viettel
IDC

Datasheet

VIETTEL VIRTUAL SOC

Nhà cung cấp hàng đầu Việt Nam về Dịch vụ Trung tâm Dữ liệu và Điện toán Đám mây
Website: https://viettelidc.com.vn/
Hotline: 1800 8088

Datasheet
VIETTEL VIRTUAL SOC

SOC Platform

Security Operation Center

Security Operation Center (S.O.C) là hệ thống có chức năng giám sát, xử lý các vấn đề về an toàn thông tin để phát hiện, phân tích, phản ứng, ngăn chặn và điều tra truy vết với các sự cố về an toàn thông tin, đảm bảo an toàn, an toàn thông tin cho một tổ chức.

S.O.C bao gồm 3 yếu tố: **Quy trình**, **Con người** và **Công nghệ**.

Dịch vụ S.O.C của Viettel

Dịch vụ Giám sát và Phản ứng sự cố An toàn thông tin mạng của Viettel hỗ trợ khách hàng giám sát toàn diện 24/7/365 trên các lớp, giúp phát hiện sớm và phản ứng lại các sự cố mất ATTT. Dịch vụ được cung cấp bởi đội ngũ chuyên gia an toàn, an ninh mạng hàng đầu của Công ty An ninh mạng Viettel, được công nhận trên toàn thế giới, đảm bảo khách hàng được trải nghiệm toàn bộ những tính năng ưu việt của dịch vụ với chi phí hợp lý, cạnh tranh, các mức cam kết chất lượng dịch vụ (SLA) rõ ràng.

Sự cần thiết của S.O.C

Trong bối cảnh toàn cầu đang hướng đến một kỷ nguyên quốc gia thông minh, cuộc cách mạng công nghiệp 4.0 đang được đẩy mạnh trên khắp mọi nơi trên thế giới. Như một điều tất yếu, các tương tác trên mạng Internet đang ngày càng phát triển dẫn đến nguy cơ xảy ra mất an toàn thông tin càng lớn bởi những nguyên nhân như:

- CNTT phát triển tạo môi trường lý tưởng để hacker tấn công với những phương thức tinh vi hơn, khó lường hơn, quy mô lớn hơn.
- Nhận thức về ATTT của người dùng còn hạn chế.
- Sự đầu tư không bài bản, chắp vá của các tổ chức trong lĩnh vực ATTT.
- Khó khăn trong việc tuân thủ các chính sách ATTT.

Dịch vụ cung cấp bao gồm

Giám sát Hệ thống máy chủ, máy trạm (Endpoint)

Hệ thống máy chủ, máy tính sẽ được thực hiện giám sát 24/7/365.

Phạm vi giám sát bao gồm:

- Giám sát và phát hiện các dấu hiệu tấn công mạng như dấu hiệu kết nối đến máy chủ điều khiển mã độc (C&C), dấu hiệu lây lan mã độc diện rộng trong hệ thống.
- Giám sát và phát hiện các dấu hiệu bất thường trên lớp Endpoint (máy trạm/máy chủ) trong hệ thống của khách hàng.
- Phát hiện các dấu hiệu xâm nhập trên lớp Endpoint.

Giám sát, phát hiện tấn công lớp mạng

Lưu lượng mạng và các gói tin sẽ được các cảm biến thu thập, bóc tách, kết hợp với công nghệ phân tích mã độc tự động (Sandboxing) để phân tích tự động và phát hiện các dấu hiệu bất thường, các nguy cơ bị tấn công tiềm ẩn trên lớp mạng. Module giám sát mạng còn cung cấp các công cụ hỗ trợ đội ngũ quản trị trong quá trình điều tra, truy vết và phân tích chuyên sâu các dấu hiệu tấn công mạng.

Quản lý, phân tích log tập trung

Hệ thống giám sát, thu thập và phân tích log tập trung là nền tảng giám sát tổng thể, đóng vai trò cốt lõi trong hệ thống S.O.C. Hệ thống này cho phép thu thập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ log, các sự kiện ATTT mạng được sinh ra trong hệ thống CNTT của tổ chức và cung cấp khả năng giám sát và phân tích dữ liệu vận hành theo thời gian thực. Có thể sử dụng giải pháp để tìm kiếm, giám sát, phân tích và xem xét trực quan các nguồn dữ liệu do tất cả các thiết bị khác nhau tạo ra giúp hỗ trợ tối đa các tổ chức, đơn vị trong việc nhanh chóng phát hiện và xử lý những sự cố, nguy cơ về ATTT trong hệ thống.

Nền tảng điều phối an ninh và phản ứng tự động

Hệ thống S.O.C của Viettel được vận hành trên nền tảng điều phối thông minh, tự động hóa phản ứng. Nền tảng này giúp tích hợp các công nghệ và các bộ quy trình bảo mật vào quá trình vận hành hệ thống một cách tự động để tạo nên một hệ sinh thái sản phẩm ATTT gắn kết hơn, tối ưu hiệu quả của quá trình giám sát, phân tích và xử lý sự cố.

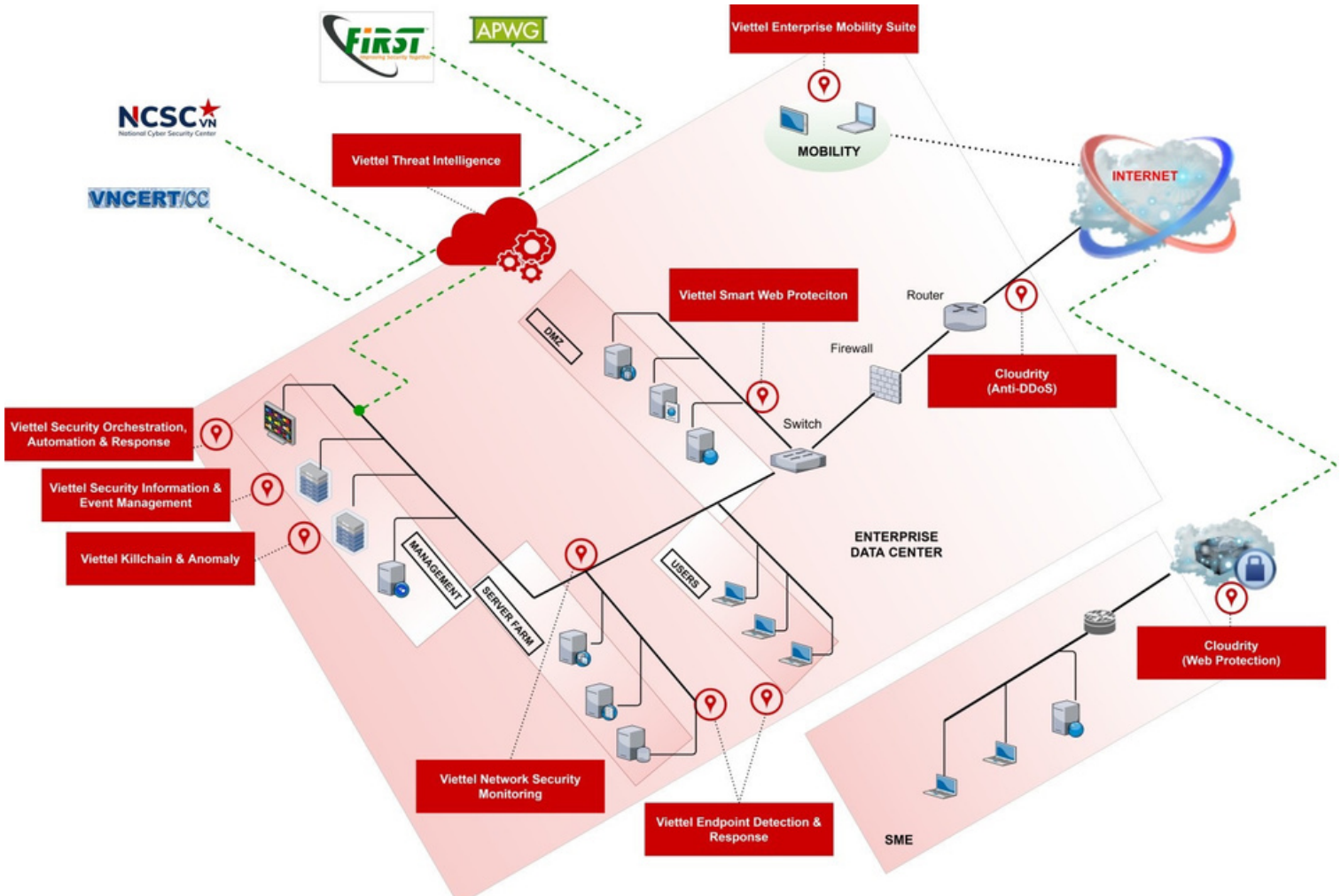
Phản hồi và ứng cứu sự cố 24/7

Hệ thống của khách hàng sẽ được giám sát 24/7 bởi đội ngũ chuyên gia của Viettel Cyber Security. Ngay khi phát hiện tấn công xâm nhập, các chuyên gia an ninh mạng sẽ tiến hành điều tra, khoanh vùng và cô lập phạm vi bị tấn công khỏi hệ thống mạng của khách hàng, sau đó thực hiện các biện pháp nghiệp vụ, rà soát, phản ứng trên toàn mạng để ứng cứu, xử lý và ngăn chặn việc leo thang, mở rộng phạm vi lây nhiễm. Sau khi hoàn thành ứng cứu sự cố, khách hàng sẽ nhận được báo cáo bao gồm cách thức xâm nhập, thời gian lây nhiễm và khuyến nghị cách thức khắc phục các lỗ hổng đã bị lợi dụng trong quá trình bị tấn công.

Cung cấp tri thức & Báo cáo ATTT

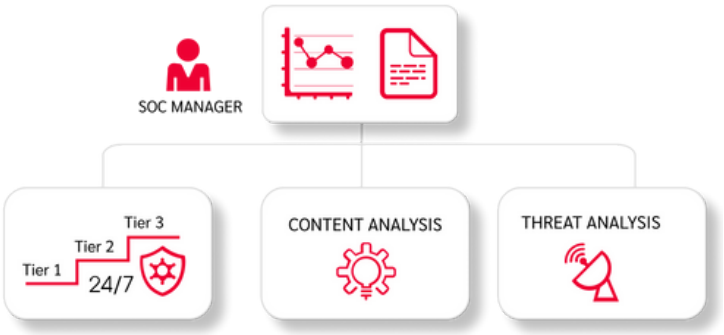
Để đảm bảo khách hàng luôn được cập nhật và nắm bắt thông tin về tình trạng ATTT trong hệ thống cũng như các xu hướng tấn công trên thế giới, các báo cáo định kỳ về tình hình sẽ được cung cấp trong suốt quá trình sử dụng dịch vụ.

Mô hình triển khai & tương tác giữa các thành phần trong hệ thống S.O.C



Tổ chức vận hành hệ thống

Viettel xây dựng cho khách hàng mô hình về các thành phần nhân sự vận hành hệ thống S.O.C đạt chuẩn quốc tế, được chia thành 6 nhóm:



- **Tier 1 (Viettel)**: Thực hiện giám sát 24/7 và chịu trách nhiệm xử lý các cảnh báo theo hướng dẫn.
- **Tier 2 (Khách hàng)**: Tiếp nhận các sự cố từ Tier 1 và xử lý các sự cố thông thường và leo thang sự cố đến Tier 3 với những sự cố không xử lý thành công.
- **Tier 3 (Viettel)**: Tiếp nhận các sự cố leo thang từ Tier 2 để xử lý chuyên sâu hơn, đồng thời viết lại hướng dẫn xử lý đối với các sự cố tương tự để hướng dẫn, đào tạo cho Tier 2.
- **Content Analysis (Viettel)**: Cải thiện, nâng cao, tối ưu hóa khả năng xử lý của hệ thống.
- **Threat Analysis (Viettel)**: Rà soát, phân tích, cập nhật các tri thức về các nguy cơ mới vào hệ thống.
- **SOC Manager (Viettel)**: Quản lý điều hành hệ thống và kiểm tra, đánh giá hiệu suất làm việc của hệ thống.

Cam kết chất lượng

Với thế mạnh là một nhà cung cấp dịch vụ viễn thông và Internet hàng đầu trong nước và các nước lân cận, Viettel có khả năng nhận biết sớm được các bất thường, các nguy cơ mất an toàn thông tin trên toàn bộ mạng lưới.
Viettel cung cấp hệ thống SOC đi kèm với hệ sinh thái giải pháp ATTT tiên tiến nhất, hoàn toàn làm chủ công nghệ cùng khả năng đảm bảo ATTT trên tất cả các lớp:

- Gateway (Cổng kết nối): VCS-WSG, VCS-ESG
- Network (Kết nối mạng): VCS-NSM, VCS-NAC, VCS-Anti DDoS
- Endpoint (Thiết bị đầu cuối): VCS-aJiant, VCS M-Suite
- Application (Ứng dụng): VCS-SWP, Cloudrity
- Management (Quản lý): VCS-CyM, VCS-CyCir, VCS-KIAN, VCS-Threat Intelligence

Bên cạnh đó, với đội ngũ chuyên gia hàng đầu, được công nhận trên toàn thế giới, Viettel cam kết cung cấp cho khách hàng những dịch vụ về SOC uy tín, đáng tin cậy nhất và đạt hiệu quả cao nhất.
Cam kết chất lượng dịch vụ (SLA) về dịch vụ SOC do Viettel cung cấp bao gồm:

- SLA về quản lý các sự kiện ATTT
- SLA về xử lý sự cố ATTT
- SLA về xử lý các lỗ hổng, vi phạm ATTT
- SLA về tối ưu cảnh báo
- SLA về quản lý các nguy cơ ATTT

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.