

1. Tìm hiểu các loại Logs của Windows và Linux

1.1. Windows Event Logs

Trong điều tra số, một trong những vị trí đem đến những thông tin vô cùng hữu ích cho người điều tra là Windows Event Logs.

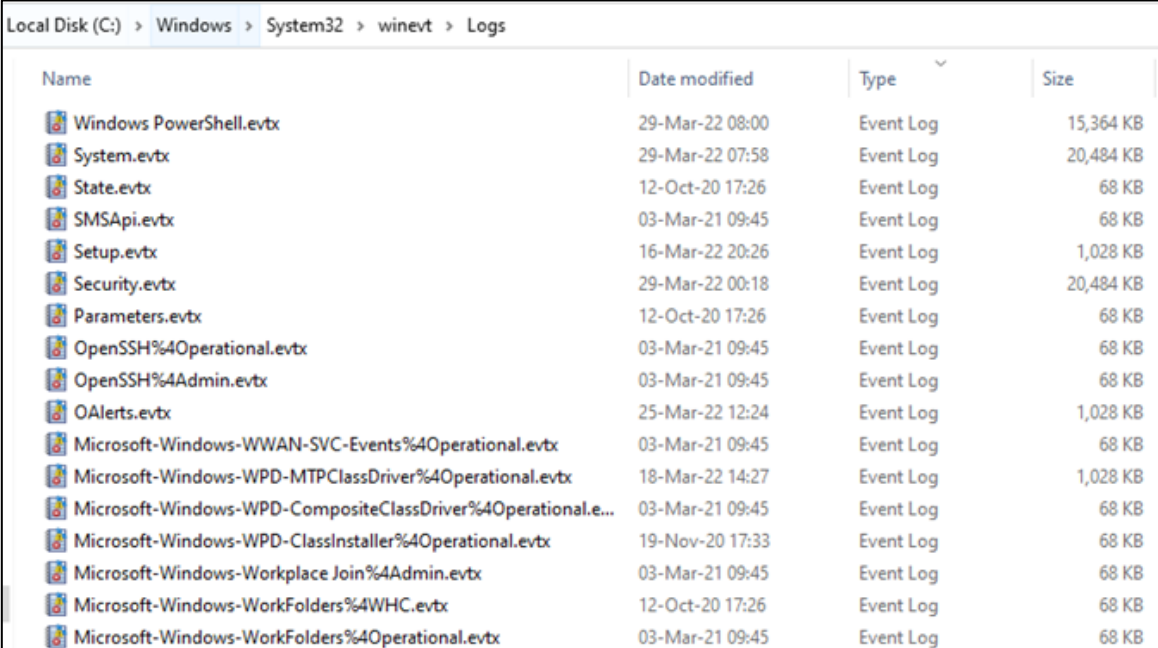
Windows Event Logs gồm những sự kiện liên quan đến software, hardware, OS, security. Service Windows Event Log chịu trách nhiệm quản lý các sự kiện, nhật ký sự kiện; nó thu thập các sự kiện từ nhiều nguồn khác nhau và lưu trữ tập chung tại một thư mục.

Các sự kiện này có thể giúp người điều tra biết được chuyện gì đã xảy ra trên hệ thống, chúng xảy ra vào thời gian nào, tham chiếu đến người dùng cụ thể liên quan đến những hành vi đó hay các thông tin của các hệ thống, tài nguyên truy cập từ xa.

1.1.1. Vị trí

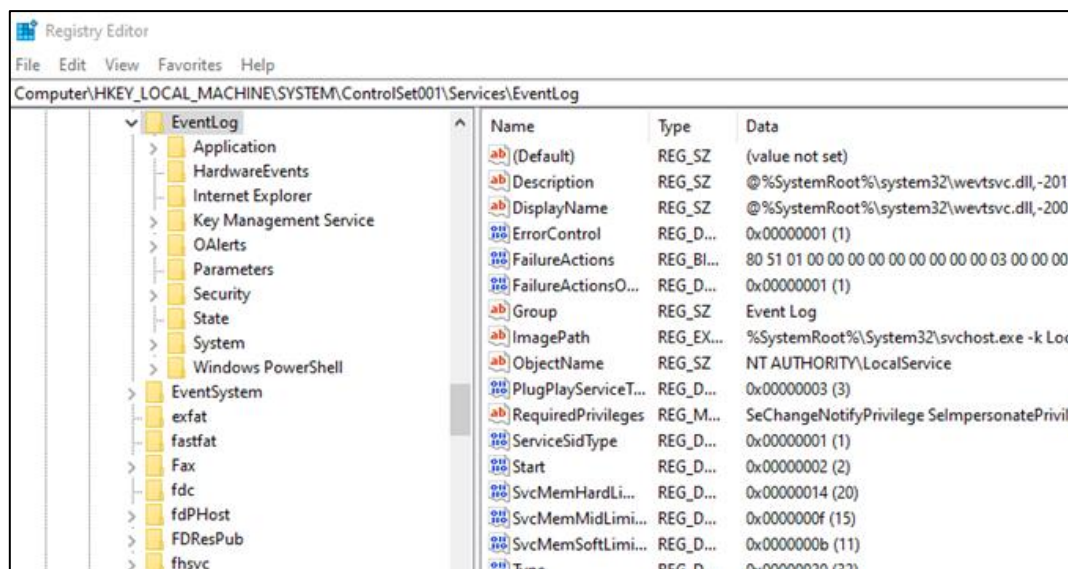
Ban đầu, ở những phiên bản hệ điều hành cũ (trước Windows Vista) event log sẽ được lưu trữ tập chung tại `systemroot%\System32\config` ở định dạng nhị phân và với phần mở rộng đuôi `.evt`.

Nhưng bắt đầu từ Windows Server 2008 và Windows Vista thì đã có sự thay đổi về định dạng log và vị trí lưu trữ của chúng. Event log được chuyển sang định dạng XML và với phần mở rộng `.evtx` và chúng được lưu trữ tại `%systemroot%\System32\winevt\logs`.



Name	Date modified	Type	Size
Windows PowerShell.evtx	29-Mar-22 08:00	Event Log	15,364 KB
System.evtx	29-Mar-22 07:58	Event Log	20,484 KB
State.evtx	12-Oct-20 17:26	Event Log	68 KB
SMSApi.evtx	03-Mar-21 09:45	Event Log	68 KB
Setup.evtx	16-Mar-22 20:26	Event Log	1,028 KB
Security.evtx	29-Mar-22 00:18	Event Log	20,484 KB
Parameters.evtx	12-Oct-20 17:26	Event Log	68 KB
OpenSSH%4Operational.evtx	03-Mar-21 09:45	Event Log	68 KB
OpenSSH%4Admin.evtx	03-Mar-21 09:45	Event Log	68 KB
OALerts.evtx	25-Mar-22 12:24	Event Log	1,028 KB
Microsoft-Windows-WWAN-SVC-Events%4Operational.evtx	03-Mar-21 09:45	Event Log	68 KB
Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx	18-Mar-22 14:27	Event Log	1,028 KB
Microsoft-Windows-WPD-CompositeClassDriver%4Operational.e...	03-Mar-21 09:45	Event Log	68 KB
Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx	19-Nov-20 17:33	Event Log	68 KB
Microsoft-Windows-Workplace Join%4Admin.evtx	03-Mar-21 09:45	Event Log	68 KB
Microsoft-Windows-WorkFolders%4WHC.evtx	12-Oct-20 17:26	Event Log	68 KB
Microsoft-Windows-WorkFolders%4Operational.evtx	03-Mar-21 09:45	Event Log	68 KB

Vị trí lưu của từng loại log có thể tìm thấy trong Registry:



Chẳng hạn như trong hình trên với các event liên quan đến Application sẽ được lưu trữ trong `%systemroot%\System32\winevt\Logs\Application.evtx`

Và người quản trị có thể thay đổi được vị trí này bằng cách thay đổi data value của registry key.

1.1.2. Định dạng Log

Với Windows 2008 trở về trước toàn bộ tệp log sẽ được ánh xạ vào bộ nhớ và điều này thực sự là một vấn đề với việc quản lý bộ nhớ, bộ nhớ luôn phải dành một không gian tối đa tới 300MB để cấp phát chỉ cho Event Log và tất nhiên hiệu suất sẽ bị giảm nhất là đối với thời điểm đó khi mà dung lượng bộ nhớ thực sự không lớn. Và đôi khi có thể dẫn đến vấn đề là người dùng sẽ tắt logging đi để nâng cao hiệu suất.

Nhưng với các bản indows OS mới hơn thì điều này đã được khắc phục, service Windows Event Log quản lý các event và event logs (logging events, querying events, subscribing to events, archiving event logs, and managing event metadata). Trong bộ nhớ lúc này chỉ chứa hững header nhỏ với các đoạn mã 64KB nằm trong bộ nhớ và nó thực sự đã giải quyết được vấn đề quản lý bộ nhớ mà không làm giảm hiệu suất.

Name	Description	Status	Startup Type
Windows Encryption Provider Host Service	Windows Encryption Provider Host Service brokers encr...		Manual (Trigger Start)
Windows Error Reporting Service	Allows errors to be reported when programs stop worki...		Manual (Trigger Start)
Windows Event Collector	This service manages persistent subscriptions to events ...	Running	Automatic (Delayed ...
Windows Event Log	This service manages events and event logs. It supports...	Running	Automatic
Windows Font Cache Service	Optimizes performance of applications by caching co...	Running	Automatic
Windows Image Acquisition (WIA)	Provides image acquisition services for scanners and ca...	Running	Automatic
Windows Insider Service	Provides infrastructure support for the Windows Insider...		Manual (Trigger Start)

Định dạng của event log cũng thay đổi với extension là .EVTX và được lưu trữ ở định dạng XML, giúp việc giải mã cấu trúc nhật ký trở nên trực quan hơn và cũng dễ dàng để tạo bộ lọc hỗ trợ việc tìm kiếm. Ví dụ với 1 event dưới đây:

```

event 4688, Microsoft Windows security auditing.
General Details
○ Friendly View ● XML View

- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{-4994-a5ba-3e3b0328c30d}" />
    <EventID>4688</EventID>
    <Version>2</Version>
    <Level>0</Level>
    <Task>13312</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2022-03-29T18:49:51.3291930Z" />
    <EventRecordID>1496500</EventRecordID>
    <Correlation />
    <Execution ProcessID="4" ThreadID="12160" />
    <Channel>Security</Channel>
    <Computer>DESKTOP-I IQ</Computer>
    <Security />
  </System>
  - <EventData>
    <Data Name="SubjectUserSid">S-1-5-18</Data>
    <Data Name="SubjectUserName">DESKTOP-I IQ$</Data>
    <Data Name="SubjectDomainName">WORKGROUP</Data>
    <Data Name="SubjectLogonId">0x3e7</Data>
  </EventData>
</Event>

```

Số lượng log đã tăng lên rất nhiều và cũng có các tùy chọn ghi log chi tiết hơn với sự tùy chỉnh của Advanced Audit Policy Configuration.

1.1.3. Phân loại Events

Có năm loại sự kiện có thể được ghi lại. Mỗi sự kiện phải thuộc một loại nào đó trong 5 loại này và mỗi loại sẽ có một biểu tượng khác nhau. VD như hình dưới:

❗ Error	29-Dec-20 8:39:17 AM
⚠ Warning	13-Jan-21 6:50:37 PM
⚠ Warning	13-Jan-21 6:50:37 PM
⚠ Warning	16-Oct-20 11:20:07 AM
ℹ Information	19-Nov-20 2:03:05 PM
ℹ Information	16-Nov-20 9:42:08 AM
ℹ Information	19-Nov-20 2:03:05 PM

Event Viewer (Local)	
Custom Views	
Windows Logs	
Application	
Security	
Setup	
System	
Forwarded Events	
Applications and Services Logs	
Hardware Events	
Intel	
Internet Explorer	
Key Management Service	

Security Number of events: 32,199	
Filtered: Log: Security; Source: ; Event ID: 4624, 4625. Number of	
Keywords	Date and Time
🔍 Audit Success	12-Mar-21 4:55:18 PM
🔍 Audit Success	12-Mar-21 5:14:18 PM
🔍 Audit Success	12-Mar-21 4:59:59 PM
🔒 Audit Failure	09-Mar-21 10:35:17 AM
🔒 Audit Failure	08-Mar-21 8:50:06 AM
🔒 Audit Failure	09-Mar-21 5:55:20 PM
🔒 Audit Failure	08-Mar-21 8:34:31 AM
🔒 Audit Failure	09-Mar-21 11:29:05 AM

a. Information (Thông tin):

- Ghi lại các hoạt động bình thường, các thông báo hệ thống và ứng dụng.

- Ví dụ: Khởi động thành công của một dịch vụ, thông báo hoàn thành tác vụ, báo cáo trạng thái hệ thống...

- Mức độ thấp, chủ yếu để theo dõi hoạt động thông thường.

b. Warning (Cảnh báo):

- Đánh dấu các sự kiện không mong đợi nhưng không gây lỗi nghiêm trọng.

- Ví dụ: Một ứng dụng có thể gặp vấn đề về hiệu suất, một dịch vụ chậm khởi động, hoặc một cảnh báo về tài nguyên hệ thống sắp cạn kiệt.

- Cho phép team SOC cảnh báo và theo dõi để phòng tránh các vấn đề có thể trở nên nghiêm trọng.

c. Error (Lỗi):

- Ghi lại các sự kiện báo lỗi, chỉ ra sự cố đã xảy ra ảnh hưởng đến chức năng hoặc hiệu suất của hệ thống, ứng dụng.

- Ví dụ: Dịch vụ không khởi động được, lỗi khi kết nối cơ sở dữ liệu, lỗi ứng dụng...

- Đây là loại sự kiện mà team SOC cần phản ứng nhanh để khắc phục sự cố.

d. Critical (Nghiêm trọng):

- Một số phiên bản Windows (và các ứng dụng) có thể phân loại sự kiện với mức độ Critical để chỉ ra những lỗi cực kỳ nghiêm trọng, thường liên quan đến sự cố hệ thống không mong đợi hoặc sự cố bảo mật nghiêm trọng.

- Những sự kiện này đòi hỏi sự can thiệp khẩn cấp.

e. Audit Success và Audit Failure (Sự kiện bảo mật thành công/thất bại):

- **Audit Success:** Ghi lại các hoạt động bảo mật đã thành công, như đăng nhập, truy cập tài nguyên, thay đổi quyền...

- **Audit Failure:** Ghi lại các hoạt động bảo mật không thành công, ví dụ như đăng nhập thất bại, truy cập bị từ chối, hành vi đáng ngờ của người dùng...

- Các sự kiện này rất quan trọng trong việc theo dõi và điều tra các hoạt động bảo mật, giúp SOC phát hiện sớm các hành vi truy cập trái phép hoặc tấn công.

1.1.4. Các loại Logs

Event log gồm các nhật ký tiêu chuẩn (Security, System và Application) ngoài ra còn có các bản additional logs đã được thêm vào log chuyên biệt (Custom log) chẳng hạn như PowerShell, Task Scheduler,...

a. Application Log (Log Ứng Dụng)

- **Mô tả:** Ghi lại các sự kiện liên quan đến các ứng dụng chạy trên Windows.

- **Nội dung:** Lỗi, cảnh báo, thông tin từ các ứng dụng; ví dụ như lỗi phần mềm, thông báo từ trình duyệt, và các ứng dụng bên thứ ba.

- **Ứng dụng SOC:** Giúp phát hiện các lỗi hoặc hành vi bất thường từ các ứng dụng có thể là dấu hiệu của tấn công hoặc phần mềm độc hại.

b. System Log (Log Hệ Thống)

- **Mô tả:** Ghi lại các sự kiện của hệ thống Windows, liên quan đến hoạt động của hệ điều hành và các thành phần phần cứng.

- **Nội dung:** Thông báo từ driver, dịch vụ hệ thống, các sự kiện liên quan đến khởi động, tắt máy, cảnh báo lỗi phần cứng...

- **Ứng dụng SOC:** Giúp theo dõi tình trạng hoạt động của hệ thống, từ đó phát hiện sớm các dấu hiệu của tấn công hệ thống hoặc sự cố hệ thống.

c. Security Log (Log Bảo Mật)

- **Mô tả:** Ghi lại các sự kiện liên quan đến an ninh, đặc biệt là các hoạt động liên quan đến đăng nhập, truy cập, thay đổi chính sách bảo mật...

- **Nội dung:** Sự kiện đăng nhập thành công hoặc thất bại, thay đổi chính sách, audit các hành động của người dùng, hành vi truy cập không hợp lệ, sử dụng tài khoản đặc quyền.

- **Ứng dụng SOC:** Là nguồn quan trọng giúp phát hiện các hành vi đáng ngờ, tấn công brute-force, truy cập trái phép, và các cuộc tấn công từ bên ngoài.

d. Setup Log (Log Cài Đặt)

- **Mô tả:** Ghi lại các sự kiện trong quá trình cài đặt hệ điều hành và các bản cập nhật quan trọng.

- **Ứng dụng SOC:** Có thể cung cấp thông tin về thay đổi cấu hình, cài đặt phần mềm mới và các sự kiện liên quan đến bảo mật hệ thống.

e. Forwarded Events (Sự Kiện Chuyển Tiếp)

- **Mô tả:** Đây là log các sự kiện được chuyển tiếp từ các máy chủ hoặc máy tính khác trong mạng. Windows Audit Collection Service chịu trách nhiệm thu thập và chuyển tiếp log.

- **Ứng dụng SOC:** Giúp tập trung theo dõi các sự kiện bảo mật từ nhiều nguồn trong mạng nội bộ, tạo ra một tổng hợp các sự kiện để phân tích.

1.2. Linux Logs

1.2.1. Sơ Lược

Linux File log là một tập hợp các bản ghi mà Linux duy trì để các quản trị viên theo dõi các sự kiện quan trọng. Các file log này sẽ chứa các thông báo về máy chủ, bao gồm kernel, dịch vụ và ứng dụng đang chạy trên nó. File log cung cấp thời gian của các sự kiện cho hệ điều hành, ứng dụng và hệ thống Linux và là một công cụ quan trọng giúp chúng ta khắc phục sự cố.

Hệ điều hành Linux cung cấp một kho lưu trữ tập trung các file log trong thư mục /var/log. Hầu hết các file log được chia thành một trong bốn loại:

- Application Logs: Nhật ký ứng dụng
- Event Logs: Nhật ký sự kiện
- Service Logs: Nhật ký dịch vụ
- System Logs: Nhật ký hệ thống

Thông qua việc giám sát các file log chúng ta có thể nắm rõ hơn về hiệu suất của máy chủ, bảo mật, thông báo lỗi và các vấn đề tiềm ẩn. Các file log cho phép chúng ta dự đoán các vấn đề sắp tới trước khi thực sự xảy ra.

1.2.2. Các file log quan trọng

a. Syslog/Messages

- **Đường dẫn:**

- + **Ubuntu/Debian:** /var/log/syslog
- + **RedHat/CentOS:** /var/log/messages

- **Mô tả:** Ghi lại các sự kiện chung của hệ thống, từ các daemon chạy nền đến các thông báo từ kernel.

- **Ứng dụng SOC:** Là nguồn cung cấp các thông tin tổng hợp về hoạt động hệ thống, cho phép phát hiện lỗi, cảnh báo và hành vi bất thường.

b. Kernel Log

- **Đường dẫn:**

- + /var/log/kern.log (Ubuntu)
- + Dmesg (thông qua lệnh dmesg)

- **Mô tả:** Ghi lại các thông báo từ kernel, bao gồm lỗi phần cứng, driver, và các sự kiện khởi động.

- **Ứng dụng SOC:** Giúp theo dõi các vấn đề liên quan đến phần cứng hoặc driver, cũng như dấu hiệu của tấn công ở tầng thấp của hệ thống.

c. Authentication Log

- **Đường dẫn:**

+ **Ubuntu/Debian:** /var/log/auth.log

+ **RedHat/CentOS:** /var/log/secure

- **Mô tả:** Ghi lại các sự kiện liên quan đến xác thực như đăng nhập, sudo, và các hành động liên quan đến bảo mật.

- **Ứng dụng SOC:** Rất quan trọng để phát hiện các hành vi đăng nhập không hợp lệ, tấn công brute-force, hoặc các hành vi truy cập trái phép.

d. Daemon Log

- **Đường dẫn:** /var/log/daemon.log (Ubuntu)

- **Mô tả:** Ghi lại các sự kiện từ các daemon chạy nền (ví dụ: cron, sshd, và các dịch vụ khác).

- **Ứng dụng SOC:** Theo dõi hoạt động của các dịch vụ hệ thống, từ đó phát hiện các vấn đề hoặc hành vi bất thường.

e. Mail Log

- **Đường dẫn:** /var/log/mail.log hoặc /var/log/maillog

- **Mô tả:** Ghi lại các hoạt động liên quan đến hệ thống email, như gửi, nhận thư và các lỗi liên quan.

- **Ứng dụng SOC:** Phân tích lưu lượng email, xác định các hành vi spam hoặc tấn công qua email.

f. Audit Log

- **Đường dẫn:** /var/log/audit/audit.log (nếu sử dụng auditd)

- **Mô tả:** Ghi lại các hành động được audit, bao gồm các sự kiện truy cập, thay đổi cấu hình và các hành động quan trọng của hệ thống.

- **Ứng dụng SOC:** Rất quan trọng trong việc kiểm tra, điều tra các hành động của người dùng và phát hiện vi phạm chính sách.

g. Application Logs (Các log ứng dụng riêng)

- **Đường dẫn:**

+ **Apache/Nginx:** /var/log/apache2/access.log, /var/log/apache2/error.log, /var/log/nginx/access.log, /var/log/nginx/error.log

+ **MySQL:** /var/log/mysql.log hoặc /var/log/mysql/error.log

+ Các ứng dụng khác: Có thể được cấu hình ghi log vào các đường dẫn tùy chỉnh.

- **Mô tả:** Các log từ ứng dụng cung cấp thông tin chi tiết về hoạt động và lỗi của từng ứng dụng.

- **Ứng dụng SOC:** Giúp phát hiện lỗi ứng dụng, các cuộc tấn công nhắm vào ứng dụng và phân tích hiệu năng.

1.3. Kết luận

Windows Logs: Bao gồm Application, System, Security, Setup và Forwarded Events. Mỗi loại log có vai trò quan trọng trong việc theo dõi các sự kiện ứng dụng, hệ thống và bảo mật.

Linux Logs: Bao gồm Syslog/Messages, Kernel log, Authentication log, Daemon log, Mail log, Audit log và các log ứng dụng riêng. Các log này cung cấp thông tin từ hệ thống, kernel, xác thực, và các dịch vụ chạy nền.

Ứng dụng SOC: Việc thu thập các log này giúp SOC theo dõi toàn diện hoạt động của hệ thống, phát hiện sớm các hành vi bất thường và tấn công, đồng thời hỗ trợ việc điều tra và phản ứng sự cố.

2. So sánh và Vai trò trong SOC

2.1. Windows Logs

Ưu Điểm	Hạn Chế
<ul style="list-style-type: none">- Cung cấp thông tin chi tiết về các hoạt động bảo mật và hệ thống qua Event Viewer.- Dễ dàng phân loại và lọc qua các loại log riêng biệt (Security, System, Application).	<ul style="list-style-type: none">- Định dạng EVTXT cần các công cụ chuyên đổi để tích hợp vào SIEM.- Các log có thể có kích thước lớn và khó phân tích khi không được xử lý tự động

2.2. Linux Logs

Ưu Điểm	Hạn Chế
<ul style="list-style-type: none">- Định dạng văn bản dễ dàng tích hợp và phân tích qua các công cụ log aggregation như ELK.- Đa dạng các loại log (syslog, auth.log, kern.log, audit.log) cung cấp cái nhìn toàn diện về hoạt động hệ thống.	<ul style="list-style-type: none">- Phân mảnh về vị trí lưu trữ (nhiều file khác nhau) đòi hỏi quy trình thu thập tập trung.- Có thể cần các công cụ chuyên biệt để xử lý log audit phức tạp.

2.3. Vai trò trong SOC:

- **Phát hiện sự cố:** SOC sử dụng các log này để phát hiện các hành vi bất thường như nỗ lực đăng nhập thất bại, truy cập trái phép, lỗi hệ thống nghiêm trọng.

- **Điều tra sự cố:** Các log chi tiết giúp xác định nguồn gốc của sự cố, thời gian xảy ra và phạm vi ảnh hưởng.

- **Phân tích xu hướng:** SOC có thể sử dụng log để phân tích xu hướng hoạt động của hệ thống, từ đó cải thiện cấu hình bảo mật và đưa ra các chiến lược phòng ngừa.

- **Báo cáo và tuân thủ:** Log đóng vai trò quan trọng trong việc cung cấp bằng chứng cho các cuộc điều tra, kiểm toán và tuân thủ các tiêu chuẩn an ninh (GDPR, HIPAA, ISO).

3. Kết luận

- **Windows Logs** (Application, System, Security, Setup, Forwarded Events) cung cấp thông tin chi tiết và có cấu trúc rõ ràng về các hoạt động của hệ thống và bảo mật, giúp SOC phát hiện và điều tra các sự kiện quan trọng.

- **Linux Logs** (Syslog/Messages, Authentication, Kernel, Daemon, Audit, Application) cho phép tích hợp dễ dàng vào hệ thống SIEM như ELK, cung cấp dữ liệu toàn diện từ nhiều nguồn khác nhau, hỗ trợ việc giám sát và phản ứng sự cố.

- Cả hai loại log đều là nguồn thông tin quý giá cho SOC, với các thông tin như timestamp, nguồn log, mức độ sự kiện, mô tả chi tiết, thông tin người dùng và IP, từ đó giúp phân tích, truy vết và xử lý sự cố an ninh một cách hiệu quả.