TCVN

# TIÊU CHUẨN QUỐC GIA

## TCVN XXXXX:2026

**Xuất bản lần 1**

# AN NINH MẠNG - SẢN PHẨM QUẢN LÝ VÀ PHÂN TÍCH SỰ KIỆN AN NINH MẠNG - YÊU CẦU CHUNG

***Cyber security - Security Information and Event Management - General requirements***

**HÀ NỘI – 2026**

**Mục lục**

## Lời nói đầu

TCVN XXXXX:2026 An ninh mạng - Sản phẩm quản lý, phân tích sự kiện an ninh mạng - Yêu cầu chung do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao biên soạn, Bộ Công an đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

## Lời giới thiệu

Tiêu chuẩn này quy định các yêu cầu kỹ thuật đối với sản phẩm quản lý, phân tích sự kiện an ninh mạng (SIEM), nhằm nâng cao năng lực giám sát, thúc đẩy quá trình chia sẻ thông tin và bảo vệ chủ động các hệ thống thông tin trước những mối đe dọa.

Để tối ưu hiệu quả cảnh báo sớm và ứng phó sự cố, các cơ quan, tổ chức được khuyến khích triển khai SIEM đáp ứng tiêu chuẩn này, kết hợp đồng bộ với các biện pháp quản lý, kỹ thuật và vận hành để xây dựng một hệ sinh thái phòng thủ toàn diện.

# An ninh mạng - Sản phẩm quản lý và phân tích sự kiện an ninh mạng - Yêu cầu chung

*Cyber security - Security Information and Event Management - General requirements*

## 1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu kỹ thuật chung đối với sản phẩm quản lý và phân tích sự kiện an ninh mạng (Sau đây viết tắt là SIEM).

Tiêu chuẩn này không quy định yêu cầu kỹ thuật đối với sản phẩm điều phối, tự động hóa và phản ứng an ninh mạng (SOAR) và sản phẩm nền tảng tình báo mối đe dọa (TIP); các sản phẩm này được quy định tại các tiêu chuẩn quốc gia riêng. Yêu cầu về khả năng tích hợp giữa SIEM với SOAR và TIP được quy định tại 5.2.5.3.

## 2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi (nếu có).

OASIS, STIX/TAXII - Cyber Threat Intelligence Standards, Version 2.1, March 2021.

## 3 Thuật ngữ, định nghĩa và chữ viết tắt

Trong tiêu chuẩn này sử dụng các thuật ngữ, định nghĩa và chữ viết tắt sau:

### 3.1 Thuật ngữ và định nghĩa

**3.1.1**

**Giải pháp quản lý và phân tích các sự kiện an ninh mạng** (Security Information and Event Management - SIEM)

Giải pháp an ninh mạng kết hợp giữa quản lý thông tin bảo mật và quản lý sự kiện bảo mật, có các chức năng thu thập, phân tích và quản lý dữ liệu từ nhiều nguồn khác nhau trong hệ thống mạng của tổ chức, giúp nhận diện, theo dõi và phản ứng nhanh với các mối đe dọa an ninh mạng.

**3.1.2**

**Bộ thu thập nhật ký** (collector)

Thành phần có chức năng thu thập dữ liệu nhật ký trực tiếp từ các đối tượng được giám sát hoặc các nguồn sinh sự kiện và chuyển tiếp luồng dữ liệu đó về hệ thống phân tích

**3.1.3**

**Bộ tiếp nhận nhật ký** (receiver)

Thành phần chịu trách nhiệm tiếp nhận dữ liệu nhật ký được gửi về từ các bộ thu thập để chuẩn bị cho các bước xử lý tiếp theo trong hệ thống.

**3.1.4**

**Bộ phân tích cú pháp** (parser)

Thành phần thực hiện việc chuẩn hóa, bóc tách và phân tích dữ liệu nhật ký thô thành các trường thông tin có cấu trúc theo định dạng quy định.

**3.1.5**

**Bộ lập chỉ mục** (indexer)

Thành phần thực hiện việc đánh chỉ mục cho khối dữ liệu đã được chuẩn hóa nhằm tối ưu hóa và tăng tốc độ tìm kiếm, truy xuất thông tin.

**3.1.6**

**Bộ lưu trữ** (storage)

Thành phần thực hiện chức năng lưu trữ và bảo vệ dữ liệu nhật ký thô cũng như dữ liệu đã qua xử lý trong một khoảng thời gian xác định theo quy định.

**3.1.7**

**Bộ phân tích tương quan** (correlator)

Thành phần phân tích mối liên kết giữa các sự kiện riêng lẻ dựa trên các quy tắc (luật) được định nghĩa sẵn để phát hiện ra các cuộc tấn công, sự cố hoặc hành vi bất thường.

**3.1.8**

**Danh sách động** (dynamic list)

Danh sách chứa các thông tin, chỉ báo (ví dụ: địa chỉ IP, tên miền, mã băm) có khả năng tự động cập nhật liên tục từ các nguồn bên ngoài phục vụ cho quá trình đối sánh và phân tích.

**3.1.9**

**Tập luật bảo vệ** (security rules)

Tập hợp các quy tắc, điều kiện được thiết lập sẵn hoặc tùy chỉnh trên hệ thống nhằm nhận diện và đưa ra cảnh báo về các mối đe dọa an ninh mạng.

**3.1.10**

**Hồ dữ liệu** (data lake)

Hệ thống lưu trữ tập trung cho phép lưu giữ khối lượng lớn dữ liệu ở nhiều định dạng khác nhau (có cấu trúc, bán cấu trúc, phi cấu trúc) dưới dạng thô gốc, phục vụ tối ưu cho công tác truy vấn và phân tích dữ liệu lớn.

**3.1.11**

**Chế độ active-active**

Chế độ dự phòng độ sẵn sàng cao, trong đó các thiết bị đều ở trạng thái hoạt động, cùng tham gia xử lý lưu lượng và duy trì dịch vụ.

**3.1.12**

**Chế độ active-standby**

Chế độ dự phòng sẵn sàng cao, trong đó một thiết bị hoạt động chính và một hoặc nhiều thiết bị ở trạng thái dự phòng, thiết bị dự phòng tự động chuyển sang hoạt động khi thiết bị chính gặp sự cố.

**3.1.13**

**Chế độ active-passive**

Chế độ dự phòng tương tự thiết lập active-standby, trong đó một nút mạng chịu trách nhiệm xử lý toàn bộ khối lượng công việc chính, nút còn lại ở trạng thái chờ và liên tục đồng bộ trạng thái để sẵn sàng tiếp quản hệ thống khi nút chính xảy ra điểm lỗi.

**3.1.14**

**Kiến trúc phân tán**

Kiến trúc hệ thống trong đó các phân hệ tính toán (như thu thập, phân tích, lưu trữ) được triển khai phân tán trên nhiều máy chủ hoặc vị trí địa lý khác nhau, nhưng được liên kết qua mạng để hoạt động phối hợp như một nền tảng thống nhất nhằm tối ưu hóa hiệu năng, độ tin cậy và khả năng mở rộng.

**3.1.15**

**Hàm băm mật mã** (cryptographic hash function)

Thuật toán một chiều chuyển đổi một khối dữ liệu có kích thước bất kỳ thành một chuỗi ký tự có độ dài cố định, khó tìm được hai khối dữ liệu khác nhau cho cùng một giá trị đầu ra và không thể tính ngược lại dữ liệu gốc.

**3.1.16**

**Đối soát tổng** (checksum)

Giá trị được tính từ một khối dữ liệu số theo một thuật toán xác định, lưu kèm dữ liệu gốc để phát hiện các thay đổi hoặc lỗi phát sinh trong quá trình truyền tải và lưu trữ.

### 3.2 Chữ viết tắt

| | | |
|---|---|---|
| API | Giao diện lập trình ứng dụng | Application Programming Interface |
| CEF | Định dạng sự kiện chung | Common Event Format |
| CNTT | Công nghệ thông tin | Information Technology |
| CPU | Bộ xử lý trung tâm | Central Processing Unit |
| CSV | Giá trị phân tách bằng dấu phẩy | Comma-Separated Values |
| EPS | Số sự kiện trên một giây | Events Per Second |
| HSM | Thiết bị bảo mật phần cứng | Hardware Security Module |
| HTML | Ngôn ngữ đánh dấu siêu văn bản | HyperText Markup Language |
| IDS | Hệ thống phát hiện xâm nhập | Intrusion Detection System |
| IP | Giao thức Internet | Internet Protocol |
| IPFIX | Xuất thông tin luồng IP | IP Flow Information Export |
| IPS | Hệ thống phòng chống xâm nhập | Intrusion Prevention System |
| JSON | Ký hiệu đối tượng JavaScript | JavaScript Object Notation |
| KMS | Hệ thống quản lý khóa | Key Management System |
| MAC | Địa chỉ điều khiển truy cập phương tiện | Media Access Control |
| MFA | Xác thực đa yếu tố | Multi-Factor Authentication |
| NetFlow | Giao thức giám sát luồng mạng | NetFlow |
| PDF | Định dạng tài liệu di động | Portable Document Format |
| sFlow | Giao thức lấy mẫu luồng mạng | sampled Flow |
| SIEM | Nền tảng quản lý, phân tích sự kiện và thông tin an ninh mạng | Security Information and Event Management |
| SNMP | Giao thức quản lý mạng đơn giản | Simple Network Management Protocol |
| SOAR | Điều phối, tự động hóa và phản hồi an ninh mạng | Security Orchestration, Automation and Response |
| SPOF | Điểm lỗi đơn lẻ | Single Point of Failure |

| | | |
|---|---|---|
| STIX/TAXII | Chuẩn chia sẻ thông tin tình báo mối đe dọa | Structured Threat Information eXpression/Trusted Automated eXchange of Intelligence Information |
| SYSLOG | Giao thức ghi nhật ký hệ thống | System Logging Protocol |
| TCP | Giao thức điều khiển truyền dẫn | Transmission Control Protocol |
| TI | Tình báo mối đe dọa | Threat Intelligence |
| TIP | Nền tảng tình báo mối đe dọa | Threat Intelligence Platform |
| TLS | Giao thức bảo mật lớp truyền tải | Transport Layer Security |
| UDP | Giao thức gói dữ liệu người dùng | User Datagram Protocol |
| WORM | Ghi một lần, đọc nhiều lần | Write Once Read Many |
| XML | Ngôn ngữ đánh dấu mở rộng | eXtensible Markup Language |

# 4 Yêu cầu chung, quản trị và an toàn của sản phẩm

## 4.1 Khái quát

Mục này quy định các yêu cầu về tài liệu, quản trị, vận hành và bảo đảm an toàn của sản phẩm SIEM, nhằm bảo đảm hệ thống được triển khai, cấu hình, quản lý và duy trì an toàn, tin cậy, liên tục và có khả năng kiểm soát, truy vết các hoạt động quản trị trong quá trình vận hành.

## 4.2 Yêu cầu cụ thể

### 4.2.1 Yêu cầu về tài liệu

#### 4.2.1.1 Hướng dẫn triển khai và thiết lập cấu hình

Nhà sản xuất phải cung cấp tài liệu hướng dẫn triển khai, cài đặt và thiết lập cấu hình SIEM, bao gồm tối thiểu: yêu cầu tài nguyên tối thiểu và khuyến nghị theo từng mức quy mô quy định tại 5.2.6.1.1; kiến trúc triển khai tham chiếu; hướng dẫn thiết lập cấu hình an toàn ban đầu.

#### 4.2.1.2 Hướng dẫn sử dụng và quản trị

Nhà sản xuất phải cung cấp tài liệu hướng dẫn sử dụng và quản trị SIEM, bao gồm tối thiểu: mô tả các chức năng nghiệp vụ; hướng dẫn vận hành theo từng nhóm vai trò quy định tại 5.2.7.1; danh mục nguồn nhật ký được hỗ trợ sẵn.

### 4.2.2 Yêu cầu về quản trị hệ thống

#### 4.2.2.1 Quản lý vận hành và giám sát các thành phần nội bộ

SIEM phải cho phép quản lý và giám sát tập trung các thành phần nội bộ thông qua giao diện đồ họa, bao gồm tối thiểu:

a) Receiver;

b) Parser;

c) Indexer;

d) Storage;

đ) Correlator.

SIEM phải cho phép thực hiện các thao tác quản lý vận hành, bao gồm:

a) Thiết lập, thay đổi và cấu hình quản trị từ xa;

b) Cấu hình tài khoản xác thực và phân quyền người dùng;

c) Cấu hình tập luật bảo vệ;

d) Thay đổi thời gian hệ thống;

đ) Xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.

**4.2.2.2 Quản trị từ xa**

SIEM phải cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) Kết nối quản trị từ xa phải sử dụng giao thức hoặc kênh truyền được bảo vệ;

b) Tự động kết thúc phiên quản trị từ xa khi hết thời gian duy trì phiên;

c) Hỗ trợ kiểm soát nguồn truy cập đối với kết nối quản trị từ xa.

**4.2.2.3 Quản lý xác thực và phân quyền**

SIEM phải cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ xác thực bằng tài khoản và mật khẩu;

b) Cho phép thiết lập yêu cầu về độ phức tạp của mật khẩu;

c) Hỗ trợ phân nhóm tài khoản với các quyền hạn khác nhau, tối thiểu gồm nhóm quản trị viên và người dùng thông thường;

d) Có cơ chế phát hiện hoặc cảnh báo đối với phương thức xác thực yếu;

đ) Hỗ trợ kiểm soát truy cập theo ngữ cảnh;

e) Hỗ trợ yêu cầu xác thực lại khi phát hiện hoạt động đăng nhập bất thường;

g) hỗ trợ tích hợp với hệ thống quản lý định danh bên ngoài thông qua giao thức tiêu chuẩn.

h) tự động khóa tài khoản sau số lần xác thực không thành công liên tiếp vượt ngưỡng cấu hình được;

i) buộc thay đổi mật khẩu mặc định trong lần đăng nhập đầu tiên;

k) cho phép cấu hình vô hiệu hóa tài khoản không phát sinh hoạt động trong khoảng thời gian xác định;

l) cho phép giới hạn số phiên đăng nhập đồng thời của một tài khoản.

CHÚ THÍCH 1: Yêu cầu chi tiết về mô hình phân quyền theo vai trò được quy định tại 5.2.7.1.

CHÚ THÍCH 2: Các yêu cầu tại các điểm d), đ) và e) có thể được đáp ứng thông qua tích hợp với hệ thống quản lý định danh hoặc hệ thống xác thực bên ngoài theo 4.2.2.4.

**4.2.2.4 Hỗ trợ tích hợp xác thực tập trung và xác thực đa yếu tố**

SIEM phải đáp ứng các yêu cầu sau:

a) Hỗ trợ tích hợp với hệ thống quản lý định danh tập trung;

b) Hỗ trợ các giao thức hoặc cơ chế xác thực tiêu chuẩn;

c) cho phép áp dụng xác thực đa yếu tố đối với các tài khoản hoặc nhóm tài khoản được xác định;

d) hỗ trợ xác thực đa yếu tố (MFA) đối với mọi tài khoản quản trị, trực tiếp hoặc thông qua tích hợp với hệ thống quản lý định danh tập trung theo điểm a).

**4.2.3 Quản trị và vận hành an toàn và duy trì hệ thống**

**4.2.3.1 Bảo vệ và kiểm soát thay đổi cấu hình**

Trong trường hợp SIEM phải khởi động lại do lỗi phát sinh, ngoại trừ lỗi phần cứng, các cấu hình đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp, bao gồm:

a) Cấu hình hệ thống;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng;

d) Cấu hình tập luật bảo vệ.

Yêu cầu về quản lý tập luật bảo vệ được quy định tại 5.2.3.2.

**4.2.3.2 Cập nhật bản vá của sản phẩm**

SIEM phải đáp ứng các yêu cầu sau về cập nhật bản vá:

a) Sản phẩm phải hỗ trợ cập nhật bản vá để khắc phục điểm yếu, lỗ hổng bảo mật;

b) Hỗ trợ kiểm tra phiên bản cập nhật;

c) Hỗ trợ cập nhật phần mềm hệ thống và các thành phần liên quan trong môi trường có kết nối hoặc không kết nối internet;

d) xác minh chữ ký số hoặc giá trị băm mật mã của gói cập nhật do nhà sản xuất phát hành trước khi cài đặt, và từ chối cài đặt khi việc xác minh không thành công.

**4.2.3.3 Đồng bộ thời gian hệ thống lõi**

SIEM phải đáp ứng các yêu cầu sau về đồng bộ thời gian:

a) Hệ thống phải hỗ trợ đồng bộ thời gian tự động;

b) Thời gian hệ thống phải được duy trì nhất quán sau khi khởi động lại;

c) hệ thống phải hỗ trợ cấu hình nguồn đồng bộ thời gian;

d) cảnh báo khi độ lệch thời gian giữa các thành phần nội bộ quy định tại 4.2.2.1 vượt ngưỡng cấu hình được.

**4.2.3.4 Nhật ký quản trị và hệ thống**

SIEM phải ghi nhận nhật ký tối thiểu các sự kiện quản trị hệ thống:

a) Đăng nhập, đăng xuất tài khoản;

b) Xác thực trước khi cho phép truy cập tài nguyên hoặc sử dụng chức năng của hệ thống;

c) Áp dụng, hoàn tác thay đổi đối với:

- Cấu hình hệ thống;

- Cấu hình quản trị từ xa;

- Cấu hình tài khoản xác thực và phân quyền người dùng;

- Cấu hình tập luật bảo vệ;

d) Kích hoạt lệnh khởi động lại, tắt hệ thống;

đ) Thay đổi thủ công thời gian hệ thống.

Nhật ký quản trị phải chứa tối thiểu:

a) Thời gian sinh nhật ký, bao gồm năm, tháng, ngày, giờ, phút và giây;

b) Địa chỉ IP hoặc định danh của máy trạm;

c) Định danh của tác nhân, ví dụ tài khoản người dùng hoặc tên hệ thống;

d) Thông tin về hành vi thực hiện, ví dụ đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác;

đ) Kết quả thực hiện hành vi, gồm thành công hoặc thất bại;

e) Lý do giải trình đối với hành vi thất bại, ví dụ không tìm thấy tài nguyên hoặc không đủ quyền truy cập.

Yêu cầu về thư viện tập luật bảo vệ được quy định tại 5.2.3.2.3; yêu cầu về quản lý phiên bản và cập nhật tập luật được quy định tại 5.2.3.2. SIEM phải ghi nhật ký đối với hoạt động cập nhật tập luật, bao gồm:

a) Kiểm tra và tải về bản cập nhật mới;

b) Cập nhật tập luật do nhà sản xuất phát hành.

# 5 Yêu cầu về chức năng nghiệp vụ của nền tảng

## 5.1 Khái quát

Mục này quy định các yêu cầu về chức năng nghiệp vụ của nền tảng SIEM, bao gồm quản lý và tiếp nhận dữ liệu nhật ký; chuẩn hóa, làm giàu, lưu trữ và bảo vệ dữ liệu; phân tích, tương quan, phát hiện và cảnh báo; điều tra, truy vấn, báo cáo; tích hợp với các hệ thống khác; và yêu cầu về hiệu năng, khả năng mở rộng, tính sẵn sàng và phục hồi.

## 5.2 Yêu cầu cụ thể

### 5.2.1 Quản lý nguồn, tiếp nhận và vòng đời dữ liệu nhật ký

#### 5.2.1.1 Quản lý danh mục đối tượng và nguồn gửi nhật ký

##### 5.2.1.1.1 Quản lý danh mục đối tượng được giám sát và nguồn gửi

SIEM phải cho phép:

a) Quản lý đối tượng được giám sát và nguồn gửi nhật ký theo các nhóm do quản trị viên định nghĩa;

b) Quản lý đối tượng được giám sát và nguồn gửi nhật ký theo địa chỉ vật lý, địa chỉ mạng và vị trí địa lý.

##### 5.2.1.1.2 Xác thực nguồn gửi

SIEM phải cho phép:

a) Xác thực nguồn gửi nhật ký;

b) Kiểm soát kết nối từ Collector;

c) Phát hiện nguồn gửi không hợp lệ.

#### 5.2.1.2 Tiếp nhận dữ liệu

##### 5.2.1.2.1 Cách thức và giao thức tiếp nhận nhật ký

SIEM phải cho phép tiếp nhận nhật ký gửi từ Collector thông qua:

a) UDP;

b) TCP;

c) TCP có mã hóa như TLS hoặc tương đương;

d) API;

đ) Bộ kết nối lấy nhật ký trực tiếp từ môi trường đám mây;

e) Hỗ trợ các nguồn dữ liệu khác theo kiến trúc của nền tảng.

##### 5.2.1.2.2 Đồng bộ thời gian dữ liệu đầu vào

SIEM phải cho phép đồng bộ thời điểm nhật ký được tiếp nhận tại Receiver với thời điểm nhật ký được thu thập tại Collector dựa trên thiết lập múi giờ.

##### 5.2.1.2.3 Phương thức thu thập bổ sung

Ngoài các phương thức quy định tại 5.2.1.2.1, SIEM nên hỗ trợ tối thiểu 03 trong số các phương thức sau:

a) tiếp nhận tệp nhật ký qua giao thức chia sẻ tệp hoặc truyền tệp an toàn;

b) đọc dữ liệu từ kho lưu trữ đối tượng;

c) tiêu thụ dữ liệu từ hàng đợi thông điệp hoặc luồng sự kiện;

d) tiếp nhận qua webhook;

đ) truy vấn trực tiếp cơ sở dữ liệu;

e) thu thập không cài đặt tác tử (agentless) đối với hệ điều hành Windows và Unix/Linux;

g) tiếp nhận bản tin SNMP;

h) tiếp nhận dữ liệu luồng mạng theo NetFlow, IPFIX hoặc sFlow.

#### 5.2.1.3 Giám sát luồng dữ liệu đầu vào

##### 5.2.1.3.1 Giám sát luồng nhật ký theo thời gian thực

SIEM phải cho phép:

a) Hiển thị thống kê dữ liệu theo thời gian thực;

b) Tìm kiếm và tạo thống kê dữ liệu theo khoảng thời gian;

c) truy vấn dữ liệu lịch sử trong toàn bộ khoảng thời gian lưu trữ do tổ chức thiết lập theo 5.2.2.2.1.

Nhà sản xuất phải công bố dung lượng lưu trữ cần thiết cho mỗi tháng dữ liệu ở từng mức quy mô triển khai quy định tại 5.2.6.1.1, tính theo mức lưu lượng nhật ký tương ứng.

**5.2.1.3.2 Giám sát hiệu năng và trạng thái quá trình tiếp nhận**

SIEM phải cho phép giám sát thông qua giao diện đồ họa:

a) Số lần thử kết nối lại;

b) Kết nối không thành công;

c) Số lượng tác vụ tiếp nhận không thành công;

d) Trạng thái kết nối tới Collector;

đ) Trạng thái quá trình tiếp nhận.

**5.2.1.3.3 Kiểm tra chất lượng dữ liệu nhật ký**

SIEM phải lưu trữ tất cả nhật ký dưới dạng dữ liệu thô, bất kể nhật ký có thể phân tích cú pháp được hay không. SIEM phải hỗ trợ:

a) Phát hiện dữ liệu không đúng định dạng;

b) Phát hiện dữ liệu thiếu trường;

c) Phát hiện dữ liệu trùng lặp;

d) Phát hiện dữ liệu không hợp lệ;

đ) Thống kê tỷ lệ dữ liệu lỗi/mất.

**5.2.1.3.4 Giám sát tính liên tục của nguồn gửi nhật ký**

SIEM phải:

a) thiết lập đường cơ sở về lưu lượng nhật ký cho từng nguồn gửi theo chu kỳ thời gian;

b) tự động cảnh báo khi một nguồn gửi ngừng gửi nhật ký quá ngưỡng thời gian cấu hình được, kể cả khi kết nối mạng tới nguồn đó vẫn ở trạng thái bình thường;

c) tự động cảnh báo khi lưu lượng nhật ký của một nguồn tăng hoặc giảm vượt ngưỡng so với đường cơ sở;

d) cảnh báo khi thời gian sinh sự kiện tại nguồn lệch so với thời gian tiếp nhận vượt ngưỡng cấu hình được;

đ) cung cấp báo cáo đối chiếu giữa danh mục tài sản được giám sát và danh sách nguồn đang gửi nhật ký, chỉ ra các tài sản chưa có nguồn nhật ký tương ứng.

#### 5.2.1.4 Quản lý bộ thu thập nhật ký

SIEM phải cho phép quản lý tập trung các Collector, bao gồm:

a) triển khai, cập nhật phiên bản và gỡ bỏ từ xa;

b) cấu hình tập trung theo nhóm Collector;

c) giám sát trạng thái hoạt động, phiên bản và mức tiêu thụ tài nguyên trên đối tượng cài đặt;

d) giới hạn mức tiêu thụ tài nguyên của Collector trên đối tượng được giám sát;

đ) đệm dữ liệu tại Collector khi mất kết nối tới Receiver và tự động gửi bù khi kết nối được khôi phục, với dung lượng và thời lượng đệm cấu hình được;

e) áp dụng cấu hình mới mà không làm gián đoạn quá trình thu thập.

#### 5.2.1.5 Xử lý dữ liệu tại đầu vào

SIEM phải cho phép:

a) lọc, loại bỏ các sự kiện theo quy tắc do quản trị viên định nghĩa trước khi lập chỉ mục;

b) gộp các sự kiện trùng lặp liên tiếp;

c) định tuyến dữ liệu tới các tầng lưu trữ hoặc hệ thống đích khác nhau theo quy tắc;

d) theo dõi và hiển thị mức tiêu thụ năng lực xử lý và dung lượng lưu trữ so với năng lực được cấp phép, kèm cảnh báo sớm khi mức tiêu thụ tiệm cận ngưỡng cấu hình được.

#### 5.2.1.6 Nạp lại dữ liệu nhật ký

SIEM phải cho phép xử lý lại dữ liệu nhật ký thô đã lưu trữ sau khi cập nhật bộ phân tích cú pháp hoặc sau sự cố, bảo đảm không phát sinh bản ghi trùng lặp và không làm mất dữ liệu đã có.

### 5.2.2 Chuẩn hóa, làm giàu, lưu trữ và bảo vệ dữ liệu

#### 5.2.2.1 Xử lý dữ liệu

##### 5.2.2.1.1 Phân tích cú pháp, chuẩn hóa và định dạng nhật ký

SIEM phải tiếp nhận và chuẩn hóa nhật ký gửi từ Collector tối thiểu 50 loại thiết bị/ứng dụng khác nhau.

SIEM phải hỗ trợ tối thiểu 03 trong các định dạng: SYSLOG; JSON; CSV; CEF; NETFLOW, trong đó bắt buộc phải có SYSLOG.

SIEM phải chuẩn hóa được nhật ký của:

a) Hệ điều hành Windows và Unix/Linux;

b) Thiết bị bảo mật như tường lửa, IPS/IDS;

c) Thiết bị mạng như Router, Switch;

d) nền tảng điều phối vùng chứa và thời gian chạy vùng chứa;

đ) nền tảng ảo hóa máy chủ.

CHÚ THÍCH: Ví dụ về nền tảng điều phối vùng chứa là Kubernetes; ví dụ về nền tảng ảo hóa máy chủ là VMware vSphere, Microsoft Hyper-V.

**5.2.2.1.2 Xử lý và ánh xạ dữ liệu địa chỉ IP/MAC cơ bản**

SIEM phải cho phép:

a) Xử lý địa chỉ Ipv4, IPv6;

b) Tìm kiếm theo địa chỉ IP hoặc dải địa chỉ;

c) ánh xạ các trường địa chỉ mạng.

**5.2.2.1.3 Làm giàu thông tin**

SIEM phải cho phép:

a) Làm giàu thông tin cho nhật ký, ví dụ phân giải chuỗi định danh thành tên tài khoản người dùng hoặc lưu lại thời điểm sinh nhật ký theo múi giờ cục bộ;

b) Tự động làm giàu dữ liệu nhật ký ngay tại thời điểm thu thập bằng cách bổ sung ngữ cảnh từ các nguồn dữ liệu bên ngoài;

c) Tích hợp các luồng dữ liệu tình báo mối đe dọa để tự động so khớp và nhận diện rủi ro.

**5.2.2.1.4 Mô hình dữ liệu chuẩn hóa**

SIEM phải:

a) áp dụng và công bố một mô hình dữ liệu chuẩn gồm danh mục các trường thông tin, kiểu dữ liệu và ý nghĩa của từng trường;

b) quản lý phiên bản của mô hình dữ liệu và công bố các thay đổi giữa các phiên bản;

c) cho phép mở rộng mô hình dữ liệu bằng các trường tùy biến do tổ chức định nghĩa;

d) lưu đồng thời thời điểm sinh sự kiện tại nguồn, thời điểm thu thập và thời điểm tiếp nhận;

đ) lưu trữ mốc thời gian theo múi giờ chuẩn và cho phép hiển thị theo múi giờ do người dùng lựa chọn, với độ phân giải tối thiểu đến mili giây.

#### 5.2.2.1.5 Xây dựng và kiểm thử bộ phân tích cú pháp

SIEM phải cho phép:

a) xây dựng bộ phân tích cú pháp mới cho các nguồn nhật ký chưa được hỗ trợ sẵn, thông qua giao diện đồ họa hoặc trình soạn thảo mã;

b) kiểm thử bộ phân tích cú pháp trên tập dữ liệu mẫu và hiển thị kết quả bóc tách trường trước khi đưa vào áp dụng;

c) quản lý phiên bản và khôi phục phiên bản trước của bộ phân tích cú pháp;

d) áp dụng bộ phân tích cú pháp mới mà không cần khởi động lại hệ thống;

đ) thống kê tỷ lệ nhật ký phân tích cú pháp thành công theo từng nguồn.

### 5.2.2.2 Lưu trữ và quản lý vòng đời

#### 5.2.2.2.1 Lưu trữ trực tuyến, ngoại tuyến và chính sách luân chuyển

SIEM phải cho phép thiết lập, cấu hình các tham số liên quan đến lưu trữ và hủy bỏ nhật ký, bao gồm:

a) Ngưỡng giới hạn dung lượng lưu trữ;

b) Khoảng thời gian lưu trữ;

c) Các tham số quản lý vòng đời dữ liệu.

SIEM phải bảo đảm dữ liệu nhật ký bị hủy khi hết thời hạn lưu trữ không còn khôi phục được thông qua chức năng của sản phẩm, và phải ghi nhật ký mỗi lần thực hiện việc hủy, bao gồm phạm vi dữ liệu bị hủy, thời điểm và căn cứ chính sách áp dụng.

Yêu cầu cảnh báo khi dung lượng lưu trữ đạt ngưỡng giới hạn được quy định tại 5.2.3.4.1.

#### 5.2.2.2.2 Quản lý chỉ mục phục vụ truy vấn

SIEM phải cho phép tìm kiếm nhật ký theo từ khóa trên tất cả các trường thông tin, bao gồm cả trường thông tin cấp thấp hơn nếu có, và phân nhóm nhật ký thành các nhóm sự kiện theo các tiêu chí khác nhau, ví dụ mức độ quan trọng, dạng tấn công, nguồn nhật ký.

#### 5.2.2.2.3 Phân tầng lưu trữ và khôi phục dữ liệu

SIEM phải:

a) hỗ trợ phân tầng lưu trữ theo mức độ sẵn sàng truy vấn, tối thiểu gồm tầng truy vấn trực tuyến và tầng lưu trữ dài hạn;

b) cho phép cấu hình thời gian lưu trữ độc lập cho từng tầng và từng nhóm nguồn nhật ký;

c) cho phép khôi phục dữ liệu từ tầng lưu trữ dài hạn về trạng thái truy vấn được, có thông báo tiến độ và thời điểm hoàn tất;

d) bảo đảm dữ liệu sau khi khôi phục giữ nguyên tính toàn vẹn, kiểm chứng được bằng giá trị băm đã lưu.

**5.2.2.3 Bảo vệ dữ liệu nhật ký**

**5.2.2.3.1 Truyền dữ liệu an toàn**

SIEM phải cho phép mã hóa dữ liệu hoặc sử dụng giao thức có mã hóa để trao đổi dữ liệu giữa Collector và Receiver.

**5.2.2.3.2 Đảm bảo tính toàn vẹn của dữ liệu lưu trữ**

SIEM phải bảo đảm dữ liệu nhật ký đã lưu không bị mất mát hoặc thay đổi trạng thái trong trường hợp hệ thống phải khởi động lại do lỗi phần mềm. SIEM phải có cơ chế bảo đảm tính toàn vẹn dữ liệu trong quá trình thu thập, phân tích và lưu trữ. SIEM phải hỗ trợ:

a) Sử dụng thuật toán băm mật mã và đối soát tổng để phát hiện, ngăn ngừa sửa đổi hoặc xóa bỏ trái phép;

b) Tự sinh nhật ký kiểm toán đối với tác vụ quản trị và thay đổi cấu hình;

c) Vô hiệu hóa khả năng chỉnh sửa hoặc xóa bản ghi nhật ký từ các cấp quyền quản trị;

d) xuất dữ liệu nhật ký sang nền tảng lưu trữ chỉ ghi một lần, đọc nhiều lần (WORM) do bên triển khai cung cấp, theo định dạng và cơ chế mà nền tảng đó tiếp nhận được;

đ) hỗ trợ kiểm tra tính toàn vẹn của các tệp nhật ký đã chuyển sang trạng thái lưu trữ tĩnh theo lịch do quản trị viên thiết lập.

**5.2.2.3.3 Mã hóa dữ liệu lưu trữ, kiểm soát truy cập dữ liệu nhạy cảm**

SIEM nên hỗ trợ mã hóa dữ liệu nhật ký ở trạng thái lưu trữ bằng thuật toán mật mã được thừa nhận rộng rãi hoặc theo quy định hiện hành, và cho phép cấu hình bật hoặc tắt cơ chế này theo từng tầng lưu trữ quy định tại 5.2.2.2.3.

SIEM nên hỗ trợ giao tiếp với thiết bị bảo mật phần cứng (HSM) hoặc hệ thống quản lý khóa (KMS) theo chuẩn quốc tế hoặc quy định hiện hành để quản lý vòng đời khóa mật mã sử dụng trong ký số và bảo vệ tính toàn vẹn dữ liệu nhật ký.

**5.2.2.3.4 Che giấu và ẩn danh dữ liệu nhạy cảm**

Yêu cầu về che dữ liệu nhạy cảm được quy định tại 5.2.7.3.

**5.2.3 Phân tích, tương quan, phát hiện và cảnh báo**

**5.2.3.1 Phân tích tương quan sự kiện theo thời gian thực dựa trên luật**

SIEM phải cho phép phân tích tương quan sự kiện theo thời gian thực đối với dữ liệu nhật ký thu thập được.

SIEM phải hỗ trợ tối thiểu các phương thức phát hiện sau:

a) phát hiện theo ngưỡng và theo tần suất trong cửa sổ thời gian;

b) phát hiện theo chuỗi sự kiện có ràng buộc về thứ tự và khoảng thời gian;

c) phát hiện theo sai lệch so với đường cơ sở thống kê;

d) phát hiện bằng đối sánh với danh sách động và bảng tham chiếu;

đ) phát hiện bằng truy vấn thực thi theo lịch;

e) phát hiện tương quan giữa các sự kiện từ nhiều nguồn nhật ký khác nhau;

g) tích lũy điểm rủi ro theo thực thể và sinh cảnh báo khi vượt ngưỡng.

**5.2.3.2 Quản lý tập luật**

**5.2.3.2.1 Chức năng quản lý tập luật**

SIEM phải cho phép:

a) Xây dựng quy tắc tương quan thông qua giao diện đồ họa;

b) Xây dựng quy tắc tương quan bằng trình soạn thảo mã nguồn;

c) Quản lý phiên bản quy tắc và theo dõi lịch sử thay đổi;

d) Tối ưu hóa thuật toán và tinh chỉnh tham số của quy tắc;

đ) Phân tích tương quan sử dụng thông tin trong danh sách động, ví dụ địa chỉ IP, tên miền hoặc giá trị hàm băm có thể được cập nhật tự động từ nhà sản xuất.

**5.2.3.2.2 Xây dựng, tùy biến quy tắc tương quan và ngưỡng phát hiện**

Các quy tắc tương quan phải cho phép xây dựng, tùy biến và tinh chỉnh để đáp ứng các kịch bản phát hiện khác nhau.

**5.2.3.2.3 Thư viện tập luật cho các kịch bản đe dọa điển hình**

SIEM phải hỗ trợ thư viện tập luật tương quan và bảng điều khiển được tối ưu cho các kịch bản đe dọa điển hình, tối thiểu:

a) mã độc tống tiền;

b) tấn công lừa đảo qua thư điện tử;

c) di chuyển ngang trong mạng nội bộ;

d) lạm dụng tài khoản đặc quyền.

#### 5.2.3.2.4 Ánh xạ luật phát hiện theo khung phân loại kỹ thuật tấn công

SIEM phải:

a) cho phép gắn cho mỗi luật phát hiện một hoặc nhiều thẻ định danh chiến thuật, kỹ thuật tấn công theo khung phân loại được thừa nhận rộng rãi;

b) cho phép tìm kiếm, lọc và lập báo cáo tập luật theo thẻ đã gắn;

c) gán các thẻ của luật cho cảnh báo và hồ sơ sự cố được sinh ra từ luật đó;

d) xuất dữ liệu ánh xạ giữa luật và khung phân loại qua giao diện lập trình hoặc tệp có cấu trúc, phục vụ phân tích bằng công cụ bên ngoài;

đ) cho phép cập nhật danh mục thẻ khi khung phân loại được sửa đổi, mà không làm mất ánh xạ đã thiết lập.

SIEM nên cung cấp báo cáo trực quan về độ phủ phát hiện theo khung phân loại, có đối chiếu với các nguồn nhật ký đang được thu thập.

CHÚ THÍCH: Ví dụ về khung phân loại kỹ thuật tấn công được thừa nhận rộng rãi là MITRE ATT&CK.

#### 5.2.3.2.5 Kiểm thử và đánh giá hiệu quả luật

SIEM phải cho phép:

a) thực thi thử một luật trên dữ liệu lịch sử và hiển thị kết quả mà không sinh cảnh báo thực;

b) ước lượng số lượng cảnh báo dự kiến phát sinh trước khi kích hoạt luật;

c) vận hành luật ở chế độ theo dõi, chỉ ghi nhận không phát cảnh báo tới người dùng;

d) thống kê theo từng luật: số lần kích hoạt, kết quả phân loại sau xử lý, thời điểm kích hoạt gần nhất, mức tiêu thụ tài nguyên khi thực thi;

đ) tự động phát hiện và cảnh báo các luật không còn hiệu lực do trường dữ liệu tham chiếu không còn được điền hoặc nguồn nhật ký liên quan đã ngừng gửi.

#### 5.2.3.2.6 Quản lý ngoại lệ

SIEM phải cho phép quản lý các ngoại lệ áp dụng cho luật phát hiện, mỗi ngoại lệ gồm tối thiểu: phạm vi áp dụng, lý do, người tạo, thời điểm tạo và thời hạn hiệu lực. SIEM phải cảnh báo khi ngoại lệ hết hạn và cho phép rà soát định kỳ toàn bộ ngoại lệ đang áp dụng.

#### 5.2.3.2.7 Quản lý luật dưới dạng mã

SIEM phải:

a) cho phép xuất và nhập luật ở định dạng văn bản có cấu trúc, đọc được bằng công cụ bên ngoài;

b) cung cấp giao diện lập trình cho phép tạo, sửa, xóa, kích hoạt và truy vấn luật;

c) cho phép nhập luật theo ít nhất một định dạng luật mở được thừa nhận rộng rãi;

d) hỗ trợ tách biệt môi trường thử nghiệm và môi trường vận hành đối với tập luật.

CHÚ THÍCH: Ví dụ về định dạng luật mở được thừa nhận rộng rãi là Sigma.

**5.2.3.3 Cung cấp ngữ cảnh phát hiện**

**5.2.3.3.1 Quản lý và liên kết ngữ cảnh tài sản**

SIEM phải hỗ trợ quản lý tài sản tập trung, lưu trữ lịch sử cấu hình của hệ điều hành, ứng dụng và liên kết thông tin tài sản với các sự kiện để phục vụ phân tích sự cố.

**5.2.3.3.2 Tiếp nhận và liên kết thông tin lỗ hổng bảo mật**

SIEM phải hỗ trợ tích hợp trực tiếp dữ liệu lỗ hổng bảo mật trên từng tài sản để phục vụ phân tích ngữ cảnh sự cố.

**5.2.3.3.3 Sử dụng thông tin tình báo mối đe dọa trong phân tích ngữ cảnh**

SIEM phải:

a) hiển thị ngữ cảnh tình báo mối đe dọa kèm theo cảnh báo và kết quả tìm kiếm khi có đối sánh với dữ liệu nhật ký, tối thiểu gồm: loại chỉ báo, mức độ tin cậy và nguồn cung cấp;

b) tự động rà soát dữ liệu nhật ký lịch sử khi tiếp nhận chỉ báo mới từ nền tảng tình báo mối đe dọa và sinh cảnh báo đối với các kết quả trùng khớp;

c) cho phép giới hạn phạm vi rà soát hồi tố quy định tại điểm b) theo khoảng thời gian và theo nhóm nguồn nhật ký để kiểm soát tải xử lý.

SIEM nên:

d) hỗ trợ tiếp nhận đồng thời nhiều nguồn tình báo mối đe dọa đối với tổ chức chưa triển khai nền tảng tình báo mối đe dọa (TIP) riêng biệt;

đ) trong trường hợp quy định tại điểm d), quản lý thuộc tính tối thiểu của từng chỉ báo tiếp nhận trực tiếp, gồm nguồn cung cấp, mức độ tin cậy và thời hạn hiệu lực, và tự động loại bỏ chỉ báo đã hết hạn.

CHÚ THÍCH: Việc quản lý vòng đời, mức độ tin cậy và khử trùng lặp chỉ báo tình báo mối đe dọa từ nhiều nguồn là chức năng chính của nền tảng tình báo mối đe dọa (TIP), được quy định tại tiêu chuẩn quốc gia riêng về TIP.

#### 5.2.3.3.4 Định danh tài sản trong môi trường động

SIEM phải:

a) định danh tài sản theo mã định danh tài nguyên, tên máy hoặc thẻ gán, không phụ thuộc duy nhất vào địa chỉ mạng;

b) lưu lịch sử ánh xạ giữa địa chỉ mạng và tài sản theo thời gian, cho phép xác định tài sản tương ứng với một địa chỉ mạng tại thời điểm sự kiện phát sinh;

c) đồng bộ danh mục tài sản từ hệ thống quản lý cấu hình, dịch vụ thư mục và giao diện lập trình của nền tảng điện toán đám mây.

### 5.2.3.4 Cảnh báo sự cố

#### 5.2.3.4.1 Cơ chế cảnh báo và phân loại mức độ nghiêm trọng

SIEM phải tự động cảnh báo theo thời gian thực đối với:

a) Việc hệ thống ngừng lưu trữ dữ liệu mới khi dung lượng lưu trữ đạt ngưỡng giới hạn;

b) Dấu hiệu, nguy cơ, sự cố, cuộc tấn công và hành vi gây mất an ninh mạng dựa trên kết quả thực thi luật phân tích tương quan;

c) Các nhóm đối tượng được giám sát, ví dụ truy cập máy chủ email hoặc truy cập từ xa vào dải địa chỉ IP dành cho máy chủ.

#### 5.2.3.4.2 Phân phối cảnh báo đa phương thức

SIEM phải hỗ trợ:

a) Hiển thị cảnh báo trên giao diện đồ họa quản lý cảnh báo;

b) Gửi cảnh báo qua thư điện tử;

c) Gửi cảnh báo thông qua API;

d) Gửi cảnh báo tới nền tảng nhắn tin thông qua webhook hoặc giao diện lập trình.

#### 5.2.3.4.3 Xử lý và tinh giản cảnh báo trước khi phân phối

SIEM phải:

a) khử trùng lặp các cảnh báo giống nhau phát sinh liên tiếp từ cùng một luật và cùng đối tượng liên quan;

b) gộp các cảnh báo liên quan thành một nhóm hoặc một sự cố theo tiêu chí cấu hình được, tối thiểu theo thực thể liên quan và theo luật phát hiện;

c) tự động giới hạn tần suất phân phối cảnh báo khi một luật phát sinh vượt ngưỡng trong khoảng thời gian xác định, đồng thời cảnh báo cho quản trị viên về hiện tượng này.

#### 5.2.3.4.4 Bảo đảm phân phối cảnh báo

SIEM phải:

a) ghi nhận trạng thái gửi của từng cảnh báo theo từng kênh phân phối quy định tại 5.2.3.4.2;

b) cảnh báo cho quản trị viên khi việc gửi cảnh báo không thành công;

c) hỗ trợ cơ chế xác nhận đã tiếp nhận cảnh báo đối với các kênh có hỗ trợ.

### 5.2.3.5 Phân tích hành vi nâng cao

SIEM phải:

a) xây dựng đường cơ sở hành vi cho từng thực thể, tối thiểu đối với tài khoản người dùng và máy chủ hoặc máy trạm, dựa trên dữ liệu nhật ký lịch sử;

b) phát hiện và cảnh báo sai lệch so với đường cơ sở quy định tại điểm a) mà không phụ thuộc vào việc có luật phát hiện tĩnh tương ứng hay không;

c) cho phép cấu hình khoảng thời gian học đường cơ sở và ngưỡng sai lệch sinh cảnh báo;

d) hiển thị căn cứ dẫn tới cảnh báo hành vi bất thường, tối thiểu gồm giá trị quan sát, giá trị đường cơ sở và mức sai lệch;

đ) cho phép người dùng phản hồi kết quả phân loại đối với cảnh báo hành vi bất thường và sử dụng phản hồi đó để hiệu chỉnh mô hình hoặc đường cơ sở.

CHÚ THÍCH: Các yêu cầu tại điều này không ràng buộc kỹ thuật cụ thể được sử dụng để xây dựng đường cơ sở và phát hiện sai lệch; các kỹ thuật thống kê, học máy hoặc kết hợp đều được chấp nhận nếu đáp ứng các yêu cầu nêu trên.

## 5.2.4 Điều tra, truy vấn, săn lùng, trực quan và báo cáo

### 5.2.4.1 Truy vấn, tìm kiếm và lọc dữ liệu sự kiện

#### 5.2.4.1.1 Khái quát

SIEM phải cho phép:

a) tìm kiếm dữ liệu nhật ký bằng từ khóa để xem lại;

b) tìm kiếm trên các trường thông tin của nhật ký và dữ liệu lịch sử.

#### 5.2.4.1.2 Năng lực của ngôn ngữ truy vấn

Ngôn ngữ truy vấn của SIEM phải hỗ trợ tối thiểu:

a) tìm kiếm theo từ khóa và theo trường thông tin, bao gồm trường lồng nhau;

b) biểu thức chính quy;

c) toán tử logic và toán tử so sánh;

d) hàm tổng hợp và thống kê;

đ) phép kết hợp dữ liệu giữa các nguồn nhật ký khác nhau và với bảng tham chiếu;

e) truy vấn lồng nhau;

g) giới hạn phạm vi theo khoảng thời gian, bao gồm cả thời gian tương đối;

h) truy vấn trên dữ liệu thô chưa được phân tích cú pháp;

i) lưu, đặt tên, chia sẻ và tái sử dụng truy vấn.

**5.2.4.1.3 Tác vụ truy vấn nền**

SIEM phải cho phép thực thi truy vấn trên khối lượng dữ liệu lớn dưới dạng tác vụ nền, có hiển thị tiến độ, cho phép hủy tác vụ, thông báo khi hoàn tất và không làm suy giảm năng lực xử lý cảnh báo theo thời gian thực.

**5.2.4.2 Săn lùng mối đe dọa, điều tra và quản lý sự cố**

**5.2.4.2.1 Khái quát**

SIEM phải cung cấp công cụ và ngôn ngữ truy vấn linh hoạt, cho phép chuyên viên an ninh mạng chủ động thực hiện các chiến dịch săn lùng mối đe dọa.

**5.2.4.2.2 Hỗ trợ luồng công việc điều tra chủ động và phân tích nguyên nhân gốc**

SIEM phải hỗ trợ:

a) Trực quan hóa luồng tấn công;

b) Tự động xâu chuỗi và liên kết các sự kiện cảnh báo rời rạc từ mạng, máy chủ và đám mây;

c) Hiển thị luồng sự kiện theo trình tự thời gian;

d) Phân tích, điều tra và xác định nguyên nhân gốc.

**5.2.4.2.3 Quản lý các trường hợp sự cố**

SIEM phải hỗ trợ quản lý trạng thái xử lý và vòng đời sự cố.

Việc quản lý trạng thái xử lý và vòng đời sự cố quy định tại đoạn trên phải bao gồm tối thiểu:

a) hiển thị cảnh báo dưới dạng hàng đợi có thể lọc và sắp xếp theo mức ưu tiên, trạng thái, thời gian phát sinh và người được giao xử lý;

b) giao cảnh báo cho một chuyên viên xử lý và ngăn ngừa việc hai chuyên viên cùng xử lý một cảnh báo tại một thời điểm;

c) chuyển đổi trạng thái xử lý cảnh báo theo một quy trình xác định trước;

d) phân loại kết quả xử lý theo danh mục chuẩn hóa, tối thiểu gồm: đúng, sai, đúng nhưng đã được chấp nhận, trùng lặp; kèm theo lý do;

đ) truy xuất từ cảnh báo tới sự kiện thô đã kích hoạt cảnh báo và tới nội dung luật phát hiện tương ứng;

e) hiển thị hướng dẫn xử lý được gắn kèm theo luật phát hiện tương ứng, nếu có;

g) ghi nhật ký đầy đủ các thao tác xử lý cảnh báo, bao gồm người thực hiện và thời điểm thực hiện.

Kết quả phân loại quy định tại điểm d) phải được lưu trữ để phục vụ đánh giá hiệu quả luật phát hiện.

**5.2.4.2.4 Hỗ trợ vận hành nghiệp vụ giám sát an ninh mạng liên tục**

SIEM nên hỗ trợ:

a) thiết lập thời hạn xử lý cảnh báo theo mức ưu tiên và cảnh báo khi quá thời hạn;

b) chuyển cảnh báo tới người xử lý tiếp theo khi quá thời hạn xử lý mà chưa được tiếp nhận;

c) lập báo cáo cảnh báo còn tồn và ghi chú phục vụ bàn giao giữa các ca trực;

d) cung cấp báo cáo và bảng điều khiển về hiệu quả vận hành, tối thiểu gồm: thời gian trung bình từ khi cảnh báo phát sinh đến khi được tiếp nhận xử lý, thời gian trung bình xử lý cảnh báo, số lượng cảnh báo theo luật và theo mức độ nghiêm trọng, tỷ lệ cảnh báo được phân loại là sai.

CHÚ THÍCH: Các chức năng quy định tại điều này có thể được thực hiện trên SIEM hoặc trên hệ thống điều phối, tự động hóa và phản ứng an ninh mạng (SOAR) tích hợp với SIEM theo 5.2.5.3.3. Tổ chức chỉ triển khai SIEM mà không triển khai SOAR có thể sử dụng các chức năng quy định tại điều này để duy trì hoạt động giám sát liên tục.

**5.2.4.2.5 Khung nhìn theo thực thể**

SIEM phải cung cấp khung nhìn tổng hợp theo thực thể, tối thiểu đối với tài khoản người dùng, máy chủ hoặc máy trạm và địa chỉ mạng, bao gồm toàn bộ sự kiện, cảnh báo, thông tin tài sản và lỗ hổng liên quan trong khoảng thời gian lựa chọn, và cho phép chuyển tiếp điều tra sang thực thể liên quan.

**5.2.4.2.6 Quản lý chiến dịch săn lùng**

SIEM phải cho phép:

a) lưu trữ giả thuyết săn lùng cùng tập truy vấn và kết quả tương ứng;

b) thực thi lại chiến dịch săn lùng theo lịch;

c) chuyển đổi truy vấn săn lùng thành luật phát hiện.

**5.2.4.2.7 Quản lý hồ sơ sự cố**

SIEM phải cho phép quản lý hồ sơ sự cố với tối thiểu các nội dung:

a) thông tin định danh, mức ưu tiên và trạng thái xử lý;

b) người được giao xử lý và lịch sử chuyển giao;

c) dòng thời gian diễn biến sự cố;

d) danh sách cảnh báo, thực thể và chỉ báo liên quan;

đ) đầu việc cần thực hiện và trạng thái hoàn thành;

e) bằng chứng đính kèm và ghi chú của chuyên viên;

g) ánh xạ tới các kỹ thuật tấn công liên quan theo 5.2.3.2.4;

h) xuất báo cáo tổng hợp về sự cố.

**5.2.4.3 Trực quan hóa và báo cáo**

**5.2.4.3.1 Bảng điều khiển tổng quan (Dashboard)**

SIEM phải cung cấp giao diện đồ họa phục vụ quản lý, trực quan hóa và theo dõi các sự kiện, cảnh báo và trạng thái hệ thống.

**5.2.4.3.2 Lập lịch, quản lý và xuất báo cáo vận hành cơ bản**

SIEM phải cho phép:

a) Tạo mới, xem lại và xóa báo cáo;

b) Tạo báo cáo theo các mẫu được định nghĩa trước;

c) Áp dụng các quy tắc tìm kiếm dữ liệu nhật ký để thêm, lọc và tinh chỉnh nội dung báo cáo;

d) Lựa chọn định dạng tệp báo cáo, tối thiểu một trong các định dạng WORD, EXCEL, PDF, HTML, XML;

đ) Tải về tệp báo cáo đã xuất.

**5.2.4.3.3 Trích xuất dữ liệu thô phục vụ điều tra**

SIEM phải cho phép:

a) Truy xuất dữ liệu thô của nhật ký thông qua kết quả tìm kiếm và cảnh báo;

b) Xuất dữ liệu nhật ký phục vụ tích hợp vào SIEM hoặc giải pháp khác về quản lý, phân tích và điều tra nhật ký.

#### 5.2.4.3.4 Báo cáo hiệu quả vận hành

SIEM nên cung cấp báo cáo và bảng điều khiển về hiệu quả vận hành bổ sung cho 5.2.4.2.4, tối thiểu gồm: khối lượng công việc theo từng chuyên viên xử lý và mức độ tuân thủ thời hạn xử lý theo mức ưu tiên.

#### 5.2.4.3.5 Xuất dữ liệu phục vụ điều tra và tố tụng

SIEM phải:

a) tạo gói dữ liệu xuất kèm tệp kê khai chứa giá trị băm mật mã của từng tệp dữ liệu;

b) ghi nhận trong gói xuất: điều kiện truy vấn, phạm vi thời gian dữ liệu, thời điểm xuất và định danh người thực hiện;

c) ghi nhật ký mọi hoạt động xuất dữ liệu, bao gồm cả trường hợp thực hiện không thành công.

SIEM nên hỗ trợ ký số gói dữ liệu xuất.

CHÚ THÍCH: Giá trị băm mật mã quy định tại điểm a) cho phép bên thứ ba kiểm chứng tính toàn vẹn của gói dữ liệu xuất bằng công cụ độc lập.

### 5.2.5 Tích hợp và tương tác với hệ thống khác

#### 5.2.5.1 Giao diện và kết nối chia sẻ dữ liệu

#### 5.2.5.1.1 Cung cấp giao diện hoặc API truy xuất dữ liệu mở

SIEM phải cung cấp khả năng kết nối và trao đổi dữ liệu thông qua giao diện hoặc API phù hợp.

#### 5.2.5.1.2 Chuyển tiếp sự kiện tới hệ thống cấp trên

SIEM phải cho phép kết nối và chia sẻ dữ liệu với:

a) Hệ thống giám sát của cơ quan chức năng, cơ quan quản lý nhà nước theo quy định hiện hành;

b) Hệ thống SIEM khác do chính nhà sản xuất phát triển.

#### 5.2.5.1.3 Giao diện lập trình cho các chức năng nghiệp vụ

SIEM phải cung cấp giao diện lập trình có tài liệu mô tả, hỗ trợ tối thiểu các nhóm chức năng: quản lý nguồn nhật ký, quản lý luật phát hiện, thực thi truy vấn và lấy kết quả, quản lý cảnh báo và hồ sơ sự cố, truy xuất trạng thái và chỉ số vận hành của hệ thống. Giao diện lập trình phải áp dụng cơ chế xác thực, phân quyền và giới hạn tần suất truy cập.

#### 5.2.5.2 Trao đổi dữ liệu

#### 5.2.5.2.1 Hỗ trợ các định dạng sự kiện phổ biến

Yêu cầu về định dạng nhật ký được hỗ trợ được quy định tại 5.2.2.1.1.

#### 5.2.5.2.2 Xác thực thiết bị, bảo mật kênh truyền và xử lý lỗi khi tương tác

SIEM phải hỗ trợ:

a) Xác thực nguồn gửi;

b) Mã hóa dữ liệu hoặc sử dụng giao thức có mã hóa khi trao đổi dữ liệu;

c) Theo dõi và thông báo lỗi trong quá trình kết nối, truyền nhận dữ liệu.

### 5.2.5.3 Tích hợp hệ thống

#### 5.2.5.3.1 Tích hợp nền tảng tình báo mối đe dọa an ninh mạng (TIP)

SIEM phải hỗ trợ tích hợp tình báo mối đe dọa, bao gồm khả năng tích hợp theo chuẩn STIX/TAXII và tự động so khớp dữ liệu tình báo với dữ liệu nhật ký.

#### 5.2.5.3.2 Tích hợp với hệ thống quản lý dịch vụ công nghệ thông tin và xử lý sự cố

SIEM phải hỗ trợ tích hợp với các hệ thống phục vụ quản lý dịch vụ CNTT và xử lý sự cố thông qua giao diện/API phù hợp.

#### 5.2.5.3.3 Đồng bộ hai chiều với hệ thống điều phối, tự động hóa, phản ứng và hệ thống quản lý dịch vụ công nghệ thông tin bên ngoài

SIEM phải hỗ trợ:

a) chuyển cảnh báo và ngữ cảnh liên quan tới hệ thống điều phối, tự động hóa và phản ứng an ninh mạng (SOAR) hoặc hệ thống quản lý dịch vụ công nghệ thông tin và xử lý sự cố quy định tại 5.2.5.3.2;

b) tiếp nhận cập nhật ngược về trạng thái xử lý và kết quả phân loại của cảnh báo từ hệ thống bên ngoài quy định tại điểm a);

c) duy trì tham chiếu định danh giữa cảnh báo trên SIEM và hồ sơ tương ứng trên hệ thống bên ngoài;

d) sử dụng kết quả phân loại tiếp nhận từ hệ thống bên ngoài làm dữ liệu đầu vào cho việc đánh giá hiệu quả luật phát hiện, tương đương với kết quả phân loại được xử lý trực tiếp trên SIEM theo 5.2.4.2.3.

### 5.2.6 Hiệu năng, khả năng mở rộng, tính sẵn sàng và phục hồi

SIEM được triển khai theo cấu hình tối thiểu trong tài liệu hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất phải đáp ứng:

#### 5.2.6.1 Yêu cầu về hiệu năng xử lý

##### 5.2.6.1.1 Năng lực xử lý sự kiện (EPS)

SIEM phải:

a) Nhà sản xuất phải công bố mức quy mô triển khai mà sản phẩm đáp ứng, tối thiểu một trong các mức sau, và sản phẩm phải đạt được năng lực xử lý tương ứng khi triển khai theo cấu hình tối thiểu đã công bố:

- Mức cơ bản: 3 000 EPS;

- Mức trung bình: 10 000 EPS;

- Mức cao: từ 50 000 EPS trở lên.

b) hỗ trợ kiểm thử năng lực xử lý bằng tập dữ liệu nhật ký mô phỏng có thành phần và tốc độ tương ứng với môi trường vận hành thực tế.

##### 5.2.6.1.2 Độ trễ xử lý từ khi nhận dữ liệu đến khi sinh cảnh báo

SIEM phải duy trì:

a) độ trễ từ khi tiếp nhận sự kiện đến khi sinh cảnh báo tối đa 02 phút đối với luật tương quan theo thời gian thực;

b) Độ trễ hiển thị dữ liệu thời gian thực trên màn hình tối đa 1 phút.

##### 5.2.6.1.3 Khả năng chịu tải đồng thời

SIEM phải đáp ứng đồng thời các yêu cầu sau:

a) tiếp nhận nhật ký theo thời gian thực đồng thời từ số lượng nguồn nhật ký tương ứng với mức quy mô triển khai quy định tại 5.2.6.1.1: tối thiểu 50 nguồn đối với mức cơ bản, 200 nguồn đối với mức trung bình và 500 nguồn đối với mức cao;

b) xử lý đồng thời theo thời gian thực tối thiểu 05 tác vụ tìm kiếm nhật ký của người dùng khác nhau đối với mức cơ bản và 20 tác vụ đối với mức cao, đồng thời với việc thực thi phân tích tương quan sự kiện.

##### 5.2.6.1.4 Thời gian đáp ứng truy vấn phân tích dữ liệu lớn

SIEM phải duy trì tốc độ truy vấn tìm kiếm trên khối lượng dữ liệu lịch sử lớn mà không làm suy giảm hiệu năng xử lý cảnh báo theo thời gian thực. Nhà sản xuất phải công bố thời gian đáp ứng truy vấn tối đa tương ứng với từng mức quy mô triển khai quy định tại 5.2.6.1.1, đo trên cấu hình tối thiểu đã công bố.

#### 5.2.6.2 Tính sẵn sàng và phục hồi

#### 5.2.6.2.1 Sao lưu và phục hồi cấu hình, tập luật, dữ liệu

Yêu cầu bảo toàn cấu hình khi hệ thống khởi động lại được quy định tại 4.2.3.1.

Ngoài ra, SIEM phải cho phép:

a) sao lưu và khôi phục cấu hình hệ thống, tập luật phát hiện, bộ phân tích cú pháp, mô hình dữ liệu, bảng điều khiển và hồ sơ sự cố;

b) sao lưu và khôi phục dữ liệu nhật ký đã lưu trữ theo phạm vi thời gian hoặc theo nhóm nguồn được lựa chọn;

c) thực hiện sao lưu theo lịch cấu hình được, có ghi nhận kết quả từng lần thực hiện;

d) kiểm chứng tính toàn vẹn của bản sao lưu trước khi khôi phục;

đ) khôi phục lên một hệ thống cài đặt mới cùng phiên bản mà không cần can thiệp thủ công vào cơ sở dữ liệu.

#### 5.2.6.2.2 Giám sát trạng thái của hệ thống

Yêu cầu về các thành phần nội bộ được giám sát quy định tại 4.2.2.1.

#### 5.2.6.2.3 Cơ chế đệm/phục hồi hàng đợi khi quá tải hoặc gián đoạn

SIEM phải:

a) duy trì hàng đợi bền vững tại thành phần tiếp nhận, bảo đảm dữ liệu đã được tiếp nhận không bị mất khi thành phần lập chỉ mục hoặc thành phần lưu trữ tạm thời không sẵn sàng;

b) cho phép cấu hình dung lượng và thời lượng tối đa của hàng đợi quy định tại điểm a);

c) cảnh báo cho quản trị viên khi mức chiếm dụng hàng đợi vượt ngưỡng cấu hình được;

d) áp dụng cơ chế kiểm soát áp lực ngược hoặc loại bỏ có kiểm soát theo thứ tự ưu tiên khi hàng đợi đầy, và ghi nhận số lượng sự kiện bị loại bỏ theo từng nguồn nhật ký.

#### 5.2.6.2.4 Dự phòng và độ sẵn sàng cao

SIEM phải:

a) Có khả năng thiết lập kiến trúc dự phòng, bảo đảm hệ thống vận hành liên tục;

b) Hỗ trợ triển khai kiến trúc phân tán cho môi trường quy mô lớn;

c) Có tùy chọn triển khai trên hạ tầng tại chỗ, hạ tầng điện toán đám mây hoặc kiến trúc lai;

d) Hỗ trợ kiến trúc mở rộng độc lập, cho phép tách biệt năng lực tính toán và năng lực lưu trữ, tích hợp với hồ dữ liệu;

đ) bảo đảm không có điểm lỗi đơn lẻ đối với từng thành phần quy định tại 5.2.6.2.2, không chỉ ở mức tổng thể hệ thống;

e) hỗ trợ cơ chế phát hiện lỗi và tự động chuyển đổi dự phòng (failover) giữa các node theo một trong các chế độ active-active, active-standby hoặc active-passive quy định tại 3.1.11, 3.1.12 và 3.1.13;

g) hỗ trợ đồng bộ trạng thái và dữ liệu giữa các node dự phòng, bảo đảm không mất dữ liệu đã được xác nhận ghi nhận khi xảy ra chuyển đổi dự phòng;

h) hỗ trợ cơ chế phát hiện và ngăn ngừa tình trạng phân mảnh trạng thái vận hành (split-brain) khi các node dự phòng mất liên lạc với nhau;

i) hỗ trợ triển khai các node dự phòng trên nhiều vùng sẵn sàng hoặc nhiều vị trí địa lý khác nhau đối với môi trường điện toán đám mây hoặc trung tâm dữ liệu phân tán;

k) cho phép kiểm tra chuyển đổi dự phòng mà không làm gián đoạn dịch vụ thu thập và phân tích dữ liệu.

Nhà sản xuất phải công bố điều kiện tiên quyết tối thiểu để cơ chế chuyển đổi dự phòng quy định tại điểm e) hoạt động đúng, tối thiểu gồm độ trễ tối đa và băng thông tối thiểu của kênh đồng bộ giữa các node.

**5.2.6.2.5 Giám sát chi tiết và xuất chỉ số vận hành**

SIEM phải:

a) cung cấp chỉ số vận hành cho từng thành phần quy định tại 5.2.6.2.2, tối thiểu gồm: trạng thái hoạt động, mức sử dụng CPU/bộ nhớ/dung lượng lưu trữ, độ trễ xử lý và tốc độ xử lý sự kiện hiện tại;

b) cung cấp cơ chế kiểm tra tình trạng hoạt động (health check) có thể truy vấn được qua giao diện lập trình cho từng thành phần;

c) hỗ trợ xuất chỉ số vận hành theo định dạng có thể thu thập được bởi các nền tảng giám sát hạ tầng bên ngoài, thông qua điểm cuối chuẩn dạng kéo (pull) hoặc đẩy (push);

d) hỗ trợ cấu hình xác thực và kiểm soát truy cập đối với điểm cuối xuất chỉ số quy định tại điểm c);

đ) hỗ trợ gửi cảnh báo về tình trạng bất thường của các thành phần nội bộ tới hệ thống giám sát hạ tầng bên ngoài, tối thiểu qua giao thức SNMP hoặc webhook.

CHÚ THÍCH: Ví dụ về định dạng và nền tảng giám sát hạ tầng bên ngoài được thừa nhận rộng rãi là định dạng OpenMetrics/Prometheus exposition format và nền tảng Prometheus, Grafana, Zabbix.

#### 5.2.6.2.6 Vận hành trong điều kiện mạng hạn chế

SIEM nên hỗ trợ:

a) thu thập nhật ký qua thiết bị chuyển đổi địa chỉ mạng, tường lửa và máy chủ ủy nhiệm;

b) nén dữ liệu và giới hạn băng thông sử dụng trên đường truyền thu thập;

c) đệm và gửi bù dữ liệu khi gián đoạn kết nối diện rộng, với thời lượng đệm cấu hình được;

d) mô hình truyền dữ liệu một chiều cho vùng mạng cách ly.

Nhà sản xuất phải công bố dung lượng lưu trữ cần thiết cho mỗi giờ đệm tại bộ thu thập nhật ký, tính theo mức lưu lượng nhật ký thiết kế của từng mức quy mô triển khai quy định tại 5.2.6.1.1.

### 5.2.6.3 Khả năng mở rộng và kiến trúc

#### 5.2.6.3.1 Hỗ trợ mở rộng theo chiều ngang và chiều dọc

SIEM phải có khả năng mở rộng quy mô linh hoạt để đáp ứng sự gia tăng về khối lượng dữ liệu. Yêu cầu về kiến trúc mở rộng độc lập giữa năng lực tính toán và năng lực lưu trữ được quy định tại 5.2.6.2.4 d).

#### 5.2.6.3.2 Hỗ trợ kiến trúc đa khách hàng/đa phân vùng

SIEM phải hỗ trợ khả năng phân vùng phù hợp với các môi trường có nhiều đối tượng sử dụng, nhiều nguồn dữ liệu hoặc nhiều miền quản lý độc lập. Yêu cầu về kiến trúc phân tán được quy định tại 5.2.6.2.4 b).

### 5.2.7 Phân quyền và kiểm soát hoạt động người dùng

#### 5.2.7.1 Mô hình phân quyền

SIEM phải hỗ trợ mô hình phân quyền theo vai trò với tối thiểu các khả năng:

a) tạo, sửa, xóa vai trò do tổ chức tự định nghĩa;

b) phân quyền theo chức năng, tối thiểu tách biệt các quyền: quản trị hệ thống; quản lý nguồn nhật ký; xây dựng và kích hoạt luật phát hiện; tìm kiếm và truy vấn dữ liệu; xử lý cảnh báo và hồ sơ sự cố; xuất dữ liệu; xem báo cáo;

c) phân quyền theo phạm vi dữ liệu, tối thiểu theo nhóm nguồn nhật ký và theo phân vùng quản lý;

d) bảo đảm nguyên tắc phân tách nhiệm vụ, cho phép cấu hình để một vai trò không đồng thời có quyền thay đổi cấu hình hệ thống và quyền xóa nhật ký hoạt động;

đ) áp dụng nguyên tắc từ chối mặc định đối với các quyền chưa được cấp.

#### 5.2.7.2 Nhật ký hoạt động của người dùng nghiệp vụ

SIEM phải ghi nhật ký các hoạt động nghiệp vụ của người dùng, tối thiểu gồm:

a) truy vấn, tìm kiếm dữ liệu, kèm nội dung điều kiện truy vấn;

b) xem, xuất, tải về dữ liệu nhật ký và báo cáo;

c) truy cập dữ liệu ở trạng thái đã được giải che, trong trường hợp SIEM triển khai cơ chế che dữ liệu theo 5.2.7.3;

d) tạo, sửa, kích hoạt, vô hiệu hóa luật phát hiện và ngoại lệ;

đ) thay đổi trạng thái cảnh báo và hồ sơ sự cố.

Nhật ký hoạt động nghiệp vụ quy định tại điều này phải được bảo vệ với mức độ tương đương nhật ký quản trị quy định tại 4.2.3.4 và không được phép chỉnh sửa hoặc xóa bởi bất kỳ cấp quyền nào.

#### 5.2.7.3 Che dữ liệu nhạy cảm

SIEM nên:

a) cho phép cấu hình che dữ liệu ở mức trường thông tin;

b) áp dụng che dữ liệu theo vai trò người dùng, trong hiển thị, kết quả truy vấn, báo cáo và dữ liệu xuất ra;

c) cho phép giải che có kiểm soát đối với vai trò được ủy quyền, có ghi nhật ký và tùy chọn yêu cầu phê duyệt;

d) bảo đảm việc che dữ liệu không làm mất khả năng tương quan và thống kê trên trường đã che.

## Thư mục tài liệu tham khảo

[1] NIST SP 800-92 (Guide to Computer Security Log Management), September 2006.

[2] SigmaHQ (Sigma Rules - Generic Signature Format for SIEM Systems).

[3] OMB (Memorandum M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents), 27 August 2021.

[4] SANS Institute (Benchmarking Security Information Event Management (SIEM)).

[5] ACSC (Best Practices for Event Logging and Threat Detection), December 2021.

[6] CCCS (Using Security Information and Event Management Solutions to Manage Cyber Security Risks), October 2021.

[7] Bộ Thông tin và Truyền thông (Quyết định số 1127/QĐ-BTTTT), Yêu cầu kỹ thuật cơ bản đối với sản phẩm quản lý và phân tích sự kiện an toàn thông tin.

[8] Filkins, Barbara. An Evaluator's Guide to NextGen SIEM. SANS Institute Information Security Reading Room, Technical Report (White Paper), December 2018.