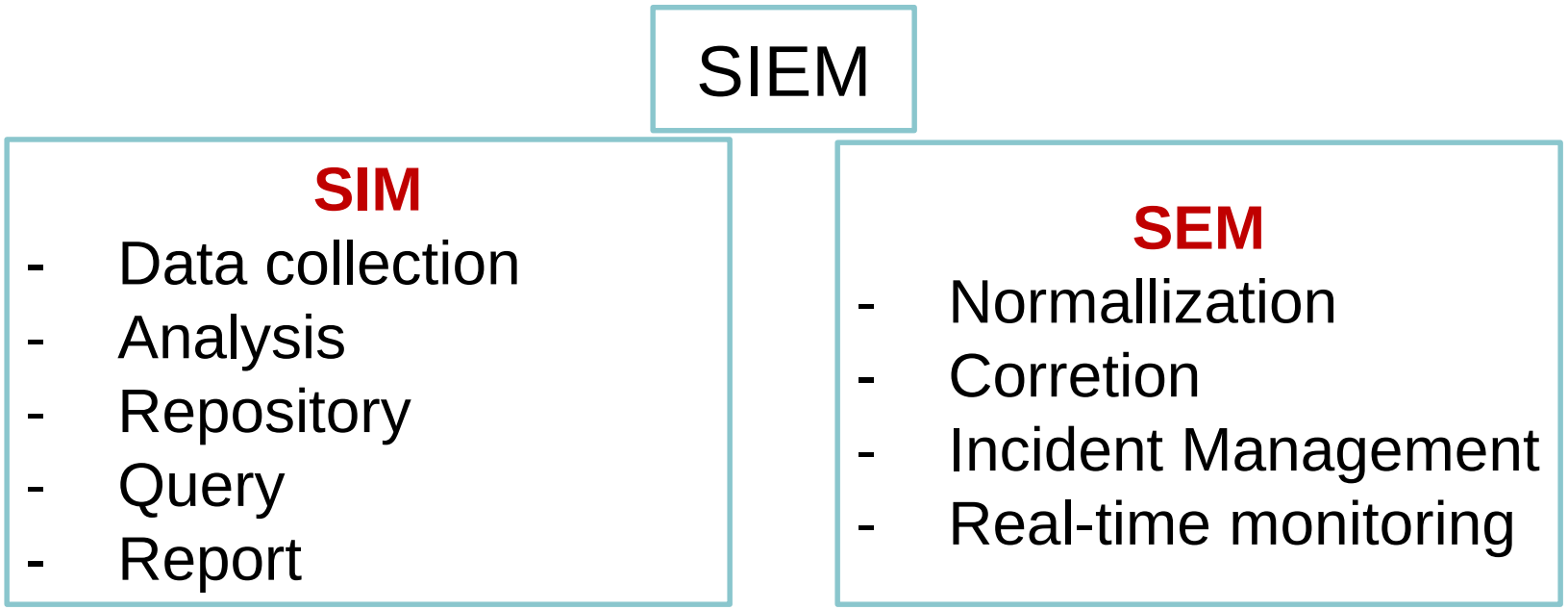
PHẦN III
PHÁT HIỆN SỰ CỐ DỰA TRÊN HỆ THỐNG SIEM

Các thành phần của SIEM

- **SIEM bao gồm có hai layer**
  - SIM (Security information management)
  - SEM (Security Event management)



Sự cần thiết của SIEM

- Cho chúng ta một bức tranh khái quá về môi trường IT của tổ chức
- Để phát hiện, phân tích, ưu tiên loại bỏ các mối đe dọa tổ chức co thể gặp phải
- Để cải thiện việc phân tích nhật ký
- Để hỗ trợ công tác điều tra phát hiện và ứng phó sự cố
- Quản lý số lượng lớn các log từ nhiều nguồn khác nhau
- Hỗ trợ việc tuân thủ các quy định
- Hỗ trợ tuân thủ quy trình và các yêu cầu về kiểm toán – audit

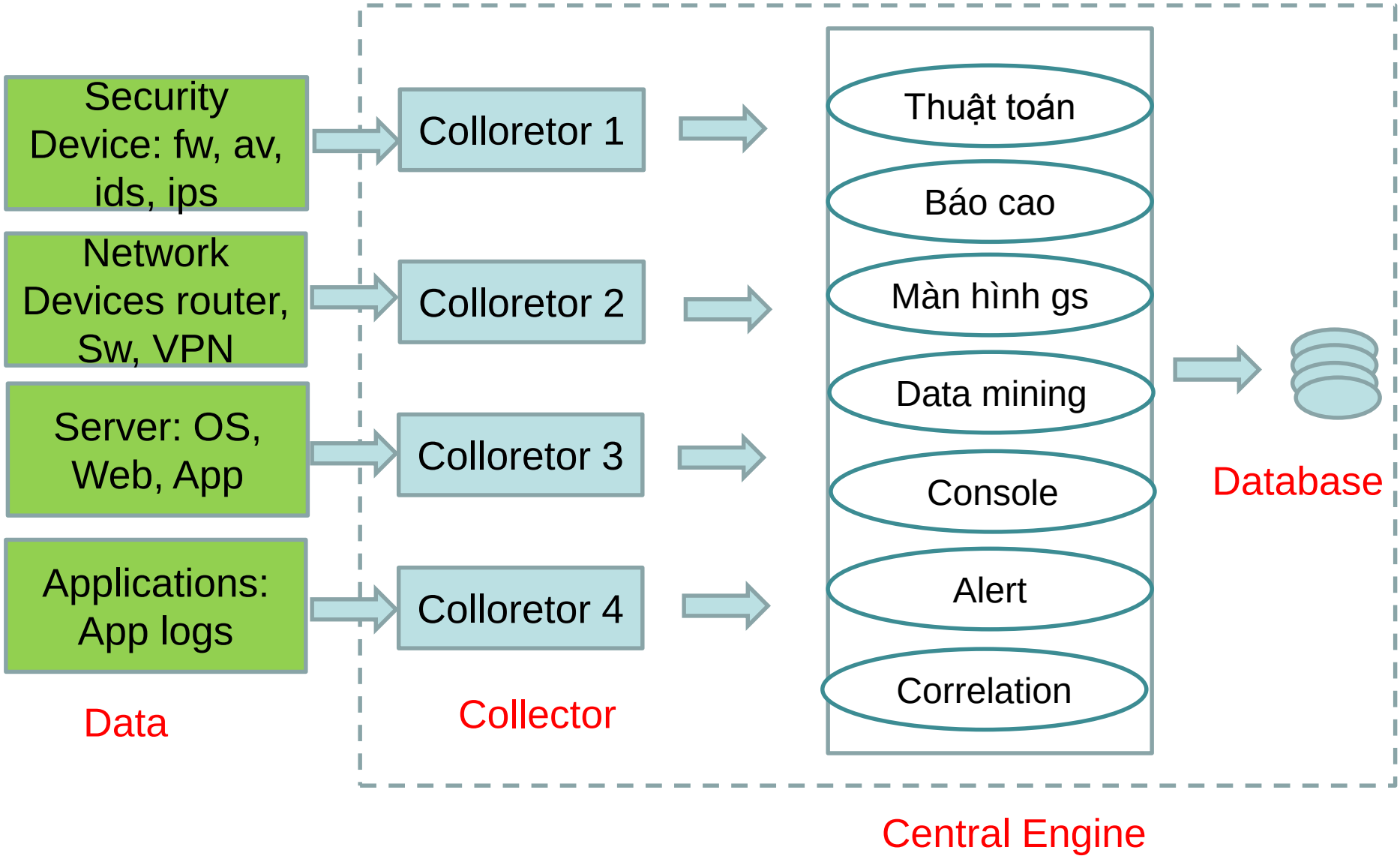
Các tính năng chính của SIEM

- Thu thập log (Log collection)
- Phân tích log (Log analysis)
- So sánh tương quan sự kiện (Event Correlation)
- Điều tra nhật ký (Log Forensics)
- Tuân thủ IT (IT Compliance)
- Giám sát nhật ký ứng dụng (Application log monitoring)
- Kiểm toán truy cập đối tượng

Các tính năng chính của SIEM (cont)

- Cảnh báo theo thời gian thực (Real-time alerting)
- Giám sát các hoạt động của User (User Activity Monitoring)
- Giám sát màn hình (Dashboards)
- Giám sát toàn vẹn các tệp (File integrity Monitoring)
- Giám sát nhật ký các thiết bị và hệ thống (System & Device log Monitoring)
- Lưu trữ nhật ký (Log Retention)

Thành phần, kiến trúc SIEM



Khó khăn, thách thức khi triển khai SIEM

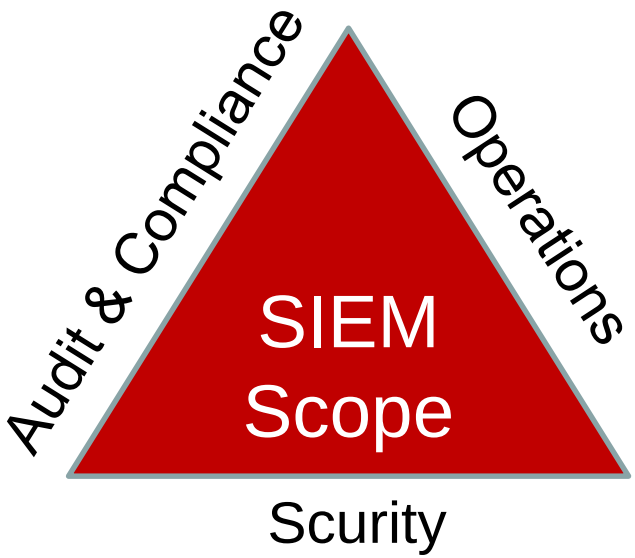
- Không rõ phạm vi và các yêu cầu liên quan
- Các chuyên gia quản trị không được đào tạo kỹ lưỡng
- Việc triển khai cấu hình không đúng cách
- Lựa chọn kiến trúc để triển khai không phù hợp

Khuyến khi triển khai SIEM

- Thực hiện triển khai SIEM theo từng giai đoạn
  - Ví dụ triển khai các thành phần về quản lý log trước, sau đó triển khai các thành phần của SIEM
  - Ưu điểm:
    - Cải thiện được hiệu năng
    - Dữ liệu log đã có sẵn để thực hiện chức năng liên quan đến việc phân tích
- Xác định phạm vi và xây dựng các yêu cầu phù hợp
- Triển khai kiến trúc phù hợp

Xác định phạm vi của SIEM

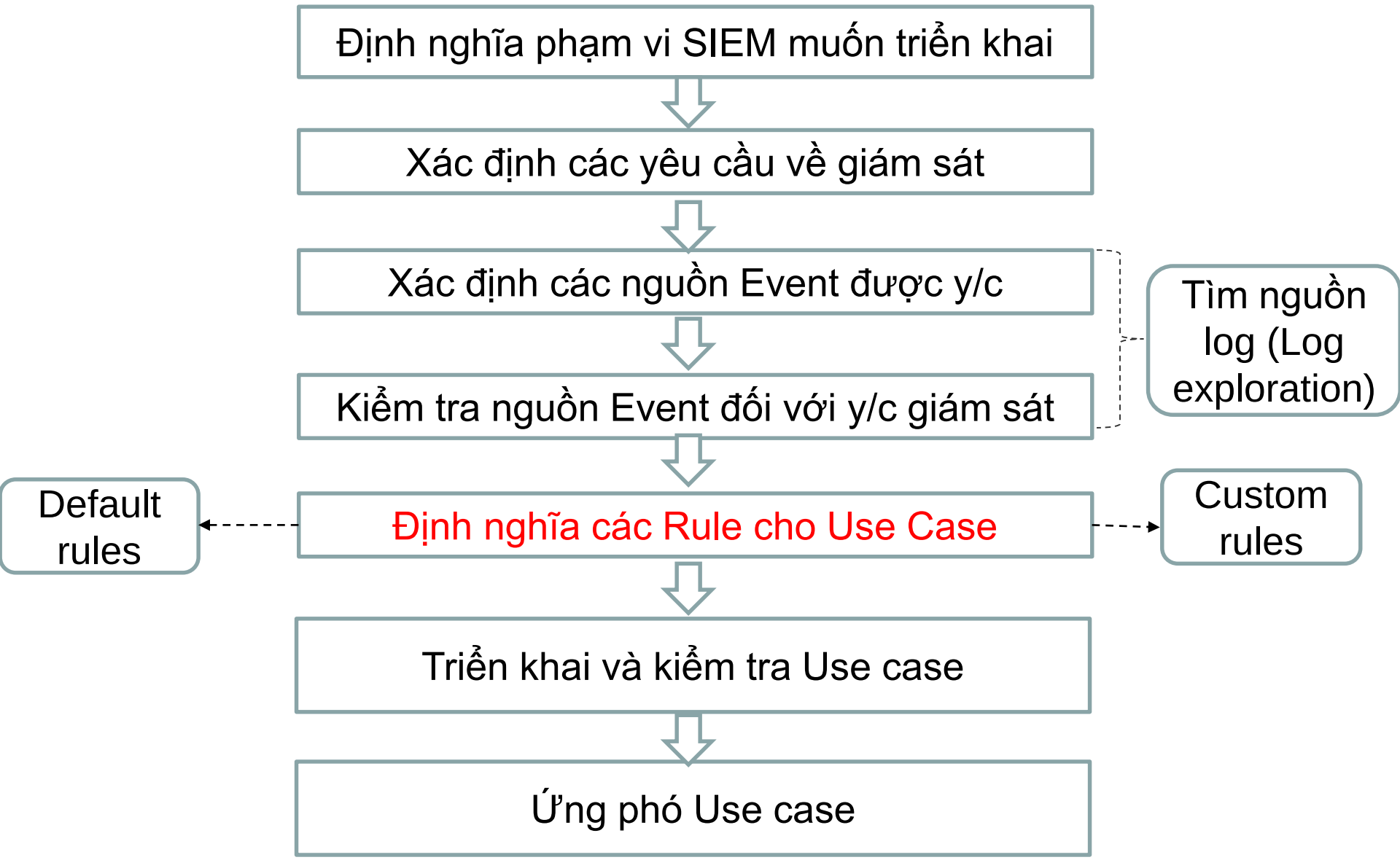
- Phạm vi nó chính là động lực phía sau của việc triển khai SIEM
- **Audit & Compliance**
  - Quy trình thực hiện việc thu thập, lưu trữ và rà soát (việc cần thiết phải thực hiện ntn)
  - Kiểm toán về Security đã tuân thủ theo theo các Policy chưa
  - Ví dụ, tuân thủ PCI-DSS cần ghi lại các loại log liên quan đến thẻ thanh toán
- **Security**
  - Chính là việc giám sát theo thời gian thực, phân tích log để xác định sự cố
- **Operations**
  - Quản lý thiết bị, maintenance phần cứng và phần mềm



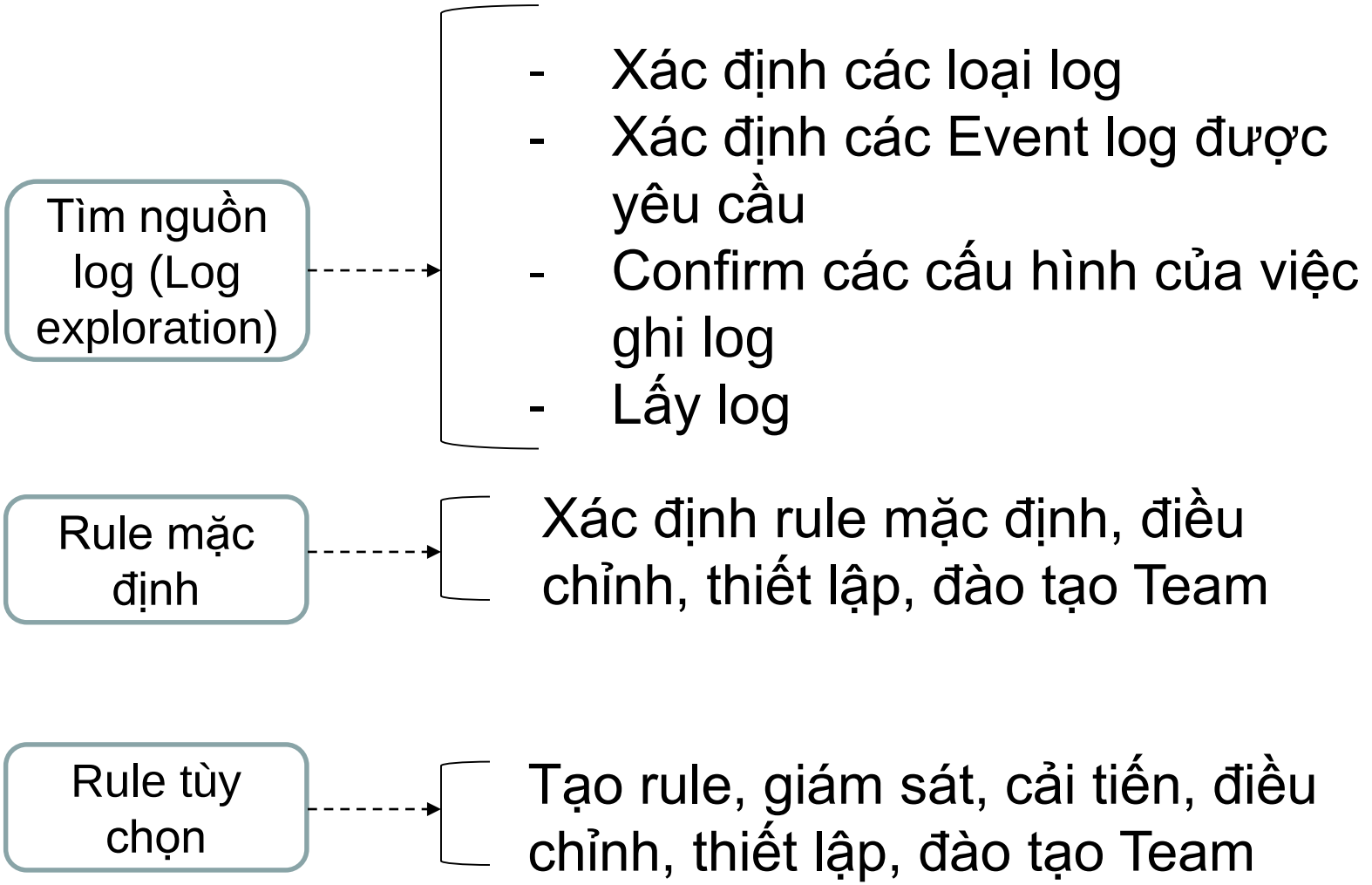
Use Cases Trong SIEM

- Khi đã xác định được scope cho SIEM thì SIEM sẽ sử dụng Use Cases đã được định nghĩa để tạo môi trường SIEM có thể quản lý được
- Các Use cases có thể là: rule, report, alert, dashboard mà đáp ứng được các yêu cầu
- Có hai loại Use cases:
  - Generic: (chung, áp dụng cho các doanh tổ chức, hoặc một tập đoàn nhiều công ty con theo mô hình phân tán),
  - Specific (cụ thể, chỉ áp dụng cho 1 tổ chức), không kết nối mạng bên ngoài
- SIEM sử dụng các Use cases này để xác định cho việc phát hiện, dấu hiệu phát hiện, so sánh tương quan

Các giai đoạn phát triển và triển khai Use cases



Phát triển và triển khai Use cases (cont)



Phát hiện sự cố dựa trên SIEM

Nguyên tắc phát hiện sự cố dựa trên SIEM

- **Phát hiện sự cố có thể dựa trên hai nguyên tắc**
  - Dự trên sự bất thường (anomaly-based): dựa trên các thiết bị cảnh báo, và cần phải có sự điều tra thêm bằng cách thủ công
  - Dựa trên signature (signature-based): log được cung cấp từ các loại thiết bị như IDS, WAF,…
  - Ví dụ:
    - ((\%3C)|<): => phát hiện tấn công XSS
    - Tân công DoS slowhttp => bình thường User-Agent kết thúc bằng [CRLF] [CRLF] => nghĩa là header đã được hoàn thành
    - Nếu bình thường User-Agent kết thúc bằng [CRLF] => nghĩa là header không được hoàn thành