WHEN TRUST MATTERS

Các yêu cầu quy định về an ninh mạng – Phần 2

Quản lý an ninh mạng trong ngành điện

DNV Singapore

08 March 2021



Nội dung

1. Các yêu cầu về phát hiện
2. Các yêu cầu ứng phó và phục hồi

NERC-CIP

https://isomer-user-content.by.gov.sg/36/2df750a7-a3bc-4d77-a492-d64f0ff4db5a/CCoP---Second-Edition_Revision-One.pdf



7 YÊU CẦU VỀ ỨNG PHÓ VÀ PHỤC HỒI

Thiết lập, quản lý và thực hiện các kế hoạch ứng phó sự cố an ninh mạng và kế hoạch thông báo về khủng hoảng để chuẩn bị sẵn sàng cho CII trước các sự cố an ninh mạng.

7.1 Quản lý sự cố

Quản lý sự cố nhằm giảm thiểu tác động của các sự cố an ninh mạng thông qua những quy trình như nhận biết, ngăn chặn và loại bỏ các mối đe dọa an ninh mạng, khôi phục hệ thống, phân tích nguyên nhân gốc rễ và thực hiện các hành động khắc phục để ngăn ngừa sự cố tái diễn. Cần có kế hoạch trong đó nêu rõ cơ cấu tổ chức của Nhóm ứng phó sự cố an ninh mạng, quy định chi tiết vai trò và trách nhiệm để thiết lập phạm vi trách nhiệm rõ ràng cũng như kênh trao đổi thông tin hiệu quả. Ngưỡng ứng phó sự cố liên quan đến doanh nghiệp cũng phải được xác định để có thể kích hoạt kế hoạch ứng phó sự cố một cách chính xác mà không bị chậm trễ. Kế hoạch thông báo cũng sẽ cho phép các bên liên quan cập nhật thông tin tình hình chính xác.

Khi tiến hành phân tích nguyên nhân gốc rễ, các tổ chức cũng nên xem xét các yếu tố về cấu trúc, hành vi, quản lý, kỹ thuật hoặc hệ thống có thể góp phần gây ra sự cố an ninh mạng để giải quyết các vấn đề tiềm ẩn và ngăn ngừa các sự cố tương tự tái diễn.

NERC-CIP

https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx



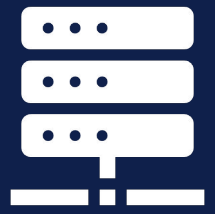
CIP-007-7 Bảng R4 - Giám sát sự kiện an ninh			
Phần	**Hệ thống áp dụng**	**Yêu cầu**	**Chỉ số đo lường**
4.3	Hệ thống an ninh của BES (BCS) tác động cao và các yếu tố liên quan: 1. EACMS; 2. PACS; và 3. PCA BCS tác động trung bình tại các Trung tâm kiểm soát và các vấn đề liên quan: 1. EACMS; 2. PACS; và 3. PCA SCI hỗ trợ Hệ thống áp dụng trong Phần này.	Lưu nhật ký các sự kiện an ninh áp dụng xác định trong Phần 4.1 trong ít nhất 90 ngày dương lịch liên tiếp gần nhất, theo khả năng của hệ thống, ngoại trừ các trường hợp rất đặc biệt trong CIP	Ví dụ về bằng chứng có thể bao gồm, nhưng không giới hạn ở, tài liệu về quy trình lưu giữ nhật ký sự kiện và báo cáo trên giấy hoặc hệ thống cho thấy cấu hình lưu giữ nhật ký được đặt ở mức 90 ngày dương lịch trở lên.
4.4	Hệ thống an ninh của BES (BCS) tác động cao và các yếu tố liên quan: 1. EACMS; và 2. PCA SCI hỗ trợ Hệ thống áp dụng trong Phần này.	Xem xét bản tóm tắt hoặc mẫu các sự kiện an ninh đã ghi lại theo quyết định của Cơ quan chịu trách nhiệm theo các khoảng thời gian cách nhau không quá 15 ngày dương lịch để xác định các Sự cố an ninh mạng chưa được phát hiện.	Ví dụ về bằng chứng có thể bao gồm nhưng không giới hạn ở tài liệu mô tả quá trình đánh giá, phát hiện từ quá trình đánh giá (nếu có) và tài liệu có ngày tháng cho thấy quá trình đánh giá đã được thực hiện.

1. Phát hiện

DNV ©

Công cụ giám sát và kiểm soát an ninh mạng

Điểm cuối



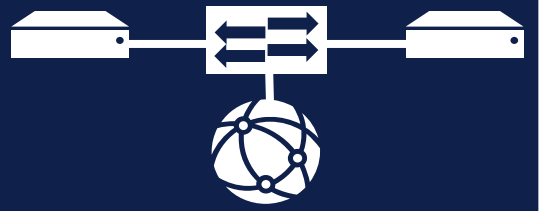
- IDPS
- AV dựa trên chữ ký
- AV dựa trên kinh nghiệm
- WAF
- Điều khiển ứng dụng
- Điều khiển thiết bị (USB)

Mạng (Nội dòng)



- Tường lửa TCP/IP
- WAF
- Proxy
- Diodes dữ liệu

Mạng (Ngoài băng tần)



- Trình phân tích lưu lượng truy cập mạng dựa trên kinh nghiệm
- NIDS / NDR / NTA
- Nhận thức về giao thức
- Không thể xuyên thủng mã hóa

Tích hợp & Quản lý



- Thông tin về mối đe dọa
- SIEM
- SOAR
- Bán vé

Phương pháp phát hiện

Việc hiểu được cách thức mà sự cố được phát hiện sẽ giúp ích rất nhiều trong việc phân loại

Phát hiện dựa trên chữ ký

- Hãy chú ý đến chữ ký (băm)
- Chữ ký cần được cập nhật thường xuyên
- Đường tránh tương đối đơn giản
- Không thể phát hiện ngày 0
- Kỹ thuật bypass (đi đường tránh) tương đối đơn giản
- Phát hiện có độ chính xác cao nhưng âm tính giả cao

Phát hiện dựa trên sự bất thường

- Tạo hồ sơ hiện trạng
- Nêu các vấn đề không phù hợp với hồ sơ cơ sở/hiện trạng này (Đáng ngờ)
- Có thể rất nhiều yếu tố nhiễu
- Cần được hiệu chuẩn thường xuyên bởi kỹ sư lành nghề
- Phản hồi tự động thường bị vô hiệu hóa để thực hiện Phát hiện dựa trên sự bất thường
- Cảnh báo thường xuyên với tỷ lệ dương tính giả cao, cần phân tích thêm
- Kẻ tấn công khó trốn tránh hơn nhiều

Nhật ký ở mọi nơi!

Từ các yếu tố bảo mật

- Nhật ký tường lửa
- Nhật ký NIDS / NTA / NDR
- Nhật ký bảo vệ điểm cuối máy chủ (AV)
- Nhật ký VPN
- Nhật ký cổng email
- Nhật ký thư mục hoạt động

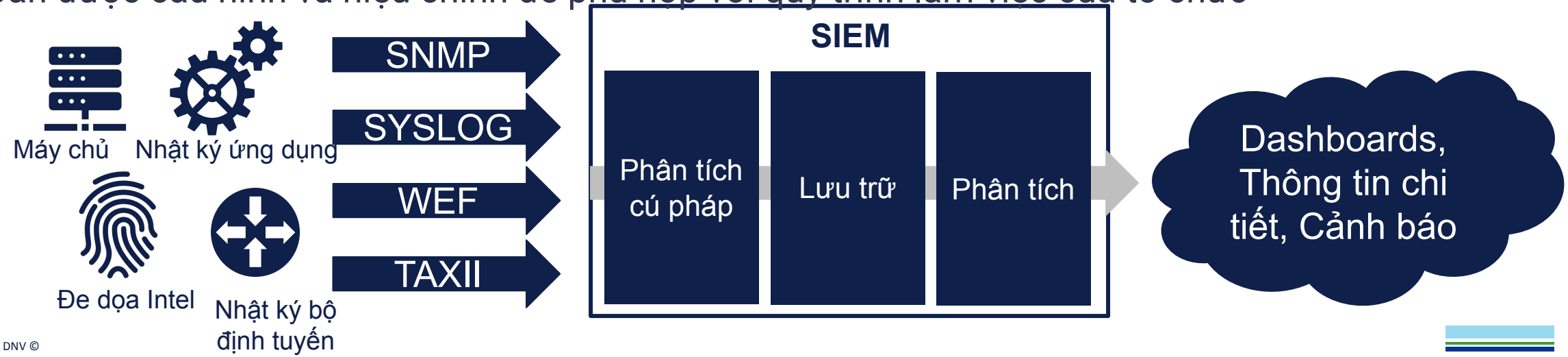
Từ các yếu tố CNTT

- Nhật ký máy chủ
- Nhật ký ứng dụng
- Nhật ký máy chủ web
- Nhật ký bộ định tuyến
- Nhật ký chuyển mạch

Và mỗi yếu tố lại được thiết lập khác nhau với hình thức khác nhau.

Bảo mật thông tin và quản lý sự kiện (SIEM)

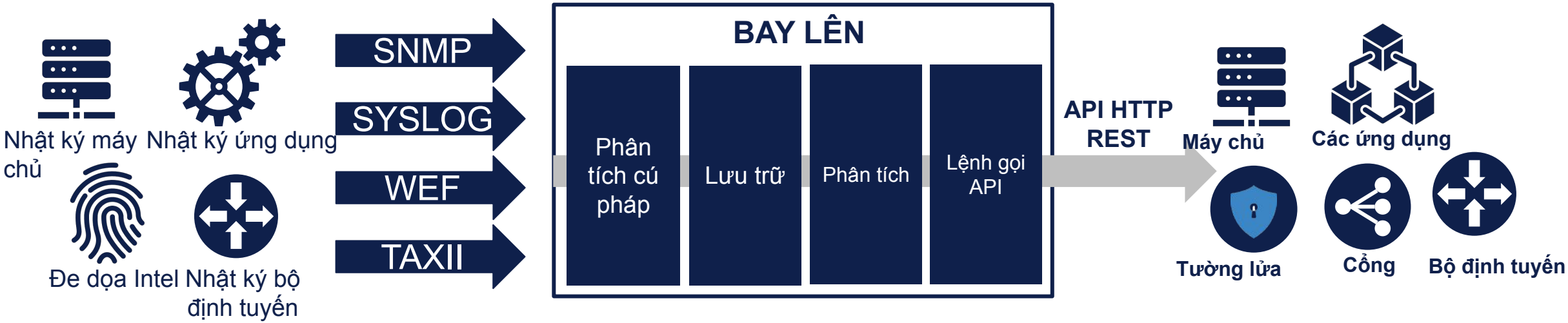
- Kho lưu trữ nhật ký tập trung từ tất cả các thành phần hệ thống
- Nhật ký thường được gửi đến SIEM thông qua SYSLOG, SNMP hoặc WEF
- Các công cụ có sẵn để phân tích các thông báo SYSLOG từ các thành phần hệ thống khác nhau
- Các tính năng có sẵn để xử lý, phân tích và tổng hợp dữ liệu được thu thập thành thông tin chi tiết hữu ích
- Cần được cấu hình và hiệu chỉnh để phù hợp với quy trình làm việc của tổ chức



DNV ©

Điều phối, tự động hóa và phản hồi bảo mật (SOAR)

- Đây là Phiên bản nâng cấp của SIEM, thể hiện ở chỗ nó có thể đưa ra các lệnh API cho các thành phần bảo mật trong mạng
- Trang bị công cụ tạo tập lệnh mở rộng để tự động hóa quy trình làm việc
- Có thể yêu cầu tập lệnh tùy chỉnh để gọi API phần tử bảo mật
- Yêu cầu khả năng viết tập lệnh nội bộ để duy trì



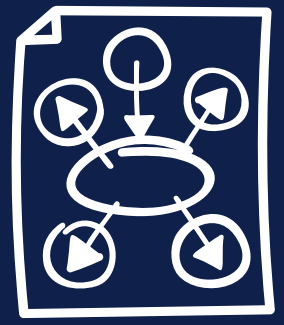
Giới thiệu về Thông tin mối đe dọa (Threat Intelligence)

- Tình báo về mối đe dọa (Threat Intelligence) là một dịch vụ (Nhà cung cấp đáng chú ý: Group IB, Mandiant, Recorded Future)
- Nghiên cứu An ninh mạng về các tác nhân đe dọa đang hoạt động, phần mềm độc hại, trang web độc hại cũng như IP liên quan đến hoạt động hack
- Sản phẩm bàn giao bao gồm:
  - Danh sách chữ ký của phần mềm độc hại đang hoạt động
  - Danh sách IP liên quan đến hoạt động hack
  - Danh sách tên miền độc hại
- Được phân phối trực tiếp đến các thành phần an ninh mạng (Tường lửa, Máy khách điểm cuối, SIEM, v.v.) bằng giao thức TAXII ở định dạng STIX
- Tăng cường SOC để thực hiện hành động tự động dựa trên thông tin về mối đe dọa nhận được
- Mô hình thương mại dựa trên đăng ký

Khái niệm cơ bản về săn lùng mối đe dọa

“Săn lùng mối đe dọa là hoạt động tìm kiếm các mối đe dọa mạng trong một hệ thống”

Sơ đồ hóa nhật ký



Nắm được danh sách trắng



Tạo đường cơ sở



Sử dụng một mô hình



DNV

Khái niệm cơ bản về săn lùng mối đe dọa (1): Lập bản đồ nhật ký của bạn

Nhật ký ứng dụng



- Xác thực ứng dụng
- Tạo người dùng ứng dụng
- Hoạt động ứng dụng
- Thay đổi cấu hình ứng dụng
- Quyền truy cập ứng dụng

Nhật ký máy chủ



- Quyền truy cập máy chủ (SSH, RDP)
- Thay đổi cấu hình
- Cài đặt/Gỡ cài đặt
- Tạo người dùng
- Thay đổi chính sách
- Truy cập dịch vụ hệ điều hành (SMB, WinRM)

Nhật ký mạng



- Gói mạng (PCAP)
- Mẫu giao tiếp máy chủ
- Quét cổng, lọc dữ liệu, v.v.
- Được thu thập bởi các giải pháp NIDS/NTA/NDR

Bạn có biết bạn ***có*** hoặc ***không có nhật ký nào không*** ?

Dành cho ứng dụng/máy chủ/phân khúc nào?

DNV ©

Khái niệm cơ bản về săn lùng mối đe dọa (2): Biết danh sách trắng của bạn

Miễn trừ AV

- Một số loại danh sách trắng
- Ngoại lệ mở rộng (exe, msi , bat, txt)
- Ngoại lệ đường dẫn tệp (C:\\System32\cmd.exe)
- Ổ đĩa ngoại lệ (C, H, I)
- Các tệp trong danh sách trắng được miễn quét AV (thậm chí quét toàn bộ)
- Cập nhật AV lần cuối

Danh sách trắng tường lửa

- Thông thường, các gói được phép không được ghi lại
- Danh sách trắng tường lửa sẽ mô tả cách một mối đe dọa có thể chuyển từ phân đoạn này sang phân đoạn khác
- Danh sách trắng IP, cổng

Bạn có biết mục đích của từng danh sách trắng?

Lần cuối bạn xem lại chúng là khi nào?

Chúng có quá rộng không?

DNV

Khái niệm cơ bản về săn lùng mối đe dọa (3): Tạo đường cơ sở

Đường cơ sở mạng

- Hồ sơ lưu lượng mạng (Destination) cho mỗi máy chủ
- Hồ sơ khối lượng dữ liệu
- Hồ sơ thường được tạo bởi các giải pháp NIDS/NTA/NDR

Đường cơ sở về truy cập

- Hồ sơ truy vấn cho cơ sở dữ liệu SQL
- Hồ sơ truy cập cho các ứng dụng chính (Ai đang truy cập ứng dụng? Từ đâu? Làm gì?)

Phát hiện bất thường dựa vào đường cơ sở vững chắc.

Nhóm có thể phát hiện quyền truy cập đáng ngờ vào một ứng dụng không?

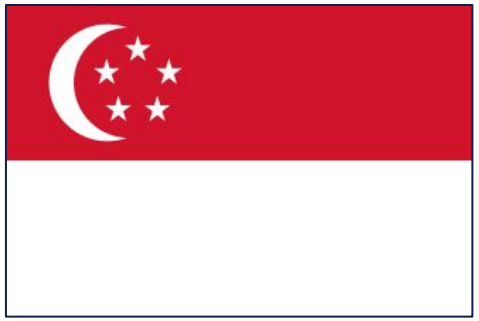
DNV

Khái niệm cơ bản về săn lùng mối đe dọa (4): Sử dụng mô hình

- Mô hình mối đe dọa mô tả Chiến thuật, Kỹ thuật & Quy trình (TTP) của kẻ đe dọa
- Nó mô tả những gì cần tìm và nơi cần tìm trong quá trình Săn tìm mối đe dọa
- Ví dụ về khung mô hình hóa mối đe dọa:
  - MITRE
  - STRIDE
  - PASTA

Làm thế nào để bạn phát hiện một cuộc tấn công SQLI?
Làm thế nào để bạn phát hiện việc quét mạng?
Dấu chân của những cuộc tấn công này có thể được tìm thấy ở đâu?

Các yêu cầu về phát hiện



Bộ quy tắc thực hành an ninh mạng

6 yêu cầu về phát hiện

- 6.1 Ghi nhật ký
- 6.2 Giám sát và phát hiện
- 6.3 Săn tìm mối đe dọa
- 6.4 Chia sẻ thông tin và dữ liệu xử lý về mối đe dọa mạng



NERC - CIP

- CIP-007 an ninh mạng - Quản lý an ninh hệ thống

Yêu cầu về phát hiện - Ghi nhật ký



6.1.1 CIIO sẽ tạo, thu thập và lưu trữ nhật ký về những nội dung sau:

a) Mọi lượt truy cập và nỗ lực truy cập CII và các hoạt động trong lượt truy cập đó,
b) Kết nối mạng giữa CII và các mạng bên ngoài CII;
c) Kết nối mạng trong CII;
d) Kết nối từ xa tới CII;
e) Kết nối giữa CII và mạng LAN không dây.

6.1.2 CIIO cũng sẽ tạo, thu thập và lưu trữ các loại nhật ký sau để theo dõi các hoạt động mạng trong CII và giữa CII với các mạng bên ngoài CII:

f) Nhật ký tường lửa mạng;
g) Nhật ký Hệ thống tên miền (DNS);
h) Nhật ký Proxy Web; và
i) Nhật ký Hệ thống phát hiện/ngăn chặn xâm nhập mạng (NIDS/NIPS).

6.1.3 CIIO sẽ cung cấp bất kỳ nhật ký nào được đề cập trong khoản 6.1.2 khi có yêu cầu của Ủy viên

Yêu cầu về phát hiện - Giám sát và phát hiện



6.2.1 CIIO sẽ tạo, thu thập và lưu trữ nhật ký về những nội dung sau:

a) **Giám sát** và phát hiện tất cả các sự kiện an ninh mạng liên quan đến CII;

b) **Thu thập** và lưu trữ hồ sơ của tất cả các sự kiện an ninh mạng đó

c) **Phân tích** tất cả các sự kiện an ninh mạng đó

d) **Kích hoạt** các kế hoạch báo cáo, ứng phó và phục hồi sự cố áp dụng nếu có hoặc đã xảy ra sự cố an ninh mạng

6.2.2 Để giám sát và phát hiện các sự kiện an ninh mạng, các cơ chế và quy trình do CIIO thiết lập sẽ bao gồm:

e) **Quét** các dấu hiệu về sự xâm nhập (IOC)

f) **Thiết lập các hoạt động vận hành hàng ngày bình thường** và lưu lượng mạng trong CII, và sử dụng điều này làm cơ sở để CIIO theo dõi các sai lệch và hoạt động bất thường; và

g) Đảm bảo rằng các cảnh báo để **điều tra thêm** được kích hoạt đối với tất cả mọi sai lệch

6.2.3 CIIO sẽ **rà soát** các cơ chế và quy trình được thiết lập theo khoản 6.2.1, bao gồm cấu hình cơ sở được đề cập trong khoản 6.2.2(b), ít nhất **12 tháng/lần** để đảm bảo rằng các cơ chế và quy trình vẫn hoạt động hiệu quả, đúng chức năng.

Yêu cầu về phát hiện - Tìm kiếm mối đe dọa



6.3.1 CIIO sẽ tiến hành tìm kiếm mối đe dọa cho CII để tìm và xác định các mối đe dọa an ninh mạng đối với CII ít nhất **24 tháng/lần**. Lần tìm kiếm mối đe dọa đầu tiên phải được hoàn thành chậm nhất là 12 tháng sau Ngày tuân thủ.

6.3.2 CIIO sẽ đưa các mối đe dọa an ninh mạng được xác định từ quá trình tìm kiếm mối đe dọa vào trong các đánh giá rủi ro an ninh mạng

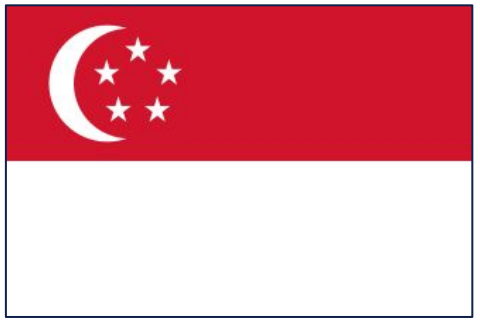
6.3.3 CIIO sẽ phân tích tất cả các mối đe dọa được xác định từ quá trình tìm kiếm

Yêu cầu về phát hiện - Dữ liệu xử lý và chia sẻ thông tin về mối đe dọa mạng

6.4.1 CIIO sẽ thiết lập và triển khai các cơ chế và quy trình để thu thập, xử lý và phân tích dữ liệu xử lý về mối đe dọa để xác định mức độ liên quan và tác động tiềm ẩn đến CII

6.4.2 CIIO sẽ thiết lập và triển khai các cơ chế và quy trình **chia sẻ thông tin** về các mối đe dọa và lỗ hổng an ninh mạng với **Ủy viên.**

6.4.3 CIIO sẽ thiết lập các biện pháp kiểm soát để giảm thiểu các mối đe dọa an ninh mạng và giải quyết các lỗ hổng được xác định từ dữ liệu xử lý về mối đe dọa



Yêu cầu về phát hiện – Ghi nhật ký

CIP-007-7.pdf

4.1 Phải lưu trữ tối thiểu các loại nhật ký sau:

- Các nỗ lực đăng nhập thành công bị phát hiện
- Các nỗ lực truy cập không thành công và các nỗ lực đăng nhập không thành công bị phát hiện;
- Mã độc bị phát hiện

4.2 Tạo cảnh báo cho các sự kiện bảo mật

- Phát hiện mã độc từ 4.1
- Phát hiện lỗi ghi nhật ký sự kiện Phần 4.1.



Yêu cầu về phát hiện – Yêu cầu về ghi nhật ký

CIP-007-7.pdf

4.3 Lưu nhật ký các sự kiện bảo mật áp dụng xác định trong Phần 4.1 trong **ít nhất 90 ngày dương lịch liên tiếp gần nhất**, theo khả năng của hệ thống



4.2 Xem xét bản tóm tắt hoặc mẫu các sự kiện bảo mật đã ghi lại theo quyết định của Cơ quan chịu trách nhiệm theo **các khoảng thời gian cách nhau không quá 15 ngày dương lịch** để xác định các Sự cố an ninh mạng chưa được phát hiện.

DNV ©

Yêu cầu về phát hiện – Yêu cầu về ghi nhật ký

CIP-007-7.pdf

Phạm vi

Hệ thống bảo mật của BES (BCS) tác động cao và các yếu tố liên quan:



1. Hệ thống giám sát hoặc kiểm soát truy cập điện tử (EACMS)
2. Hệ thống lưu trữ và truyền thông hình ảnh (PACS)
3. PCA BCS tác động trung bình và các yếu tố liên quan:
    1. EACMS;
    2. PACS; và
    3. PCA SCI hỗ trợ Hệ thống áp dụng trong Phần này

Tóm tắt

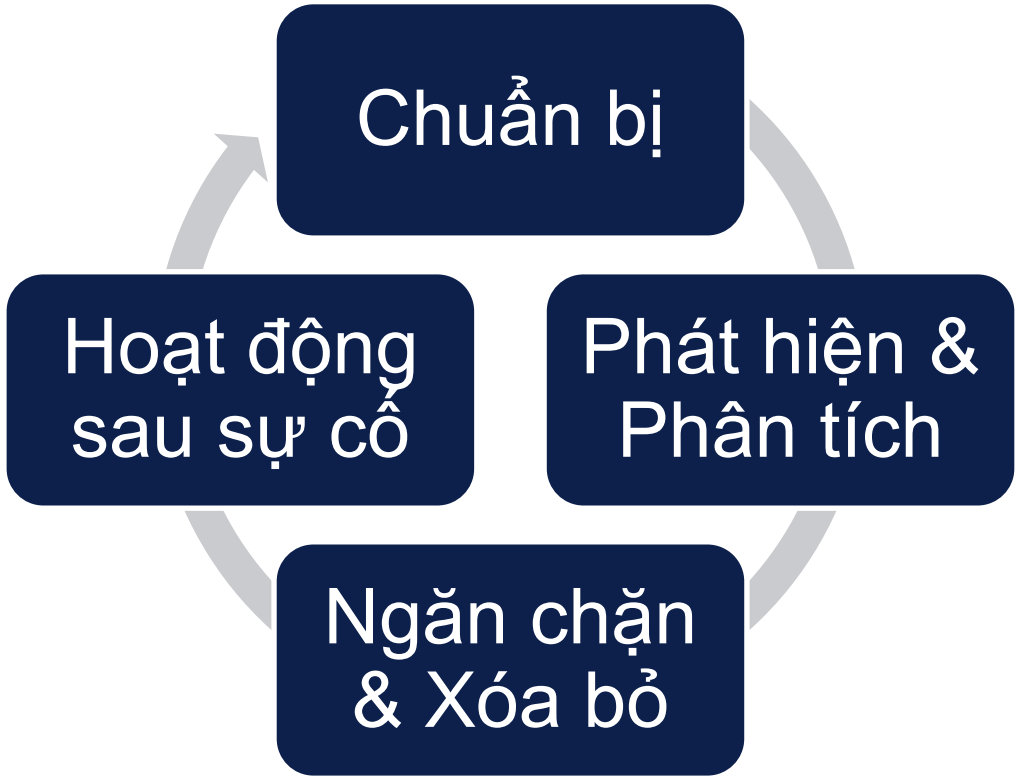
- Mô tả loại dữ liệu cần được ghi nhật ký và giám sát
- Thời gian lưu trữ các bản ghi
- Các biện pháp được áp dụng để hỗ trợ phát hiện
- Nghĩa vụ kiểm toán và nộp báo cáo theo quy định
- Phạm vi yêu cầu trong bản của Singapore rộng hơn nhiều
- Mỗi loại đều có:
  - Khung thời gian rõ ràng
- NERC-CIP
  - Xác định các hệ thống trong phạm vi điều chỉnh của tiêu chuẩn
  - Xác định tài liệu cần nộp cho kiểm toán
  - Mức độ nghiêm trọng của vi phạm

1. Ứng phó và phục hồi

DNV ©

Tại sao chúng ta cần xử lý sự cố?

- Phản ứng có hệ thống đối với sự cố
- Giảm thiểu mất mát hoặc đánh cắp thông tin và gián đoạn dịch vụ do sự cố
- Thu thập thông tin để cải thiện an ninh của tổ chức và ứng phó trong tương lai đối với các sự cố

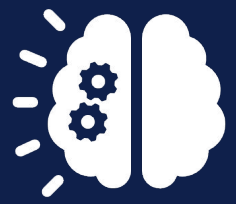


Hướng dẫn xử lý sự cố an ninh máy tính của NIST 800-61 Rev 2

DNV ©

Các giai đoạn xử lý sự cố

Sự chuẩn bị



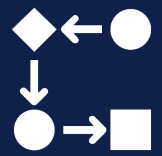
- **Chính sách và quy trình**
- **Thực hành và tập huấn**

Phát hiện & Phân tích



- Nhận biết
- ***Phân tích sự cố***
- Ưu tiên sự cố

Ngăn chặn & Phục hồi



- ***Ngăn chặn***
- Thu thập bằng chứng
- Xóa bỏ
- Khôi phục

Hoạt động sau sự cố

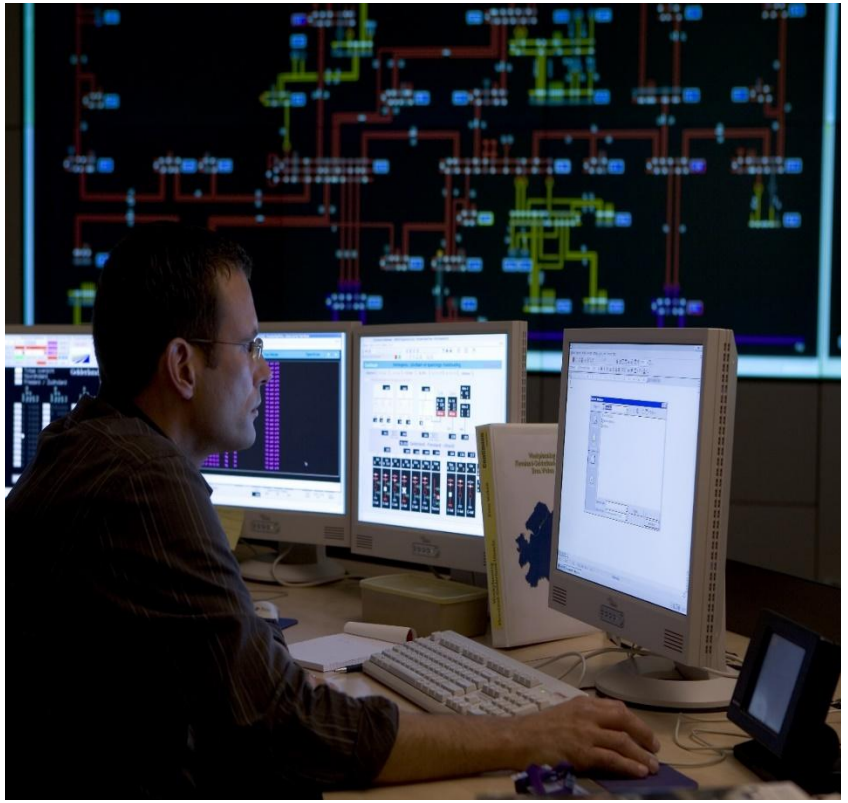


- ***Báo cáo***
- ***Cải tiến***

DNV ©

Đừng hoảng sợ và hãy làm theo cẩm nang
Chuẩn bị

- Playbook là một tài liệu trình bày chi tiết các quy trình từng bước để ứng phó với một sự cố
- Playbook khác nhau dành cho các đội khác nhau phục vụ các chức năng khác nhau trong thời gian xảy ra sự cố
- Mô tả chi tiết về vai trò của từng thành viên trong nhóm khi ứng phó sự cố
- Phải chứa thông tin xác thực/quyền truy cập khẩn cấp vào hệ thống/công cụ để ứng phó với sự cố
- Đã được cấp quản lý cao nhất phê duyệt
- Hãy nhớ luyện tập nhé! Xác thực cẩm nang (Bài tập tại bàn)



Khi nào cần kích hoạt ứng phó sự cố?
Phát hiện & Phân tích

> *Việc xác định xem một sự kiện cụ thể có thực sự là một sự cố hay không **đôi khi là vấn đề mang tính phán đoán** . Có thể cần phải cộng tác với các nhân viên an ninh thông tin và kỹ thuật khác để **đưa ra quyết định** . Trong nhiều trường hợp, một tình huống nên được xử lý theo cùng một cách bất kể nó có liên quan đến an ninh hay không.*
>
> -nist.sp.800-61r2 trang 28

- Hàng trăm cảnh báo mỗi ngày về những điều nhỏ nhặt
- Bạn cần chắc chắn đến mức nào trước khi kích hoạt ứng phó sự cố?
- Ai có thể xác định xem một sự kiện có phải là sự cố an ninh hay không và kích hoạt ứng phó sự cố?
- Quyền hạn và nhiệm vụ của đội ứng phó sự cố khi xảy ra sự cố là gì?



Ma trận mức độ nghiêm trọng của sự cố

Mức độ nghiêm trọng	Mô tả
Cần cung cấp thông tin	Là sự kiện liên quan đến an ninh được quan sát có thể là dấu hiệu về mối đe dọa hoặc cần quan tâm từ các góc độ khác, nhưng không có sự cố hoặc mối đe dọa trực tiếp về an ninh CNTT hoặc OT. Nói chung, các sự kiện được coi là ở mức thấp thì chỉ cần theo dõi để phân tích thống kê.
Trung bình	Là sự cố an ninh CNTT hoặc OT nhỏ có tác động cục bộ và nguy cơ lây lan hoặc lan truyền thấp. Cần được theo dõi và có hành động tiếp theo, nhưng nhìn chung các sự cố có mức độ nghiêm trọng trung bình không đòi hỏi phải hành động ngay lập tức.
Nghiêm trọng	Là sự cố an ninh CNTT hoặc OT ảnh hưởng đến một số hệ thống vừa phải hoặc chỉ ảnh hưởng đến các tài sản không quan trọng. Tác động bất lợi là vừa phải, nhưng không có nguy cơ lan rộng hoặc lan truyền ngay lập tức. Cần điều tra kịp thời.
Rất nghiêm trọng	Là các sự cố an ninh CNTT hoặc OT có tác động nghiêm trọng có nguy cơ gây tác động tiêu cực đáng kể đến một số lượng lớn hệ thống và/hoặc con người hoặc làm gián đoạn tài sản đang hoạt động, có khả năng lây lan hoặc lan truyền đáng kể. Nó cũng gây ra mối đe dọa đối với dữ liệu bí mật hoặc nhạy cảm hoặc các tài sản khác. Các sự cố an ninh CNTT hoặc OT nghiêm trọng cần được chú ý ngay lập tức để khắc phục hoặc giảm thiểu

DNV ©

Thiết kế Chiến lược Ngăn chặn
Ngăn chặn & Phục hồi

Các tiêu chí để xác định chiến lược phù hợp bao gồm:

- Loại sự cố
- Tiềm năng thiệt hại và đánh cắp tài nguyên
- Tính sẵn có của dịch vụ (ví dụ: kết nối mạng, dịch vụ được cung cấp cho các bên bên ngoài)
- Thời gian và nguồn lực cần thiết để thực hiện chiến lược
- Hiệu quả của chiến lược (ví dụ, ngăn chặn một phần, ngăn chặn toàn bộ)
- Thời hạn của giải pháp



Thiết kế chiến lược ngăn chặn
Các hoạt động sau sự cố

Yêu cầu báo cáo

- Có thể được xác định theo chính sách của công ty hoặc các yêu cầu pháp lý
- Yêu cầu cụ thể bao gồm các mốc thời gian



Bài học kinh nghiệm

- Hiểu biết đầy đủ về TTP tấn công
- Hiệu quả của biện pháp phòng thủ
- Các lĩnh vực cần cải thiện

Cách ly mạng IT/OT và vận hành đảo

Deutsche Windtechnik hit with a cyberattack, a third on Germany's wind energy sector

Updated on: April 27, 2022 1:11 PM

Vilius Petkauskas, Deputy Editor



Conti claims responsibility for an attack on wind turbine giant Nordex

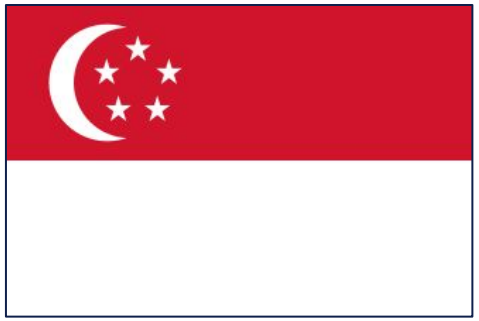
Updated on: April 15, 2022 12:39 PM

Vilius Petkauskas, Deputy Editor



- Cả hai công ty đều bị tấn công bằng Ransomware trong vòng một tháng
- Hệ thống IT bị xâm nhập, OT ngay lập tức bị cô lập
- Tiếp tục hoạt động ở phạm vi đảo hay đóng cửa là một quyết định rủi ro

Các yêu cầu về phát hiện



Bộ quy tắc thực hành an ninh mạng

7 Yêu cầu về ứng phó và phục hồi

7.1 Quản lý sự cố

7.2 Kế hoạch truyền thông khủng hoảng

7.3 Diễn tập an ninh mạng

8 Yêu cầu về khả năng phục hồi mạng

- 8.1 Kế hoạch sao lưu và khôi phục
- 8.2 Kế hoạch duy trì hoạt động và Kế hoạch phục hồi sau thảm họa

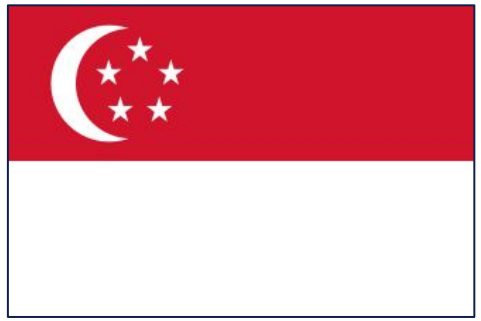


NERC - CIP

- CIP-008 an ninh mạng - Báo cáo sự cố và lập kế hoạch ứng phó
- CIP-009 an ninh mạng - Kế hoạch phục hồi cho Hệ thống mạng BES

Yêu cầu về ứng phó và phục hồi – Quản lý sự cố

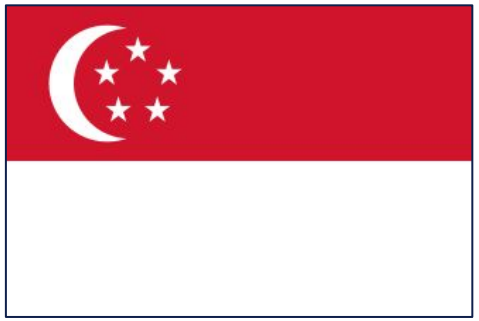
7.1.1 CIIO sẽ xây dựng Kế hoạch ứng phó sự cố an ninh mạng, trong đó nêu rõ cách CIIO nên ứng phó với sự cố an ninh mạng.



7.1.4 CIIO sẽ xây dựng và triển khai các quy trình để xác định, điều tra và giải quyết nguyên nhân gốc rễ gây ra mỗi sự cố an ninh mạng, bao gồm các yếu tố về cấu trúc, hành vi, quản lý, kỹ thuật hoặc hệ thống, để ngăn các sự cố tương tự tái diễn.

7.1.6 CIIO sẽ rà soát Kế hoạch ứng phó sự cố an ninh mạng để đảm bảo kế hoạch này luôn được cập nhật và có tính phù hợp **ít nhất 12 tháng/lần.**

Yêu cầu về ứng phó và phục hồi - Diễn tập an ninh mạng (1)



7.3.1 CIIO sẽ tiến hành diễn tập an ninh mạng theo kịch bản để kiểm tra và xác nhận tính hiệu quả của các kế hoạch sau:

(a) Kế hoạch ứng phó sự cố an ninh mạng;

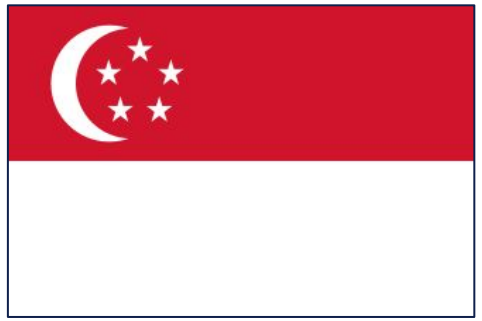
(b) Kế hoạch duy trì hoạt động;

(c) Kế hoạch phục hồi sau thảm họa; và

(d) Kế hoạch truyền thông khủng hoảng.

7.3.2 CIIO sẽ tiến hành các đợt diễn tập an ninh mạng dựa trên kịch bản được đề cập tại khoản 7.3.1 ít nhất **12 tháng/lần**.

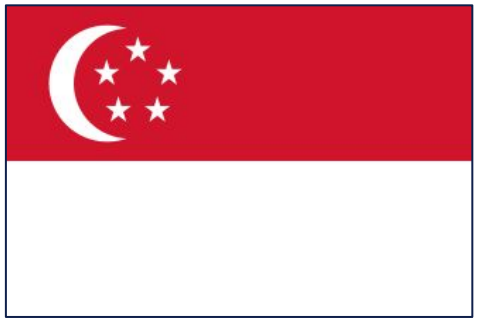
Yêu cầu về ứng phó và phục hồi - Diễn tập an ninh mạng (2)



7.3.5 Khi được Ủy viên yêu cầu, CIIO sẽ nộp một bản báo cáo về bất kỳ đợt diễn tập an ninh mạng nào đã hoàn thành, cùng với các kế hoạch khắc phục của CIIO, cho Ủy viên **trong vòng 30 ngày làm việc kể từ khi nhận được yêu cầu.**

7.3.6 Liên quan đến các cuộc diễn tập an ninh mạng do Ủy viên thực hiện theo phần 16 của Đạo luật, CIIO sẽ tuân thủ mọi yêu cầu của Ủy viên về cung cấp thông tin liên quan đến CII, bao gồm Kế hoạch ứng phó sự cố an ninh mạng và Kế hoạch truyền thông khủng hoảng liên quan, nhằm mục đích lập kế hoạch và tiến hành các cuộc diễn tập đó.

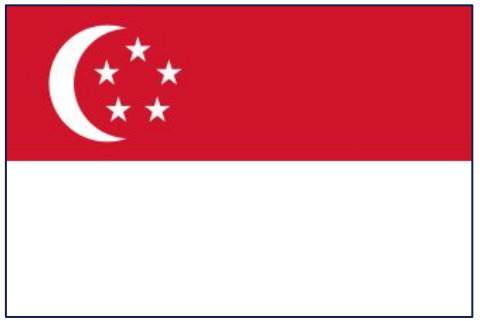
Yêu cầu về khả năng phục hồi mạng - Kế hoạch sao lưu và khôi phục



8.1.3 CIIO phải đảm bảo rằng các bản sao lưu được lưu trên các thiết bị không kết nối với bất kỳ máy tính nào hoặc Internet và tách biệt với các tài sản CII tương ứng, đồng thời được bảo vệ khỏi việc truy cập, sửa đổi và xóa trái phép.

8.1.5 CIIO sẽ rà soát kế hoạch sao lưu và khôi phục ít nhất **12 tháng/lần** để đảm bảo rằng kế hoạch vẫn còn phù hợp.

Yêu cầu về khả năng phục hồi mạng - Kế hoạch duy trì hoạt động và Kế hoạch phục hồi sau thảm họa



8.2.1 CIIO sẽ xây dựng Kế hoạch duy trì hoạt động (“BCP”) và Kế hoạch phục hồi sau thảm họa (“DRP”) để đảm bảo cung cấp liên tục các dịch vụ thiết yếu trong trường hợp gián đoạn do sự cố an ninh mạng.

8.2.5 CIIO sẽ rà soát các kế hoạch BCP và DRP ít nhất **12 tháng/lần** để đảm bảo tính hiệu quả.

Ứng phó và Phục hồi – Báo cáo sự cố và lập kế hoạch ứng phó

https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-7.pdf



1.1 Một hoặc nhiều quy trình để xác định, phân loại và ứng phó với sự cố an ninh mạng.

2.1 Kiểm tra từng kế hoạch ứng phó sự cố an ninh mạng ít nhất 15 tháng dương lịch/lần:

1. Thông qua ứng phó thực tế với sự cố an ninh mạng cần báo cáo;
2. Thông qua bài tập thực hành trên giấy hoặc tại bàn đối với sự cố an ninh mạng cần báo cáo; hoặc
3. Thông qua bài tập thực hành về sự cố an ninh mạng cần báo cáo.

Ứng phó và Phục hồi – Báo cáo sự cố và lập kế hoạch ứng phó

https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-7.pdf



3.1 **Không muộn hơn 90 ngày dương lịch** sau khi hoàn thành kiểm thử kế hoạch ứng phó sự cố an ninh mạng hoặc ứng phó thực tế với sự cố an ninh mạng cần báo cáo:

3.1.1 Ghi lại các bài học kinh nghiệm hoặc ghi lại việc không có bài học kinh nghiệm nào;

3.1.2 Cập nhật kế hoạch ứng phó sự cố an ninh mạng dựa trên các bài học kinh nghiệm được ghi lại liên quan đến kế hoạch

3.1.3 Thông báo cho từng cá nhân hoặc nhóm có vai trò xác định trong kế hoạch ứng phó sự cố an ninh mạng về các bản cập nhật kế hoạch dựa trên bài học kinh nghiệm được ghi chép lại.

Ứng phó và Phục hồi – Báo cáo sự cố và lập kế hoạch ứng phó



https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-7.pdf

4.1 Thông báo và cập nhật ban đầu phải bao gồm các nội dung sau, ở mức tối thiểu, trong phạm vi hiểu biết:

4.1.1 Tác động đến chức năng;

4.1.2 Vectơ tấn công được sử dụng; và

4.1.3 Mức độ xâm nhập đã đạt được hoặc đã cố gắng thực hiện.

Ứng phó và phục hồi – Báo cáo sự cố và Lập kế hoạch ứng phó (Bằng chứng)



https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-7.pdf

1. Bằng chứng có thể bao gồm nhưng không giới hạn ở tất cả những tài liệu sau: Tài liệu có đề ngày về biên bản họp đánh giá sau sự cố hoặc báo cáo sau đó cho thấy các bài học kinh nghiệm liên quan đến kết quả kiểm thử kế hoạch ứng phó sự cố an ninh mạng, hoặc ứng phó thực tế Sự cố an ninh mạng cần báo cáo, hoặc tài liệu có đề ngày nêu rõ không có bài học kinh nghiệm nào được rút ra;
2. Kế hoạch ứng phó sự cố an ninh mạng sửa đổi có đề ngày, nêu rõ mọi thay đổi dựa trên các bài học kinh nghiệm; và
3. Bằng chứng về việc phân phát bản cập nhật kế hoạch, bao gồm nhưng không giới hạn:
   - Email;
   - USPS hoặc dịch vụ bưu chính khác;
   - Hệ thống phân phối điện tử; hoặc
   - Phiếu kí tên tham gia đào tạo.

Ứng phó và phục hồi – Kế hoạch phục hồi cho Hệ thống an ninh mạng của BES

https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-7.pdf



1.1 Điều kiện kích hoạt kế hoạch phục hồi.

1.2 Vai trò và trách nhiệm của người ứng phó

1.3 Một hoặc nhiều quy trình sao lưu và lưu trữ thông tin cần thiết để phục hồi chức năng Hệ thống áp dụng.

1.4 Một hoặc nhiều quy trình để xác minh việc hoàn tất thành công các quy trình sao lưu trong Phần 1.3 và để xử lý mọi lỗi sao lưu.

1.5 Một hoặc nhiều quy trình để bảo toàn dữ liệu, theo khả năng của hệ thống, nhằm xác định nguyên nhân sự cố an ninh mạng dẫn đến kích hoạt kế hoạch phục hồi. Việc bảo toàn dữ liệu không được cản trở hoặc hạn chế khả năng phục hồi.

Ứng phó và phục hồi – Kế hoạch phục hồi cho Hệ thống an ninh mạng của BES



https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-7.pdf

2.1 Kiểm tra từng kế hoạch phục hồi được dẫn chiếu trong Yêu cầu R1 ít nhất 15 tháng dương lịch/lần:

- Thông qua phục hồi sau một sự cố thực tế;
- Thông qua bài tập trên giấy hoặc tại bàn;
- Thông qua một diễn tập thực hành

2.2 Kiểm tra mẫu thông tin đại diện được sử dụng để khôi phục chức năng Hệ thống áp dụng ít nhất **15 tháng dương lịch/lần** để đảm bảo rằng thông tin có thể sử dụng được và tương thích với cấu hình hiện tại.

2.3 Kiểm tra từng kế hoạch phục hồi được dẫn chiếu trong Yêu cầu R1 ít nhất **36 tháng dương lịch/lần** thông qua diễn tập thực hành các kế hoạch phục hồi trong môi trường đại diện cho môi trường sản xuất.

Tóm tắt

- Yêu cầu xây dựng kế hoạch ứng phó sự cố
- Yêu cầu diễn tập, thực hành và cập nhật
- Nghĩa vụ kiểm toán và nộp báo cáo theo quy định
- Mỗi loại đều có:
  - Dòng thời gian rõ ràng
- NERC-CIP
  - Xác định các hệ thống trong phạm vi điều chỉnh của tiêu chuẩn
  - Xác định tài liệu cần nộp cho kiểm toán
  - Mức độ nghiêm trọng của vi phạm

Nghiên cứu trường hợp xử lý sự cố

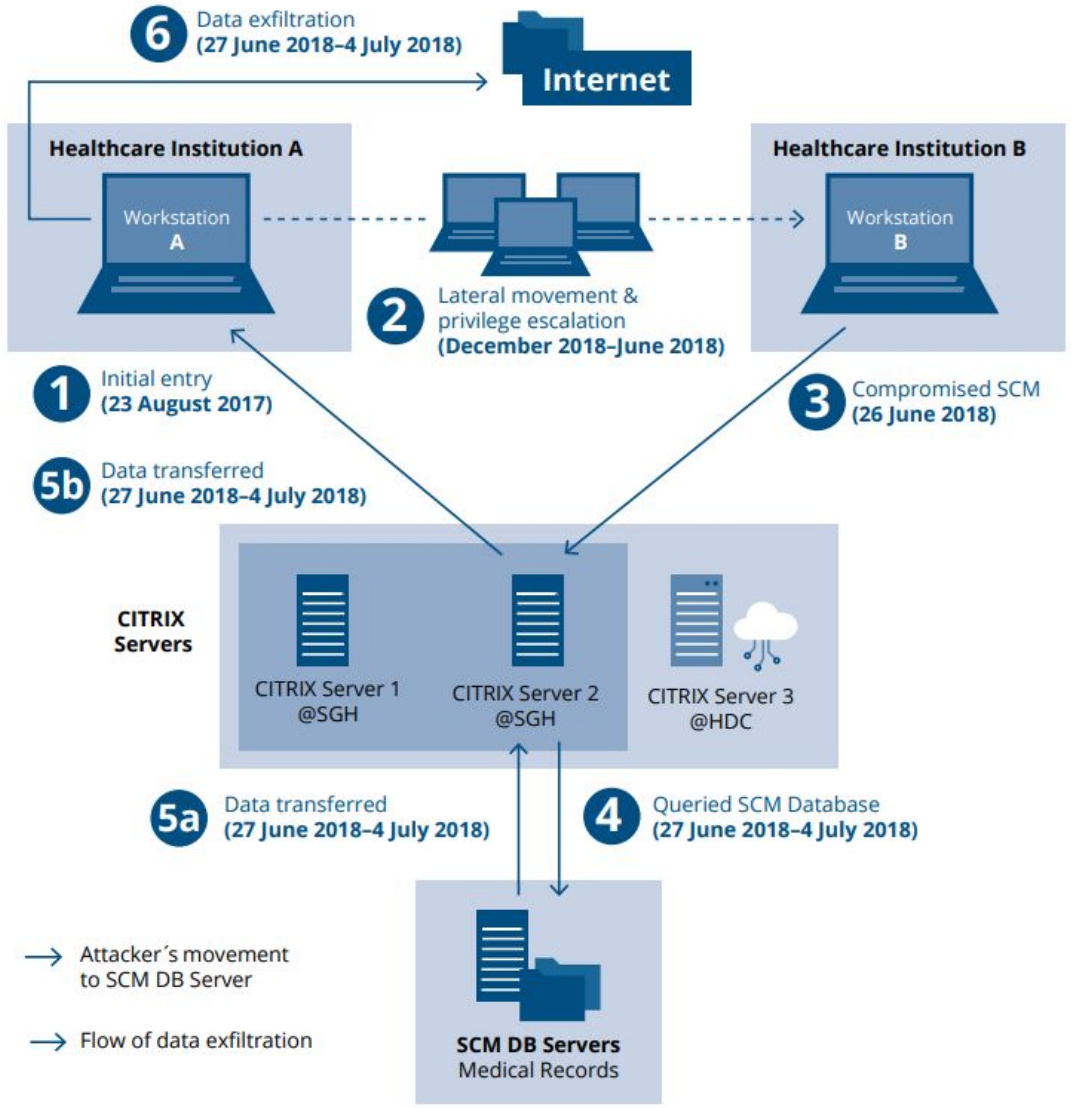
DNV ©

Vụ Vi phạm dữ liệu SingHealth 2018
Bối cảnh

- 1,5 triệu bệnh nhân SingHealth và hồ sơ thuốc được cấp phát ngoại trú của 160.000 bệnh nhân bị đánh cắp
- Hồ sơ bệnh án của Thủ tướng bị nhắm mục tiêu cụ thể
- Vi phạm dữ liệu được phát hiện vào ngày 4 tháng 7 năm 2018
- Điều tra cho thấy kẻ tấn công đã vào mạng từ tháng 12 năm 2017 **(6 tháng)**

Chi tiết về cuộc tấn công

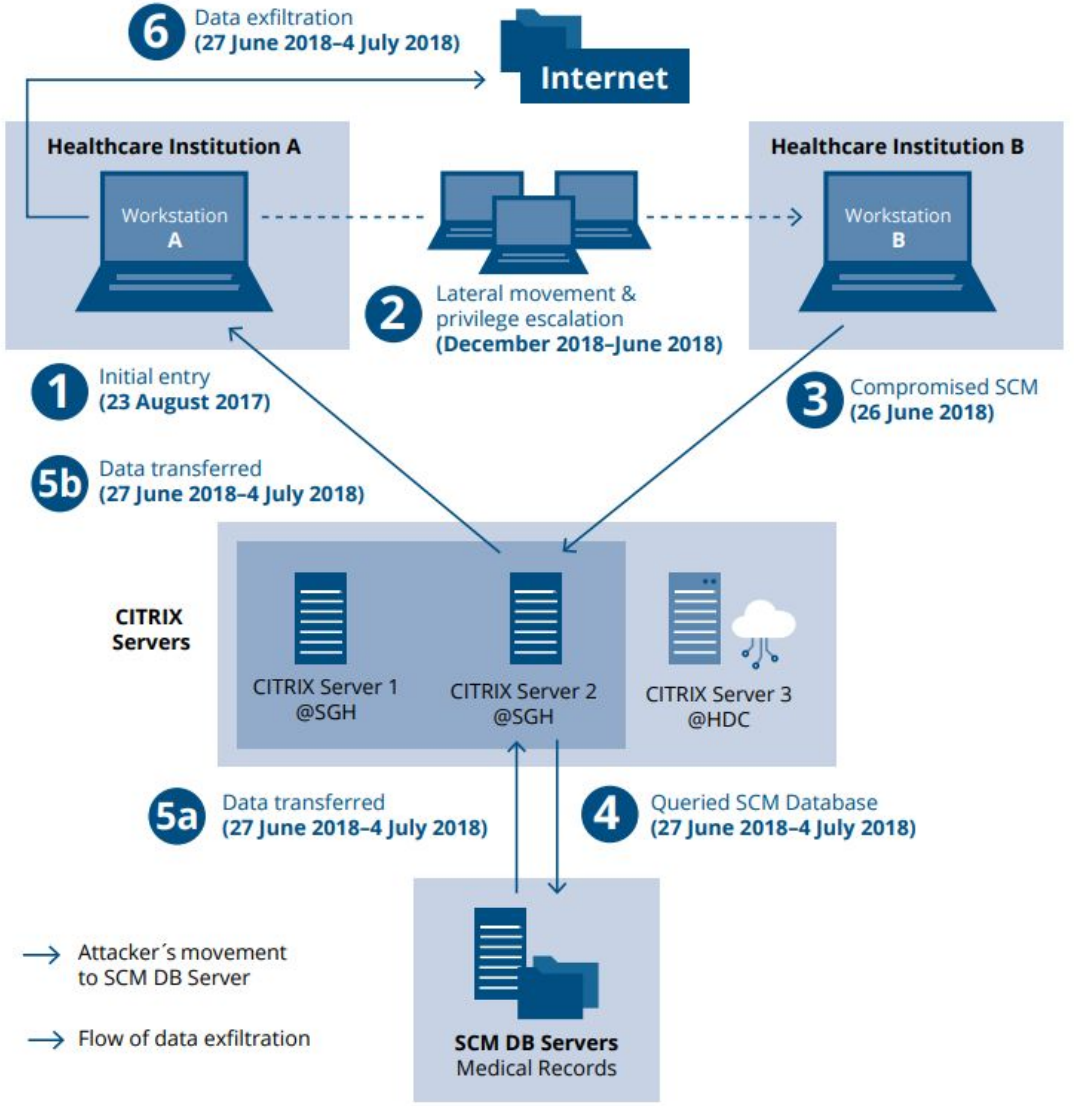
1. Đột nhập ban đầu thông qua payload đính kèm trên email lừa đảo. Khai thác lỗ hổng chưa được vá trên máy khách Outlook
2. Di chuyển theo chiều ngang & leo cao hơn theo đặc quyền (17/12 – 18/6)
3. Xâm phạm máy lưu trữ ứng dụng SCM
4. Truy vấn Cơ sở dữ liệu thông qua ứng dụng SCM cho hồ sơ bệnh án
5. Lọc dữ liệu qua máy bị xâm nhập ban đầu



DNV ©

Khám phá mối đe dọa vi phạm

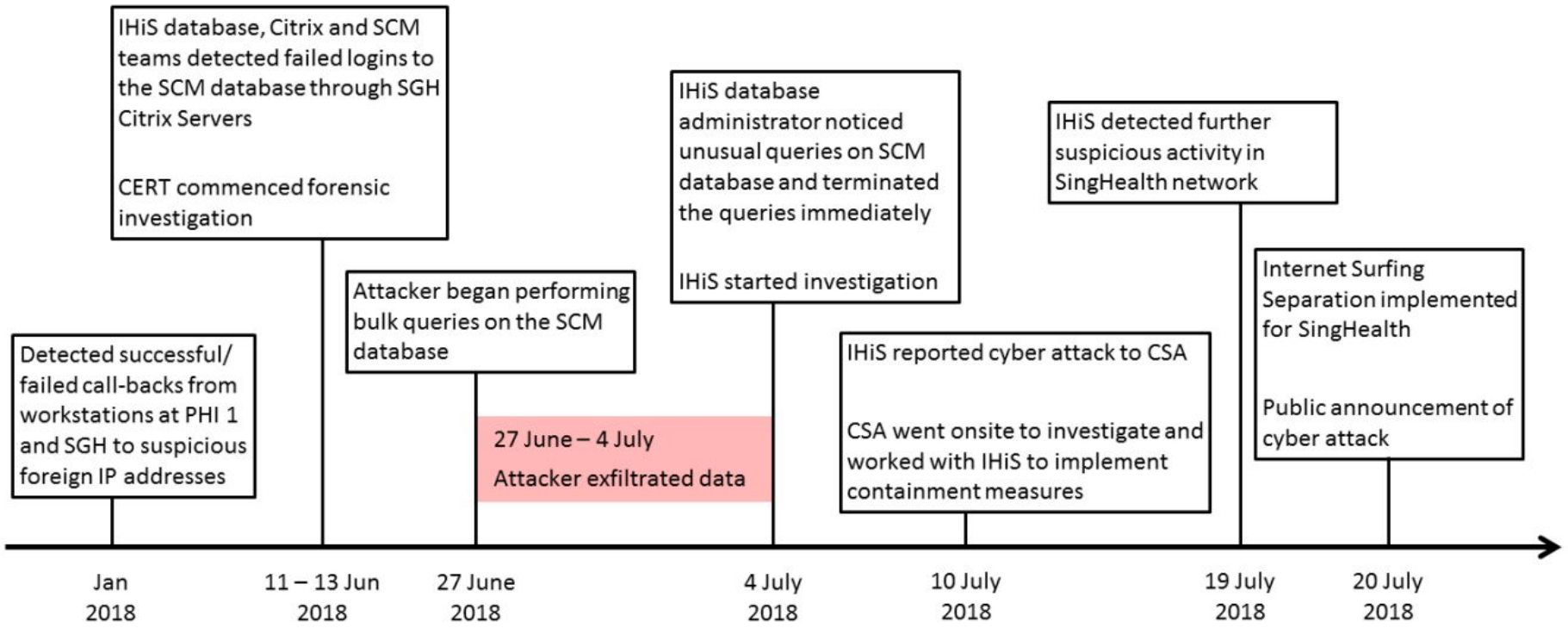
- Hoạt động xâm nhập bị Quản trị viên cơ sở dữ liệu phát hiện vào ngày 4 tháng 7 năm 2018 trong quá trình bảo trì định kỳ.
- Quản trị viên cơ sở dữ liệu nhận thấy số lượng lớn truy vấn khối lượng lớn đã được thực thi.
- 6 ngày trước khi sự việc được báo cáo cho chính phủ sau khi các truy vấn được tạo lại và tìm thấy dữ liệu trả về.



DNV ©

Vụ Vi phạm dữ liệu SingHealth 2018
Báo cáo COI

Figure 12: Timeline of events pertaining to IHiS' incident response



singhealthcoi.pdf (go.gov.sg)

Lỗi xử lý sự cố vi phạm

- Nhân viên CNTT nhận thấy lỗi đăng nhập trên máy chủ SCM nhiều tháng trước khi phát hiện ra mối đe dọa. Sự cố không được báo cáo, không có văn bản nào về việc báo cáo những quan sát không chắc chắn.
- Trưởng nhóm Ứng phó sự cố an ninh (SIRT) đã được thông báo về các quan sát lỗi đăng nhập nhưng không kích hoạt SIRT.
- Không có văn hóa báo cáo những quan sát bất thường.
  - “người khai báo quan sát bất thường cảm thấy ngại ngùng” –Báo cáo COI
- SCM máy chủ chưa được vá do sự sơ suất của đội ngũ quản lý.
- Các truy vấn SQL khối lượng lớn không được phát hiện trong khoảng 8 ngày (27 tháng 6 – 8 tháng 7).

DNV ©

Vụ Vi phạm dữ liệu SingHealth 2018
Hậu quả sau đó và hành động khắc phục

- SingHealth đã bị cô lập khỏi Internet như một phần của quá trình xử lý sự cố và vẫn duy trì như vậy cho đến ngày nay
- 2 nhân viên bị sa thải, 1 nhân viên bị giáng chức
- Lãnh đạo cấp cao IHIS bị phạt cá nhân
- Tất cả nhân viên CNTT phải được đào tạo về cách xác định sự cố an ninh mạng
- Tất cả các sự cố CNTT đáng ngờ sẽ phải được báo cáo trong vòng 24 giờ
- Các công cụ kiểm soát và giám sát bổ sung đã được đưa ra để giám sát mạng
- Các nguồn lực và nhiệm vụ bổ sung đã được đưa ra để cập nhật và vá các hệ thống dễ bị tổn thương
- Hướng dẫn quốc gia về quản lý CII được ban hành ngày 1 tháng 9 năm 2018

Tài liệu tham khảo

- https://file.go.gov.sg/singhealthcoi.pdf (Báo cáo COI)
- https://www.kas.de/documents/288143/14393910/4.1+Prevention+is+No+Cure.pdf/93ae2097-91a7-6ddd-9e83-d5723f69bde0?t=1654138595653
- https://en.wikipedia.org/wiki/2018_SingHealth_data_breach
- https://www.todayonline.com/singapore/singhealth-cyber-Attack-result-human-lapses-it-system-weaknesses-coi-report
- https://www.todayonline.com/singapore/ihis-deputy-director-shocked-find-data-stolen-after-being-told-otherwise)
- https://medium.com/digital-asia-ii/prevent-is-no-cure-26e9e2e1c7f5#_ftn27
- https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/scm-services-set-an-instance-to-start-automatically?view=sql-server-ver16

DNV

Yêu cầu quy định về an ninh mạng – Phần 2

Quản lý an ninh mạng trong ngành điện

Wei.Ming.Quek@dnv.com
+65 9827 8699

www.dnv.com

DNV ©