IT Serving
Convenient and Safe

TRUNG TÂM ĐIỀU HÀNH AN TOÀN HỆ THỐNG

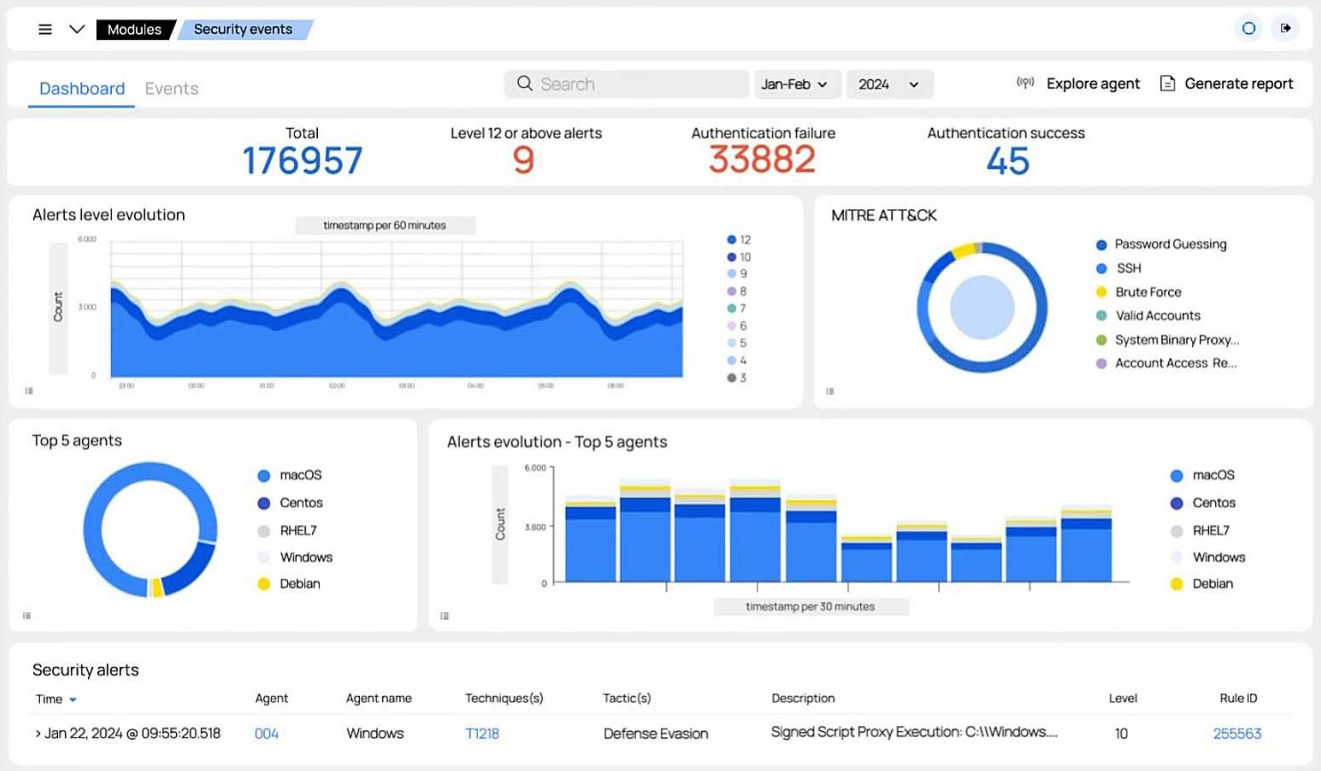
Hỗ trợ bảo mật thiết bị đầu cuối đa nền tảng:

ITServing
Convenient and Safe

Security Operations Center Platform

Hợp nhất SIEM và XDR bảo vệ thiết bị đầu cuối và Cloud Workload

Bảo vệ toàn diện hạ tầng công nghệ tổ chức



Giải pháp Trung tâm điều hành an ninh (SOC) cung cấp khả năng giám sát và bảo vệ an ninh mạnh mẽ cho mọi tài sản CNTT doanh nghiệp bằng cách sử dụng các chức năng Quản lý sự kiện và thông tin bảo mật (SIEM), Phát hiện và phản hồi mở rộng (XDR). Giải pháp SOC được thiết kế để bảo vệ tài sản kỹ thuật số và gia cường thế trận an ninh mạng toàn diện cho tổ chức.

Bảo vệ thiết bị đầu cuối

- Đánh giá cấu hình hệ thống
- Phát hiện mã độc
- Giám sát tính toàn vẹn tập tin

Tình báo mối nguy hại

- Săn tìm mối nguy
- Phân tích dữ liệu nhật ký
- Phát hiện lỗ hổng

Hoạt động an toàn

- Phản hồi sự cố
- Tuân thủ quy chuẩn an ninh
- Chuẩn hóa hoạt động CNTT

Bảo mật Cloud

- Bảo mật Container
- Quản lý hành vi
- Bảo vệ Workload

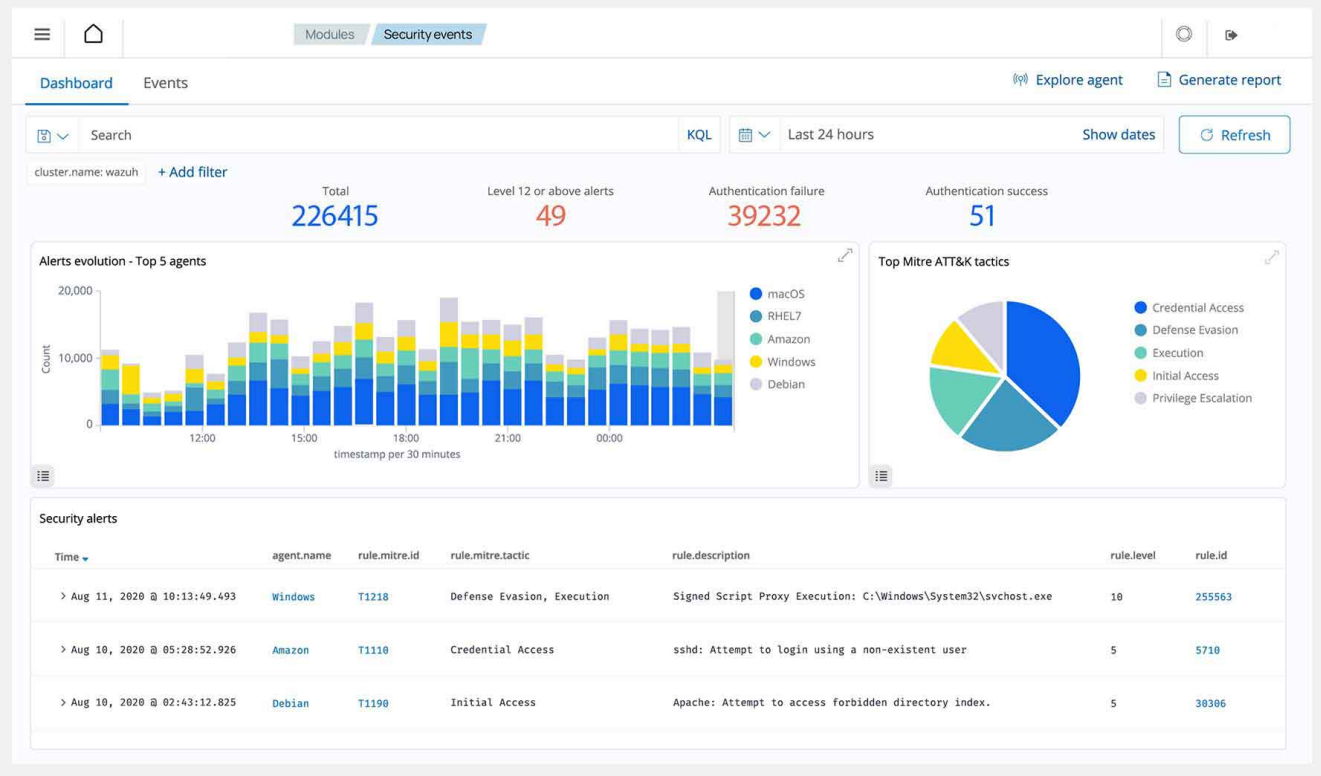
Hỗ trợ bảo mật thiết bị đầu cuối đa nền tảng:

Security Operations Center Platform

Hợp nhất SIEM và XDR bảo vệ thiết bị đầu cuối và Cloud Workload

Giải pháp toàn diện SIEM

Giải pháp Quản lý sự kiện và thông tin bảo mật (SIEM) là một nền tảng tập trung để tổng hợp và phân tích dữ liệu theo thời gian thực để phát hiện mối đe dọa và mức độ tuân thủ an toàn thông tin. Máy chủ SIEM giám sát thời gian thực toàn bộ hiện trạng an toàn thông tin của hệ thống thông qua việc thu thập dữ liệu sự kiện từ nhiều nguồn khác nhau: thiết bị đầu cuối (servers/desktops), thiết bị mạng, đám mây và các ứng dụng trong hệ thống thông tin của tổ chức.



Khả năng vận hành

Phân tích nhật ký bảo mật

Bảo vệ cơ sở hạ tầng tổ chức, đáp ứng nhu cầu tuân thủ quy định an toàn bằng việc giám sát, kiểm tra, thông báo hoạt động thiết bị đầu cuối.

Phát hiện lỗ hổng

Giám sát, phát hiện và thông báo chi tiết các lỗ hổng trên thiết bị đầu cuối.

Đánh giá an toàn cấu hình hệ thống

Dùng tiêu chí SCA của Trung tâm An ninh Internet (CIS) để xác định các cấu hình sai, lỗ hổng bảo mật trong cơ sở hạ tầng doanh nghiệp.

Tuân thủ quy định

Giải pháp giúp tổ chức theo dõi và chứng minh sự tuân thủ với nhiều khuôn khổ quy định khác nhau như PCI DSS, NIST 800-53, GDPR, TSC SOC2 và HIPAA.

Chức năng

Cảnh báo và thông báo

Cảnh báo và thông báo thời gian thực khi có sự cố bảo mật xảy ra. Nhà quản lý có thể tùy chỉnh cảnh báo phù hợp các nhu cầu cụ thể.

Báo cáo chi tiết SIEM

Tạo các báo cáo chuyên sâu cung cấp khả năng phân tích cao cấp về các sự kiện bảo mật diễn ra trong hệ thống thông tin tổ chức.

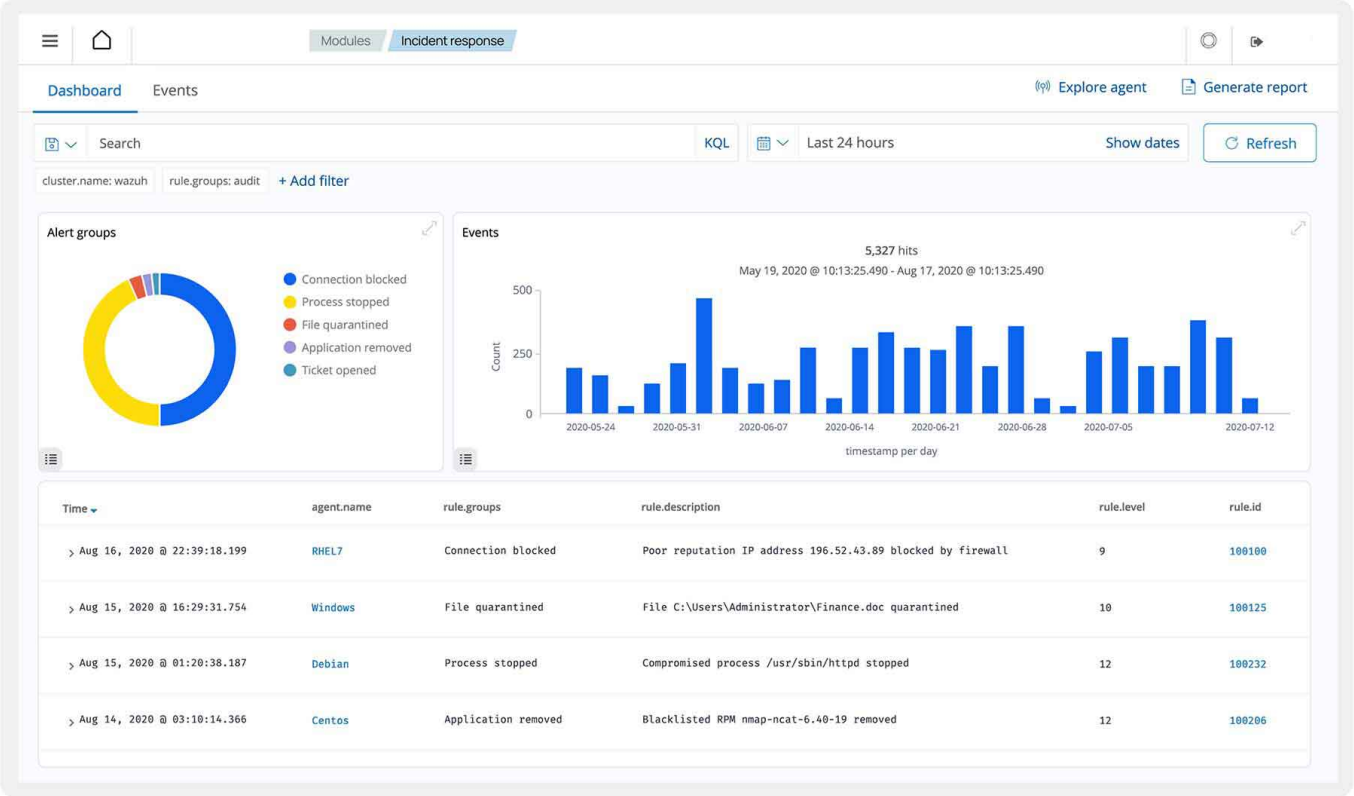
ITServing
Convenient and Safe

Security Operations Center Platform

Hợp nhất SIEM và XDR bảo vệ thiết bị đầu cuối và Cloud Workload

XDR chủ động bảo vệ hệ thống thông tin

Nền tảng Phát hiện và Phản hồi Mở rộng (XDR) cung cấp giải pháp an ninh toàn diện giúp phát hiện, phân tích và phản hồi đối với các mối đe dọa an ninh liên thông đa nền tảng trên nhiều lớp cơ sở hạ tầng CNTT doanh nghiệp. Máy chủ XDR thu thập dữ liệu từ các thiết bị đầu cuối, thiết bị mạng, dịch vụ đám mây, API của bên thứ ba và các nguồn khác để thống nhất giám sát và bảo vệ hệ thống an toàn.



Khả năng vận hành

Săn tìm mối nguy

Cô động dữ liệu báo cáo giúp nhà quản lý rút ngắn thời gian cho việc phân tích dữ liệu từ xa trên nhiều nền tảng bảo mật khác nhau.

Phân tích hành vi

Phát hiện và ứng phó với các mối đe dọa dựa trên các kiểu hành vi bất thường/nguy hại.

Phản hồi tự động

Tự động phản hồi trước các mối đe dọa giúp giảm thiểu rủi ro an ninh hệ thống thông tin của tổ chức.

Bảo vệ đám mây dịch vụ

Bảo vệ đám mây thuần túy và đám mây kết hợp, bao gồm cơ sở hạ tầng container bằng cách phát hiện và ứng phó với các mối đe dọa mới.

Báo cáo và tuân thủ

Thực hiện các cuộc kiểm tra tuân thủ quy định đối với các quy chuẩn và tiêu chuẩn bảo mật như PCI-DSS, HIPAA, GDPR, v.v.

Chức năng

Cảm biến đa năng bảo vệ thiết bị đầu cuối

Cảm biến chạy trên các hệ điều hành phổ biến nhất để phát hiện mã độc, giám sát tính toàn vẹn của tập tin, đọc dữ liệu thiết bị đầu cuối từ xa, thực hiện đánh giá lỗ hổng, quét cấu hình hệ thống và tự động phản hồi các mối đe dọa tiềm ẩn.

Tích hợp với các giải pháp của bên thứ ba

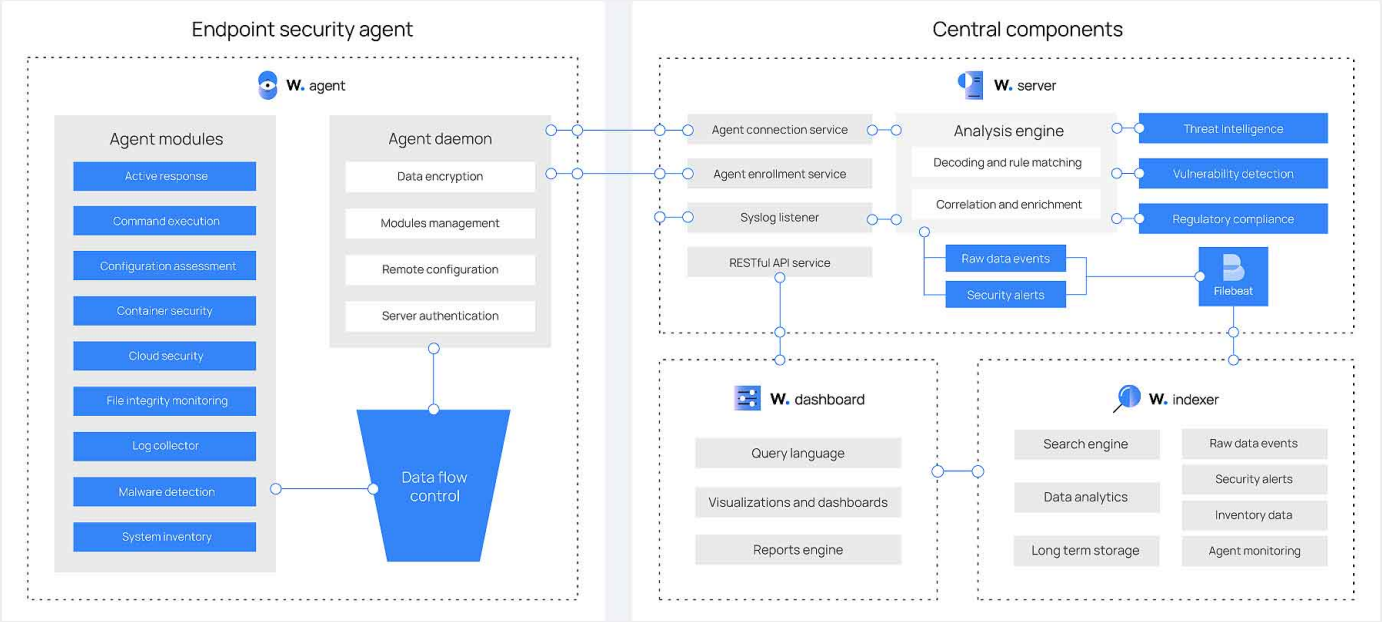
Giải pháp mở rộng khả năng phát hiện mối đe dọa bằng cách tích hợp các giải pháp của bên thứ ba và hợp nhất dữ liệu đo từ xa từ nhiều nguồn khác nhau để hợp nhất dữ liệu nhật ký thời gian thực.

Security Operations Center Platform

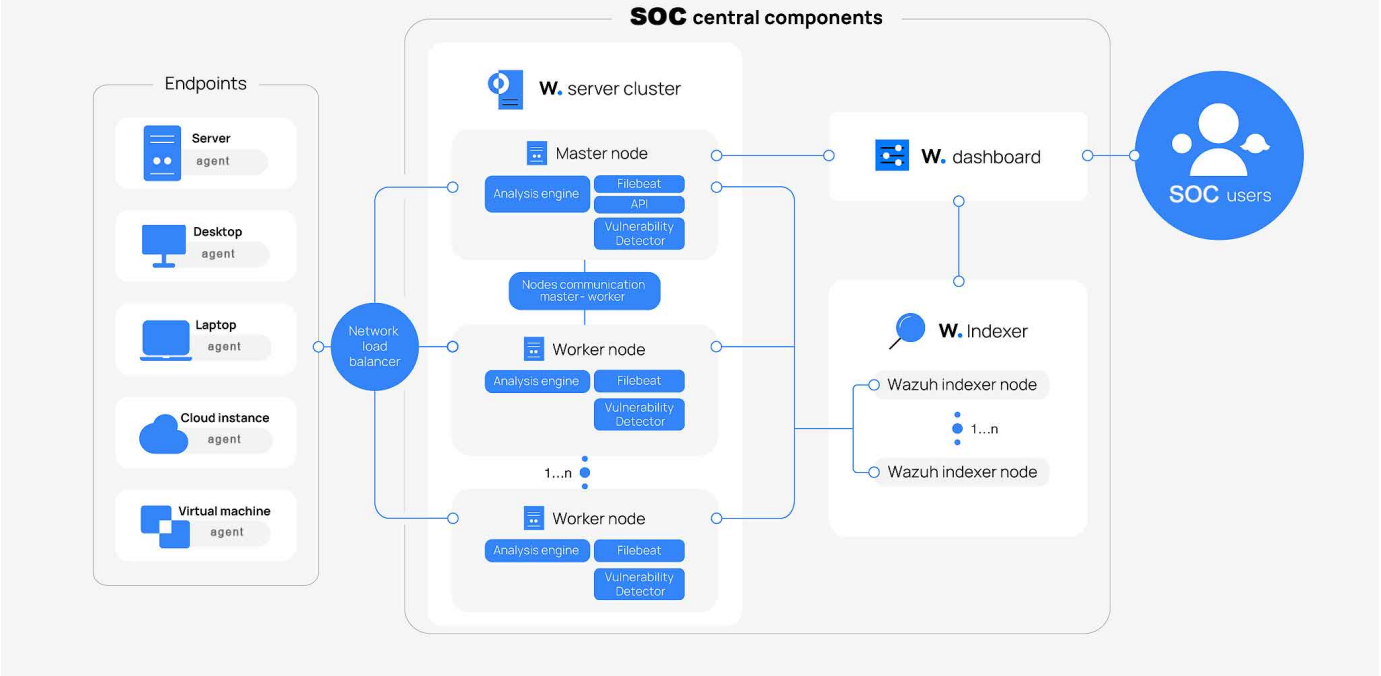
Hợp nhất SIEM và XDR bảo vệ thiết bị đầu cuối và Cloud Workload

Kiến trúc và Phần hợp thành

Nền tảng SOC cung cấp các tính năng XDR và SIEM bảo vệ đám mây dịch vụ, container, máy chủ, máy tính cấu thành hệ thống thông tin doanh nghiệp. Các tính năng này bao gồm phân tích dữ liệu nhật ký, phát hiện xâm nhập, phần mềm độc hại, giám sát tính toàn vẹn tập tin, đánh giá cấu hình, phát hiện lỗ hổng và hỗ trợ tuân thủ quy định theo quy chuẩn an ninh mạng toàn cầu. Giải pháp SOC dựa trên cảm biến được triển khai trên các thiết bị đầu cuối được giám sát dựa trên ba thành phần trung tâm chính: Server, Indexer và Dashboard.



Các cảm biến liên tục gửi các sự kiện đến SOC để phân tích và phát hiện mối đe dọa. Để khởi tạo việc chuyển dữ liệu này, các cảm biến được thiết lập kết nối đến máy chủ dịch vụ theo cổng mạng quy định (có thể cấu hình theo yêu cầu). SOC chịu trách nhiệm giải mã và kiểm tra quy tắc các sự kiện đã nhận bằng công cụ phân tích chuyên dụng. Các sự kiện vi phạm quy tắc sẽ được cảnh báo và liệt kê chi tiết bao gồm: ID và Tên. Các hành vi vi phạm có thể được đưa vào một hoặc cả hai tập tin, tùy thuộc vào hành vi vi phạm có khớp với quy chuẩn an ninh xác định hay không.



Security Operations Center Platform

Hợp nhất SIEM và XDR bảo vệ thiết bị đầu cuối và Cloud Workload

Các tổ chức trên thế giới đã tin dùng SOCP

15+ Million
Protected endpoints

100+ Thousand
Enterprise users

Giải pháp SOC hiện đang bảo vệ các doanh nghiệp có giá trị hàng nghìn tỷ đô la Mỹ và trên hàng triệu thiết bị đầu cuối. Giải pháp này được các công ty lớn thuộc top Fortune 100 và hàng trăm nghìn công ty tin dùng trong việc bảo vệ hệ thống thông tin và hạ tầng công nghệ.

Tại sao khách hàng lại chọn giải pháp SOC này?

Bất cứ nơi đâu và bằng bất cứ cách nào

Cho dù bạn đang tìm kiếm giải pháp tại chỗ, trên đám mây hay kết hợp, giải pháp SOC luôn sẵn sàng vận hành ở bất cứ đâu bạn cần và theo cách bạn muốn, thuận tiện nhất cho bạn.

Khả năng mở rộng dễ dàng

Giải pháp có khả năng linh hoạt, độ mở rộng cao và đơn giản, đồng thời thích ứng với nhu cầu đa dạng của mọi loại hình và quy mô tổ chức.

Hiệu suất nâng cao

Có thể triển khai duy nhất một cảm biến trên máy tính, máy ảo và container. Cảm biến có thể cài đặt trên hầu hết các hệ điều hành phổ biến nhất hiện nay để mang lại hiệu quả vận hành tối đa.

Một nền tảng toàn diện

Giải pháp ứng dụng đa dạng cho nhiều trường hợp sử dụng và dịch vụ giúp doanh nghiệp quản lý bảo mật toàn hệ thống. Chúng tôi cung cấp giải pháp bảo mật 360 độ chỉ với một nền tảng.

Giải pháp và dịch vụ hỗ trợ của chúng tôi

Trung tâm điều hành an ninh (SOC) là một đơn vị quản trị tập trung chuyên nghiệp với mục tiêu chính: cải thiện tình hình an ninh mạng doanh nghiệp bằng hoạt động giám sát, phát hiện, phân tích, cảnh báo sớm và ứng phó kịp thời với các sự cố an toàn an ninh mạng theo thời gian thực. Nhóm quản trị SOC, có thể là nội bộ hoặc bên thứ ba chịu trách nhiệm bảo vệ cơ sở hạ tầng CNTT của tổ chức với vai trò Blue team bao gồm: phòng thủ, giám sát, bảo vệ hệ thống mạng, hệ thống thông tin và ứng dụng tổ chức.

Các chức năng chính của SOC bao gồm:

- **Liên tục giám sát:** Theo dõi toàn bộ môi trường CNTT 24/7 để phát hiện mọi hoạt động đáng ngờ hoặc mối đe dọa tiềm ẩn.
- **Ứng phó sự cố:** Phản ứng nhanh chóng và hạn chế các sự cố an toàn an ninh hệ thống giúp giảm thiểu thiệt hại cho doanh nghiệp.
- **Luôn theo dõi các mối đe dọa:** Sử dụng phân tích dữ liệu và nguồn cấp dữ liệu về mối đe dọa bên ngoài để cập nhật thông tin về các mối đe dọa và lỗ hổng an ninh mạng mới nhất.
- **Quản lý tài sản số:** Duy trì kiểm kê tất cả tài sản CNTT và công cụ bảo mật để đảm bảo bảo vệ toàn diện.

Bằng cách phối hợp các hoạt động này, SOC giúp các tổ chức duy trì khả năng phòng thủ chủ động chống lại các mối nguy hiểm và gia cường thế trận an ninh an toàn mạng lưới thông tin tổ chức.

Nhóm công nghệ ITServing® luôn sẵn sàng hỗ trợ doanh nghiệp bảo vệ hệ thống thông tin và tuân thủ các quy chuẩn an toàn an ninh mạng toàn cầu.

3rd Floor, An Phu Plaza Building, 117-119 Ly Chinh Thang street, Vo Thi Sau Ward, District 3, HCMC

Hotline: 0901333237 - 0901333987 Email: contact@itserving.org / support@itserving.org