CHƯƠNG 1

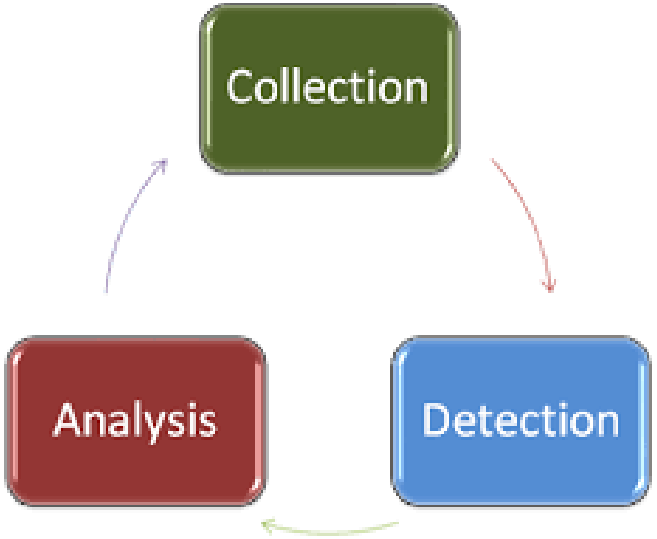
GIỚI THIỆU GIÁM SÁT AN TOÀN MẠNG

NỘI DUNG

1. Khái niệm và thuật ngữ
2. Các hệ thống liên quan
3. Hệ thống NSM
4. Một số ứng dụng của NSM

1. KHÁI NIỆM VÀ THUẬT NGỮ

- Có thể bảo vệ máy tính và dữ liệu khỏi tội phạm mạng bằng nhiều cách khác nhau
- Một cách hiệu quả nhất để thực hiện việc này là thực thi *giám sát an toàn mạng* - ***network security monitoring - NSM***
- NSM bao gồm:
  - Thu thập dữ liệu
  - Phát hiện xâm nhập
  - Phân tích dữ liệu an ninh mạng



NSM KHÔNG PHẢI LÀ

Quản lý thiết bị

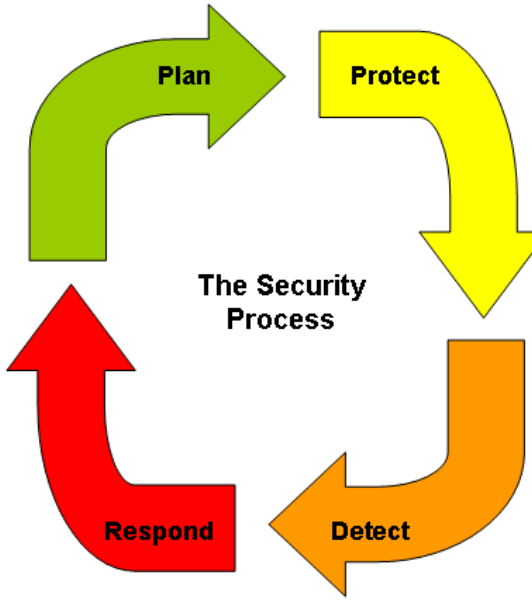
Quản lý sự kiện an ninh

Điều tra số cho mạng máy tính

Ngăn chặn xâm nhập

NSM được phân loại theo các miền sau:

- Bảo vệ:
  - ngăn chặn xâm nhập và khai thác trái phép vào hệ thống
- Dò tìm (phát hiện):
  - phát hiện ra tấn công đang xảy ra hoặc đã xảy ra trước đây
- Đáp ứng/Phản ứng:
  - phản ứng lại sau khi có một tấn công đã xảy ra
- Duy trì:
  - quản lý con người, các tiến trình và công nghệ liên quan đến việc bảo vệ mạng máy tính (Computer Network Defense - CND)



CÁC THUẬT NGỮ

- Tài sản (Asset):
  - Đề cập đến những gì thuộc phạm vi mạng tin cậy của một tổ chức: là bất cứ thứ gì có giá trị trong tổ chức, bao gồm máy tính, máy chủ, thiết bị mạng,…
  - Ngoài ra, tài sản còn bao gồm dữ liệu, con người, quy trình, sở hữu trí tuệ và danh tiếng của tổ chức.

CÁC THUẬT NGỮ

- Nguy cơ (đe dọa) (Threat): là một bên có khả năng và ý định khai thác một lỗ hổng trong một tài sản. Gồm :
  - Nguy cơ có cấu trúc: sử dụng chiến thuật và thủ tục hành chính, và đã xác định được rõ mục tiêu
  - Nguy cơ không có cấu trúc: không có động cơ, kỹ năng, chiến lược, hoặc kinh nghiệm

CÁC THUẬT NGỮ

- Lỗ hổng (Vulnerability):
  - Là một phần mềm, phần cứng, hoặc một điểm yếu thủ tục mà có thể hỗ trợ kẻ tấn công đạt được quyền truy cập trái phép vào một tài sản mạng
    - Ví dụ như một hệ thống xác thực không đúng cách sẽ có thể cho phép kẻ tấn công đoán ra tên đăng nhập của người dùng.
  - Chú ý là con người cũng có thể được coi là một lỗ hổng

CÁC THUẬT NGỮ

- Khai thác (Exploit):
  - Là phương pháp tấn công một lỗ hổng.
    - Ví dụ, trong trường hợp khai thác phần mềm, đoạn mã khai thác có thể chứa payload (tải) cho phép kẻ tấn công thực hiện một số hành động trên hệ thống từ xa (như sinh ra lệnh shell);
    - trong một ứng dụng web, lỗ hổng trong cách xử lý đầu vào và đầu ra có thể cho phép kẻ tấn công khai thác ứng dụng với SQL injection.

CÁC THUẬT NGỮ

- Rủi ro (risk):
  - Là khả năng có một mối đe dọa nhằm khai thác một lỗ hổng
  - Việc xác định định lượng rủi ro là một điều khó khăn vì nó liên quan đến việc đặt một giá trị trên mạng và tài sản dữ liệu
- Bất thường (Abnomaly):
  - Là một sự kiện quan sát được trong hệ thống hoặc mạng được coi là khác thường
    - Ví dụ bất thường có thể là một hệ thống bị sập, các gói tin bị thay đổi,…
  - Bất thường tạo ra các cảnh bảo bởi các công cụ phát hiện, như hệ thống phát hiện xâm nhập trái phép, hoặc các ứng dụng xem xét nhật ký (log).

CÁC THUẬT NGỮ

- Sự cố (Incident):
  - Một sự cố là sự vi phạm hoặc nguy cơ sắp xảy ra có liên quan đến các chính sách bảo mật máy tính, các chính sách sử dụng chấp nhận hoặc các chính sách bảo mật chuẩn
  - Sự cố là một điều xấu đã xảy ra, hoặc đang diễn ra trên mạng của tổ chức
    - Ví dụ, có một tấn công vào thư mục gốc của một máy tính, cài đặt phần mềm độc hại đơn giản, tấn công từ chối dịch vụ, hoặc thực thi thành công mã độc từ một email (thư điện tử) giả mạo

2. CÁC HỆ THỐNG LIÊN QUAN

2.1. Hệ thống phát hiện xâm nhập

- Phát hiện xâm nhập là một thành phần của NSM hiện đại

- Đặc điểm:
  - Bảo vệ (phòng thủ) lỗ hổng bảo mật
  - Phát hiện trong tập dữ liệu quan trọng
  - Phần lớn dựa trên chữ ký
  - Cố gắng phân tích tự động hoàn toàn

2.2. Một số hệ thống khác

- Quản lý sự kiện và thông tin bảo mật (Security Information and Event Management - SIEM)
  - hệ thống có khả năng thu thập, tổng hợp và lọc, hợp nhất, lưu trữ và tìm kiếm, tương quan, thông báo và phản hồi, trực quan hóa, phân tích cú pháp/điều tra các sự kiện an toàn thông tin
  - SIEM là sản phẩm, cũng có thể coi như một quy trình

2.2. Một số hệ thống khác

- Các quy trình được xây dựng xung quanh một sản phẩm SIEM có thể chia thành ba nhóm:
  1. Các quy trình cơ bản (hỗ trợ): Thu thập, đánh giá, Cái đặt
  2. Quy trình tuân thủ mô tả các quy trình sau: Xem xét báo cáo, Phản ứng với việc không tuân thủ quy định
  3. Các quy trình liên quan đến giám sát và điều tra liên tục trong thời gian thực: Xử lý thông báo sự cố, Lập hồ sơ hành vi, Phân tích đánh giá, Giảm khả năng tái xuất sự cố…

2.2. Một số hệ thống khác

- Trung tâm điều hành an ninh (Security Operations Center - SOC):
  - nhóm bảo mật thông tin tập trung làm việc để *giảm thiểu rủi ro của tổ chức*, chịu trách nhiệm theo dõi và phân tích bảo mật của tổ chức bằng cách sử dụng các công nghệ và quy trình để phát hiện, ngăn chặn, phân tích và giảm thiểu sự cố
  - SOC=“nền tảng SIEM + quy trình SIEM + nhân sự”

2.2. Một số hệ thống khác

- Các công cụ cần cho SOC:
  - EDR (Endpoint detection and response - Phát hiện và phản hồi điểm cuối)
  - NDR (Network detection and response - Phát hiện và phản hồi mạng)
  - XDR (Extended Detection and Response - Phát hiện và phản hồi mở rộng)
  - MDR (Managed detection and response - Phát hiện và phản hồi được quản lý)

3. HỆ THỐNG NSM

3.1. Giới thiệu NSM

- NSM xuất phát và được ủng hộ bởi những người/tổ chức có tư duy phòng thủ, ví dụ như trong quân đội, nơi mà các hoạt động có tầm quan trọng và dữ liệu cần có tính bảo mật cao
- Các hoạt động và mục tiêu có thể là:
  - Phá hủy, Phá vỡ,
  - Làm suy giảm, Từ chối, Đánh lừa, Khai thác, Gây ảnh hưởng,
  - Bảo vệ, Phát hiện, Khôi phục, Ứng phó

Các đặc tính của NSM

- Các đặc tính của NSM khác biệt hoàn toàn so với phát hiện xâm nhập truyền thống:
  - Phòng chống đến cùng cho dù thất bại

➔ Khi đã chấp nhận là cuối cùng tài sản có thể bị tổn hại, thì các tổ chức sẽ thay đổi cách bảo vệ tài sản của họ. Thay vì chỉ dựa vào phòng thủ, các tổ chức cần tập trung thêm vào việc phát hiện và phản ứng.

Các đặc tính của NSM

- Tập trung vào tập dữ liệu
  - Chỉ cung cấp cho các chuyên gia phân tích những dữ liệu mà họ cần thì họ có thể đưa ra quyết định nhanh và an toàn hơn nhiều
- Tiến trình theo chu trình
  - Mô hình phát hiện xâm nhập cũ là một tiến trình tuyến tính ➔ đơn giản và thiếu trách nhiệm
  - Tiến trình phát hiện và ứng phó với xâm nhập cần phải có tính chu trình

Các đặc tính của NSM

- Phòng thủ theo nguy cơ
  - *Phòng thủ theo lỗ hổng* tập trung vào "làm thế nào", thì *phòng thủ theo nguy cơ* tập trung vào "ai" và "tại sao"
  - Khó khăn do:
    1. Tầm nhìn sâu rộng vào hệ thống mạng của tổ chức
    2. Khả năng thu thập và phân tích thông tin tình báo liên quan đến mục đích và khả năng của kẻ tấn công.

3.2. Phòng thủ theo lỗ hổng bảo mật và phòng thủ theo mối đe dọa

- Phòng thủ theo **lỗ hổng bảo mật**
  - Tương đương *xây bức tường gạch*
    - Vững chắc
    - Bảo vệ được nhiều mục tiêu
  - Vấn đề:
    - Gạch hỏng theo thời gian, cần khắc phục liên tục
- Phòng thủ theo **nguy cơ**
  - Tương đương *dùng thủ môn bảo vệ*
    - Có thể bị thất bại trong những lần đầu
    - Tích lũy kinh nghiệm để phát triển, thay đổi chiến thuật bảo vệ phù hợp
  - Ưu điểm:
    - Học, thích nghi, và phát triển

SO SÁNH

Phòng thủ theo lỗ hổng bảo mật	Phòng thủ theo nguy cơ
• Dựa vào kỹ thuật phòng chống • Tập trung vào phát hiện xâm nhập • Giả thiết có thể biết được tất cả các nguy cơ • Phân tích mỗi tấn công trong ngữ cảnh đơn giản • Phụ thuộc nhiều vào phát hiện dựa trên chữ ký • Ít khả năng phát hiện ra các nguy cơ chưa biết • Tiến trình tuyến tính	• Biết rằng việc phòng chống cuối cùng sẽ thất bại • Tập trung vào tập dữ liệu • Biết rằng các nguy cơ sẽ sử dụng các công cụ, chiến thuật và thủ tục khác nhau • Kết hợp thông minh từ mọi tấn công • Sử dụng toàn bộ dữ liệu nguồn • Rất có khả năng phát hiện ra các hoạt động tấn công ngoài những dấu hiệu đã biết • Tiến trình theo chu trình

3.3. Chu trình giám sát an toàn mạng

Bước 1: Thu thập dữ liệu

- Bước bắt đầu, quan trọng nhất
  - Sự kết hợp của cả phần cứng và phần mềm
  - Tạo, sắp xếp và lưu trữ dữ liệu cho việc phát hiện xâm nhập và phân tích dữ liệu trong hệ thống NSM
  - Định hình khả năng của một tổ chức trong việc phát hiện xâm nhập và phân tích dữ liệu hiệu quả
- Các loại dữ liệu
  - Dữ liệu nội dung đầy đủ
  - Dữ liệu phiên
  - Dữ liệu thống kê
  - Dữ liệu kiểu chuỗi trong gói tin
  - Dữ liệu cảnh báo

Bước 1: Thu thập dữ liệu

- Cần nhiều lao động nhất trong chu trình NSM
- Cần nỗ lực từ lãnh đạo tổ chức, đội ngũ an ninh thông tin, các nhóm mạng và các nhóm quản trị hệ thống
- Bao gồm các nhiệm vụ:
  - Xác định các vị trí có nhiều điểm yếu tồn tại trong tổ chức
  - Xác định các nguy cơ ảnh hưởng đến mục tiêu tổ chức
  - Xác định nguồn dữ liệu có liên quan
  - Tinh chế nguồn dữ liệu thu thập được
  - Cấu hình cổng SPAN để thu thập dữ liệu gói tin
  - Xây dựng lưu trữ SAN cho lưu giữ nhật ký
  - Cấu hình phần cứng và phần mềm thu thập dữ liệu

Bước 2: Phát hiện xâm nhập

- Là quá trình mà qua đó dữ liệu thu thập được kiểm tra và cảnh báo sẽ được tạo ra dựa trên các sự kiện quan sát được và dữ liệu thu thập không được như mong đợi
- Được thực hiện thông qua một số hình thức chữ ký, sự bất thường, hoặc phát hiện dựa trên thống kê.
- Kết quả là tạo ra các dữ liệu cảnh báo

Bước 2: Phát hiện xâm nhập

- Thường là một chức năng của phần mềm với một số gói phần mềm phổ biến
  - Snort IDS và Bro IDS của một hệ thống phát hiện xâm nhập mạng (NIDS), và OSSEC, AIDE hoặc McAfee HIPS của một hệ thống phát hiện xâm nhập máy chủ (HIDS).
- Một số ứng dụng như Quản lý sự kiện và thông tin an ninh (Security Information and Event Management - SIEM) sẽ sử dụng cả dữ liệu dựa trên mạng và dữ liệu dựa trên máy chủ để phát hiện xâm nhập dựa trên các sự kiện liên quan

Bước 3: Phân tích dữ liệu

- Diễn giải và xem xét dữ liệu cảnh báo
- Cần xem xét thu thập dữ liệu bổ sung từ các nguồn dữ liệu khác
- Gồm:
  - Phân tích gói tin
  - Phân tích mạng
  - Phân tích máy chủ
  - Phân tích phần mềm độc hại

Bước 3: Phân tích dữ liệu

- Là phần tốn thời gian nhất trong chu trình NSM
- Một sự kiện có thể được chính thức nâng lên thành sự cố, và bắt đầu với các biện pháp ứng phó
- Chu trình NSM kết thúc bằng các bài học kinh nghiệm trong việc phát hiện xâm nhập và phân tích dữ liệu cho bất kỳ sự bất thường nào và tiếp tục hình thành các chiến lược thu thập dữ liệu cho tổ chức

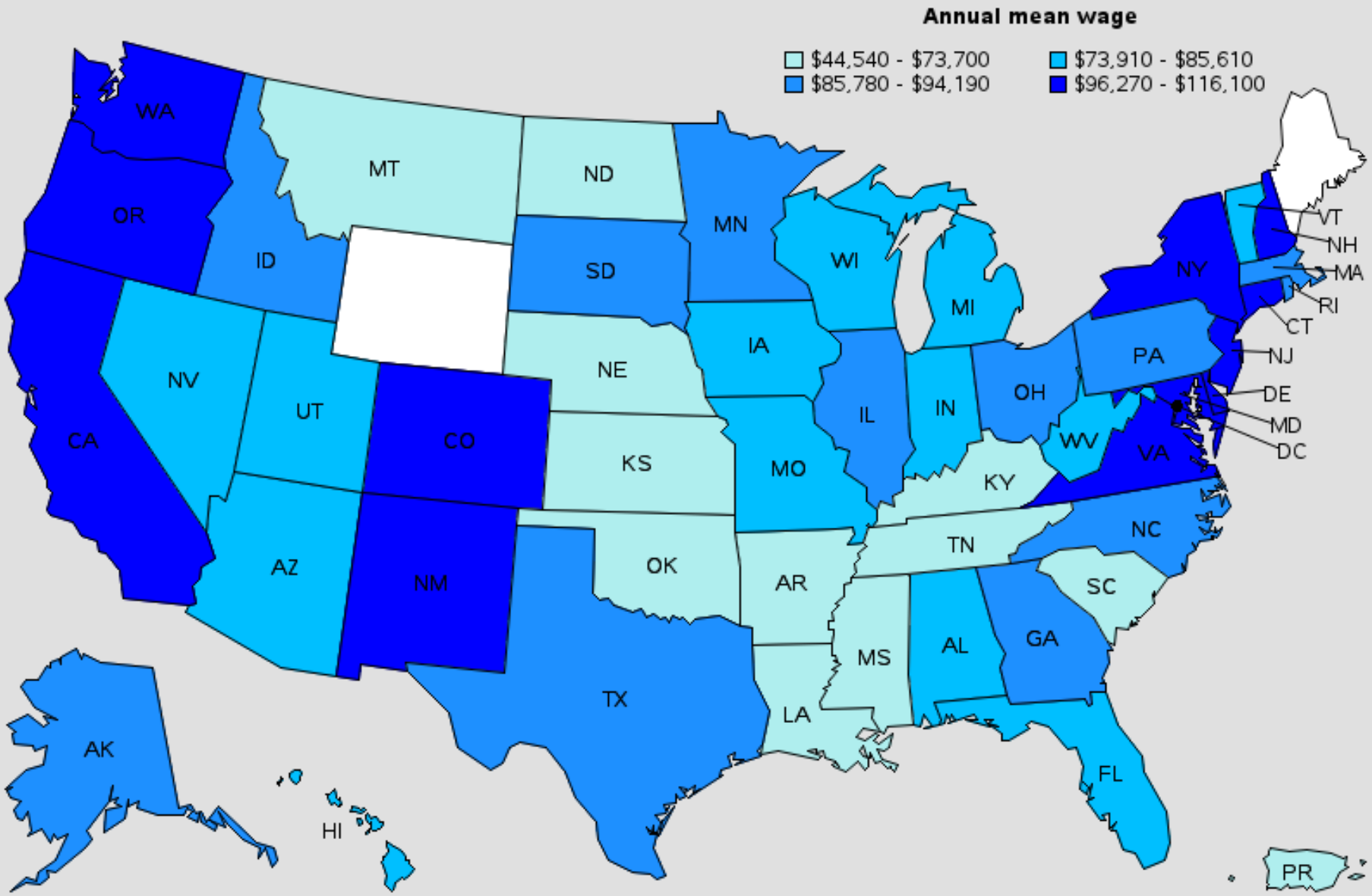
3.4 Thách thức đối với hệ thống NSM

- Là lĩnh vực mới nên khó khăn trong việc chuẩn hóa thuật ngữ và phương pháp: giữa lý thuyết và thực hành
- Nguồn nhân lực về NSM không đủ đáp ứng yêu cầu về kinh nghiệm và kiến thức cần thiết
- Chi phí cần thiết để thiết lập và duy trì một chương trình NSM:
  - Phần cứng cần thiết để thu thập và phân tích lượng dữ liệu lớn
  - Lao động cần thiết làm phân tích NSM
  - chi phí để hỗ trợ cơ sở hạ tầng NSM cho các chuyên gia phân tích

3.5 Nhân sự cho hệ thống NSM

- Là thành phần quan trọng nhất của một hệ thống NSM
- An toàn hệ thống mạng của một tổ chức phụ thuộc vào khả năng làm việc hiệu quả của các chuyên gia phân tích
- Sẽ diễn giải dữ liệu cảnh báo, phân tích và xem xét xem những dữ liệu nào có liên quan đến nhau; xác định xem sự kiện xảy ra có phải là thật hay không, hay cần có những phân tích và điều tra thêm
- Có thể tham gia vào quá trình ứng phó sự cố hoặc thực hiện các nhiệm vụ khác như phân tích máy tính hoặc phân tích phần mềm độc hại
- Yêu cầu: Phải thường xuyên được cập nhật các công cụ, các chiến thuật và thủ tục mới nhất mà đối phương có thể sử dụng

Annual mean wage of information security analysts, by state, May 2015



Blank areas indicate data not available.

Kỹ năng cần thiết:

- Phòng thủ theo nguy cơ, NSM, và chu trình NSM
- Chồng giao thức TCP/IP
- Các giao thức tầng ứng dụng
- Phân tích gói tin
- Kiến trúc Windows
- Kiến trúc Linux
- Phân tích dữ liệu cơ bản (BASH, Grep, SED, AWK,…)
- Cách sử dụng IDS (Snort, Suricata,…)
- Dấu hiệu tấn công và hiệu chỉnh chữ ký IDS
- Mã nguồn mở
- Phương pháp chẩn đoán phân tích cơ bản
- Phân tích phần mềm mã độc cơ bản

Phân loại chuyên gia phân tích

- Chuyên gia phân tích cấp 1 (L1)
  - Không có khả năng giải quyết vấn đề liên quan đến chuyên môn đặc biệt
  - Dành phần lớn thời gian của họ để xem xét các cảnh báo IDS và thực hiện phân tích dựa trên những phát hiện của họ
  - Làm việc chủ yếu dựa trên kinh nghiệm
  - phần lớn các chuyên gia phân tích thuộc loại L1

Phân loại chuyên gia phân tích

- Chuyên gia phân tích cấp 2 (L2)
  - L2 như là một người cố vấn cho L1
  - Tham gia vào việc hỗ trợ hình thành các tiến trình phát hiện xâm nhập trong nhóm bằng cách tạo chữ ký dựa trên các sự kiện mạng khác hoặc nghiên cứu OSINT (Open-source intelligence)
  - Thông qua các nguồn dữ liệu khác nhau bằng tay để cố gắng tìm các sự kiện tiềm tàng thay vì chỉ dựa vào các công cụ phát hiện tự động

Phân loại chuyên gia phân tích

- Chuyên gia phân tích cấp 3 (L3)
  - Chuyên gia phân tích cấp cao nhất trong một tổ chức
  - Được giao nhiệm vụ tư vấn cho các chuyên gia phân tích khác, phát triển và hỗ trợ đào tạo cũng như cung cấp các hướng dẫn về những điều tra phức tạp
  - Chịu trách nhiệm trong việc hỗ trợ để phát triển và tăng cường khả năng thu thập dữ liệu và phân tích xâm nhập cho tổ chức
  - Tạo và phát triển các công cụ mới, cũng như đánh giá các công cụ hiện có

4. MỘT SỐ ỨNG DỤNG CỦA NSM

Các trường hợp an toàn thông tin trong thực tế cần theo dõi giám sát liên tục:

1. Giám sát thực thể đặc quyền.
2. Xác thực thất bại do vét cạn.
3. Xác thực bất thường
4. Phiên bất thường.
5. Bất thường về tài khoản.
6. Các chỉ số lọc dữ liệu
7. Chữ ký khớp với kết quả quét lỗ hổng bảo mật đã biết
8. Bất kỳ lỗi dịch vụ nào thấy xuất hiện quá nhiều
9. Chỉ báo mối đe dọa từ bên trong
10. Các điều kiện lỗi của dữ liệu nhật ký bảo mật