

HSOC PLATFORM

NỀN TẢNG TRUNG TÂM ĐIỀU HÀNH AN NINH MẠNG HỢP NHẤT

DATASHEET SẢN PHẨM

THÔNG TIN HÀNG HÓA	NỘI DUNG
Tên hàng hóa	Hệ thống giám sát tập trung / Phần mềm Nền tảng trung tâm điều hành ANM
Mã hàng	HSOC Platform
Hãng	HSOC
Nhà phát triển / cung cấp	HPT Vietnam Corporation
Xuất xứ	Việt Nam
Mô hình ưu tiên	On-Premise; sẵn sàng mở rộng Hybrid / Cloud
Năng lực cấu hình tham chiếu	5.000 EPS, mở rộng theo tài nguyên và kiến trúc triển khai

1. Về sản phẩm

HSOC Platform là nền tảng trung tâm điều hành an ninh mạng do HPT phát triển, hợp nhất các năng lực thu thập dữ liệu, quản lý sự kiện, phát hiện, điều tra, quản lý sự cố, tự động hóa phản ứng và báo cáo trên một hệ sinh thái. Nền tảng được tổ chức theo kiến trúc mô-đun, cho phép chia sẻ dữ liệu, ngữ cảnh, chỉ báo xâm nhập, cảnh báo và trạng thái xử lý xuyên suốt vòng đời sự cố.

Điểm nổi bật

- Hợp nhất SIEM, SIRP, SOAR, NSM, EDR/Agent, VM, Threat Hunting, Threat Intelligence và ASM.
- Thu thập đa nguồn, chuẩn hóa, lập chỉ mục, tìm kiếm và tương quan theo thời gian thực.
- Hỗ trợ luật/pattern, chuỗi sự kiện, IOC, MITRE ATT&CK, Kill Chain, UEBA và phân tích bất thường bằng ML.
- Quản lý toàn bộ vòng đời cảnh báo/sự cố, cộng tác theo vai trò và lưu dấu vết xử lý.
- Tự động hóa phản ứng bằng playbook, hỗ trợ chế độ tự động hoặc có phê duyệt.
- Dashboard quản trị và vận hành theo thời gian thực; theo dõi cảnh báo, sự cố, EPS, tài sản, lỗ hổng, MTTD/MTTR.
- Triển khai On-Premise, Cloud/SOCaaS hoặc Hybrid; ưu tiên On-Premise cho TBDU.

2. Kiến trúc nền tảng hợp nhất

2.1 Các phân hệ lõi

PHÂN HỆ	MÔ TẢ CHỨC NĂNG
SIEM	Thu thập, chuẩn hóa, lưu trữ, tìm kiếm, tương quan, cảnh báo và báo cáo sự kiện an ninh.
SIRP	Quản lý cảnh báo/case/ticket và toàn bộ vòng đời sự cố, bằng chứng, lịch sử, người xử lý và SLA.
SOAR	Điều phối công cụ và tự động hóa quy trình bằng playbook, hỗ trợ phê duyệt và nhật ký từng bước.
NSM	Phân tích lưu lượng mạng thời gian thực, IDS/NSM, phiên mạng, PCAP và ngữ cảnh điều tra.
EDR / Agent	Thu thập telemetry đầu cuối, giám sát tiến trình, kết nối, file/registry và hỗ trợ phản ứng.
VM	Quét, tổng hợp, đánh giá rủi ro, ưu tiên khắc phục và theo dõi trạng thái lỗ hổng.
TH	Truy vấn và rà soát chủ động trên log, mạng, endpoint và TI để phát hiện nguy cơ chưa tạo cảnh báo.
TI	Quản lý IOC IP/domain/URL/hash/file, làm giàu, đối chiếu, chia sẻ và tích hợp với luật/playbook.
ASM	Nhận diện tài sản và điểm phơi nhiễm; liên kết tài sản, lỗ hổng, mối đe dọa và sự cố theo ngữ cảnh.

2.2 Luồng dữ liệu xuyên suốt

Nguồn dữ liệu → Collector/Agent/API → Parse & Normalize → Index & Retention → Correlation/UEBA/TI → Alert → Case/Incident → Playbook/Response → Closure → Dashboard/Report. Dữ liệu và lịch sử được duy trì xuyên suốt từ khi tiếp nhận đến khi đóng sự cố, hỗ trợ điều tra, kiểm toán và tuân thủ.

HSOC PLATFORM

Kiến trúc luồng dữ liệu & xử lý sự cố



3. Thông số kỹ thuật chính

HẠNG MỤC	THÔNG SỐ / KHẢ NĂNG
Kiểu triển khai	On-Premise là cấu hình chính; hỗ trợ Cloud/SOCaaS và Hybrid theo phương án triển khai.
Năng lực xử lý	Cấu hình tham chiếu 5.000 EPS; mở rộng theo tài nguyên tính toán, lưu trữ và phân tách node. Không giới hạn EPS/GB.
Nguồn thu thập	Firewall, IDS/IPS, WAF, EDR/EPP, server Windows/Linux/Unix, ứng dụng, CSDL, thiết bị mạng, hạ tầng ảo hóa, cloud, Office 365, scanner và nguồn tùy biến.
Giao thức/kết nối	Syslog UDP/TCP/Secure Syslog, SNMP, NetFlow/IPFIX, WMI, Windows Event, file đơn/đa dòng, HTTP/HTTPS, WebSocket, API, JDBC, Kafka/RabbitMQ, agent.
Lưu trữ	Tập trung 12 tháng theo dung lượng và chính sách lưu trữ được thiết kế. Hỗ trợ raw log, index, backup và truy vết lịch sử.
Tìm kiếm	Full-text/keyword, bộ lọc đa chiều, thời gian, biểu thức Boolean, nhóm/aggregation, regex và truy vấn lịch sử.
Tích hợp TI	IOC IP/domain/URL/hash/file; API; STIX/TAXII hoặc cơ chế tương đương theo module/tích hợp; MITRE ATT&CK.
Quản trị	Giao diện thống nhất, RBAC, nhật ký quản trị/vận hành, cấu hình luật, dashboard, báo cáo, quy trình và playbook.
API & mở rộng	API tích hợp công cụ bảo mật, ITSM và nguồn dữ liệu; kiến trúc mô-đun/Marketplace hoặc cơ chế tương đương.
Báo cáo	Theo thời gian thực, định kỳ hoặc theo yêu cầu; hỗ trợ xuất PDF, CSV, Excel, XML và gửi Email theo cấu hình.

4. Mô tả chi tiết tính năng

- Hỗ trợ theo dõi tình trạng mất log, gián đoạn kết nối nguồn thu thập, tỷ lệ parsing thành công và xu hướng tăng trưởng dữ liệu phục vụ capacity planning.
- Cơ chế chuẩn hóa dữ liệu đưa các nguồn log khác nhau về mô hình dữ liệu thống nhất, giúp xây dựng dashboard, báo cáo và luật tương quan dùng chung trên toàn hệ thống.
- HSOC Platform hỗ trợ kiến trúc Collector phân tán, cho phép đặt collector tại các vùng mạng hoặc đơn vị thành viên khác nhau nhằm giảm tải đường truyền và đáp ứng yêu cầu phân tách vùng bảo mật.

4.1 Thu thập và quản lý dữ liệu an ninh

- Hỗ trợ thu thập đa nguồn bằng cả push và pull; ưu tiên agentless, đồng thời dùng agent cho telemetry sâu, EDR và giám sát toàn vẹn.
- Collector thực hiện parse, normalize, timestamp, gắn nguồn/host, lập chỉ mục và chuyển tiếp dữ liệu hoặc xử lý tại chỗ.
- Hỗ trợ nguồn chưa có sẵn connector bằng parser/quy tắc chuẩn hóa tùy chỉnh; sau chuẩn hóa vẫn sử dụng được tìm kiếm, báo cáo và tương quan.
- Giám sát trạng thái thu thập, EPS, loại nguồn dữ liệu và trạng thái agent trên dashboard.
- Năng lực cấu hình tham chiếu 5.000 EPS, có thể mở rộng bằng cách bổ sung tài nguyên compute, storage, collector/indexer và phân tách vai trò node.
- Triển khai chính On-Premise tại từng đơn vị; toàn bộ log, dữ liệu và quá trình xử lý được thực hiện trong hạ tầng đơn vị. Kiến trúc sẵn sàng mở rộng sang Hybrid/Cloud.

4.1.1 Lưu trữ, tìm kiếm và duy trì dữ liệu

- Lưu trữ log tập trung 12 tháng và được sizing theo EPS trung bình/đỉnh, kích thước sự kiện, hệ số nhân bản, backup và tăng trưởng.
- Hỗ trợ full-text search, keyword, Boolean, regex, aggregation, truy vấn theo thời gian, filter đa chiều và truy vết lịch sử phục vụ điều tra, kiểm toán và tuân thủ.
- Dữ liệu được duy trì xuyên suốt từ ingest, chuẩn hóa, phân tích, tạo cảnh báo, lập hồ sơ sự cố, thực thi phản ứng đến khi đóng sự cố.
- Hỗ trợ đánh giá mức độ ảnh hưởng theo tài sản quan trọng, mức độ ưu tiên kinh doanh và ngưỡng cảnh điều tra nhằm giảm cảnh báo giả.
- Cho phép xây dựng nhiều lớp phát hiện gồm use case vận hành, use case tuân thủ, IOC matching, behavioral analytics và correlation nâng cao.
- Kho dữ liệu tập trung hỗ trợ điều tra chuyên sâu, pivot theo tài sản, người dùng, địa chỉ IP, tên miền, hash hoặc mã sự kiện liên quan.

4.2 SIEM và phân tích nâng cao

- Tương quan rule-based, pattern, chuỗi sự kiện và ngưỡng cảnh theo thời gian thực; kích hoạt trên mẫu sự kiện phức tạp.
- Kết hợp UEBA, ML/abnormal detection, user behavior, IOC, Kill Chain, APT detection và MITRE ATT&CK mapping.
- Cho phép xây dựng, điều chỉnh, quản lý luật; phân loại theo nguồn, loại mối đe dọa, tài sản và mức độ nghiêm trọng.
- HSOC AI Assistant hỗ trợ hỏi đáp SOC, phân tích cảnh báo/sự cố, báo cáo trạng thái và khuyến nghị phản ứng; việc dùng chatbot cho từng chức năng phụ thuộc quyền và cấu hình.
- Hỗ trợ phát hiện chuỗi sự kiện phức tạp theo thời gian thực; xây dựng, điều chỉnh và quản lý tập luật; phân loại cảnh báo theo nguồn, loại mối đe dọa, tài sản và mức độ nghiêm trọng.
- Tích hợp Threat Intelligence với IOC IP, domain, URL, file/hash; ánh xạ MITRE ATT&CK; STIX/TAXII hoặc phương thức tương đương được cung cấp theo module/tích hợp.
- Cho phép theo dõi SLA xử lý, quá hạn, thời gian phản hồi và hiệu quả thực hiện theo cá nhân hoặc nhóm vận hành.
- Mỗi hồ sơ sự cố có thể lưu trữ nhật ký điều tra, bằng chứng, file đính kèm, hành động xử lý và kết quả khắc phục phục vụ kiểm toán sau này.
- SIRP cung cấp cơ chế chuẩn hóa quy trình vận hành giữa Tier 1, Tier 2, Tier 3 và các bộ phận CNTT của đơn vị.

4.3 SIRP và quản lý sự cố

- Tạo hồ sơ/case/ticket từ cảnh báo hoặc thủ công; phân loại, ưu tiên, gán người xử lý, trạng thái, thời hạn và lịch sử thao tác.
- Chuẩn hóa các bước tiếp nhận, xác minh, phân tích, điều tra, xử lý, khắc phục, đóng sự cố và báo cáo sau sự cố.
- Lưu bằng chứng, ghi nhận kết luận/khuyến nghị và hỗ trợ cộng tác Tier 1, Tier 2, Tier 3 cùng quản trị viên đơn vị.
- Quản lý tập trung toàn bộ cảnh báo và sự cố; hỗ trợ assignee, priority/severity, trạng thái, bằng chứng, lịch sử thao tác, thời hạn xử lý và khả năng truy vết từ khi tạo cảnh báo đến khi đóng sự cố.
- Cho phép áp dụng cơ chế phê duyệt nhiều cấp đối với các hành động có nguy cơ ảnh hưởng đến hoạt động sản xuất kinh doanh.
- Hỗ trợ tích hợp với email, firewall, EDR, Active Directory, ITSM và các nền tảng bảo mật khác thông qua API hoặc connector.
- Playbook có thể được xây dựng theo dạng kéo thả hoặc theo các bước xử lý chuẩn hóa của tổ chức.

4.4 SOAR và phản ứng tự động

- Thiết kế, tùy chỉnh, kiểm thử, kích hoạt và theo dõi playbook; chạy tự động hoặc yêu cầu phê duyệt.
- Điều phối hành động như cô lập endpoint, chặn IP/domain, khóa tài khoản, cập nhật policy, thu thập bằng chứng và gửi thông báo khi hệ thống đích hỗ trợ API/connector.
- Ghi log từng bước, kết quả và lỗi thực thi; góp phần giảm MTTA/MTTR và chuẩn hóa phản ứng.
- Hỗ trợ điều phối cô lập endpoint, chặn IP/tên miền, khóa hoặc vô hiệu hóa tài khoản, cập nhật chính sách, thu thập bằng chứng và gửi thông báo, với điều kiện hệ thống đích có API/connector phù hợp.
- Hỗ trợ xây dựng kịch bản phản ứng dựa trên kết hợp giữa cảnh báo mạng và cảnh báo endpoint.
- Dữ liệu endpoint được liên kết với dữ liệu mạng và sự kiện bảo mật để tăng cường độ chính xác khi điều tra.
- Năng lực NSM cung cấp khả năng quan sát mạng theo thời gian thực, hỗ trợ xác minh nhanh nguồn gốc và phạm vi truyền lan của sự cố.

4.5 NSM và EDR/Agent

- Giám sát thời gian thực lớp mạng, phát hiện APT, signature, bất thường, exploit, dịch vụ bất thường và C&C; hỗ trợ session search và PCAP.
- Agent thu thập Windows/Linux log, tiến trình, kết nối mạng, driver/image load, file/registry/configuration integrity và flat-file ứng dụng.
- Hành động phản hồi đầu cuối được thực hiện qua EDR/connector phù hợp, theo chế độ tự động hoặc có phê duyệt.
- Hỗ trợ cô lập thiết bị, ngăn chặn tiến trình hoặc đối tượng độc hại và cung cấp dữ liệu đầu cuối cho nền tảng phân tích, điều tra tập trung theo module EDR/Agent được chào.
- Threat Hunting hỗ trợ xây dựng giả thuyết điều tra, truy vấn IOC hàng loạt và rà soát dấu hiệu tấn công nâng cao trên nhiều nguồn dữ liệu.
- ASM giúp nhận diện tài sản công khai, dịch vụ phơi lộ và các điểm tiếp xúc có thể bị khai thác từ bên ngoài.
- VM hỗ trợ xây dựng quy trình quản lý lỗ hổng khép kín từ phát hiện, đánh giá đến xác nhận khắc phục.

4.6 VM, ASM, Threat Hunting và TI

- VM hỗ trợ quét định kỳ/theo yêu cầu, xác thực phát hiện, chấm điểm rủi ro, khuyến nghị, khắc phục và quét lại.
- ASM mở rộng quản lý tài sản/phơi nhiễm và ưu tiên rủi ro theo ngưỡng cảnh;
- Threat Hunting hỗ trợ truy vấn log, mạng, endpoint và IOC nhằm tìm dấu vết chưa tạo cảnh báo và mở rộng phạm vi ảnh hưởng.
- TI lưu và duy trì IOC, APT/campaign, thông tin CVE, khai thác, malware và nguồn nội bộ/bên ngoài; làm giàu cảnh báo và hỗ trợ luật/playbook.
- Quản lý vòng đời chỉ báo, độ tin cậy, thời hạn hiệu lực và sử dụng IOC trong luật phát hiện, điều tra, playbook; các trường confidence/expiry cần được xác nhận theo phiên bản và demo.
- VM phát hiện, tổng hợp và quản lý lỗ hổng; đánh giá rủi ro, ưu tiên khắc phục và theo dõi trạng thái. ASM nhận diện tài sản và điểm phơi nhiễm, liên kết tài sản, lỗ hổng, mối đe dọa và sự cố theo ngưỡng cảnh.
- Threat Hunting cung cấp tìm kiếm, truy vấn và rà soát chủ động trên log, mạng, endpoint và TI nhằm xác định dấu vết, mở rộng phạm vi ảnh hưởng và phát hiện nguy cơ chưa tạo cảnh báo.
- Hỗ trợ xuất bản báo cáo phục vụ kiểm toán nội bộ, đánh giá an toàn thông tin và các yêu cầu của cơ quan quản lý nhà nước.
- Các biểu đồ xu hướng giúp theo dõi thay đổi mức độ rủi ro, hiệu quả xử lý và mức độ tuân thủ theo thời gian.
- Dashboard được thiết kế theo nhiều tầng thông tin từ lãnh đạo, quản lý đến vận hành kỹ thuật.

4.7 Dashboard, báo cáo và Security Posture

- Dashboard theo vai trò cho lãnh đạo, quản trị và vận hành; hiển thị cảnh báo, sự cố, severity, xu hướng, trạng thái xử lý, EPS, agent, tài sản và lỗ hổng.
- Theo dõi MTTD, MTTA, MTTR theo dữ liệu vòng đời cảnh báo/sự cố và cấu hình KPI.
- Hỗ trợ dashboard/báo cáo cấp Tỉnh, cấp đơn vị và tùy biến giao diện theo nhu cầu;
- Báo cáo định kỳ, báo cáo quản trị, báo cáo sự cố, báo cáo tuân thủ và xuất dữ liệu phục vụ kiểm toán.
- Dashboard tối thiểu hiển thị số lượng cảnh báo, sự cố, severity, xu hướng, trạng thái xử lý, MTTD và MTTR; đồng thời theo dõi tải vận hành, tài sản, lỗ hổng và mối đe dọa.
- Hỗ trợ dashboard theo vai trò, báo cáo cấp Tỉnh/cấp đơn vị, giao diện tiếng Việt và thêm bớt giao diện theo yêu cầu; phạm vi tùy biến phải được chứng minh trong demo/UAT.
- Hỗ trợ cảnh báo sớm khi xuất hiện bất thường về hiệu năng hoặc lỗi tích hợp ảnh hưởng đến dịch vụ nghiệp vụ.
- Cho phép hiển thị tình trạng dịch vụ CNTT quan trọng trên cùng giao diện với chỉ số an toàn thông tin.
- Có khả năng kết hợp dữ liệu giám sát ứng dụng với sự kiện bảo mật để xác định nhanh nguyên nhân gốc khi xảy ra sự cố.

4.8 Theo dõi API và ứng dụng

- HSOC Platform có thể tiếp nhận log/metric/trạng thái từ API, ứng dụng, web service và hạ tầng cloud thông qua API, HTTP/HTTPS, agent hoặc connector.
- Các chỉ số availability, response time, error rate và truy vết điểm nghẽn kiểu APM được đáp ứng thông qua module/nguồn giám sát tích hợp.
- Hỗ trợ kiểm tra tính sẵn sàng, thời gian phản hồi và lỗi API/ứng dụng; dữ liệu giám sát được đưa vào dashboard, cảnh báo hoặc quy trình xử lý tùy theo connector/module tích hợp.

5. Mô hình triển khai

MÔ HÌNH	MÔ TẢ
On-Premise	Thu thập, xử lý, phân tích và lưu trữ trong hạ tầng đơn vị; log thô không rời site. Có thể chỉ chuyển metadata cảnh báo cho đội ngũ SOC qua kênh bảo mật.
Cloud / SOCaaS	Log được chuyển qua kênh VPN/mã hóa tới hạ tầng SOC tập trung để xử lý, lưu trữ và quản lý từ xa.
Hybrid	Phân bổ xử lý/lưu trữ giữa on-premise và cloud; giữ dữ liệu nhạy cảm tại chỗ và sử dụng năng lực tập trung cho phần phù hợp.

Khả năng mở rộng

- Mở rộng EPS/GB ngày bằng bổ sung compute, storage, collector/indexer và phân tách vai trò node mà không thay đổi kiến trúc tổng thể.
- Bổ sung nguồn dữ liệu bằng connector, parser tùy chỉnh, agent hoặc API.
- Bổ sung phân hệ và kịch bản vận hành theo mô-đun, tích hợp/Marketplace hoặc cơ chế tương đương.
- Sẵn sàng mở rộng từ On-Premise sang Hybrid/Cloud theo chính sách dữ liệu của đơn vị.

6. Quản trị, tích hợp và chuyển giao

- Quản trị tập trung, phân quyền theo vai trò và phạm vi đơn vị/tenant; lưu nhật ký quản trị và vận hành.
- Cấu hình chính sách, rule, use case, dashboard, báo cáo, workflow và playbook theo đặc thù đơn vị.