>
> Theo SC-03, WAF và IPS chỉ là lớp bù đắp có thời hạn. Tổ chức nên dùng WAF để giảm rủi ro ngay, đồng thời sửa tận gốc trong mã nguồn: kẻ tấn công đã vào được mạng nội bộ có thể gọi thẳng dịch vụ phía sau mà không đi qua WAF.
>
> Với ứng dụng tích hợp chatbot, trợ lý AI, tổ chức nên bổ sung kiểm soát prompt injection, rò rỉ dữ liệu và lạm dụng (ngoài phạm vi Hướng dẫn v1.0, bổ trợ SC-23).

Dịch vụ HPT tham khảo:

- Kiểm thử xâm nhập ứng dụng web, API, mobile
- Kiểm thử xâm nhập liên tục; WAF as a Service
- Đo lường an toàn chuỗi cung ứng
- Bảo vệ hệ thống, ứng dụng AI/LLM

5. Trụ cột 3 – Least Privilege

Tương ứng Mục 5 của Hướng dẫn. Khi một ứng dụng bị khai thác, mã của kẻ tấn công chạy dưới danh tính tài khoản dịch vụ; vì vậy siết quyền tài khoản dịch vụ và tài khoản quản trị là cách trực tiếp nhất để giới hạn thiệt hại.

Vấn đề thường gặp

- Không biết có bao nhiêu tài khoản dịch vụ, ai sở hữu, quyền gì; nhiều ứng dụng chạy bằng LocalSystem, root, sysadmin (LP-09, LP-11).
- Mật khẩu quản trị dùng chung, tài khoản mặc định (sa, SYS, root, Administrator) còn hoạt động (LP-28, LP-31, LP-53).
- Quản trị viên truy cập thẳng máy chủ, không MFA, không ghi phiên (LP-50 – LP-52).
- Lo ngại thay đổi quyền gây gián đoạn ứng dụng nên trì hoãn.

Bước thực hiện	Việc cần làm	Kết quả cần đạt	Mã hướng dẫn
Lập danh mục tài khoản dịch vụ	Liệt kê tài khoản dịch vụ, application pool, login CSDL, unit systemd, tài khoản dịch vụ Kubernetes; xác định chủ sở hữu, mục đích và quyền hiện tại theo mẫu Phụ lục D	Danh mục tài khoản dịch vụ có chủ sở hữu	LP-05, LP-09, LP-11
Kiểm tra dấu hiệu lạm dụng trước khi thay đổi	Trước khi siết quyền và thay bí mật, kiểm tra tài khoản dịch vụ, tài khoản quản trị có bị lạm dụng hay không; tìm cơ chế duy trì truy cập, kết nối bất thường, dấu hiệu di chuyển ngang	Kết luận có hoặc không có dấu hiệu xâm nhập	LP-18; SD-24
Thu hẹp quyền tài khoản dịch vụ	Chuyển ứng dụng khỏi LocalSystem, root, sysadmin; tắt tính năng chạy lệnh của CSDL; rà soát linked server/DB link, RBAC Kubernetes theo Mục 5.4 và Phụ lục C.5; thực hiện theo thứ tự ít rủi ro nhất	Quyền thừa được thu hồi; mỗi tài khoản chỉ giữ quyền cần thiết	LP-09 – LP-43; Mục 5.6
Kiểm soát tài khoản đặc quyền	Vô hiệu hóa tài khoản mặc định không sử dụng, đổi mật khẩu tài khoản còn dùng; loại bỏ mật khẩu quản trị dùng chung; quản lý đặc quyền tập trung, cấp quyền có thời hạn (JIT), ghi phiên; quản trị qua jump host	Không còn mật khẩu dùng chung; phiên quản trị được ghi lại	LP-28, LP-31, LP-50, LP-52 – LP-54
Triển khai MFA chống phishing	Áp dụng MFA chống phishing cho truy cập quản trị, truy cập từ xa, sau đó mở rộng cho người dùng; chống dò mật khẩu	MFA áp dụng cho các nhóm tài khoản ưu tiên	LP-51, SC-10; Mục 5.2
Thu hẹp quyền trên cloud	Chuyển access key dài hạn sang managed identity; rà soát chính sách kho lưu trữ, quyền liệt kê, scope của API client	Không còn khóa truy cập dài hạn không cần thiết	LP-44 – LP-46

Bước thực hiện	Việc cần làm	Kết quả cần đạt	Mã hướng dẫn
Giám sát hành vi tài khoản	Cảnh báo khi tài khoản dịch vụ đăng nhập tương tác, đăng nhập từ máy lạ, sinh dòng lệnh, hoặc khi nhóm đặc quyền thay đổi	Use case tương ứng được bật và kiểm thử	LP-07, LP-17; UC3, UC16

Gợi ý bắt đầu: Ưu tiên chuỗi ứng dụng hướng Internet (Giai đoạn 1 của Hướng dẫn); kiểm tra dấu hiệu xâm nhập song song với rà soát tài khoản dịch vụ để không bỏ sót tài khoản đã bị chiếm. Để hạn chế gián đoạn, thay đổi quyền theo từng nhóm nhỏ, thử nghiệm trước trên môi trường kiểm thử, theo dõi log lỗi truy cập sau mỗi thay đổi và chuẩn bị phương án khôi phục.

Dịch vụ HPT tham khảo:

- Đánh giá an toàn cấu hình (tài khoản và phân quyền)
- PAM, PAM as a Service; Identity Security – MFA
- Threat Hunting, Compromise Assessment
- Cloud Security, CSPM; MDR, SOC as a Service 24/7

6. Trụ cột 4 – Defense in Depth

Tương ứng Mục 6 của Hướng dẫn. Mỗi lớp được thiết kế với giả định lớp trước đã bị vượt qua, vì vậy tổ chức cần triển khai đủ các lớp và kiểm chứng các lớp thực sự độc lập với nhau.

Lớp (Mục 6)	Biện pháp kỹ thuật	Việc cần làm	Mã hướng dẫn
Biên và Internet	WAF; chống DDoS; cân bằng tải, reverse proxy	Không NAT thẳng máy chủ ra Internet; origin chỉ nhận kết nối từ lớp bảo vệ; WAF, bot management ở chế độ chặn; luôn bật access log	DD-01 – DD-03
Mạng	NGFW; NAC; NDR	Phân vùng theo bảng tại Mục 6.2, mặc định từ chối giữa các vùng; lọc lưu lượng ra qua proxy có danh sách cho phép; kiểm soát thiết bị vào mạng người dùng; phát hiện đường hầm, di chuyển ngang	DD-04 – DD-11; UC8
Định danh và truy cập	PAM; MFA	Xem Mục 5 của tài liệu này	Mục 5 Hướng dẫn
Ứng dụng và API	WAF, API gateway; kiểm thử bảo mật	Xem Mục 3 và 4 của tài liệu này	Mục 3.6, 4
Máy chủ	EDR/XDR; baseline cấu hình	EDR trên toàn bộ máy chủ ở chế độ ngăn chặn, bật chống can thiệp; tinh chỉnh chính sách để không ảnh hưởng nghiệp vụ; bật log PowerShell, auditd; bảo vệ thông tin xác thực hệ điều hành; bật firewall trên máy	DD-12 – DD-17
Dữ liệu	Database Firewall; mã hóa dữ liệu; DLP	Giới hạn nguồn kết nối vào CSDL; giám sát truy vấn khối lượng lớn, truy cập bảng nhạy cảm; mã hóa khi lưu và khi truyền, quản lý khóa tập trung; chống thất thoát qua email, web, endpoint	DD-05, DD-18, DD-21; UC18
Sao lưu và khôi phục	Sao lưu 3-2-1; bản sao bất biến	Sao lưu theo nguyên tắc 3-2-1, có bản bất biến; thử khôi phục định kỳ; đưa kịch bản tấn công vào hạ tầng sao lưu vào phạm vi kiểm thử	DD-19, DD-20
Giám sát và phản ứng	SIEM; EDR; SOAR	Xem Mục 7 của tài liệu này	Mục 7 Hướng dẫn
Kiểm chứng toàn bộ các lớp	Kiểm thử xâm nhập; Red Team	Mô phỏng chuỗi tấn công thực tế, từ khai thác ứng dụng hướng Internet tới CSDL lõi và hệ thống sao lưu, để kiểm chứng mỗi lớp có cắt được chuỗi tấn công hay không	Mục 6; MN-07

> **Lưu ý bổ sung**
>
> Bảo vệ email (chống phishing, mã độc qua email) không nằm trong phạm vi Hướng dẫn v1.0 nhưng là lớp bổ trợ quan trọng cho rủi ro người dùng bị lừa đảo nêu tại Mục 5.2.

Dịch vụ HPT tham khảo: NGFW; NAC; chống DDoS; EDR/XDR, MDR; Database Firewall, mã hóa dữ liệu, DLP; bảo vệ email; Red Team.

7. Trụ cột 5 – Giám sát an ninh 24/7

Tương ứng Mục 7 của Hướng dẫn. Mục 7.1 đưa ra các tiêu chí để tổ chức xây dựng, lựa chọn và đánh giá năng lực giám sát, dù tự vận hành hay sử dụng dịch vụ bên ngoài.

7.1 Các tiêu chí cần đáp ứng

Yêu cầu trong hướng dẫn	Tổ chức cần thực hiện
MN-01: vận hành 24/7/365 với chuyên viên trực	Bố trí nhân sự trực ca 24/7/365; mọi cảnh báo được người phân tích xác minh và xử lý, không chỉ chuyển tiếp tự động
MN-02, MN-08 – MN-11: độ phủ nguồn log	Thu thập log theo bảng tại Mục 7.2 (WAF, máy chủ, API gateway, firewall, EDR, CSDL, AD/IdP, PAM, VPN, cloud, DNS, proxy); cảnh báo khi nguồn log ngừng gửi; theo dõi độ phủ hằng tháng
MN-03: use case phát hiện tối thiểu	Xây dựng và tinh chỉnh use case theo danh mục UC1 – UC19 tại Mục 7.3, ánh xạ MITRE ATT&CK, điều chỉnh theo hệ thống và luồng nghiệp vụ của tổ chức
MN-04, Mục 7.4: thời hạn phản ứng	Xác định thời hạn tiếp nhận, phân tích và ngăn chặn theo mức độ nghiêm trọng; đo lường và báo cáo định kỳ
MN-05: chuỗi leo thang 24/7	Lập ma trận liên lạc, leo thang tới người có thẩm quyền; định kỳ kiểm tra thông tin liên lạc còn hiệu lực
MN-06: threat intelligence và săn tìm	Theo dõi tài khoản lộ lọt, tên miền giả mạo, rò rỉ dữ liệu, IOC theo ngành; săn tìm mối đe dọa định kỳ theo chỉ dấu mới
MN-07: diễn tập phát hiện và phản ứng	Diễn tập định kỳ (Red Team hoặc mô phỏng tấn công) để đánh giá khả năng phát hiện và phản ứng; cập nhật use case sau diễn tập
MN-12 – MN-15: ngăn chặn và playbook	Phê duyệt trước danh sách hành động ngăn chặn (cô lập máy qua EDR, chặn IP, tên miền, vô hiệu hóa tài khoản người dùng); xây dựng playbook cho các kịch bản chính và tự động hóa khi phù hợp; mở rộng tầm nhìn ở lớp mạng nội bộ
Mục 7.6: điều tra số, xác định phạm vi	Chuẩn bị năng lực thu thập chứng cứ, phân tích dấu vết, xác định nguyên nhân và phạm vi; lập kế hoạch ngăn chặn, khôi phục và rút kinh nghiệm

7.2 Lựa chọn mô hình vận hành

Mô hình	Phù hợp khi	Lưu ý khi triển khai
Tự vận hành	Tổ chức có đủ nhân sự trực 24/7 và nền tảng giám sát	Đầu tư nền tảng SIEM, SOAR, EDR/XDR; duy trì use case, playbook và đào tạo nhân sự
Thuê ngoài	Tổ chức chưa có đội trực 24/7 hoặc cần đạt các tiêu chí Mục 7.1 trong thời gian ngắn	Đánh giá đơn vị cung cấp theo các tiêu chí Mục 7.1; thống nhất rõ danh sách hành động ngăn chặn và chuỗi leo thang
Kết hợp	Đội nội bộ làm giờ hành chính, cần bổ sung giám sát ngoài giờ hoặc năng lực chuyên sâu	Phân công theo bảng RACI tại Mục 7.6; thống nhất cách bàn giao ca và chia sẻ thông tin

Với nhà máy, kho vận, chi nhánh có nhiều camera, cảm biến và thiết bị kết nối, tổ chức nên mở rộng phạm vi giám sát ra các thiết bị IoT, ngoài hạ tầng CNTT truyền thống.

Dịch vụ HPT tham khảo:

- SOC as a Service 24/7 (HSOC)
- MDR; SIEM, XSIAM, SOAR; NDR; Threat Intelligence; Threat Hunting
- Điều tra số và ứng cứu sự cố (DFIR)
- Giám sát thiết bị IoT

8. Lộ trình triển khai theo giai đoạn

Bảng dưới sắp xếp các việc cần làm theo lộ trình tại Mục 8.1 của Hướng dẫn. Thứ tự cụ thể nên được điều chỉnh theo kết quả đánh giá hiện trạng của tổ chức.

Giai đoạn	Mục tiêu	Việc cần làm	Kết quả cần đạt
Giai đoạn 1 **0 - 30 ngày**	Đóng các rủi ro cao nhất	• Lập danh mục và gỡ tài sản không cần thiết khỏi Internet • Quét và vá lỗ hổng nghiêm trọng trên tài sản hướng Internet • Kiểm tra dấu hiệu xâm nhập • Rà soát tài khoản dịch vụ; tắt tính năng chạy lệnh của CSDL • Đặt ứng dụng public sau WAF • Bật EDR ở chế độ ngăn chặn cho máy chủ hướng Internet, CSDL • Thiết lập giám sát 24/7, chuỗi leo thang và danh sách ngăn chặn phê duyệt trước	Không còn tài sản lộ ngoài danh mục; ứng dụng public sau WAF; máy chủ trọng yếu được giám sát 24/7
Giai đoạn 2 **31 - 90 ngày**	Thu hẹp phạm vi thiệt hại	• Phân vùng mạng, lọc lưu lượng ra • Quản lý tài khoản đặc quyền; MFA chống phishing • Kiểm soát truy cập CSDL; mã hóa dữ liệu • API gateway mặc định từ chối • Rà soát cấu hình và quyền trên cloud • Playbook ngăn chặn; giám sát lưu lượng mạng nội bộ • Đủ use case Mục 7.3	Kẻ tấn công vào được một điểm không lan được sang vùng khác; đặc quyền được kiểm soát và ghi phiên
Giai đoạn 3 **91 - 180 ngày**	Đưa vào quy trình	• Kiểm thử bảo mật theo nhịp phát hành • Theo dõi bề mặt tấn công liên tục • Diễn tập Red Team • Threat intelligence • Đánh giá tuân thủ theo ngành, theo cấp độ • Đánh giá rủi ro nhà cung cấp	Bảo mật trở thành cổng kiểm soát trong vòng đời hệ thống; khả năng phòng thủ được kiểm chứng định kỳ

9. Duy trì và cải tiến liên tục

Sau khi hoàn thành các giai đoạn, tổ chức duy trì kết quả thông qua các hoạt động định kỳ dưới đây.

Yêu cầu duy trì	Cách thực hiện
MN-16: tự đánh giá theo Phụ lục A trước go-live và 6 tháng một lần	Đánh giá theo checklist Phụ lục A, kết hợp dò quét và kiểm thử để có bằng chứng cho từng hạng mục; đưa các hạng mục chưa đạt vào kế hoạch khắc phục
MN-17: báo cáo chỉ số Mục 8.2 cho lãnh đạo hằng quý	Theo dõi các chỉ số như độ phủ log, thời gian tiếp nhận và ngăn chặn, tỷ lệ tuân thủ thời hạn vá, độ phủ EDR; báo cáo xu hướng qua các quý
MN-18: cập nhật sau mỗi sự cố, rà soát hằng năm	Rút kinh nghiệm sau sự cố; cập nhật use case, playbook; điều chỉnh checklist khi hệ thống hoặc mối đe dọa thay đổi

10. Dịch vụ hỗ trợ tham khảo

Tổ chức có thể tự triển khai toàn bộ nội dung trong tài liệu này. Trường hợp cần bổ sung công cụ, chuyên môn hoặc nhân sự vận hành, Trung tâm Điều hành An ninh mạng HPT có các nhóm dịch vụ dưới đây để tổ chức tham khảo.

10.1 Các nhóm dịch vụ

Nhóm dịch vụ	Phù hợp với bước	Dịch vụ, giải pháp tiêu biểu
Đánh giá và kiểm thử	Đánh giá hiện trạng; kiểm chứng	Đánh giá an toàn cấu hình; dò quét lỗ hổng; kiểm thử xâm nhập; kiểm thử xâm nhập liên tục; Red Team; đánh giá tuân thủ theo ngành và theo cấp độ; đánh giá nhận thức người dùng
Giải pháp và triển khai	Khắc phục và triển khai	WAF, API Security; NGFW; NAC; chống DDoS; EDR/XDR; PAM; MFA; Database Firewall; mã hóa dữ liệu; DLP; Cloud Security; bảo vệ email; bảo vệ ứng dụng AI/LLM; SIEM, XSIAM, SOAR; quản lý lỗ hổng; quản lý bề mặt tấn công
Giám sát và ứng cứu (HSOC)	Giám sát và duy trì	Giám sát ATTT 24/7 (SOC as a Service); MDR; NDR; SOAR; Threat Intelligence; Threat Hunting, Compromise Assessment; điều tra số và ứng cứu sự cố (DFIR); quản lý lỗ hổng, bản vá, WAF, PAM, bảo mật đám mây dạng dịch vụ; giám sát IoT; đo lường an toàn chuỗi cung ứng

10.2 Gợi ý theo tình huống

Tình huống của tổ chức	Dịch vụ có thể tham khảo
Chưa biết hệ thống đang ở đâu so với hướng dẫn	Đánh giá hiện trạng theo checklist Phụ lục A: đánh giá cấu hình, dò quét lỗ hổng và ASM
Nghi ngờ đã bị xâm nhập, thấy dấu hiệu bất thường nhưng chưa chắc chắn	Compromise Assessment; nếu xác nhận có sự cố, chuyển sang DFIR
Đang có sự cố	DFIR: ngăn chặn, điều tra, xác định phạm vi và hỗ trợ khôi phục
Sắp đưa ứng dụng mới ra Internet	Kiểm thử xâm nhập và rà soát checklist Phụ lục A.1 trước go-live
Phát hành ứng dụng liên tục, nhiều phiên bản mỗi tháng	Kiểm thử xâm nhập liên tục
Ứng dụng có lỗ hổng nhưng chưa sửa mã kịp	WAF as a Service (vá ảo có thời hạn) song song với kế hoạch sửa mã
Không có nhân sự trực an ninh 24/7	SOC as a Service 24/7; MDR

Tình huống của tổ chức	Dịch vụ có thể tham khảo
Đã có SIEM nhưng cảnh báo quá nhiều, xử lý chậm	Tinh chỉnh use case; SOAR; mô hình giám sát kết hợp
Nhiều tài khoản quản trị dùng chung, không ghi phiên	PAM kết hợp MFA chống phishing
Đang chuyển hệ thống lên cloud	Cloud Security, CSPM; kiểm thử lại trước khi go-live trên hạ tầng mới (SD-14)
Muốn biết các lớp phòng thủ có chịu được tấn công có chủ đích	Red Team
Có yêu cầu tuân thủ của cơ quan quản lý	Đánh giá tuân thủ theo ngành (TT 09/2020/TT-NHNN, SWIFT CSCF, TT 12/2022/TT-BTTTT); tư vấn hệ thống thông tin theo cấp độ
Nhà máy, kho vận có nhiều thiết bị IoT	Giám sát thiết bị IoT

Liên hệ

Trung tâm Điều hành An ninh mạng | Email: hsoc@hpt.vn

Liên hệ

Văn phòng Tổng công ty
Lô E2a-3 Đường D1, Khu Công nghệ cao, Phường Tăng Nhơn Phú, TP. HCM
Tel: +(84 28) 38 266 206 | **Email:** info@hpt.vn
Website: https://hpt.vn

HPT Vietnam Corporation

Trung tâm Dịch vụ Khách hàng
Số 37 Nguyễn Trường Tộ, Phường Xóm Chiếu, TP. HCM
Tel: +(84 28) 38 266 206 | **Hotline:** 18006686

Văn phòng Chi nhánh Hà Nội
Tầng 10, tòa nhà Việt, số 1 Thái Hà, Phường Đống Đa, TP. Hà Nội
Tel: +(84 28) 38 266 206