AN TOÀN MẠNG MÁY TÍNH

Chương 4. Hệ thống giám sát an toàn thông tin

1. Tổng quan về hệ thống SIEM
2. Kiến trúc và thành phần
3. Triển khai vận hành SIEM
4. Phát hiện sự cố với SIEM

Giáo trình và Tài liệu tham khảo

1. TS. Lê Đình Thích & ThS. Hoàng Sỹ Tương, Giáo trình An toàn mạng máy tính, Học viện KTMM, 2013
2. Joseph Migga Kizza, Guide to Computer Network Security (Computer Communications and Networks) (4th Editiion), Springer, 2017
3. Mark Ciampa, Lab Manual for Security+ Guide to Network Security Fundamentals (5th Edition), Cengage Learning, 2015
4. Vincent J. Nestler, Keith Harrison, Matthew P. Hirsch and Wm. Arthur Conklin, Principles of Computer Security Lab Manual (4th Edition), McGraw-Hill Education, 2014
5. Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals 6th Edition, Cengage Learning, 2017

1. Tổng quan về hệ thống SIEM
2. Kiến trúc và thành phần
3. Triển khai vận hành SIEM
4. Phát hiện sự cố với SIEM

Operation Aurora (1/2)

- **2009, hãng Google bị dính hàng loạt vụ tấn công mang tên Operation Aurora.**
  - Ngoài ra, 30 tập đoàn lớn nữa cũng bị ảnh hưởng bởi loại mã độc này như Adobe, Juniper, Intel, Yahoo…

Operation Aurora (2/2)

❑ **Mã độc lây lan chủ yếu qua trình duyệt IE.**

- Người dùng bị lừa bấm vào 1 trang web độc hại
- Trình duyệt tải mã độc về máy nạn nhân
- Mã độc thực hiện liên kết tới C&C
- Leo thang đặc quyền
- Mật khẩu Active Directory bị lấy trộm và bẻ khóa
- Kết nối VPN với các tài khoản thu được
- Các dữ liệu có giá trị được gửi về Trung Quốc

➔ Các giải pháp bảo vệ thông thường như Anti-virus, Firewall không còn hiệu quả.

Need of SIEM (1/2)

- Giải pháp:
  - Proxy, Firewall, HIDS/NIDS, IPS…
- Nguy cơ:
  - "Control" thất bại
  - "Prevention" thất bại
  - "Initial detection" thất bại

Need of SIEM (2/2)

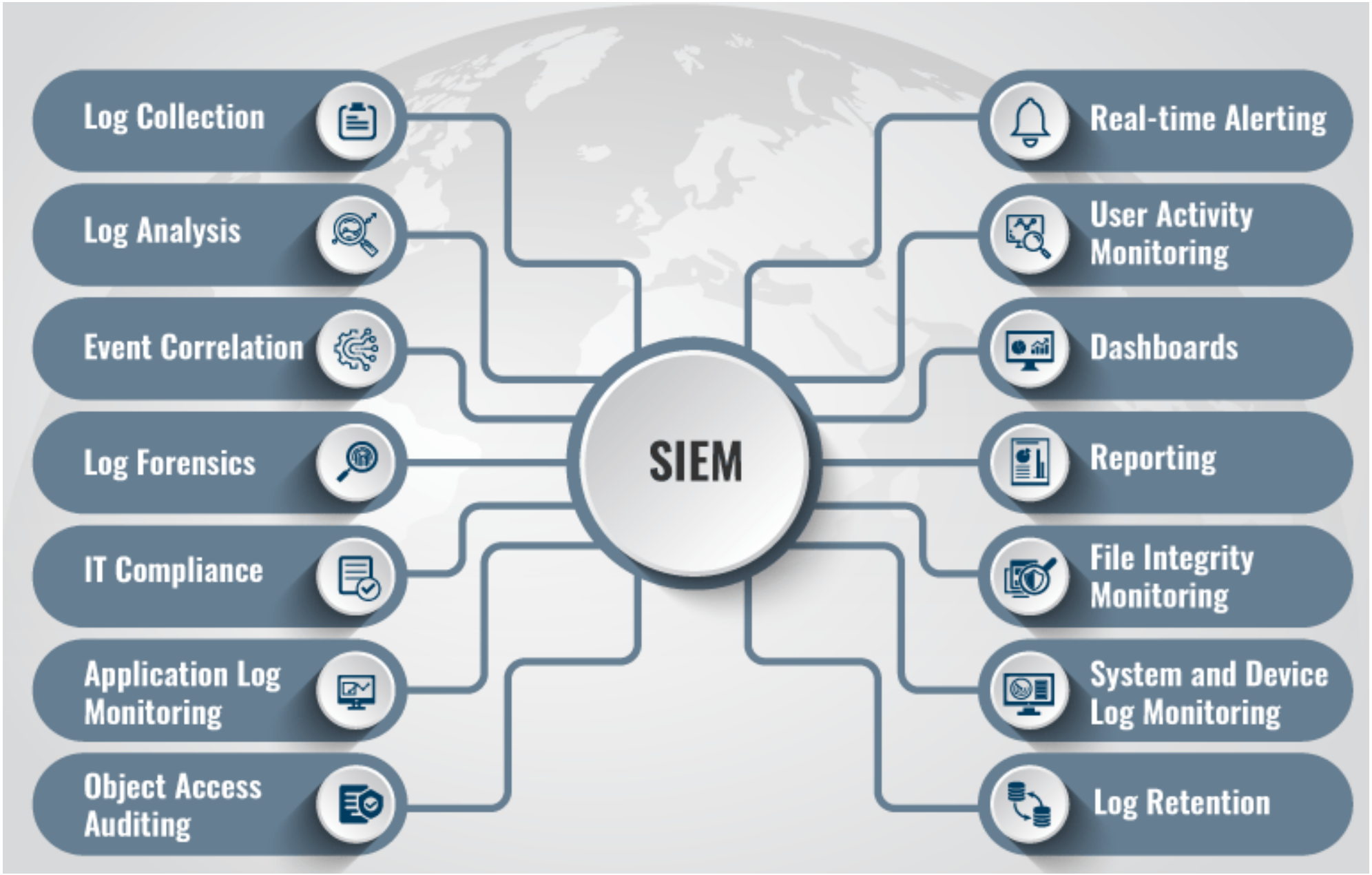
❑ Một số vấn đề:

- Không có khả năng phân tích toàn bộ nhật ký
- Số lượng cảnh báo lớn, phân tán
- Thiếu khả năng bao quát tổng thể hệ thống
- Khả năng phát hiện, phân tích và ưu tiên trong việc chống lại các mối đe dọa còn hạn chế
- Mỗi hệ thống có một định dạng nhật ký khác nhau, gây khó khăn cho việc phân tích
- Không có khả năng điều tra khi sự cố xảy ra
- Không đảm bảo tuân thủ các quy định về ATTT, quy định về audit

Security Information and Event Management (SIEM)

- Hệ thống giám sát an toàn thông tin (SIEM – Security information and event management) là hệ thống cốt lõi của SOC được thiết kế nhằm *thu thập* thông tin nhật ký sự kiện từ các thiết bị đầu cuối và *phân tích* chúng với mục đích phát hiện các hành vi lạ thường và kịp thời ứng phó, cho phép cơ quan/tổ chức hạn chế được các rủi ro, tiết kiệm thời gian và nhân lực.
- Nhiệm vụ chính của SIEM:
  - Log management: Thực hiện quản lý nhật ký hiểu quả
  - Security Analytics: Phát hiện các sự kiện an toàn theo thời gian thực (real-time)
- SIEM là sự kết hợp của 2 hệ thống trước đó là SIM (Security information management) và SEM (Security event management)
  - SEM thực hiện giám sát, tương quan sự kiện và quản lý sự cố
  - SIM thực hiện thu thập, lưu trữ, phân tích và đưa ra báo cáo

Typical SIEM Capabilities



Typical SIEM Capabilities

- Log Collection: SIEM thu thập logs từ nhiều nguồn khác nhau như hệ thống Windows, Unix/Linux, ứng dụng, DB, routers, switches…
  - Thu thập từ agent
  - Kết nối trực tiếp với thiết bị
- Log Analysis: Sử dụng các kỹ thuật như học máy, mô hình thống kê để xây dựng liên kết sâu hơn giữa các loại dữ liệu và tiến hành phân tích
- Event Correlation: Thực hiện liên kết các nguồn dữ liệu khác nhau có liên quan thành một sự kiện an toàn chính xác.
  - Tương quan dựa trên luật
  - Tương quan dựa trên thống kê
- Log Forensic: Quá trình phân tích chuyên sâu dữ liệu được lưu trữ để tái cấu trúc toàn bộ sự cố nhằm tìm ra nguyên nhân, nguồn gốc sự việc

Typical SIEM Capabilities

- IT Compliance: Khả năng tạo ra các báo cáo tuân thủ các tiêu chuẩn như HIPAA, PCI/DSS, FISMA, SOX, GLBA.
- Object access auditing: SIEM thông báo cho users về các thông tin liên quan đến tập tin và thư mục của họ như ai đã truy cập, ngày giờ chỉnh sửa, xóa…
- Real-time alerting: phân tích các sự kiện và gửi cảnh báo tới nhân viên chuyên trách
- User activity monitoring: cho phép theo dõi các hành vi đáng ngờ của người dùng
- Dashboards: Cung cấp công cụ, giao diện trực quan hóa dữ liệu và cho phép quản trị viên giao tiếp với dữ liệu được lưu trữ trong SIEM.
- Threat Hunting: Khả năng chủ động săn tìm các mối đe dọa và đưa ra các khuyến nghị nhằm ngăn chặn các mối đe dọa tìm được.
- Threat Intelligence Feeds: Sử dụng các dữ liệu hiện có kết hợp với nghiên cứu, cập nhật các lỗ hổng, các hoạt động đe dọa tiềm tàng, và sau đó ánh xạ với tài sản của khách hàng để thực hiện và nâng cao khả năng phòng thủ chủ động

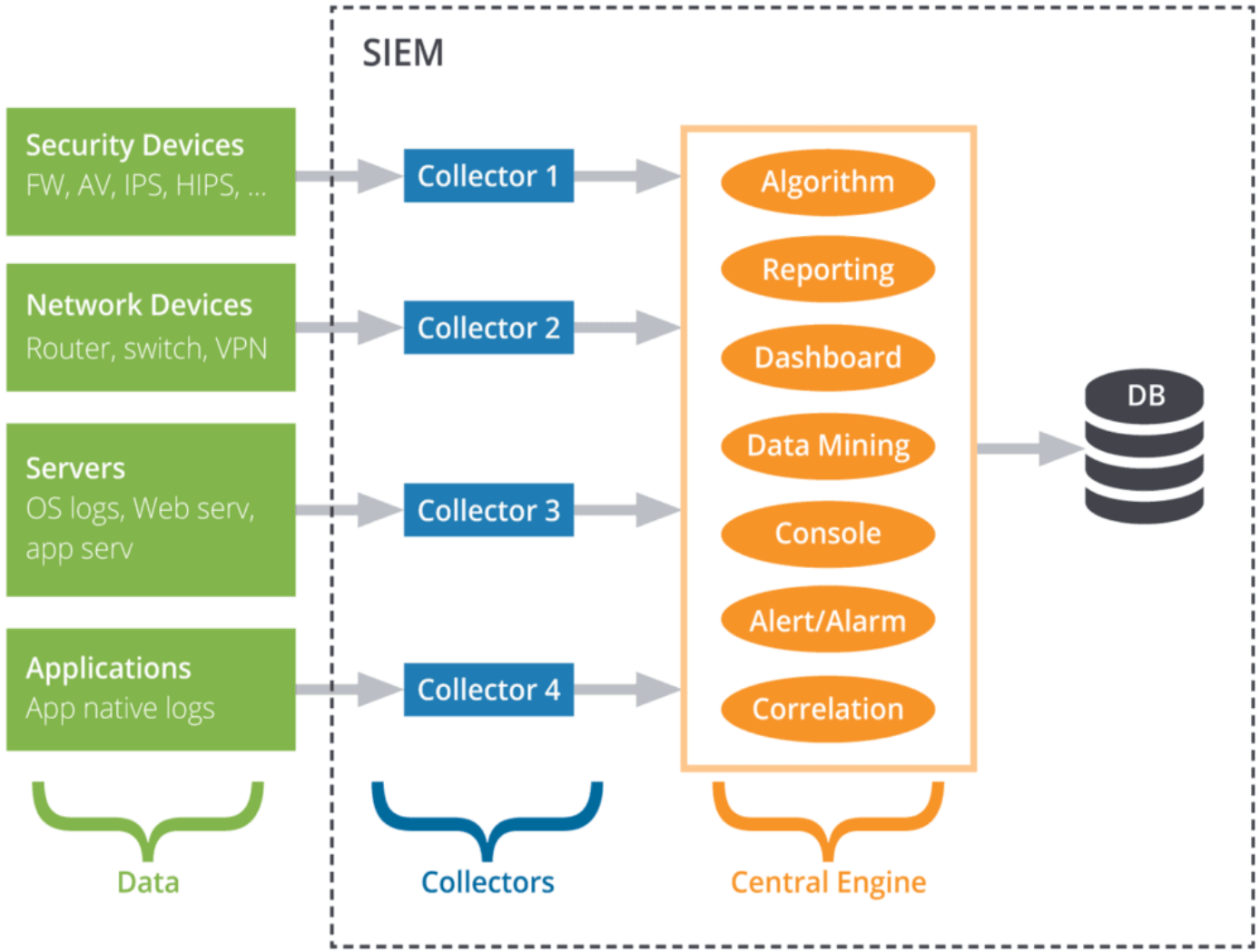
Typical SIEM Capabilities

- Incident Response: Dữ liệu thu thập được giúp đội ứng phó sự cố xác định nguồn gốc tấn công và phản ứng lại một cách nhanh nhất có thể.
- SOC Automation: Khả năng tự động ứng phó sự cố đối với các hệ thống SIEM tiên tiến
- File integrity monitory: Giám sát tính toàn vẹn của các tập tin nhạy cảm
- Log Retention: dữ liệu gửi tới SIEM cần phải lưu trữ với mục đích lưu giữ và truy vấn sau này.

1. Tổng quan về hệ thống SIEM
2. Kiến trúc và thành phần
3. Triển khai vận hành SIEM
4. Phát hiện sự cố với SIEM

SIEM Architecture and Its Component

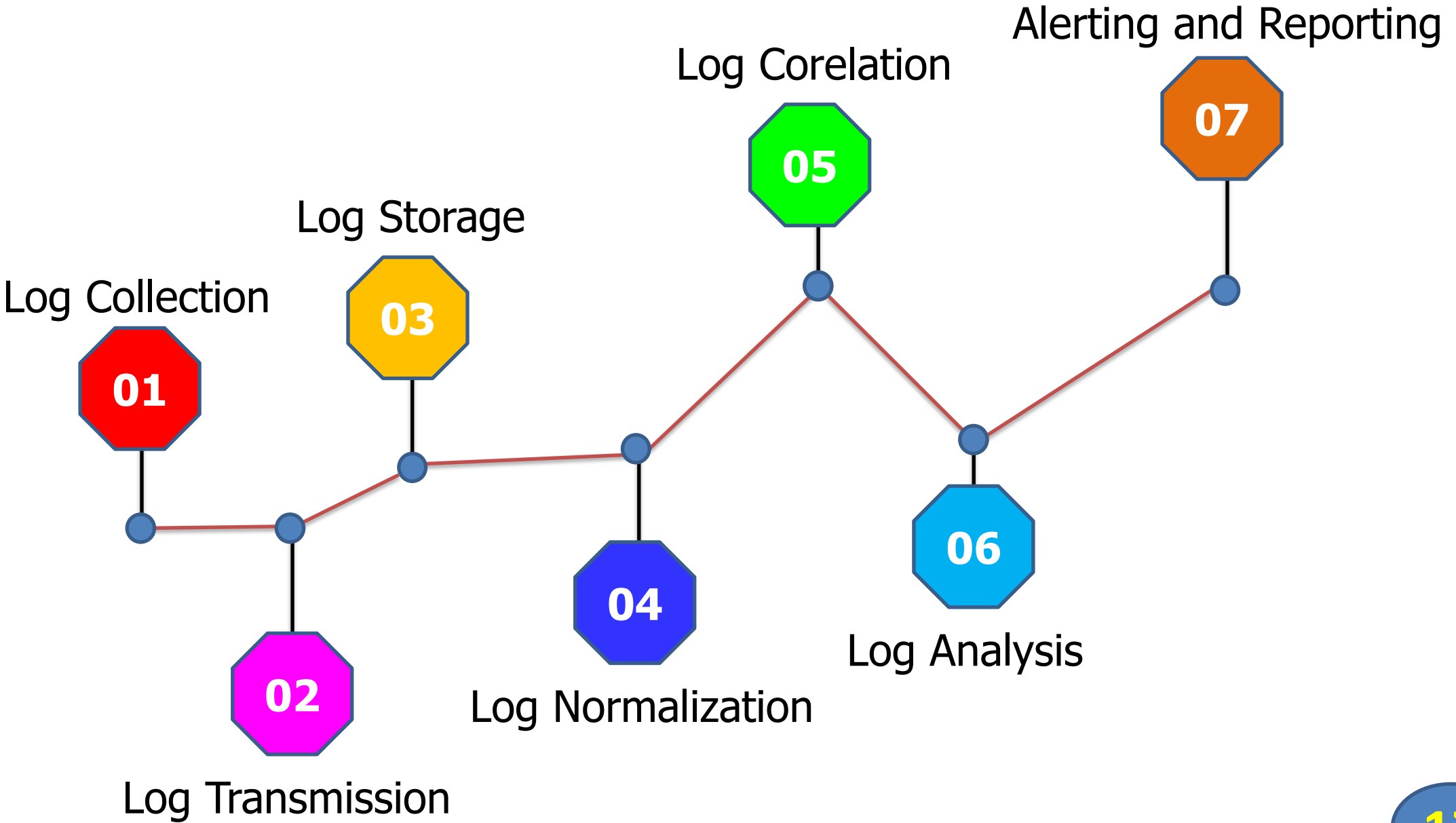
- SIEM bao gồm:
  - Thành phần thu thập dữ liệu (Collectors/agents/Connectors).
  - Thành phần quản trị tập trung (Central Engine).
  - Cơ sở dữ liệu (Database).
- SIEM thu thập dữ liệu từ:
  - Security devices – IDPS, FW…
  - Network devices – Routers, Switches, AP…
  - Servers – App Server, Databases…
  - Applications – Web App, SaaS App



SIEM Architecture and Its Component

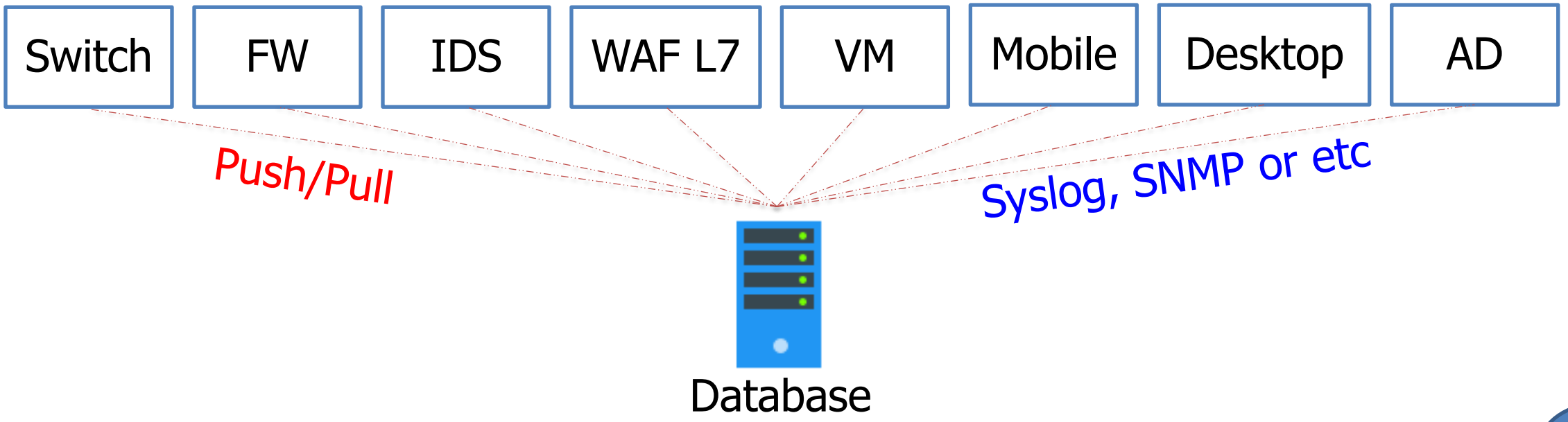
- ❑ Thành phần thu thập dữ liệu (Collector/agent/connector):
  - có chức năng thu nhận dữ liệu từ các nguồn về hệ thống giám sát.
- ❑ Thành phần quản trị tập trung (Central Engine):
  - Thành phần này tiếp nhận dữ liệu từ thành phần thu thập, thực hiện các chức năng chuẩn hóa, phân tích, tương quan sự kiện, cảnh báo sự cố, hiện thị thông tin sự kiện.
- ❑ Cơ sở dữ liệu(Database):
  - Sau khi sự kiện được chuẩn hóa thì sẽ được lưu vào cơ sở dữ liệu để tiện phục vụ khi cần tiến hành điều tra xử lý sự cố.

Centralized Logging, Monitoring and Analysis Process



Step 1: Log Collection

- Dữ liệu được gửi về từ nhiều nguồn khác nhau
- Dữ liệu được chia thành 2 loại
  - Nhật ký hệ thống (Event Logs) – sử dụng phương pháp đẩy/kéo (push/pull) để thu thập
  - Lưu lượng mạng (Traffic flow) – sử dụng hub, span port, network tap để thu thập



Step 2: Log Transmission

- Logs được gửi về nơi lưu trữ tập trung sử dụng các cơ chế truyền tải khác nhau. Cơ chế truyền tải logs hiệu quả phải đảm bảo:
  - Duy trì tính bí mật, toàn vẹn, sẵn sàng của logs
  - Tuân thủ trình tự sự kiện, đồng bộ thời gian
- Một số cơ chế truyền tải logs phổ biến
  - Syslog TCP/UDP
  - Encrypted Syslog
  - HTTP/HTTPS
  - SOAP over HTTP
  - SNMP
  - SCP, FTP

Step 3: Log Storage (1/2)

- Tất cả logs được thu thập từ nhiều nguồn và được lưu trữ trong CSDL.
- "Log messages" được lưu trữ và truy xuất từ CSDL theo một cách hệ thống.
- Các yêu cầu lưu trữ đối với logs được lựa chọn dựa trên kích thước, tầm quan trọng hay khả năng truy cập.

Step 3: Log Storage (2/2)

Storage Duration

- Thời gian lưu trữ logs tùy thuộc vào từng loại.
- Logs cần phân tích sau có thể được lưu trữ trên cloud
- Logs cần phân tích thường xuyên hoặc được lưu trữ trong thời gian ngắn sẽ được lưu trữ trong hệ thống lưu trữ phân tán.

Volume of Data to Be Stored

- Hệ thống lưu trữ được sử dụng phải có khả năng mở rộng và có thể hoạt động bình thường ngay cả với dữ liệu lớn

Ways of Accessing the Logs

- Xem xét thiết lập quyền truy cập phù hợp
- Nếu việc truy cập logs gặp khó khăn thì một số hệ thống lưu trữ không thể sử dụng để phân tích theo thời gian thực

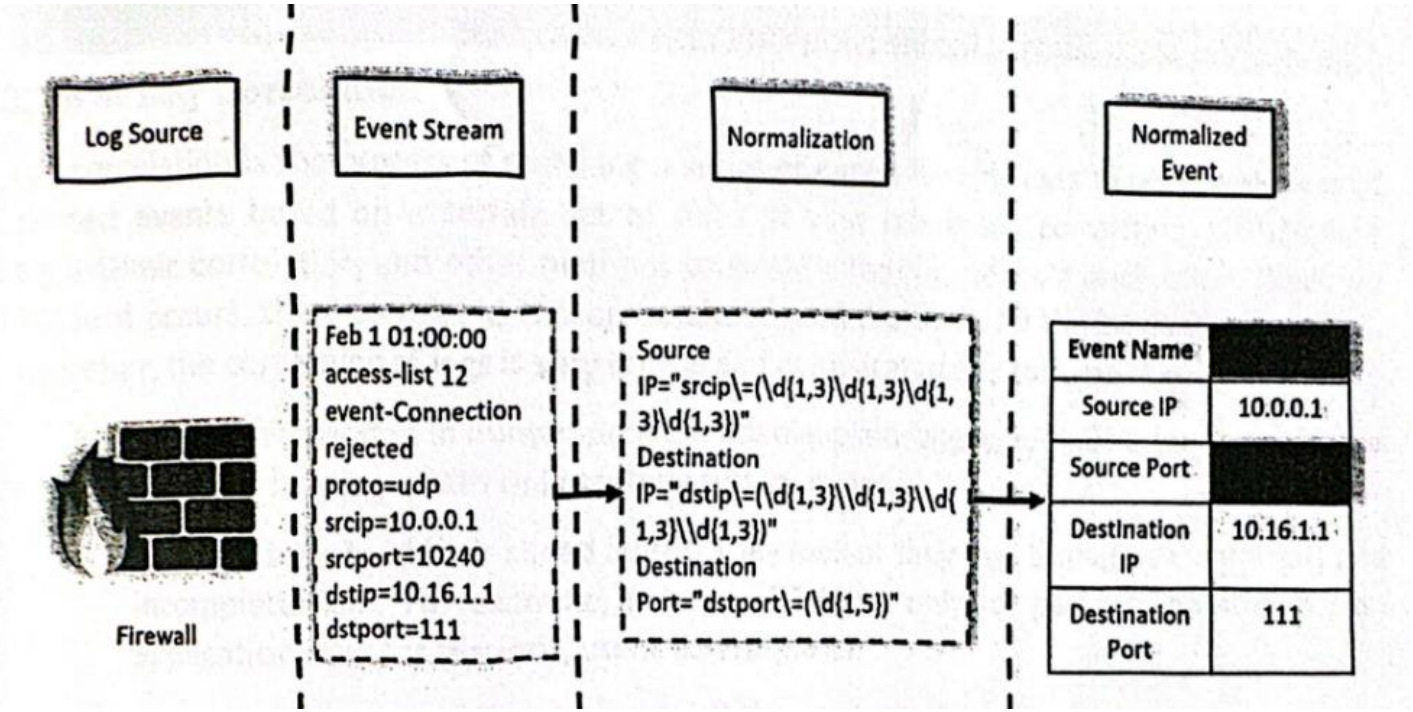
Step 4: Log Normalization (1/2)

- Chuẩn hóa log là quá trình chấp nhận logs từ các nguồn không đồng nhất với các định dạng khác nhau và chuyển đổi chúng thành định dạng chung.
- Trong quá trình chuẩn hóa, "raw log data" được thu thập từ các nguồn khác nhau và sử dụng biểu thức phù hợp để chuẩn hóa.
  - Logs được ánh xạ với các lược đồ và framework tiêu chuẩn để "parse" dữ liệu
  - Hầu hết các hệ thống phân tích logs đều sử dụng biểu thức phù hợp để "parse" dữ liệu
- Log messages được phân loại thành nhiều thông tin có ý nghĩa hơn, có thể dự đoán được và nhất quán hơn sau khi chuẩn hóa

Step 4: Log Normalization (2/2)

❑ Các bước chuẩn hóa:

- Collector thu thập logs từ các nguồn khác nhau.
- Loại nguồn (source type) được xác định dựa trên sự kiện.
- "Parser" được sử dụng và regex được thiết lập để xác định các trường trong sự kiện.
- Việc chuẩn hóa được thực hiện và logs được phân loại.
- Việc tổng hợp và lọc được áp dụng.



Step 5: Log Correlation

- Tương quan nhật ký là quá trình so khớp chuỗi dữ liệu nhật ký đã được chuẩn hóa để xác định một tập các sự kiện có liên quan dựa trên các luật nhất định
- Các nhật ký tương quan được sử dụng để xác định sự cố xảy ra trong hệ thống

Micro-level Corelation

- Tương quan các trường trong một sự kiện hoặc một tập hợp các sự kiện.
- Bao gồm tương quan trường (field correlation) và tương quan luật (rule correlation)

Macro-level Corelation

- Tương quan từ nhiều nguồn để xác thực và thu thập thông tin tình báo trên luồng sự kiện

Step 6: Log Analysis

- Phân tích nhật ký là một quá trình xác định các mẫu và bất thường trong dữ liệu nhật ký tương quan
- Phân tích nhật ký có thể hỗ trợ khắc phục sự cố hệ thống, điều tra tấn công mạng, kiểm tra xem các chính sách, quy định, kiểm toán nội bộ có được tuân thủ hay không, xác định hành vi người dùng…

Type of SIEM solutions

In-house SIEM

- In-house SIEM (SIEM nội bộ): SIEM được triển khai trong một công ty, tổ chức mà không có sự tham gia từ bên thứ 3. Tổ chức phải mua và cài đặt phần mềm, phần cứng cần thiết.
- Ưu điểm
  - Đảm bảo kiểm soát toàn bộ hệ thống.
  - Có thể cập nhật luật bất cứ khi nào.
  - Dễ dàng tùy chỉnh tùy thuộc mức độ an toàn cần thiết lập.
- Nhược điểm
  - Tương đối đắt trong quá trình triển khai và vận hành.
  - Nhân viên phải có khả năng vận hành quản lý, mất thời gian đào tạo chuyên gia.
  - Khó có thể đảm bảo toàn bộ công cụ cần thiết.

Type of SIEM solutions

Cloud-based SIEM

- Cloud-based SIEM: Bên thứ ba cung cấp các tính năng cần thiết của SIEM và tổ chức sử dụng SIEM như một dịch vụ, trong đó phía khách hàng đăng ký một gói dịch vụ với các tính năng cụ thể trong một khoảng thời gian nhất định.
- Ưu điểm:
  - SIEM platform được cập nhật liên tục.
  - Được hỗ trợ khi cần thiết bởi các chuyên gia ở nhiều mức độ khác nhau.
  - Khách hàng không cần cài đặt thêm thiết bị phần cứng.
- Nhược điểm:
  - Sử dụng càng nhiều tính năng thì chi phí phải trả càng lớn.
  - Phụ thuộc nhiều vào bên vận hành, cung cấp dịch vụ.

Type of SIEM solutions

Managed SIEM

- Managed SIEM: Có thể triển khai tại chỗ hoặc trên đám mây
- SIEM này bao gồm tất cả các tính năng công nghệ cần thiết để triển khai tự động cũng như để đáp ứng các mục tiêu bảo mật
- Ưu điểm
  - Loại bỏ gánh nặng tuyển dụng, đào tạo và giữ chân nhân viên vì nó đi kèm với công nghệ tiên tiến và con người có trình độ cao
  - Không tốn không gian so với in-house SIEM
- Nhược điểm
  - Tồn tại một số rủi ro liên quan đến quyền riêng tư

SIEM Solutions

- Micro Focus ArcSight Enterprise Security Manager (ESM)
- Elastic Stack (ELK)
- Splunk Enterprise Security (ES)
- LogRhythm SIEM
- IBM Security QRadar
- Wazuh
- AlientVault Unified Security Management (USM)
- SolarWinds Log and Event Manager
- McAfee Enterprise Security Manager (ESM)
- Micro-Focus Sentinel Enterprise

1. Tổng quan về hệ thống SIEM
2. Kiến trúc và thành phần
3. Triển khai vận hành SIEM
4. Phát hiện sự cố với SIEM

Challenges in SIEM deployment

- Những thách thức khi triển khai hệ thống giám sát
  - Tổ chức không xác định được phạm vi, trường hợp sử dụng, các yêu cầu rõ ràng
  - Thiếu nhân sự chuyên trách có trình độ
  - Không xem xét, đánh giá nhu cầu giám sát và hoạt động của hệ thống
  - Lựa chọn kiến trúc triển khai SIEM không phù hợp
- Khuyến cáo để triển khai SIEM thành công
  - Sử dụng cách triển khai SIEM theo từng "Pha"
  - Xác định phạm vi và các trường hợp sử dụng, đồng thời xây dựng các yêu cầu liên quan cần thiết để thực hiện thành công các trường hợp sử dụng
  - Triển khai, lựa chọn kiến trúc phù hợp

Recommendations for Successful SIEM Deployment

1. Tổng quan về hệ thống SIEM
2. Kiến trúc và thành phần
3. Triển khai vận hành SIEM
4. Phát hiện sự cố với SIEM

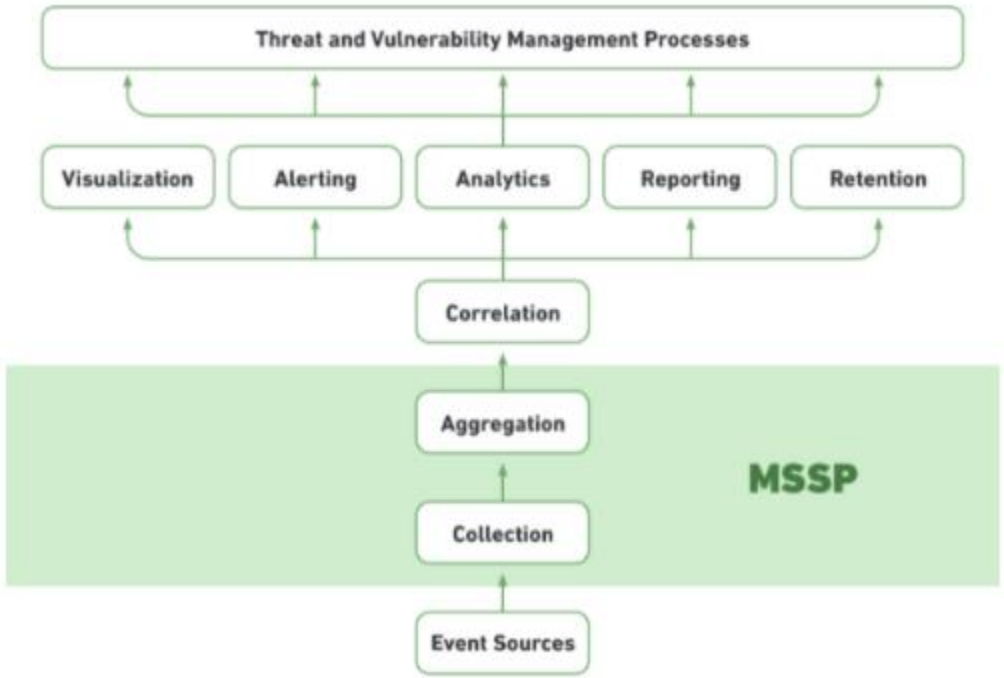
5.1. Mô hình triển khai SIEM

❑ **Doanh nghiệp tự quản lý, tự lưu trữ:**

- Đây là mô hình triển khai SIEM truyền thống
- Lưu trữ SIEM trong trung tâm máy chủ cục bộ, thường bằng thiết bị SIEM chuyên dụng, duy trì hệ thống lưu trữ và quản lý hệ thống bởi các chuyên viên ATTT.
- Mô hình này phức tạp và tốn kém để duy trì.

5.1. Mô hình triển khai SIEM

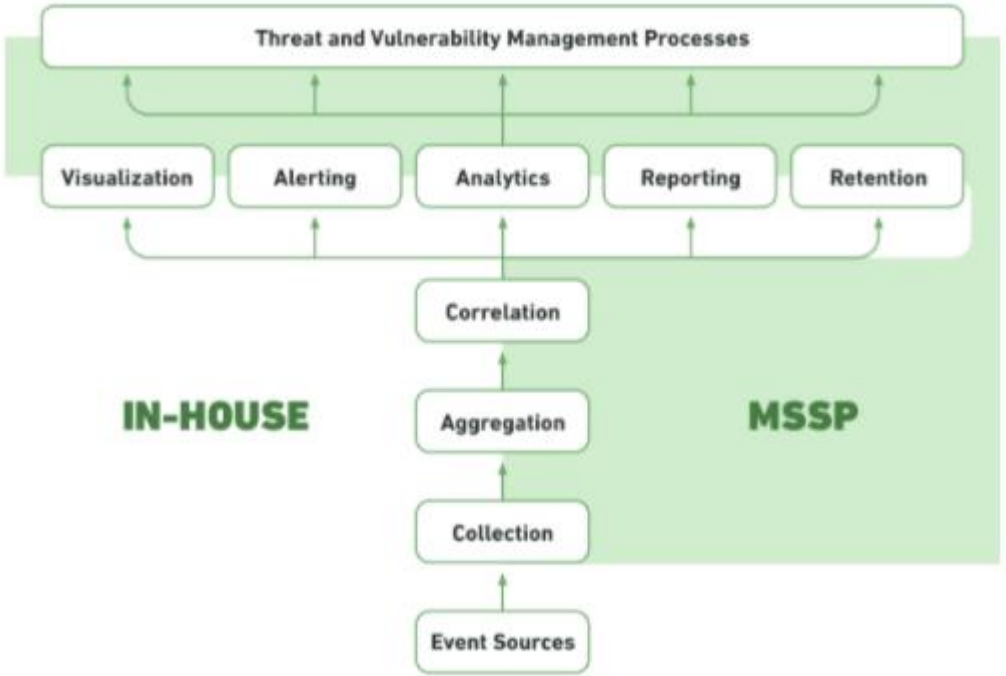
❑ **Cloud SIEM, doanh nghiệp tự quản lý:**



- **MSSP xử lý:** Tiếp nhận các sự kiện từ hệ thống của tổ chức, thu thập và tổng hợp.
- **Quản trị hệ thống:** Tương quan, phân tích, cảnh báo và giám sát bảng điều khiển, các quy trình an toàn sử dụng dữ liệu từ SIEM.

5.1. Mô hình triển khai SIEM

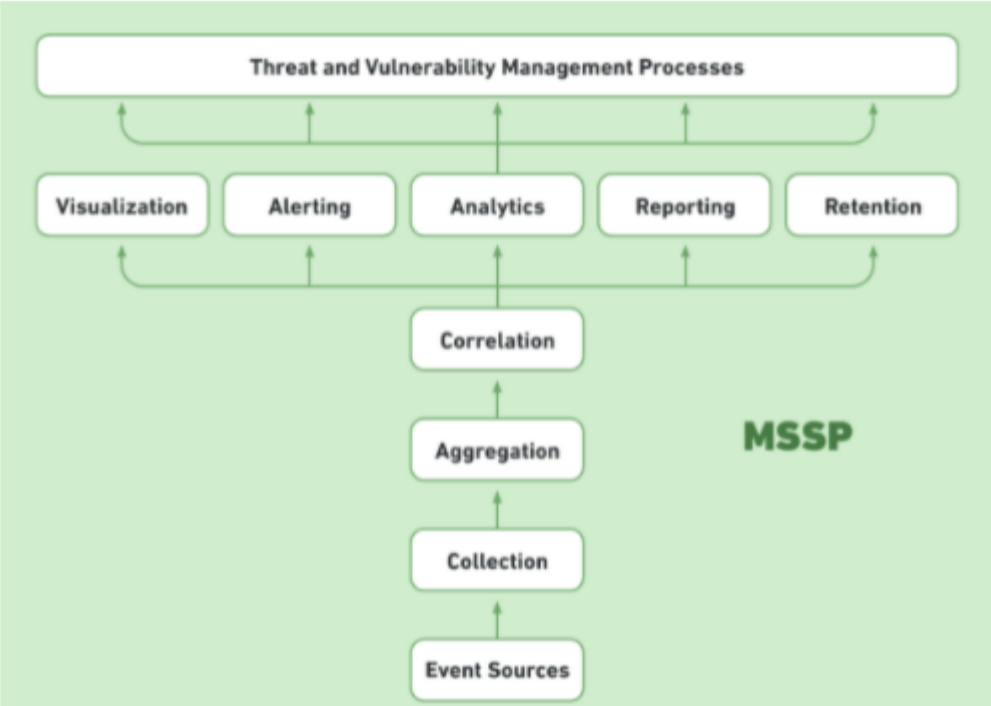
❑ **Lưu trữ, quản lý kết hợp giữa doanh nghiệp với đám mây:**



- **MSSP xử lý:** Triển khai thu thập / tổng hợp sự kiện SIEM, tương quan, phân tích, cảnh báo và giám sát bảng điều khiển.
- **Quản trị hệ thống:** Mua phần mềm và cơ sở hạ tầng phần cứng.

5.1. Mô hình triển khai SIEM

❑ **SIEM là một dịch vụ:**



- **MSSP xử lý:** Thu thập, tổng hợp, tương quan, phân tích, cảnh báo và giám sát bảng điều khiển sự kiện.
- **Quản trị hệ thống:** Các quy trình an toàn sử dụng dữ liệu từ SIEM.

5.1. Mô hình triển khai SIEM

Thảo luận:

Doanh nghiệp nên sử dụng mô hình nào?

5.2. Yêu cầu khi triển khai SIEM

- Số lượng sự kiện an toàn / giây (Velocity)
- Khối lượng
- Phần cứng

5.2. Yêu cầu khi triển khai SIEM

❑Số lượng sự kiện an toàn/giây:

- Phần lớn SIEM hiện nay được triển khai trong mạng nội bộ.
- Do vậy các tổ chức phải xem xét cẩn thận khối lượng dữ liệu log và sự kiện được tạo ra trong hệ thống cũng như tài nguyên hệ thống cần thiết để quản lý chúng.
- Tính toán số lượng sự kiện / giây (EPS: Events Per Second)

$$\frac{\#\ \text{OF SECURITY EVENTS}}{\text{TIME PERIOD IN SECONDS}} = \text{EPS}$$

- EPS có thể thay đổi giữa thời gian bình thường và cao điểm.
- Ví dụ: Router Cisco có thể tạo ra trung bình 0,6 sự kiện mỗi giây. Nhưng trong lúc tấn công xảy ra, nó có thể tạo ra tới 154 EPS.

5.2. Yêu cầu khi triển khai SIEM

❑Dự đoán chỉ số EPS:

- Tính toán EPS tại thời điểm thông thường và lúc cao điểm từ dữ liệu lịch sử trong 90 ngày.
- Tính toán số lần cao điểm trong ngày

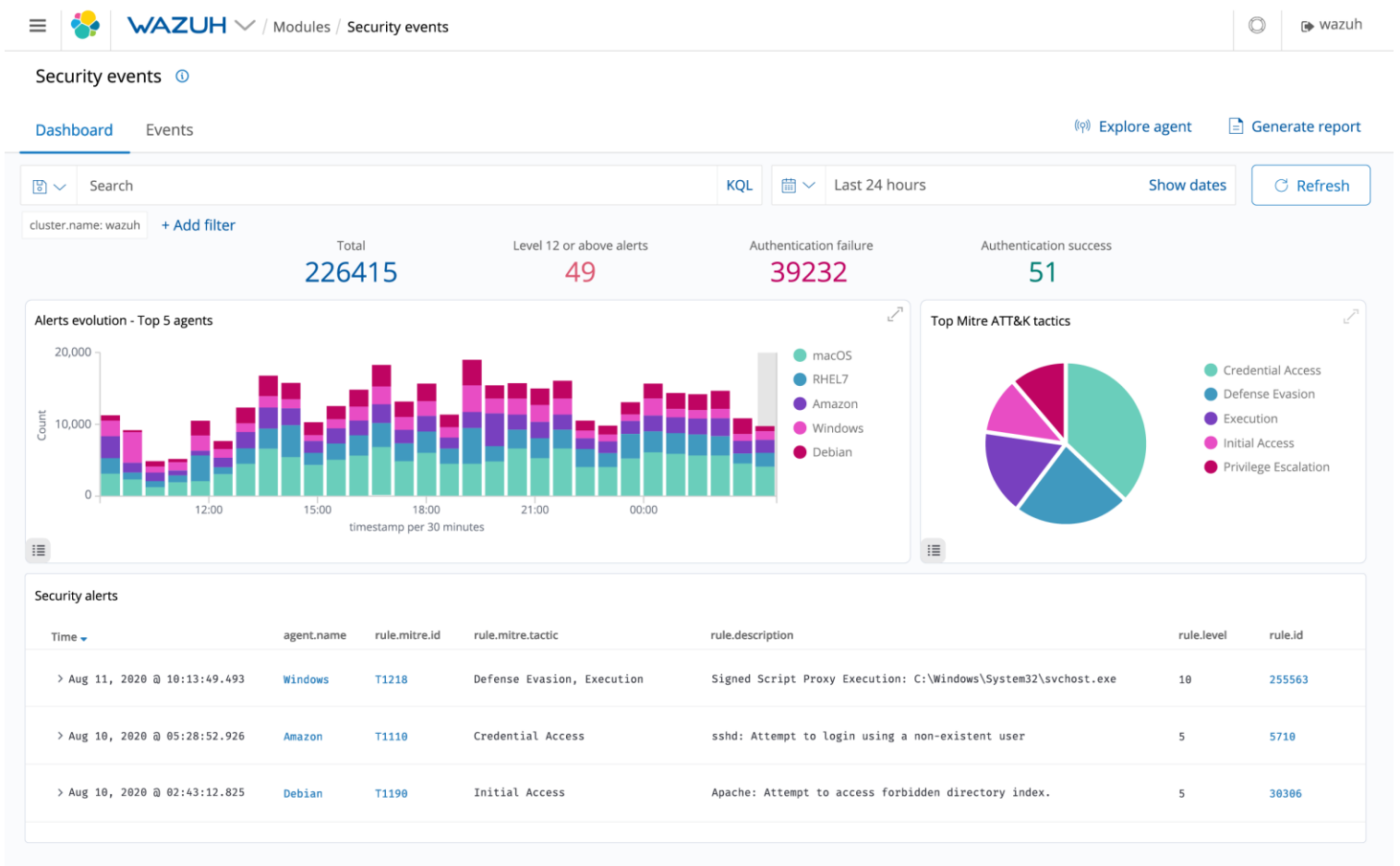
5.2. Yêu cầu khi triển khai SIEM

- Tốc độ
- Khối lượng
- Phần cứng

I. Hệ thống giám sát ATTT

6. Một số sản phẩm tiêu biểu

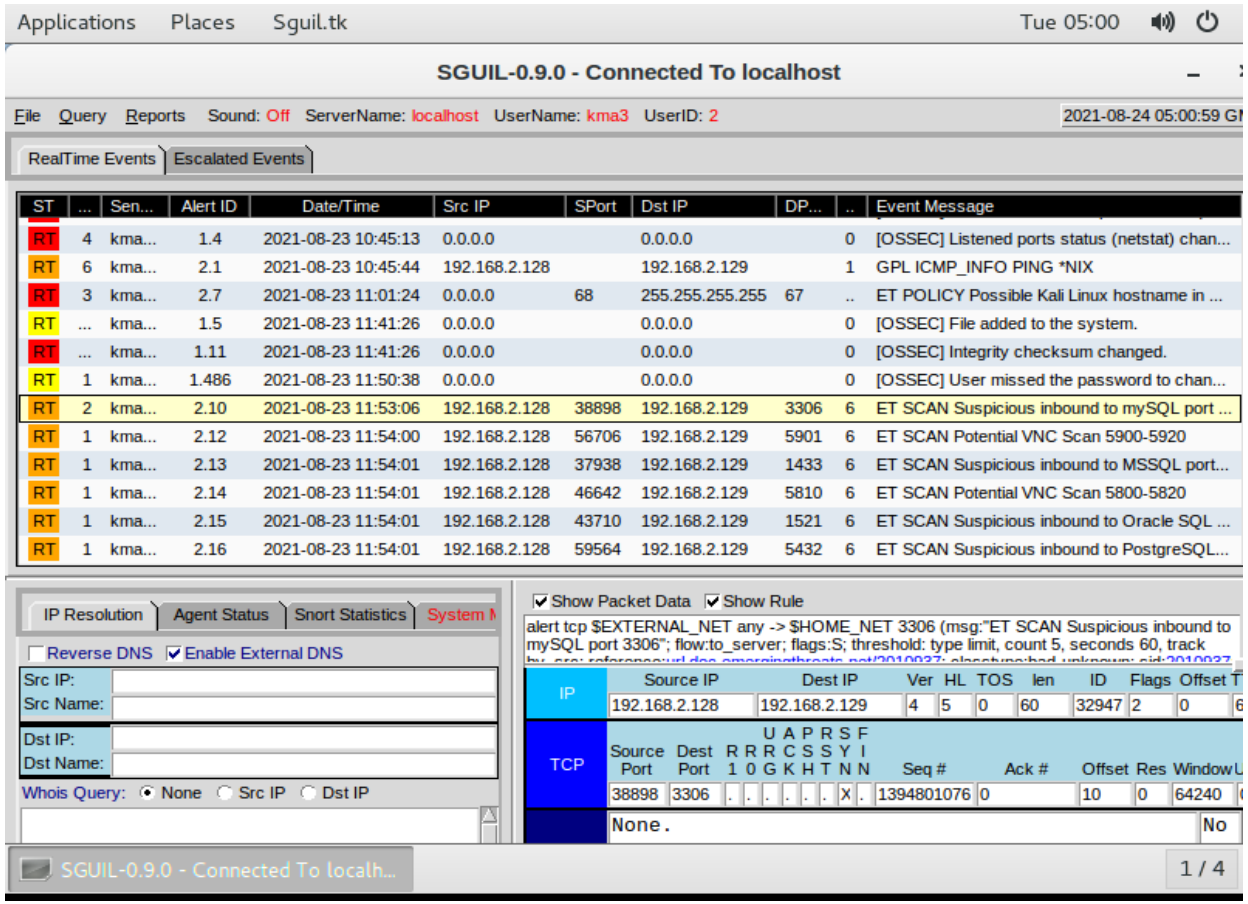
a) Wazuh:



I. Hệ thống giám sát ATTT

6. Một số sản phẩm tiêu biểu

b) Security Onion:



I. Hệ thống giám sát ATTT

6. Một số sản phẩm tiêu biểu

c) IBM Qradar: