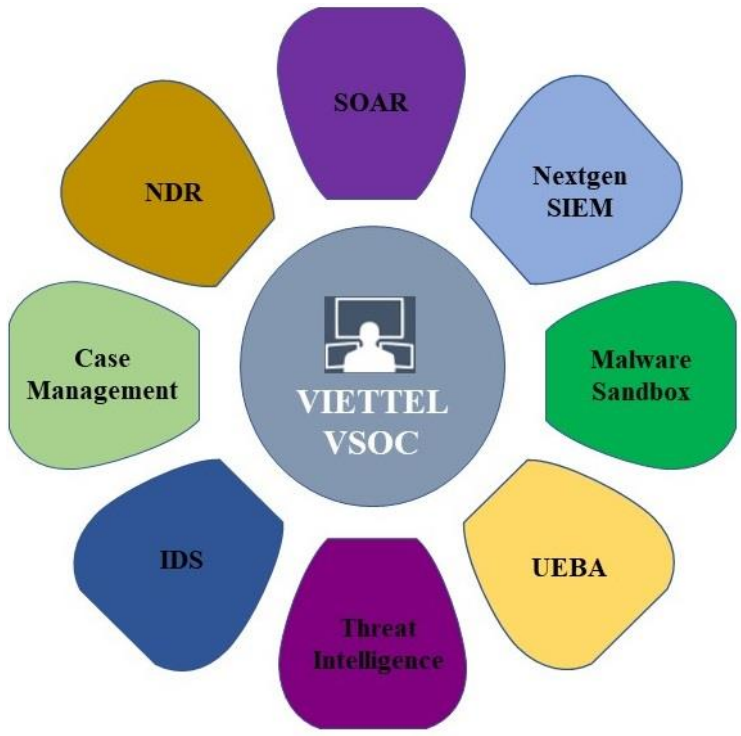
HIGHLIGHTS

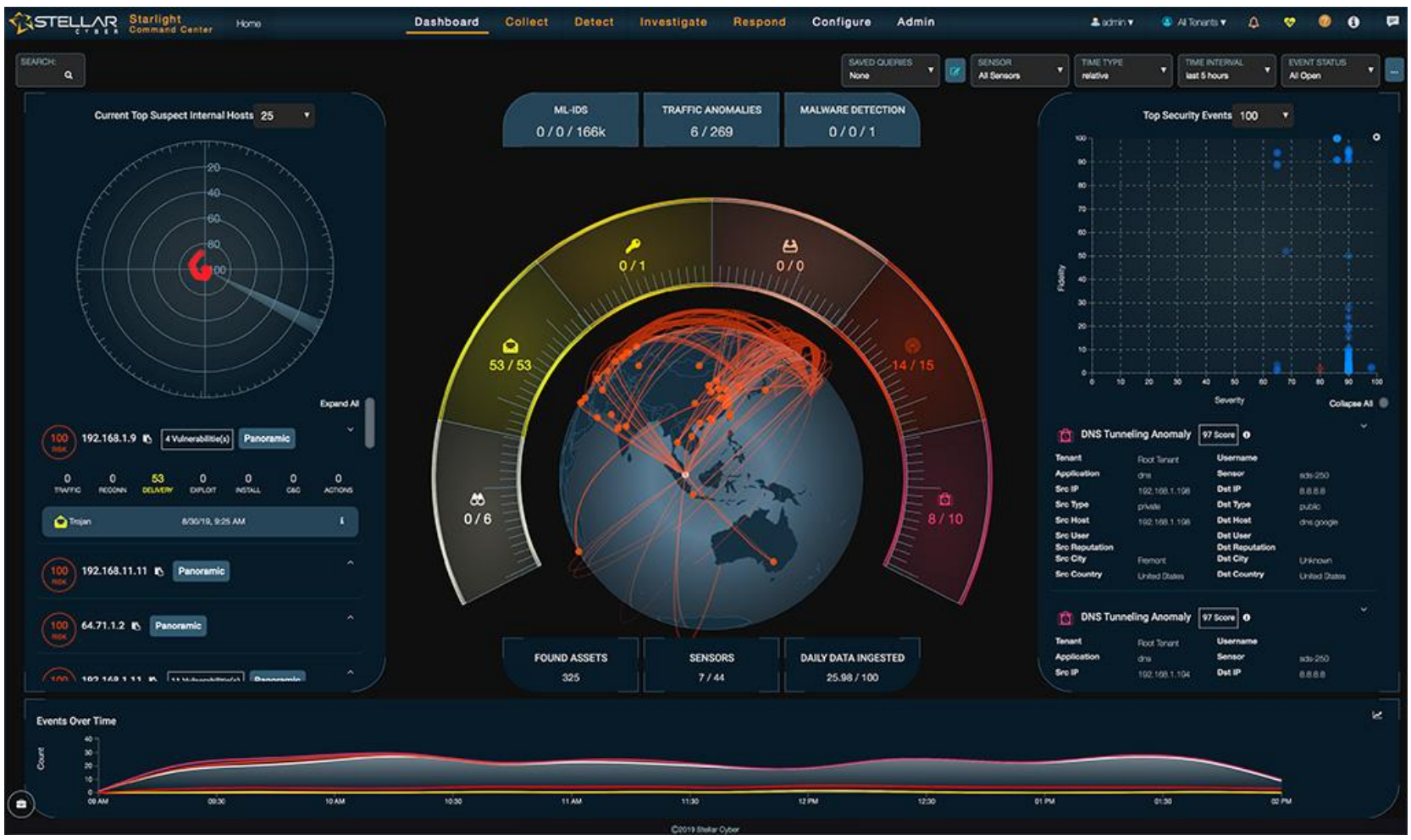
- Giải pháp Security Operation Center (SOC) được xây dựng dựa trên nền tảng Open XDR (Open eXtended Dectection and Response).
- Phát hiện, phân tích, ngăn chặn, phản ứng, điều tra truy vết với các mối đe dọa an ninh thông tin trên một nền tảng duy nhất.
- Hỗ trợ mô hình multi-site, nhiều chi nhánh tại nhiều vị trí địa lý khác nhau
- Hỗ trợ đa dạng các mô hình triển khai: On Premise, Cloud, Hybrid.
- Mô hình Cloud cung cấp tới khách hàng dịch vụ SOC 24/7 tin cậy, chuyên nghiệp.
- Dễ dàng tích hợp với hạ tầng mạng hiện tại của khách hàng và các giải pháp của các bên thứ 3
- Linh hoạt trong điều chỉnh, mở rộng quy mô triển khai
- Giải pháp bảo mật toàn diện với chi phí tối ưu, phù hợp với khả năng và nhu cầu của nhiều khách hàng.
- Dịch vụ giám sát và phản ứng sự cố an ninh thông tin với đội ngũ chuyên gia bảo mật hàng đầu của Viettel

TỔNG QUAN

Viettel vSOC cung cấp giải pháp giám sát và xử lý các mối đe dọa về an ninh thông tin tập trung. Giải pháp giúp các tổ chức có thể nhanh chóng phát hiện và phản ứng với các mối đe dọa bảo mật, giảm thiểu rủi ro, nguy cơ trước và sau các cuộc tấn công mạng.



Viettel IDC cung cấp tới khách hàng dịch vụ giám sát Viettel VSOC 24/7 trên nền tảng Cloud. Đội ngũ chuyên gia của Viettel sẽ hỗ trợ đảm bảo an ninh thông tin toàn diện để khách hàng có thể tập trung vào các nghiệp vụ sản xuất, kinh doanh.



TÍNH NĂNG

Giải pháp SOC giám sát toàn diện

- Cung cấp đầy đủ thành phần, chức năng của Trung tâm Điều hành An ninh mạng – SOC bao gồm: Con người, Quy trình và Công nghệ.
- Hỗ trợ thu thập, giám sát và phân tích dữ liệu từ nhiều môi trường và nền tảng khác nhau: Application, Endpoint, Network, Multi-Cloud.
- Hỗ trợ mô hình multi-site, cho phép triển khai với các khách hàng có nhiều văn phòng, chi nhánh tại nhiều địa điểm địa lý khác nhau

Sử dụng nền tảng Open XDR hiện đại

- Cung cấp đầy đủ, đa dạng các công cụ phân tích an ninh bảo mật trên một nền tảng Open XDR duy nhất: NG SIEM, NDR, ML-IDS, APT SANDBOX, NTA, UEBA, SOAR, SIEM, CASE MANAGEMENT, MULTI TENANCY, THREAT INTELLIGENCE
- Hợp nhất các bước thu thập, phát hiện, phân tích, phản ứng, ngăn chặn, điều tra truy vết trên một giao diện tập trung duy nhất:
  - Thu thập và xử lý thông tin: thu thập thông tin từ nhiều nguồn khác nhau (Network traffic, log server, log từ thiết bị mạng, môi trường ảo hóa public/private cloud, container), chuyển đổi dữ liệu thành metadata, kiến trúc hóa lại dưới dạng Interflow, làm sạch, làm giàu dữ liệu bằng threat Intelligence, geo location, tương quan dữ liệu…
  - Phân tích, phát hiện: sử dụng AI, Threat Intelligence, IDS, SANDBOX, UEBA, anti-Phishing, Deception, NTA…
  - Điều tra: Bằng Threat hunting (manually hoặc tự động), tạo ra các query với nhiều điều kiện lọc khác nhau…
  - Phản ứng, ngăn chặn: Dùng module SOAR để phản ứng lại mối đe dọa một cách tự động (gửi thông tin đến firewall, Endpoint để block cuộc tấn công, gửi email, tạo ticket…).

Nâng cao khả năng bảo mật của hệ thống

- Cung cấp, bổ xung đầy đủ các công cụ bảo mật mà một hệ thống bảo mật mạng cần có.
- Giảm thời gian phát hiện trung bình (MTTD) và thời gian phản ứng trung bình (MTTR) đối với các mối đe dọa
- Có khả năng phát hiện và phản ứng với các cuộc tấn công có chủ đích APT
- Thu thập, tích hợp dữ liệu liên quan để nhanh hơn phân tích sự cố chính xác hơn
- Áp dụng Big Data và Machine Learning phát hiện các nguy cơ phức tạp từ sớm và nâng cao khả năng hệ thống theo thời gian

Đơn giản hóa thao tác vận hành và khai thác hệ thống

- Giải pháp cung cấp giao diện web thân thiện, dễ sử dụng, có khả năng tùy chỉnh bằng Tiếng Việt
- Cung cấp khả năng tự động hóa cho các tác vụ lặp đi lặp lại, tự động cảnh báo, tự động báo cáo
- Hỗ trợ nhiều loại biểu đồ, hình ảnh đồ họa trực quan
- Đơn giản hóa quá trình giám sát, phân tích: hỗ trợ tự động xử lý dựa trên nền tảng hợp nhất, giảm số lượng log và cảnh báo, đưa ra hướng dẫn và tham chiếu cho các trường hợp xử lý cụ thể

Dễ dàng triển khai, tích hợp, thử nghiệm

- Hỗ trợ, tương thích nhiều mô hình triển khai khác nhau: On-Premise, Cloud, Hybrid
- Dễ dàng tích hợp với hạ tầng hiện tại của khách hàng
- Hỗ trợ tích hợp giải pháp của các hãng thứ 3 thông qua API mở.
- Tích hợp 2 chiều với 100% các hãng firewall, gửi phản ứng tự động xuống firewall để ngay lập tức ngăn chặn
- Linh hoạt trong việc điều chỉnh, mở rộng quy mô sử dụng

Dịch vụ giám sát và xử lý sự cố an ninh thông tin chuyên nghiệp

- Hệ thống lõi được đặt trên hệ thống cloud của Viettel IDC, đảm bảo các yếu tố về tính sẵn sàng, hiệu năng, tốc độ truy cập, bảo mật thông tin
- Giám sát, phản hồi và ứng cứu sự cố 24/7
- Cung cấp dịch vụ điều tra, truy vết sự cố an toàn thông tin.
- Tư vấn, đưa ra các khuyến nghị để nâng cao khả năng bảo mật hệ thống khách hàng
- Hỗ trợ đầy đủ nhân sự, chuyên gia ở từng SOC tier với nhiều năm kinh nghiệm và có chứng chỉ uy tín.
- Báo cáo về các nguy cơ Threat Intelligence và An toàn thông tin

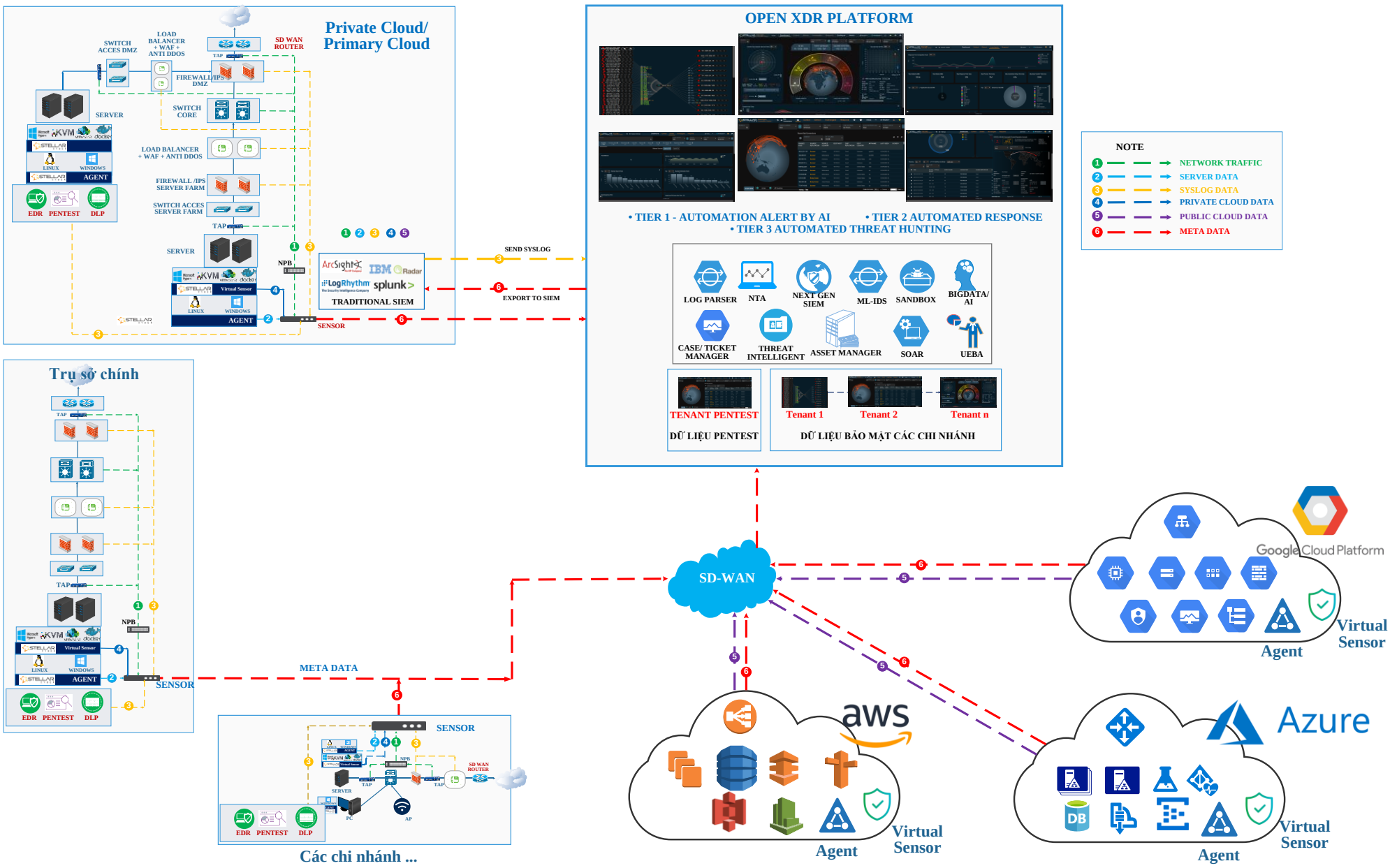
MÔ HÌNH TRIỂN KHAI

Thành phần trong hệ thống

- Hệ thống phân tích và phản ứng ATTT - Open XDR tập trung được đặt tại Cloud của Viettel có nhiệm vụ phân tích thông tin tập trung, cấu hình quản trị hệ thống và cập nhật các thông tin tình báo mối đe dọa mới nhất.
- Khách hàng sẽ được cung cấp account để login vào giao diện quản trị và xem được toàn bộ các cảnh báo xảy ra trên hệ thống của mình
- Hệ thống các sensor tại site khách hàng: Có nhiệm vụ thu thập, phân tích, tương quan các nguồn dữ liệu, kiến trúc hóa về dạng metadata JSON để đẩy về trung tâm qua đường mã hóa HTTPS
- Phần mềm Sensor Agent cài đặt tại các Server Windows /Linux của khách hàng: Cung cấp khả năng giám sát các tiến trình, tính toàn vẹn của file cũng như phát hiện các hoạt động bất thường trên server
- Cung cấp API tích hợp với các ứng dụng và giải pháp khác.

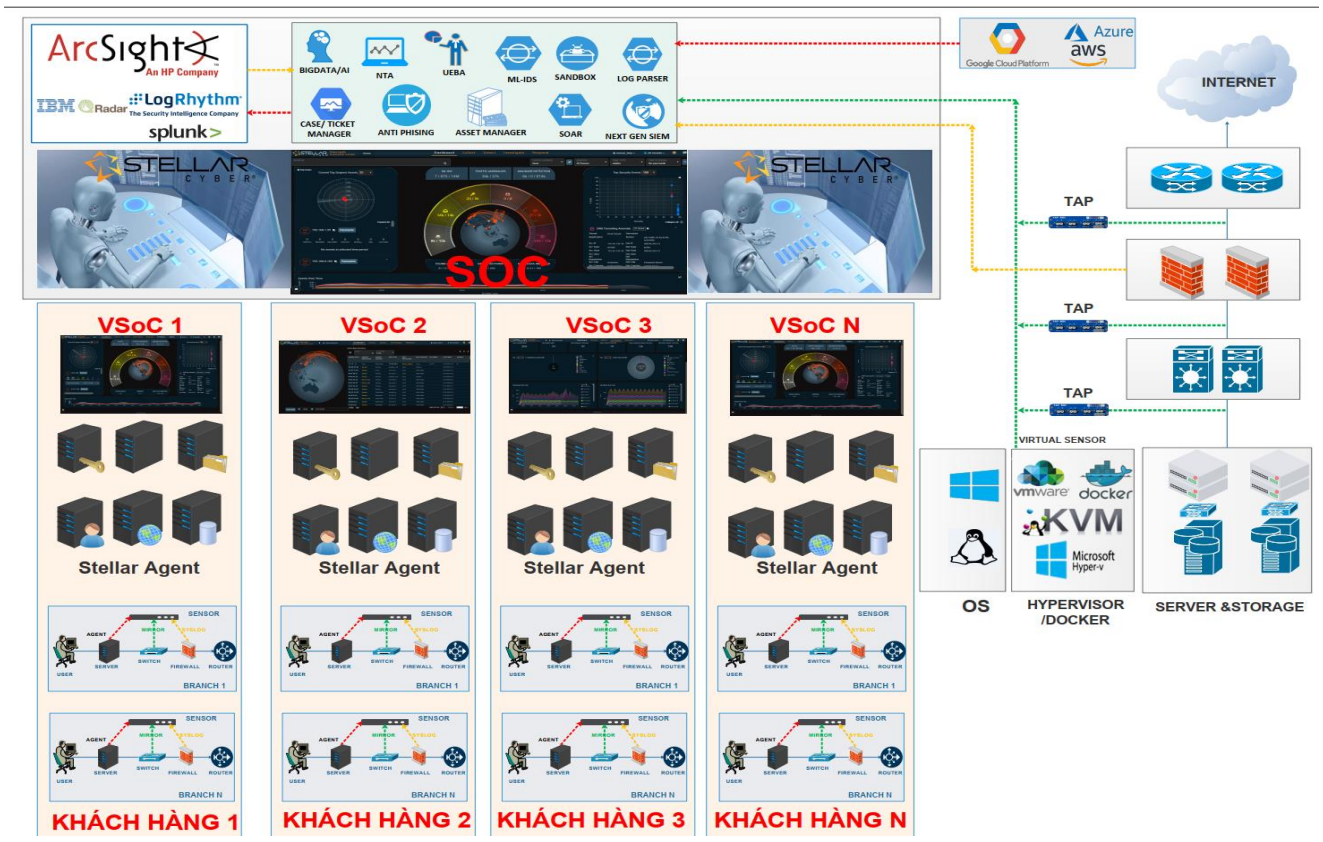
Cách thức hoạt động giao tiếp giữa Sensor và bộ xử lý tập trung

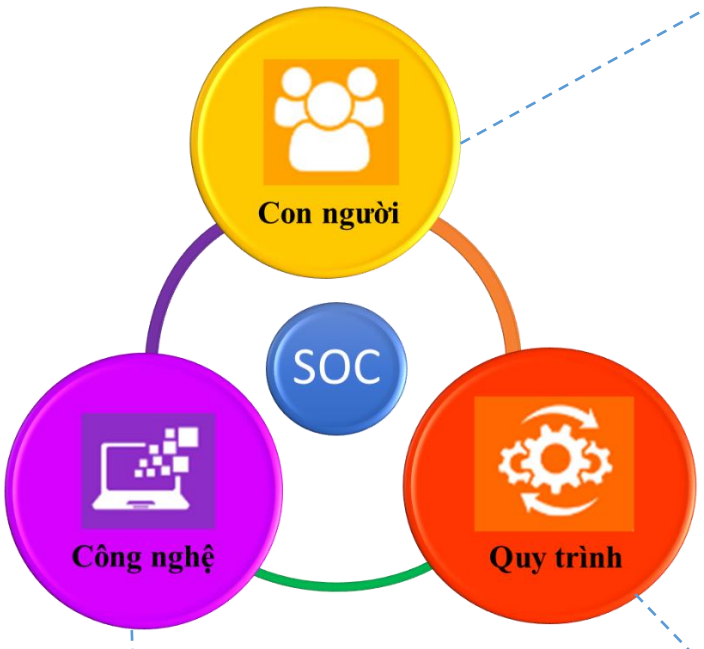
- Người quản trị truy cập giao diện quản trị tập trung để giám sát trực tiếp các cảnh báo trên hệ thống của mình qua kết nối Internet sử dụng SSL/TLS.
- Agent sensor được cài trên các Server Windows/Linux của khách hàng. Sau khi cài Agent, server sẽ đẩy dữ liệu về hệ thống phân tích và phản ứng ATTT – Open XDR tập trung
- Thiết bị Sensor sẽ thu thập các dữ liệu sau:
  - Dữ liệu Network traffic tại tất cả các phân đoạn mạng bằng cách SPAN/mirror port từ Switch
  - Dữ liệu syslog từ các hệ thống bảo mật của khách hàng như Firewall, IPS, WAF, DDOS, Endpoint Security…vv
  - Đẩy các tín hiệu xuống các hệ thống bảo mật hiện có của khách hàng như firewall, AD, switch để ngăn chặn kịp thời các cuộc tấn công.
- Hệ thống phân tích và phản ứng ATTT - Open XDR tập trung sẽ quản lý toàn bộ các agent và sensor. Có thể cấu hình, cập nhật OS hoặc reboot từ xa đến sensor



DỊCH VỤ VSOC QUA HẠ TẦNG CLOUD CỦA VIETTEL IDC

SOC - Security Operration Center: Trung tâm Điều hành an ninh mạng là một đơn vị gồm các chuyên gia bảo mật giàu kinh nghiệm, chịu trách nhiệm theo dõi, phân tích, ứng phó sự cố an ninh mạng bằng cách kết hợp các giải pháp công nghệ và quy trình đánh giá nhằm đảm bảm an toàn cho tổ chức.





CON NGƯỜI

- Giám sát liên tục 24/07/365
- Bảo trì, phòng ngừa, và triển khai hệ thống
- Có 3 Tier SOC Team
  - Tier 1:
    - Giám sát, phân tích, phân loại sự cố,xử lý, ngăn chặn, loại bỏ các mối đe doại, gửi cảnh báo cho khách hàng
    - Gửi báo cáo tổng hợp tuần/tháng/quý
  - Tier 2
    - Khách hàng: thực hiện kiểm tra, xử lý thông tin cảnh báo từ IDC.
    - IDC: Phân tích, xử lý các sự cố Tier 1 không xử lý được, tạo Rule theo yêu cầu của KH
  - Tier 3: Phân tích chuyên sâu sự cố ATTT, đưa ra báo cáo.
- Điều tra nâng cao

Quy trình:

- Quy trình giám sát, quản lý sự cố
- Quy trình cải tiến liên tục
- Chính sách đo lường hiệu suất, chất lượng (SLA)
- Threat Analiysis
- Vulnerrability Management

Công nghệ:

- Cung cấp giải pháp SOC trên nền tảng Open XDR
- Hệ thống lõi được cài đặt trên hạ tầng Cloud của Viettel IDC
- Khách hàng được cung cấp giao diện vSOC để khai thác và vận hành với đầy đủ các chức năng

TẠI SAO CHỌN VIETTEL IDC?

Hạ tầng chuẩn Quốc tế

Hạ tầng được đặt tại các Trung tâm dữ liệu của Viettel IDC đạt chuẩn TIA-942 Rated 3 Constructed Level, các chứng chỉ quốc tế ISO 9001: 2015, 50001: 2018, các chứng chỉ về bảo mật, an toàn thông tin: ISO 27001: 2013, 27017:2015 (chuyên cho các dịch vụ Cloud) và PCI DSS đảm bảo đáp ứng các tiêu chí khắt khe nhất về hạ tầng, chất lượng dịch vụ và an toàn, bảo mật thông tin.

Công nghệ hiện đại, phù hợp xu thế

Viettel IDC cam kết áp dụng những công nghệ hiện đại, tốt nhất cho Khách hàng. Với Viettel VSOC chúng tôi triển khai các công nghệ mới trong lĩnh vực giám sát, phát hiện, cảnh báo sớm sự cố an toàn thông tin.

Triển khai nhanh chóng

Được thiết kế với hạ tầng sẵn sàng khả năng cung cấp tài nguyên phục vụ khách hàng nên việc triển khai được thực hiện nhanh chóng. Kết hợp với đội ngũ chuyên gia nhiều năm kinh nghiệm đã triển khai cho nhiều khách hàng nên thời gian triển khai được rút ngắn, tối ưu.

Quản trị đơn giản

Giao diện quản trị trực quan, đơn giản nhưng hiệu quả trong việc khai thác và sử dụng Viettel VSOC. Điều này giúp khách hàng tối ưu hoá các công cụ quản lý, giúp việc quản trị trở nên dễ dàng.

Chi phí hợp lý

Sử dụng Viettel VSOC giúp giảm thiểu ngân sách đầu tư bằng việc thuê hạ tầng, nhân sự hỗ trợ vận hành và khai thác hệ thống.

Đội ngũ chuyên gia và kỹ sư giàu kinh nghiệm

Đội ngũ hỗ trợ kỹ thuật 24/7 cùng lớp kỹ sư, chuyên gia giàu kinh nghiệm giúp giải quyết các giám sát và xử lý các sự cố an ninh thông tin của Khách hàng một cách toàn diện.