VIETNAM CYBERSPACE SECURITY TECHNOLOGY JSC

VNCS Global Services

Distribution | **Service** | **Development**

CHUYỂN ĐỔI SỐ

Ngành Y tế. Bảo mật ?

Bệnh viện thông minh

Thanh toán viện phí

Quản trị thông minh

Hồ sơ bệnh án điện tử

Phòng bệnh thông minh

Y tế từ xa

Yêu cầu đảm bảo ATTTT

Các văn bản yêu cầu Cơ quan nhà nước thực hiện đảm bảo ATTT :

- Quyết định số 749/QĐ-TTg ngày 03/6/2020, chuyển đổi số trong lĩnh vực y tế nằm trong một số lĩnh vực ưu tiên chuyển đổi số.
- Nghị định số 85/2016/NĐ-CP về đảm bảo an toàn hệ thống thông tin theo cấp độ.
- Quyết định 1017/QĐ-TTg ngày 14/8/2018 Phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến 2025.
- Công văn số 2973/BTTTT-CATTT ngày 04/9/2019 về việc triển khai hoạt động **giám sát an toàn thông tin** trong cơ quan, tổ chức nhà nước
- Theo Nghị đinh 85/2016/NĐ-CP và Thông tư 03/2017/TTT-BTTT, các đơn vị nhà nước cần thực hiện **đánh giá tình trạng bảo mật định kỳ** và đưa ra các biện pháp đảm bảo an toàn thông tin.
- Theo Chỉ thị số 14/CT-TTg ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng mỗi đơn cũng cần danh ra **10% chi phí đầu tư CNTT** để đảm bảo an toàn thông tin.

Thực tế

Thiếu, kiêm nhiệm

24/7

Phản ứng thụ động
Thiếu khả năng phân tích, điều tra

Trung tâm điều hành an ninh mạng (VNCS SOC)

VNCS GLOBAL

Standard,
Knowleged

TRILOGY

Security Services

Công văn 1552/BTTTT – 28/4/2020

Bộ Thông tin và Truyền thông đề nghị các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; các Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương tổ chức triển khai bảo đảm an toàn thông tin (ATTT) cho hệ thống thông tin thuộc phạm vi quản lý theo mô hình "4 lớp": (1) Lực lượng tại chỗ, (2) Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp, (3) Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ, (4) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia, cụ thể như sau:

1. "Lớp 1" Lực lượng tại chỗ

Chỉ định, kiện toàn đầu mối đơn vị chuyên trách về ATTT mạng để làm tốt công tác tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, an ninh mạng.

2. "Lớp 2" Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp

Tự thực hiện giám sát, ứng cứu sự cố ATTT mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý hoặc lựa chọn/thuê tổ chức, doanh nghiệp có đủ năng lực để thực hiện cung cấp dịch vụ giám sát, ứng cứu sự cố, bảo vệ ATTT mạng.

3. "Lớp 3" Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ

Lựa chọn/thuê tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá ATTT mạng đối với hệ thống thông tin cấp độ 3 trở lên thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật;

Đối với các hệ thống thông tin cấp độ 3 và cấp độ 4, định kỳ hàng năm thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền thông trước ngày 14 tháng 12 để tổng hợp, báo cáo Thủ tướng Chính phủ;

Đối với hệ thống thông tin quan trọng quốc gia (cấp độ 5), định kỳ 06 tháng một lần thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền thông trước ngày 14 tháng 6 và ngày 14 tháng 12 hàng năm để tổng hợp, báo cáo Thủ tướng Chính phủ.

4."Lớp 4" Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia

Kết nối, chia sẻ thông tin giám sát an toàn thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông; và cung cấp các dải địa chỉ IP Public của các hệ thống thông tin trong cơ quan, tổ chức nhà nước thuộc phạm vi quản lý.

Đề nghị các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; các Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương:

- Hoàn thành việc triển khai bảo đảm ATTT cho hệ thống thông tin theo mô hình "4 lớp" trước ngày 30/9/2020;

- Định kỳ báo cáo trước ngày 25 hàng tháng về tình hình triển khai (gửi về hộp thư điện tử: athttt@mic.gov.vn);

VIETNAM CYBERSPACE SECURITY TECHNOLOGY JSC

1. Dịch vụ giám sát an ninh mạng (SOC)

Distribution | Service | Development

SOC ?

Là nơi tập trung **giám sát** phát hiện, **phân tích**, **cảnh bảo** và **phản ứng** ngăn chặn các sự cố an ninh mạng

SOC ?

Công cụ giám sát

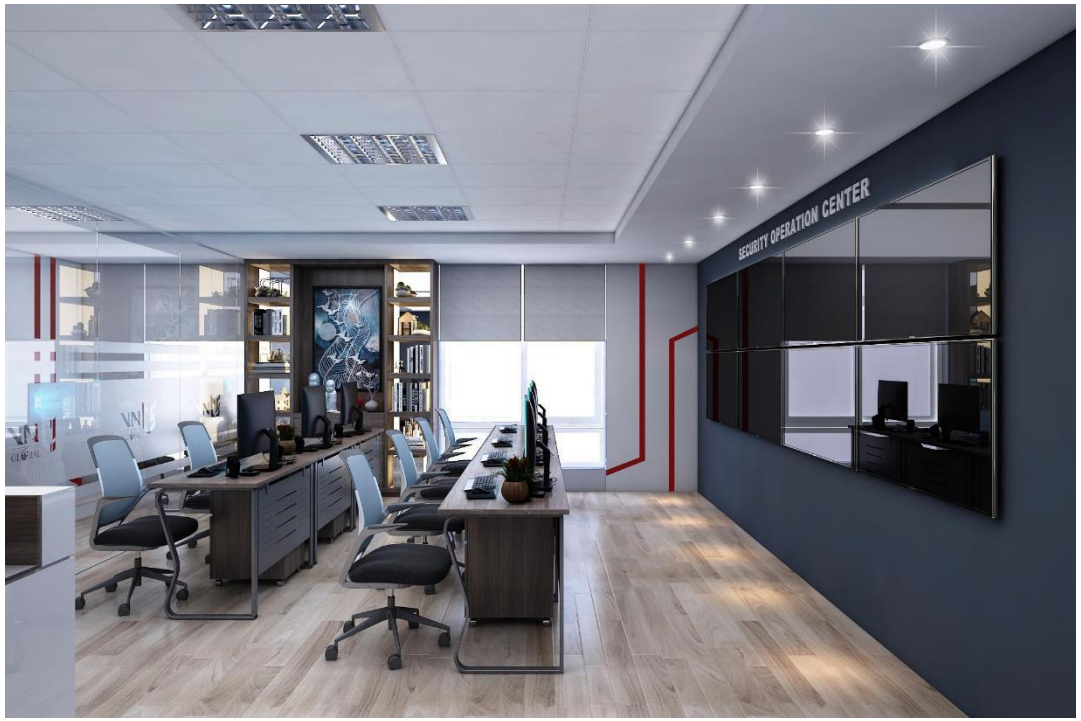
Team giám sát

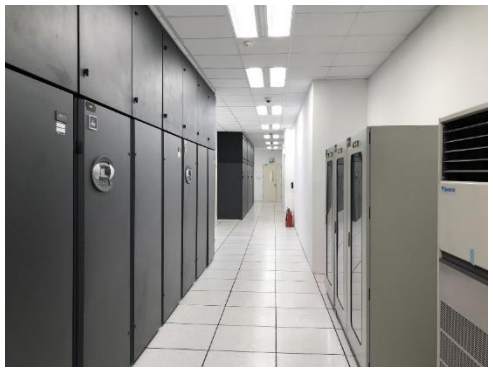
Team xử lý sự cố

Trung tâm điều hành an ninh mạng

VNCS SOC

Cung cấp dịch vụ giám sát liên tục, bảo vệ và phản ứng lại sự cố 24/7

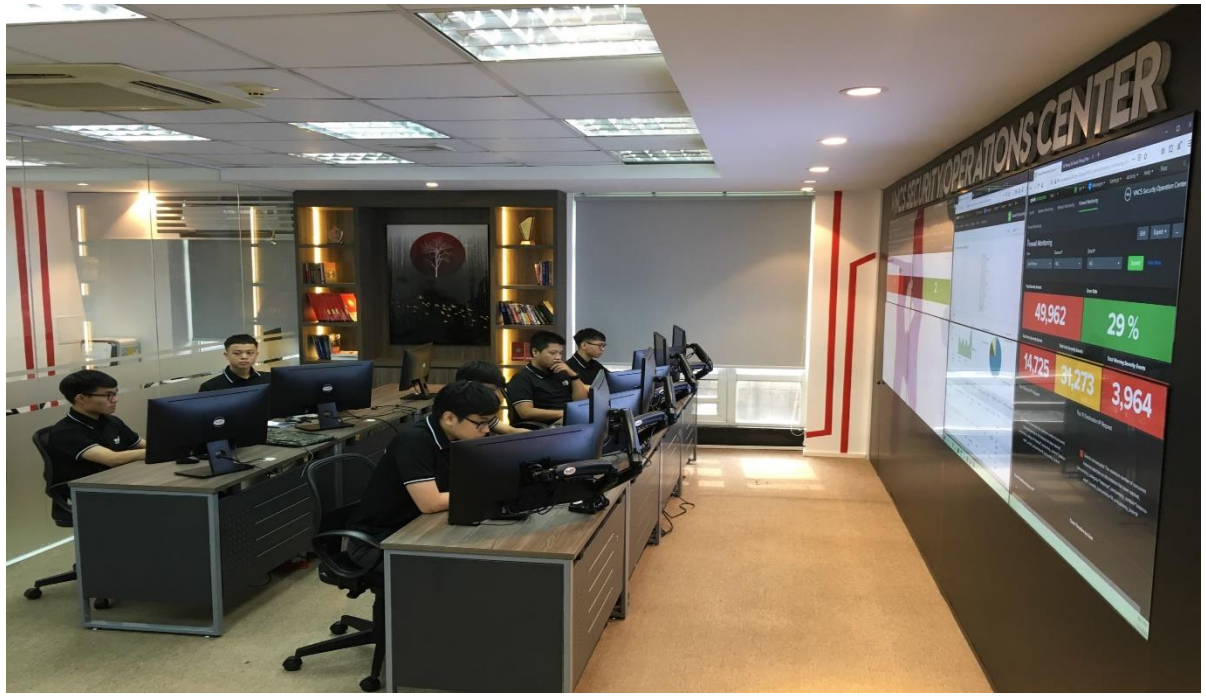




Trung tâm điều hành an ninh mạng

VNCS SOC

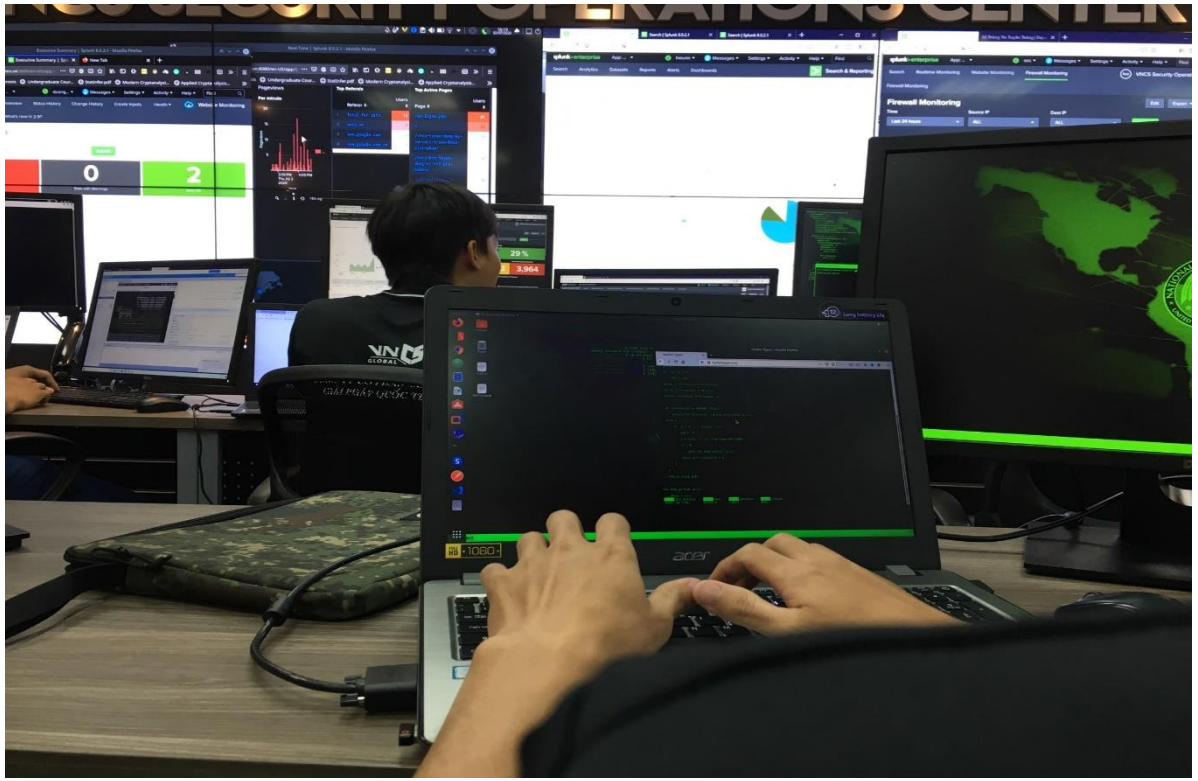
Cung cấp dịch vụ giám sát liên tục, bảo vệ và phản ứng lại sự cố 24/7



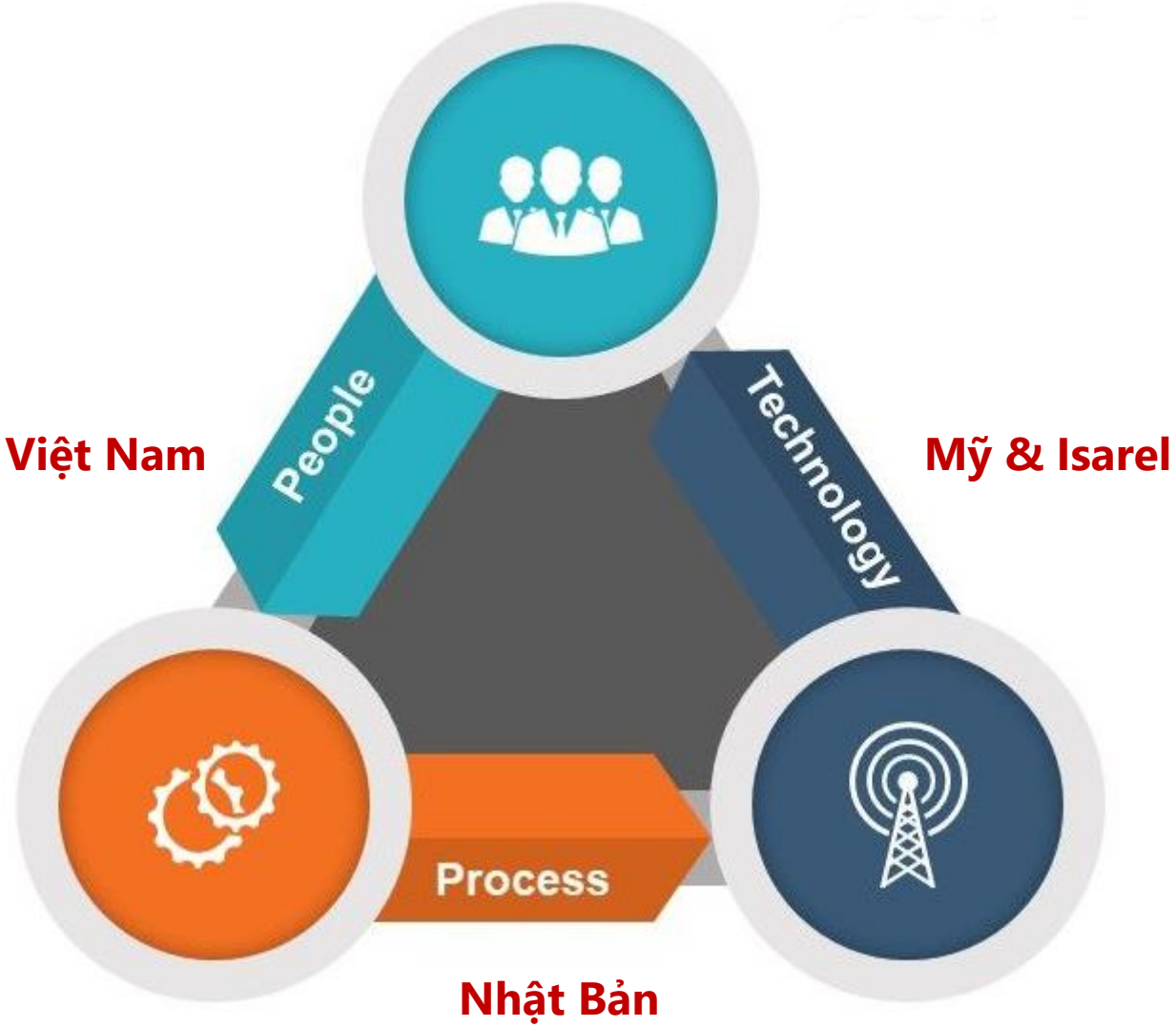
Trung tâm điều hành an ninh mạng

VNCS SOC

Cung cấp dịch vụ giám sát liên tục, bảo vệ và phản ứng lại sự cố 24/7



Lợi thế VNCS SOC ?



Lợi thế VNCS SOC ?

Được Bộ TTTT là **1 trong 8 đơn vị cung cấp SOC** và có **kết nối liên thông** đến Cục ATTT

CỤC AN TOÀN THÔNG TIN

TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

XÁC NHẬN

Công ty Cổ phần Công nghệ giải pháp quốc tế VNCS

Đã hoàn thành việc

KẾT NỐI, CHIA SẺ THÔNG TIN VỚI TRUNG TÂM GIÁM SÁT AN TOÀN AN NINH MẠNG QUỐC GIA

Q. Giám Đốc

Hà Nội, Ngày 2 Tháng 7 Năm 2020

Trần Quang Hưng

Lợi thế VNCS SOC ?

Được Bộ TTTT **công nhận** và có **kết nối liên thông** đến Cục ATTT

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỤC AN TOÀN THÔNG TIN

AUTHORITY OF INFORMATION SECURITY

GIỚI THIỆU | HOẠT ĐỘNG - SỰ KIỆN | PHÁP LUẬT - PHÁP QUY | HÀNH CHÍNH CÔNG | THÔNG TIN THỐNG KÊ | CHU

9:33 Chủ Nhật, 07/06/2020

Trang chủ / Thông tin thống kê / Thông tin tham khảo

Danh sách doanh nghiệp cung cấp sản phẩm, dịch vụ giám sát ATTT (SOC) tính đến tháng 4/2020

03:14 PM 26/04/2020

A- A+

1 . Công ty An ninh mạng Viettel

2 . Trung tâm An toàn thông tin VNPT

3. Trung Tâm An ninh mạng, Tập đoàn CN BKAV

4. Công ty cổ phần công nghệ Giải pháp quốc tế VNCS Global

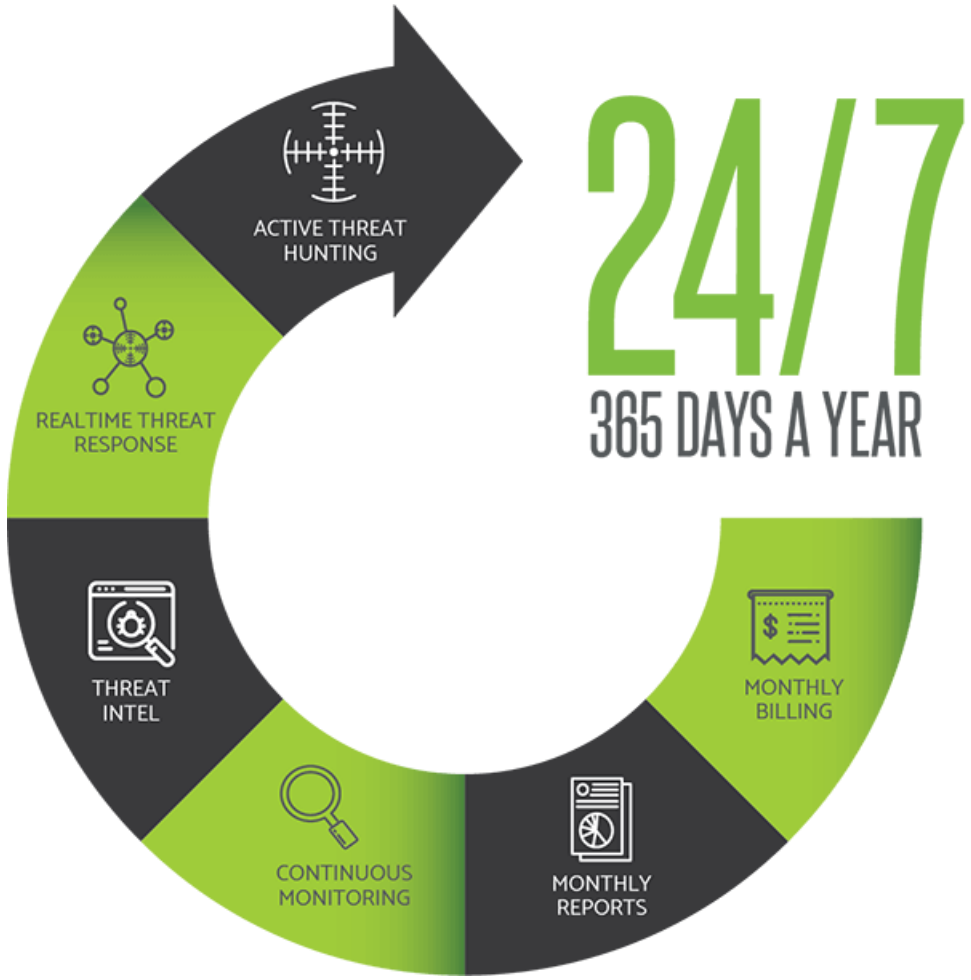
5 . Công ty TNHH Hệ thống Thông tin FPT (FPT IS)

6. Công ty Cổ phần an toàn thông tin CyRadar (CyRadar)

7 . Công ty Cổ phần Công nghệ SAVIS

8 . Công ty CMC Cyber Security

Lợi ích từ dịch vụ

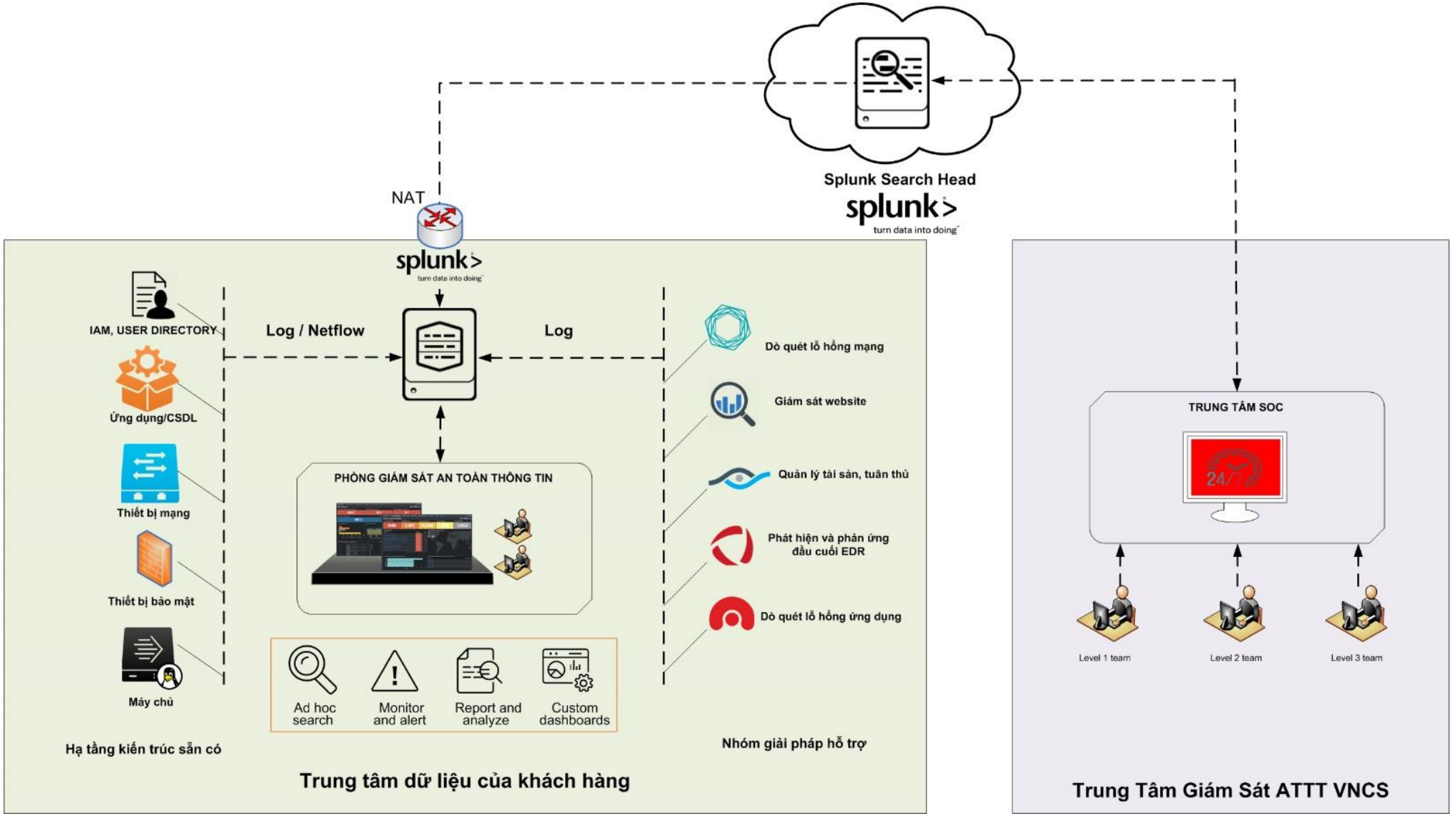


- **Đáp ứng** các yêu cầu của Chính phủ, Bộ TTTT
- **Cảnh báo** xâm nhập, malware, nguy cơ tấn công mạng
- **Rà soát** lỗ hổng bảo mật trên các hệ thống
- **Báo cáo** định kỳ (hàng tháng)
- **Hỗ trợ** (hướng dẫn) xử lý sự cố nghiêm trọng từ xa
- **Đảm bảo** hoạt động thông suốt Dv công, chính phủ điện tử
- **Bảo vệ** danh tiếng, thứ hạng của các đơn vị
- **Vận hành** các giải pháp an toàn thông tin (SIEM, Firewall, IPS,...) theo yêu cầu

Các nguồn thông tin đầu vào

- Cài đặt Agent (Forwarder) trên các máy chủ quan trọng và máy chủ dịch vụ như DNS, AD, Web, Mail, Cổng TTĐT, Dịch vụ công...
- Thu thập log từ các thiết bị mạng và thiết bị bảo mật: Routers, Switch, Fortinet, Bluecoat, Sophos....
- Thu thập Netflow từ Core Switch (SPAN Port)
- Thông tin lỗ hổng thông qua việc quét lỗ hổng định kỳ

MÔ HÌNH TRIỂN KHAI TỔNG THỂ



Các mức độ cung cấp dịch vụ - Tùy chọn dịch vụ

- **Giám sát an toàn thông tin (SOC):** Chỉ giám sát, đưa ra cảnh báo và hướng dẫn xử lý; Báo cáo định kỳ (hàng tháng) về hiện trạng bảo mật và các nguy cơ lớn xảy ra đối với hệ thống
- Vận hành hạ tầng bảo mật (Firewall, IPS, Ddos Protector, SIEM...)
- Phản ứng sự cố: Hỗ trợ và tham gia xử lý các sự cố an toàn thông tin (manual và hướng tới xử lý tự động)

Một số lợi thế công nghệ của VNCS SOC

Lợi thế	Mô tả
Sử dụng giải pháp thương mại để đảm bảo chất lượng	Sử dụng Splunk, Fireeye, Acunetix, Tenable và các giải pháp thương mại nổi tiếng trên thế giới.
Sử dụng nền tảng Bigdata	Khả năng monitor và phân tích events real time từ **không giới hạn nguồn dữ liệu /** đảm bảo **hiệu năng cao**
Khả năng thay đổi / mở rộng	Dễ dàng **thay đổi** dashboard / alert / report **theo nhu cầu thực tế** và phục vụ báo cáo
Hỗ trợ nghiên cứu và áp dụng machine learning	Có sẵn các ứng dụng hỗ trợ áp dụng các giải thuật **machine learning** vào các bài toán thực tế
Phản ứng sự cố	Có khả năng cung cấp dịch vụ (**auto response)** trong giai đoạn 2 theo yêu cầu của khách hàng
Nền tảng mở	Cung cấp API và SDKs để kết nối đến và đi từ các hệ thống khác

VIETNAM CYBERSPACE SECURITY TECHNOLOGY JSC

2. Dịch vụ Đánh giá bảo mật (Pentest)

Distribution | Service | Development

Mục đích

- ❑ Đánh giá hiện trạng bảo mật của toàn bộ hạ tầng CNTT
- ❑ Phát hiện tối đa các lỗ hổng bảo mật trên hệ thống ?
- ❑ Đóng vai trò như hacker để tấn công thử -> Nguy hiểm không ?
- ❑ Đặt ưu tiên xử lý, ưu tiên đầu tư trước khi bị tấn công

Phạm vi

- ❑ Đánh giá toàn diện hạ tầng CNTT (bao gồm Chính sách)
- ❑ Đánh giá mạng
- ❑ Đánh giá hệ thống
- ❑ Đánh giá ứng dụng (website), ứng dụng mobile
- ❑ Đánh giá bảo mật vật lý, wireless
- ❑ ....

Phương pháp tiếp cận

❑ Nguyên tắc chung về thực hiện đánh giá bảo mật

- ✓ Áp dụng các tiêu chuẩn như ISO, SANS, OSSTMM, ISSAF, OWASP để đánh giá an ninh cho hệ thống khách hàng.
- ✓ Các chuyên gia trực tiếp thực hiện có chứng chỉ bảo mật của các hãng
- ✓ NDA đảm bảo thông tin khách hàng
- ✓ Cần sự hợp tác của tất cả các cấp từ khách hàng

Một số dự án đánh giá và tư vấn bảo mật

- Đánh giá bảo mật, tư vấn lộ trình trang bị phát triển lực lượng cho BCA
- Đánh giá bảo mật và tư vấn chiến lược đầu tư bảo mật cho Vietnamobile
- Đánh giá chính sách bảo mật và tư các biện pháp nâng cao an ninh cho Dầu khí Hoàng Long
- Đánh giá bảo mật cho các đơn vị thuộc Bộ thông tin và truyền thông
- Đánh giá bảo mật ứng dụng cho Bảo hiểm MSIG Việt Nam

Phương pháp tiếp cận

❑ Đánh giá từ bên ngoài (Black box) - Pentest

Phương pháp tiếp cận

- Đánh giá cấu hình bên trong (White box) - Audit

Quy trình thực hiện chung

Quá trình đánh giá được thực hiện 02 lần, bao gồm các giai đoạn:

- ***Giai đoạn 1:*** **Data collection:** Thực hiện việc thu thập các thông tin về hệ thống, các dữ liệu cần thiết cho việc đánh giá bảo mật như: Domain Names, Server Names, IP Addresses, Network Map, ISP / ASP information, System and Service Owners, OS Identification, port scanning, Services identification…

- ***Giai đoạn 2:*** **Vulnerability Assessment:** Thực hiện quét, kiểm tra, đánh giá để tìm và phát hiện các lỗ hổng tồn tại trên hệ thống. sử dụng các tiêu chuẩn đánh giá để đánh giá lỗ hổng.

- ***Giai đoạn 3:*** **Actual Exploit:** Thực hiện các tấn công thử nghiệm để kết luận các lỗ hổng thực sự nguy hiểm tới hệ thống.

- ***Giai đoạn 4:*** **Result analysis and report:** Thực hiện các phân tích, đánh trọng số, phân loại lỗ hổng và tạo các bản báo cáo cuối cùng cho khách hàng

Điều kiện thực hiện

- ❑ Đội ngũ chuyên gia tư vấn đánh giá bảo mật nhiều năm kinh nghiệm, chuyên gia tác nghiệp (tấn công + giải pháp)
- ❑ Quy trình chuẩn quốc tế
- ❑ Công cụ đánh giá chuyên sâu
  - Đánh giá hệ thống, mạng
    - ✓ Tenable, Retina, Metasploit
  - Đánh giá ứng dụng (website)
    - ✓ Acunetix, Burpsuite
  - Đánh giá mã nguồn ứng dụng (code review)
    - ✓ Checkmarx, Synopsys

VIETNAM CYBERSPACE SECURITY TECHNOLOGY JSC

3. Các dịch vụ khác

Distribution | Service | Development

VNCS GLOBAL SERVICES

Security Operation Center

Information security monitoring and operation services

Penetration Testing

Information security assessments services

Incident Response

Information security incident response and incident handling service

Compromise Assessment

Assessment if your system be compromised or not

Threat Intelligence

Threats that have, will, or are currently targeting the organization

Digital Threat Monitoring

Monitor and alert when your information is leaked and public out

VNCS GLOBAL OT SECURITY

VNCS Global provide OT security solution for customer

NOZOMI NETWORKS

Honeywell

VNCS Global got knowledge and usecases transfer from Terilogy

Các dịch vụ khác

Compromise Assessment **Penetration Testing**	Đánh giá bảo mật. Hệ thống có lỗ hổng ? Đã bị xâm nhập và trộm dữ liệu ?
Digital Threat Monitoring	Giám sát và cảnh báo khi có dữ liệu thất thoát trên Internet
Incident Response	Xử lý sử cố cao cấp
Threat Intelligence	Cung cấp tri thức về các nguy cơ bảo mật

THANK YOU!

VIETNAM CYBERSPACE SECURITY TECHNOLOGY JSC

VIETNAM CYBERSPACE SECURITY TECHNOLOGY,. JSC (VNCS)

- Head Office**:** Km27, Thang Long Highway, Ha Bang Ward, Thach That Dist., Hanoi, Vietnam.
- Hanoi Office: R401, 4th Floor, Kham Thien Building, Dong Da Dist.,Hanoi, Vietnam.
- HCM Office: 2nd Floor, HTC Building, 385C Nguyen Trai St, HCMC, Vietnam.
- Office: (+84) 24 62 911 416 | Hotline: (+84) 924 37 37 37 Email: sales@vncs.vn