UBND TỈNH THANH HÓA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1314 /STTTT-VP

V/v đề nghị cung cấp báo giá phục vụ xây dựng Báo cáo Nghiên cứu khả thi dự án: Xây dựng và triển khai hệ thống theo dõi, cảnh báo sớm nguy cơ, điều phối ứng cứu sự cố an toàn thông tin mạng cho các cơ quan đơn vị trên địa bàn tỉnh Thanh Hóa.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Thanh Hóa, ngày 08 tháng 6 năm 2024

Kính gửi: Các đơn vị cung cấp thiết bị lĩnh vực Công nghệ thông tin

Hiện nay, Sở Thông tin và Truyền thông Thanh Hoá đang trong quá trình xây dựng, hoàn thiện Báo cáo nghiên cứu khả thi dự án: Xây dựng và triển khai hệ thống theo dõi, cảnh báo sớm nguy cơ, điều phối ứng cứu sự cố an toàn thông tin mạng cho các cơ quan đơn vị trên địa bàn tỉnh Thanh Hóa. Để có cơ sở xem xét, phục vụ lập Tổng mức đầu tư thuộc dự án, Sở Thông tin và Truyền thông kính đề nghị các đơn vị có năng lực cung cấp báo giá thiết bị Công nghệ thông tin thuộc dự an nêu trên, với nội dung cụ thể như sau:

1. Dang mục thiết bị cần báo giá: Chi tiết theo phụ lục đính kèm.

2. Nội dung báo giá của quý đơn vị (kèm theo Hồ sơ năng lực) đề nghị gửi về Sở Thông tin và Truyền thông Thanh Hoá theo địa chỉ: Toà nhà Trung tâm Công nghệ thông tin, Phố Ái Sơn 2, Phường Đông Hải, Thành phố Thanh Hoá, tỉnh Thanh Hoá (trước 16h, ngày 11/6/2024).

Sở Thông tin và Truyền thông rất mong nhận được sự quan tâm, phối hợp của Quý đơn vị./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (B/c);
- Lưu: VT, BQLDA,VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH THANH HÓA

Nguyễn Văn Tước

Phụ lục danh mục thiết bị đề nghị báo giá

(Kèm theo Công văn số: /STTTT-VP, ngày /6/2024 của Sở Thông tin và Truyền thông)

TT	Danh mục thiết bị	Thông số kỹ thuật	ĐVT	Số lượng
1	**Hệ thống máy chủ**			
1.1	**Máy chủ**		**Bộ**	**8**
	Kiểu dáng	Rackmount		
	Kích thước	2U		
	Bộ xử lý trung tâm	02 x Bộ xử lý Intel Xeon-Gold 5420+ 2.0GHz 28-core 205W Processor hoặc tương đương		
	Chipset	Intel C741 Chipset		
	Bộ nhớ trong	512GB (16x32GB) DDR5 4800 MT/s		
		Hỗ trợ mở rộng 8TB		
		Hỗ trợ công nghệ bộ nhớ SmartMemory		
	Ổ cứng	≥ 02 ổ cứng 480GB SSD ≥ 04 ổ cứng 1.92TB NVMe SSD		
		Có khả năng thay thế nóng		
		Hỗ trợ các loại ổ đĩa: SATA, SAS, SSD		
	Khả năng lắp đặt ổ cứng tối đa	Hỗ trợ mở rộng lên 38 ổ cứng 2.5 inch trong thân máy		
	Card điều khiển hệ thống ổ cứng	Bộ nhớ đệm 4GB.		
		Hỗ trợ ít nhất các mức RAID sau: 0, 1, 5, 6, 10, 50, 60		
	Card giao tiếp mạng	2x Dual Port 10/25Gb SFP28, kèm 4x25Gb SFP+ SR Transceiver 4x1Gbps Ethernet		
	Card giao tiếp quang	2x Dual Port 32Gb Fibre Channel Adapter		
	I/O slots	Có sẵn 3 khe cắm PCIe 5.0, hỗ trợ 8 khe cắm PCI Express 5.0		
	Graphics	Có 1 cổng VGA hỗ trợ độ phân giải: 1920 x 1200 (32 bpp)		
	Hệ thống nguồn	Có đủ số nguồn theo thiết kế, tối thiểu 02 nguồn xoay chiều tối thiểu 800W hỗ trợ thay nóng (hot swap/hot plug)		
	Hỗ trợ các hệ điều hành	Windows Server VMware vSphere Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Ubuntu Oracle Linux		
	Bảo hành	3 năm chính hãng		
1.2	**Phần mềm ảo hóa kèm phần mềm quản lý ảo hóa dành cho 8 máy chủ trong 5 năm**		**License**	**448**

	Phần mềm ảo hóa VMWare vSphere kèm chức năng quản lý ảo hóa Vcenter Standard trên một core cho phần cứng các máy chủ bổ sung (8 máy chủ x 2 CPU x 28 core = 448 license) trong 5 năm)			
2	**Hệ thống lưu trữ**			
2.1	Thiết bị lưu trữ		Hệ thống	1
	Bộ điều khiển	2 bộ điều khiển (controller), 256GiB Cache Hoạt động ở chế độ Mesh – Active hoặc Active – Active		
	Dung lượng yêu cầu	Tối thiểu 22 x 3.84TB SAS SFF (2.5in) SSD Tối thiểu 160 x 2.4TB SAS 10K SFF (2.5in) HDD		
	Loại ổ cứng hỗ trợ	NVMe SSD, SAS SSD, HDD		
	RAID hỗ trợ	RAID single parity (4 or 5) or Dual parity (6 or 3D)		
	Cổng giao tiếp (có sẵn)	08 port 32Gb FC		
		04 cổng kết nối 10/25GbE		
	Tính sẵn sàng	100% data availability guarantee		
		Các thành phần hoạt động dự phòng và có khả năng thay thế nóng bao gồm: Controllers, Power Supplies, SSDs		
	Khả năng quản lý hiệu năng và báo cáo	Phần mềm quản trị hệ thống cung cấp công cụ báo cáo dữ liệu lịch sử của hệ thống		
	Hệ điều hành hỗ trợ	Microsoft Windows;HPE HP-UX, IBM AIX, IBM Virtualization, Oracle Linux, Oracle Solaris, Oracle VM, Red Hat Enterprise Linux,| SUSE® Linux Enterprise Server (SLES), VMware ESX and ESXi, VSI OpenVMS		
	Bảo hành	03 năm theo tiêu chuẩn của nhà sản xuất		
2.2	Thiết bị chuyển mạch		Bộ	2
	Số lượng cổng	24 port		
	Tốc độ hỗ trợ	32, 16, 8, 4Gb/s, lựa chọn với transceiver 32 hoặc 16Gb/s		
	Kèm sẵn	16 port activated (included SFP 32Gbps, cáp LC/LC Multimode 15m)		
	Bảo hành	03 năm theo tiêu chuẩn của nhà sản xuất		
3	**Thiết bị chuyển mạch**		**Bộ**	**2**
	Số cổng downlink	24 cổng 1/10G, sử dụng SFP/SFP+		
	Số cổng uplink	4 cổng 40GbE/100GbE, sử dụng QSFP+		
	Dung lượng chuyển mạch	1.28 Tbps		
	Thông lượng	>= 952 Mpps		
	Packet Buffer	32 MB		
	Bảng địa chỉ IPv4 hỗ trợ	>= 65000		
	Bảng địa chỉ IPv6 hỗ trợ	>= 65000		
	Bộ vi xử lý	4 nhân 64-bit		
	Bộ nhớ	16GB RAM		
	Lưu trữ	32GB		

	Tính năng quản trị	Hỗ trợ SNMP v2/3, ACL, sFlow, RMON		
	Tính năng khác	hỗ trợ MCLAG, ERPS, VRRP, BFD, UDLD		
	Công suất tiêu thụ tối đa	>= 400W		
	Tiêu chuẩn an toàn	IEC 62368-1:2014, IEC 62368-1:2018		
	Tiêu chuẩn chống nhiễm từ	EN55032:2015/CISPR 32, Class A		
	Bảo hành	3 năm chính hãng.		
4	**Hệ thống giám sát, cảnh báo sớm nguy cơ mất an toàn, an ninh thông tin tập trung**		Phần mềm	1
4.1	Phần mềm tổng hợp, phân tích và cảnh báo sự cố an toàn thông tin từ hệ thống giám sát vệ tinh			
		'- Tổng hợp, phân tích dữ liệu nhận được từ phần mềm thu thập dữ liệu đầu cuối trên các máy tính người dùng - Kích hoạt các cảnh báo khi các nguy cơ hoặc bất thường được phát hiện ra. - Có kênh trao đổi được mã hóa và xác thực với phần mềm thu thập dữ liệu đầu cuối trên các máy tính người dùng - Quản lý đăng ký các phần mềm thu thập dữ liệu đầu cuối trên các máy tính người dùng kết nối tới. - Quản lý kết nối các thu thập dữ liệu đầu cuối trên các máy tính người dùng. - Thực hiện phân tích các dữ liệu nhận được từ thu thập dữ liệu đầu cuối trên các máy tính người dùng, thực hiện nhận dạng kiểu dữ liệu được xử lý (như Windows Event, SSHD Log, Web Server Log, …), và truy xuất các dữ liệu thành phần liên quan từ các bản tin log (như Source IP, Event ID, Username, …).		
		'- Sử dụng các tập luật để nhận dạng các dấu hiệu cụ thể để kích hoạt các cảnh báo. - Cung cấp tính năng phát hiện các chỉ báo xâm nhập đã biết (well-known Indicators Compromise) dựa trên các thông tin dữ liệu nhận dạng về IP Reputation, File Hashes, … - Ánh xạ các tập luật được thiết lập với nền tảng MITRE ATT&CK để thực hiện phân loại các cảnh báo và đưa ra một bức tranh an toàn thông tin toàn cảnh và tốt hơn. - Cung cấp một cơ sở dữ liệu CVE (Common Vulnerabilities & Exposures) được cập nhật thường xuyên từ các nguồn lỗ hổng khác nhau, từ		

		đó có thể nhận dạng các ứng dụng có lỗ hổng và đưa ra báo cáo về các rủi ro. - Cung cấp lưu trữ các thông tin về phần cứng và phần mềm của máy tính người dùng được giám sát. Các thông tin được lưu trữ bao gồm: + System Inventory: CPU, Memory, Diskspace, giao diện mạng, cổng mở, các tiến trình đang hoạt động và danh sách các ứng dụng. + File State: trạng thái file của hệ điều hành, ứng dụng, ví dụ mã checksum MD5, SHA1, SHA256, kích thước, quyền truy cập, quyền sở hữu, nội dung thay đổi, người tác động, … + Integration: tích hợp với VirusTotal, là nền tảng tổng hợp dữ liệu từ nhiều sản phẩm phòng chống mã độc khác nhau, để cung cấp cơ sở dữ liệu về dấu hiệu nhận biết các mã độc.		
4.2	Phần mềm nền tảng tri thức ATTT		Phần mềm	1
		Phần mềm nền tảng tri thức ATTT: - Thu thập dữ liệu về các mối đe dọa ATTT từ các nguồn tại Việt Nam và trên thế giới - Cung cấp thông tin về các mối de dọa cho các giải pháp khác như SIEM, IMS, … - Cung cấp các thông tin cơ bản về các mối đe dọa và xác định mức độ nguy hiểm của các mối đe dọa - TIP cho phép kết nối với các loại hệ thống sau để chia sẻ dữ liệu: + Các giải pháp và nền tảng khác loại (tối thiểu là SIEM, IDS/IPS, EDR). + Hệ thống giám sát an toàn không gian mạng quốc gia; - TIP cho phép chia sẻ dữ liệu log thông tin mối đe dọa theo chuẩn quốc tế STIX/TAXII.		
		'- TIP cho phép quản lý log đáp ứng các yêu cầu sau: + Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ, …). + Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có); + Cho phép tìm kiếm log thông tin mối đe dọa theo thời gian và phân nhóm; + Cho phép truy xuất log thông tin mối đe dọa thông qua cảnh báo; + Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào TIP khác hoặc giải pháp khác về quản lý, phân tích, điều tra log. - TIP cho phép phân loại và gán nhãn tên phân		

		nhóm cho log thông tin mối đe dọa theo các nhóm sau: + Điểm yếu, lỗ hổng an toàn thông tin đã được công bố; + Họ mã độc; + Kỹ thuật tấn công; + Chiến dịch tấn công; + Mục đích tấn công; + Loại đối tượng, tổ chức bị tấn công; + Đối tượng, tổ chức thực hiện tấn công; + Tên miền, địa chỉ IP của khách hàng có kết nối đến cơ sở hạ tầng của đối tượng, tổ chức thực hiện tấn công; + Điểm yếu, lỗ hổng an toàn thông tin đối với hệ thống của khách hàng.		
		'- TIP có chức năng cho phép thống kê các mối đe trên thế giới thông qua giao diện đồ họa đáp ứng các yêu cầu sau: + Cho phép thống kê xu hướng mối đe dọa dưới dạng biểu đồ. + Cho phép tìm kiếm dữ liệu xu hướng mối đe dọa theo thời gian (tối thiểu theo 04 mức: năm, quý, tháng, ngày). - TIP có chức năng cho phép quản lý thiết lập cảnh báo mối đe dọa đến người dùng đáp ứng các yêu cầu sau: + Cho phép nhận cảnh báo theo các phân nhóm; + Cho phép thiết lập thời gian nhận cảnh báo; + Cho phép tải nội dung cảnh báo dưới dạng tập tin; + Cho phép hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo; + Cho phép nhận cảnh báo qua phương thức gửi thư điện tử;		
		- TIP được triển khai phải đảm bảo đáp ứng các yêu cầu sau: + TIP đảm bảo rằng độ trễ thời gian tìm kiếm log với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 02 phút. + Dữ liệu tri thức các mối đe dọa của TIP có tối thiểu 100.000 bản ghi - TIP cho phép thu thập và lưu trữ log thông tin mối đe dọa từ các nguồn sau: + Các trang mạng xã hội (tối thiểu 01 trang); + Các trang web báo chí (tối thiểu 01 trang); + Nhà cung cấp sản phẩm TI. - TI cho phép thu thập và lưu trữ log thông tin mối đe dọa có các loại thông tin sau: + Mô tả tổng quan mối đe dọa; + Mức độ nguy hiểm của mối đe dọa; + Các phân nhóm được gán cho mối đe dọa; + Các thuộc tính mô tả chi tiết mối đe dọa.		

		- TIP cho phép ghi log quản trị hệ thống với đầy đủ thông tin - Trong trường hợp TIP phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), TIP đảm bảo các loại cấu hình hệ thống, quản trị, tài khoản và dữ liệu log phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp.		
5	**Hệ thống điều phối, tự động và phản ứng an toàn thông tin mạng (SOAR – Security Orchestration, Automation & Response)**			
5.1	Phần mềm điều phối, tự động hóa phản ứng an ninh thông tin		Phần mềm	1
		'- Cung cấp sẵn thư viện tích hợp nhiều công nghệ bảo mật khác nhau như: Endpoint Security, Network Security, Malware Analysis, Vulnerability & Risk Management, … SOAR cần cung cấp sẵn thư viện tích hợp và cho phép thiết lập cấu hình tham số kết nối tới hệ thống công nghệ thông tin. - SOAR cho phép cung cấp một hoặc nhiều API trên mỗi tích hợp để sử dụng dụng tối đã tính năng của nhà cung cấp. Mỗi API được hiểu là một chức năng trên một hệ thống công nghệ thông tin. - SOAR cho phép tích hợp với hệ thống công nghệ thông tin theo hai chiều: + Hỗ trợ truy vấn API lấy thông tin từ hệ thống công nghệ thông tin để làm giàu thông tin cho các đối tượng trên SOAR; + Hỗ trợ truy vấn API thực hiện lệnh tác động lên hệ thống thông tin để thực hiện việc phản ứng sự cố an toàn thông tin. - SOAR cho phép người dùng tự phát triển Playbook với các yêu cầu sau: + Cho phép tạo mới, xem lại và xóa Integration đã được tạo; + Cho phép tạo mới, xem lại và xóa Playbook đã được tạo; - Hỗ trợ tạo các thư viện playbook xử lý các sự cố ATTT, hỗ trợ thực hiện tự động/bán tự động		
		'- SOAR hỗ trợ Playbook thực hiện tự động hoàn toàn với yêu cầu sau: + Cho phép cấu hình tự động chạy Playbook bằng các điều kiện được xây dựng theo các quy tắc tìm kiếm Cảnh báo, Case;		

		+ Cho phép xem kết quả thực thi bao gồm: dữ liệu đầu vào, dữ liệu đầu ra, thời gian thực hiện, trạng thái thành công/thất bại. - SOAR cho phép người vận hành tham gia vào một bước của Playbook (Human Task), với yêu cầu sau: + Cho phép người dùng nhập dữ liệu đầu vào cho Human task với tối thiểu các định dạng: số, chuỗi kí tự, lựa chọn một trong các giá trị có sẵn, thời gian, đính kèm file; + Cho phép gán Human Task cho một người hoặc một nhóm người xử lý; + Cho phép đặt khoảng thời gian cho phép xử lý; + Cho phép sử dụng kết quả xử lý của người dùng cho các bước tiếp theo trong Playbook; + Cho phép xem kết quả thực thi bao gồm: dữ liệu người dùng đã nhập, thời gian xử lý, tài khoản xử lý. - Quản lý báo cáo: + Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo; + Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 01 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML; + Cho phép đặt lịch gửi báo cáo định kì tới email được cấu hình. - Trong trường hợp SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SOAR đảm bảo các cấu hình hệ thống, tài khoản người dùng, dữ liệu cảnh báo, dữ liệu trường hợp xử lý cảnh báo phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp.		
5.2	Phần mềm quản lý sự cố ATTT		Phần mềm	1
		'- Tự động thu thập cảnh báo và sự kiện ATTT từ SIEM, phân loại mức độ ưu tiên của cảnh báo - Quản lý các cảnh báo ATTT: + Cho phép thiết lập và cấu hình các cài đặt liên quan đến hệ thống cần thu thập cảnh báo. + Cho phép tìm kiếm cảnh báo theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có); + Cho phép lưu trữ và phân nhóm cảnh báo theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng, các dạng tấn công, …); + Cho phép gán kết quả xử lý cảnh báo với tối thiểu là cảnh báo sai (False Positive); + Cho phép xác định thời gian xử lý cảnh báo quá hạn hay không; + Cho phép chạy một Playbook trên SOAR với Cảnh báo.		

		'- Quản lý các case sự cố ATTT: + Cho phép tìm kiếm cảnh báo theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có); + Cho phép lưu trữ và phân nhóm case theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng, các dạng tấn công, …); + Cho phép gán kết quả xử lý cảnh báo với tối thiểu là cảnh báo sai (False Positive); + Cho phép xác định thời gian xử lý Case quá hạn hay không; + Cho phép gán 1 hoặc nhiều cảnh báo vào một Case; + Cho phép xem lịch sử tác động đến Case gồm: thời gian tác động, người tác động, nội dung tác động; + Cho phép chạy một Playbook với Case; + Cho phép gán người hoặc nhóm vận hành cho một Case; + Hỗ trợ cộng tác nhiều người xử lý cùng một Case.		
		'- Ghi lại toàn bộ quá trình phát hiện, kiểm tra, đánh giá, xử lý các sự kiện an toàn thông tin - Quản lý sự cố ATTT: + Đồ thị trực quan với tối thiểu các đối tượng: IP, email, domain; + Cho phép thu thập bằng chứng liên quan đến các sự cố và cho phép bằng chứng đó liên quan đến đối tượng nào trong sự cố; + Cho phép hiển thị dòng thời gian của cuộc tấn công với thông tin: thời điểm tấn công, đối tượng liên quan. - Quản lý báo cáo: + Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo; + Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 01 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML; + Cho phép đặt lịch gửi báo cáo định kì tới email được cấu hình. - Trong trường hợp IMS phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), IMS đảm bảo các loại cấu hình hệ thống, quản trị, tài khoản và dữ liệu log phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp		
5.3	Phần mềm quản lý dịch vụ ATTT		Phần mềm	1
		- Giám sát/Theo dõi các phiếu xử lý sự cố ATTT: các phiếu ưu tiên cao nhất, các phiếu sắp hết hạn, các phiếu theo người dùng, chất lượng xử lý các phiếu. - Tạo các phiếu xử lý sự cố ATTT: sự cố, điều tra		

		sự cố, quá trình xử lý. - Cho phép tìm kiếm các phiếu xử lý sự cố ATTT theo độ ưu tiên, trạng thái, khách hàng, các phiếu hỗn hợp, … - Cho phép đội ngũ giám sát ATTT thực hiện xử lý và cập nhật thông tin phiếu, truy vết lịch sử luồng xử lý của phiếu. - Thống kê chất lượng dịch vụ xử lý sự cố ATTT. - Trích xuất báo cáo xử lý phiếu: theo người yêu cầu, theo từng phiếu. - Quản lý thông tin tài khoản đội ngũ giám sát ATTT: cấp mới, thay đổi thông tin, vô hiệu hóa, xóa tài khoản. - Quản lý thông tin tài khoản người dùng: cấp mới, thay đổi thông tin, vô hiệu hóa, xóa tài khoản.		
6	**Tại các hệ thống thông tin UBND cấp xã**			
6.1	Phần mềm thu thập dữ liệu đầu cuối trên các máy tính người dùng		License 5 năm	8.810
		'- Hoạt động được trên đa dạng hệ điều hành gồm Linux, Windows, macOS, Solaris, AIX, … - Có kênh trao đổi được mã hóa và xác thực với phần mềm tổng hợp, phân tích và cảnh báo sự cố an toàn thông tin từ hệ thống giám sát vệ tinh - Có mô-đun thực hiện đọc các file flat log và các sự kiện Windows, thu thập các bản tin log của hệ điều hành và ứng dụng - Có mô-đun chạy định kỳ các lệnh được ủy quyền, thu thập các dữ liệu đầu ra được sử dụng để giám sát dung lượng ổ cứng, lấy danh sách truy cập gần nhất của người dùng, … - Có mô-đun giám sát các file hệ thống, báo cáo về các sự kiện liên quan như khi nào file được tạo, xóa hoặc thay đổi, theo dõi cả các thuộc tính, quyền hạn, sở hữu và nội dung của file - Có mô-đun thực hiện rà quét, thu thập dữ liệu về endpoint như phiên bản hệ điều hành, giao diện mạng, các tiến trình đang chạy, các ứng dụng cài đặt, và danh sách các port mở - Có mô-đun phát hiện các bất thường và sự hiện diện có thể có của các rootkit, đồng thời cũng giám sát hoạt động hệ thống, tìm kiếm các tiến trình ẩn, file ẩn, và port ẩn.		