TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM
Khoa Mạng máy tính & Truyền thông

# Security Monitoring, SIEM, SOC

NT204 – Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

GV: Đỗ Hoàng Hiển

**hiendh@uit.edu.vn**


# Nội dung hôm nay…

**Hôm nay có gì?**

**Security Monitoring, SIEM, SOC**

Nội dung tham khảo từ:

**Khoá học CCNA Cybersecurity Operations**

**Chương 11: Security Monitoring**

# Nội dung và Mục tiêu

- **1. Các công nghệ và giao thức**
  - **Giải thích cách các công nghệ an ninh ảnh hưởng đến giám sát an ninh**
    - **Giải thích hoạt động của các giao thức mạng thông dụng trong ngữ cảnh giám sát an ninh**
    - **Giải thích các công nghệ bảo mật ảnh hưởng như thế nào đến khả năng của các giao thức giám sát mạng thông dụng**
- 2. Các file log
  - Giải thích về các loại file log được sử dụng trong giám sát an ninh
    - Mô tả các kiểu dữ liệu được dùng trong giám sát an ninh
    - Mô tả các thành phần có trong file log của thiết bị đầu cuối (end device)
    - Mô tả các thành phần có trong file log của thiết bị mạng (network device)
- 3. Các khái niệm SIEM, SOC

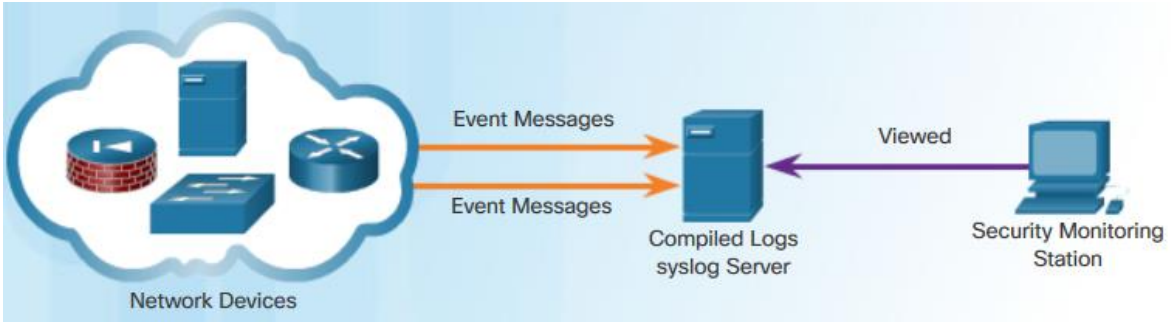
# Security monitoring – Giám sát an ninh

- **Security monitoring – Giám sát an ninh**
  - Cách gọi khác:
    - “Security Information Monitoring (SIM)“
    - “Security Event Monitoring (SEM)”
  - Bao gồm **thu thập** và **phân tích** thông tin để **phát hiện** các hành vi đáng ngờ hoặc các thay đổi hệ thống trái phép trên mạng, xác định loại hành vi nào nên được **cảnh báo**, và **hành động** cần thực hiện khi có cảnh báo

Giám sát các giao thức thông dụng

# **Syslog** (System Logging Protocol)

- **Syslog** và **Network Time Protocol (NTP)** là các giao thức cần thiết cho hoạt động phân tích an ninh mạng
  - Syslog là giao thức chuẩn dùng để gửi các log hệ thống hoặc các thông điệp sự kiện đến 1 server (server **syslog**), để ghi lại các sự kiện từ các thiết bị mạng và các thiết bị đầu cuối
  - Server syslog thường lắng nghe trên port **UDP 514** (cũng có thể dùng TCP)
  - Các server syslog có thể trở thành mục tiêu bị tấn công
  - Hacker có thể ngăn việc truyền và nhận dữ liệu, làm giả dữ liệu log hoặc giả mạo các phần mềm tạo và truyền log
  - Một số cải tiến được cung cấp trong **syslog-ng** (next generation)




Docs: https://www.rsyslog.com/doc/master/index.html

Giám sát các giao thức thông dụng

# syslog – syslog-ng - rsyslog

syslog

**syslog**

Creator : Eric Allman

Developed In : 1980

Type Protocol / Specification

Logging protocol standard, specifies log message, transmission and reliability

Related to
syslog-ng, rsyslog, sysklog

rsyslog

**rsyslog**

Creator : Rainer Gerhards

Developed In : 2004

Type Syslog implementation

Implements REPL, TCP forwarding, TLS and advanced filtering

Related to
syslog-ng, sysklog


**syslog-ng**

Creator : Balázs Scheidler

Developed In : 1998

Type Syslog implementation

Leverages syslog with TCP transmission and content based filtering

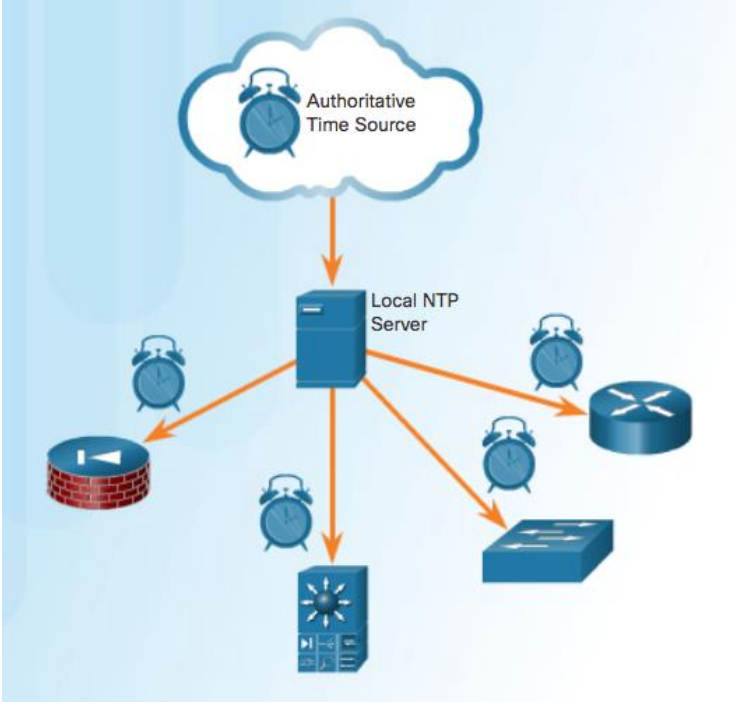
Related to
rsyslog, sysklog

Read more: https://news.cloud365.vn/log-ly-thuyet-tong-quan-ve-log-syslog-rsyslog/

## Giám sát các giao thức thông dụng

# NTP

- Gói tin syslog thường được gán nhãn thời gian với giao thức **Network Time Protocol (NTP)**
- NTP hoạt động trên port **UDP 123**
- Nhãn thời gian rất quan trọng trong việc phát hiện tấn công
  - Kẻ tấn công có thể tấn công vào NTP để làm gián đoạn thông tin thời gian dùng cho việc liên kết các sự kiện mạng đã được ghi log
  - Kẻ tấn công có thể dùng các hệ thống NTP để chỉ đạo thực hiện tấn công DDoS




```
~ — -zsh — 79×24
2020-03-11 21:05:27 status half-configured mount:amd64 2.31.1-0.4ubuntu3
2020-03-11 21:05:27 status unpacked mount:amd64 2.31.1-0.4ubuntu3
2020-03-11 21:05:27 status half-installed mount:amd64 2.31.1-0.4ubuntu3
2020-03-11 21:05:27 status half-installed mount:amd64 2.31.1-0.4ubuntu3
2020-03-11 21:05:27 status unpacked mount:amd64 2.31.1-0.4ubuntu3.5
2020-03-11 21:05:27 status unpacked mount:amd64 2.31.1-0.4ubuntu3.5
2020-03-11 21:05:27 upgrade libcom-err2:amd64 1.44.1-1 1.44.1-1ubuntu1.3
2020-03-11 21:05:27 status half-configured libcom-err2:amd64 1.44.1-1
2020-03-11 21:05:27 status unpacked libcom-err2:amd64 1.44.1-1
2020-03-11 21:05:27 status half-installed libcom-err2:amd64 1.44.1-1
```

Giám sát các giao thức thông dụng

# DNS

- **DNS được sử dụng trong nhiều loại malware**
- Kẻ tấn công đóng gói các giao thức mạng khác nhau bên trong DNS để qua mặt các thiết bị an ninh
- Một số malware sử dụng DNS để giao tiếp với server command-and-control (CnC) và đánh cắp các dữ liệu được nguỵ trang dưới dạng các truy vấn DNS thông thường
- Malware có thể mã hoá (encode) dữ liệu đánh cắp được trong **phần subdomain** trong truy vấn DNS cho 1 domain có nameserver đã bị kiểm soát bởi kẻ tấn công
- Các truy vấn DNS với các tên domain được tạo ngẫu nhiên, hoặc các subdomain dạng chuỗi ngẫu nhiên rất dài đều **đáng ngờ**, đặc biệt nếu chúng xuất hiện với số lượng nhiều bất thường trong mạng

>> Xem thêm

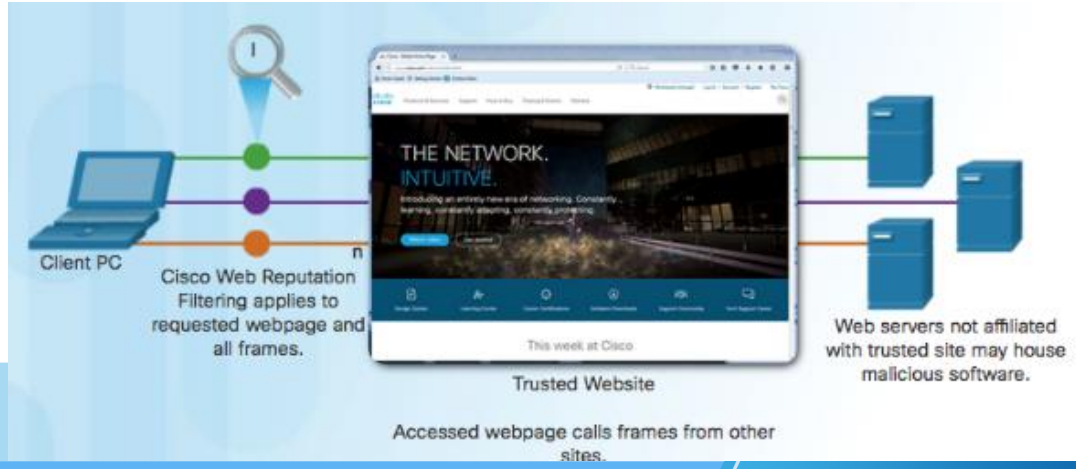
>> Video demo

Giám sát các giao thức thông dụng

# HTTP và HTTPS

- Tất cả thông tin truyền nhận bằng giao thức HTTP đều được truyền dưới dạng **plaintext** từ máy nguồn đến máy đích
- HTTP không bảo vệ dữ liệu khỏi các hành vi thay đổi hoặc chặn gói
- Các tấn công dựa trên web thường gồm các đoạn mã độc hại được cài vào webserver để chuyển hướng các trình duyệt client đến các server đã bị nhiễm thông quan việc load các iframe
  - Trong tấn công iFrame injection, kẻ tấn công chiếm 1 web server và cài mã độc tạo 1 iFrame ẩn trên các trang web thường được truy cập
  - Khi iFrame này được load trên trình duyệt của client, malware sẽ được tải về máy

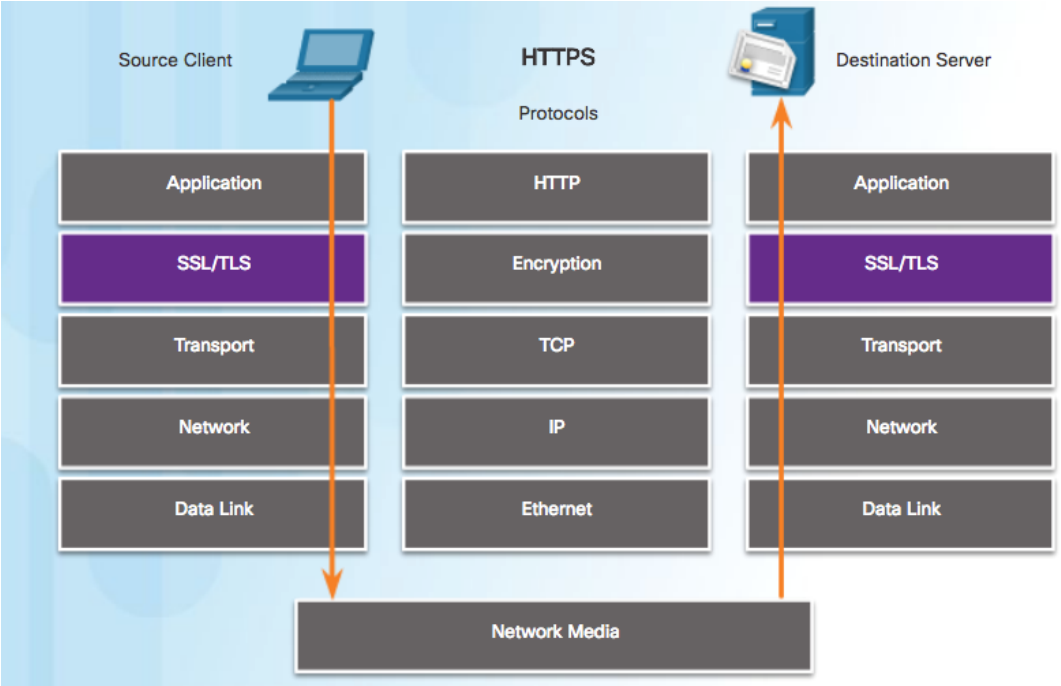
**Tấn công**
**HTTP iFrame Injection**



Giám sát các giao thức thông dụng

# HTTP và HTTPS (tt)

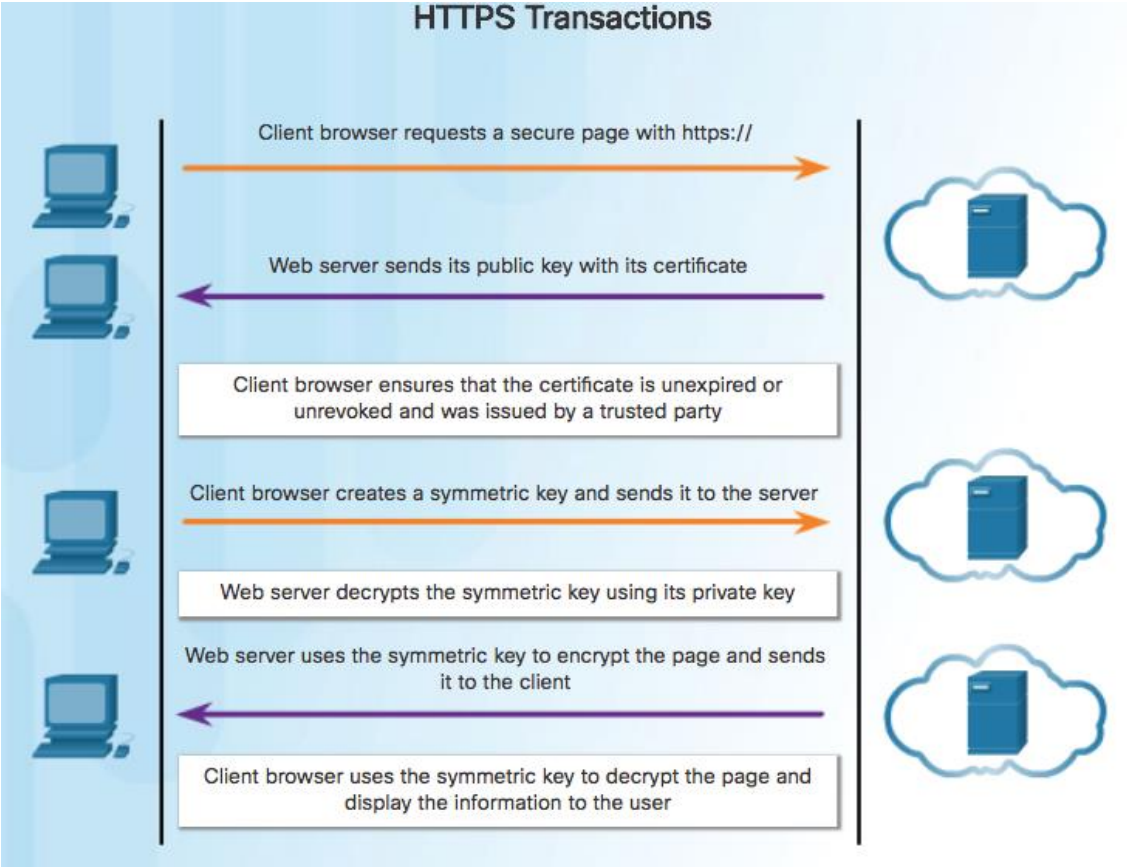
- HTTPS thêm 1 lớp mã hoá (encryption) vào giao thức HTTP bằng cách sử dụng Secure socket layer (SSL)
  - SSL đảm bảo các dữ liệu HTTP không thể đọc được khi được gửi đi cho đến khi đến được máy đích



Giám sát các giao thức thông dụng

# HTTP và HTTPS (tt)

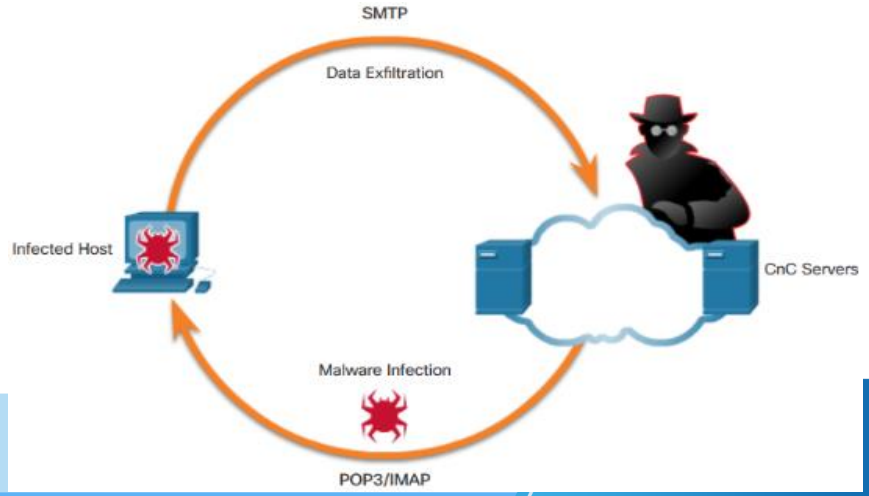
- Traffic đã mã hoá của HTTPS có thể làm phức tạp hoạt động giám sát an ninh mạng, cũng như việc bắt các gói tin HTTPS phức tạp hơn



Giám sát các giao thức thông dụng

# Các giao thức Email

- Các giao thức Email như **SMTP, POP3, và IMAP** có thể bị các kẻ tấn công sử dụng để lan truyền malware, đánh cắp dữ liệu hoặc tạo các kênh giao tiếp với server CnC
  - SMTP gửi dữ liệu từ 1 host đến server mail và giữa các server mail, việc này không phải lúc nào cũng được giám sát
  - IMAP và POP3 thường được dùng để tải các email từ server mail về host và có thể dùng để tải các malware về host
  - Giám sát an ninh có thể **nhận dạng 1 malware dưới dạng file đính kèm đi vào mạng và xác định host nào sẽ bị ảnh hưởng đầu tiên**



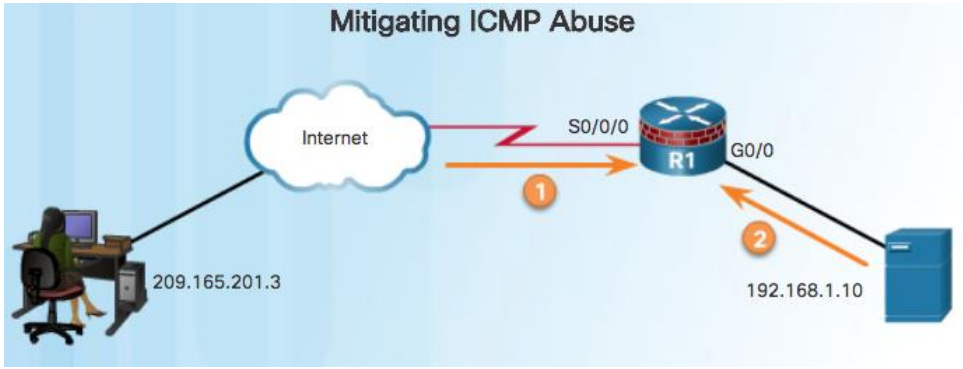
Giám sát các giao thức thông dụng

# ICMP

- ICMP có thể được sử dụng để thực hiện nhiều loại tấn công khác nhau
  - Có thể được dùng để xác định các host có trong mạng, kiến trúc của mạng, và xác định hệ điều hành sử dụng trong mạng,…
  - Cũng có thể được dùng để thực hiện nhiều loại tấn công DoS
  - ICMP cũng có thể được dùng để **đánh cắp dữ liệu** thông qua traffic ICMP từ bên trong mạng
    - ICMP tunneling – Malware tạo các gói ICMP để truyền file từ host bị nhiễm đến kẻ tấn công

# ACLs

- ACLs có thể tạo ra 1 cảm giác sai về an toàn (false sense of security)
  - Kẻ tấn công có thể xác định được các IP, giao thức và port nào được cho phép bởi ACL, thông qua các hoạt động như *Port scanning, penetration testing, hoặc thông qua các hoạt động do thám mạng khác*
  - Kẻ tấn công có thể tạo các gói tin sử dụng địa chỉ IP nguồn giả mạo hoặc các ứng dụng có thể tạo kết nối với port bất kỳ




1. Rules on R1 for ICMP traffic from the Internet

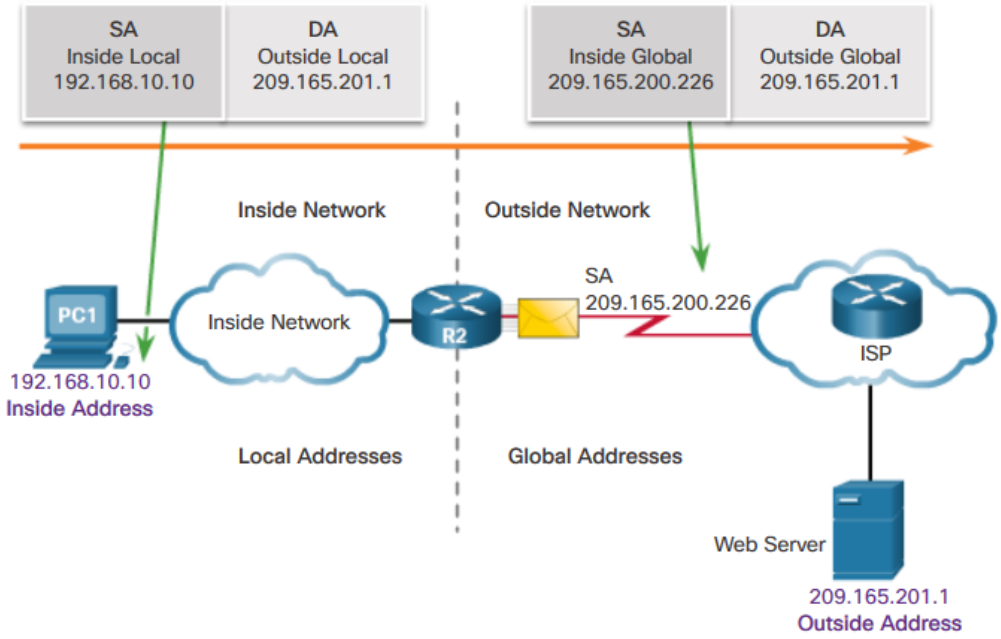
```
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

2. Rules on R1 for ICMP traffic from inside the network

```
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
access-list 114 deny icmp any any
```

# NAT và PAT

- **NAT** (Network Address Translation) và **PAT** (Port Address Translation) có thể khiến việc giám sát an ninh mạng trở nên phức tạp
  - Nhiều địa chỉ IP cùng được ánh xạ đến một hoặc nhiều địa chỉ IP công cộng sử dụng được trên Internet
  - Ẩn các địa chỉ IP riêng bên trong mạng



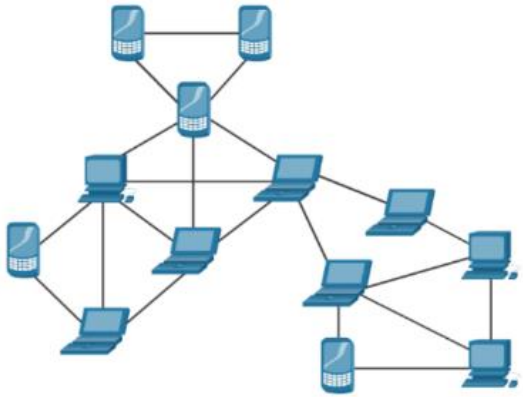
# Mã hoá (Encryption) và Tunneling

- Mã hoá (Encryption)
  - Nội dung traffic không thể đọc được, ngay cả với người phân tích an ninh mạng
  - Là 1 phần trong hoạt động của Virtual Private Network (VPN) và HTTPS
- Kết nối ảo point-to-point giữa 1 host bên trong mạng và các thiết bị của kẻ tấn công
  - Malware có thể tạo 1 tunnel được mã hoá sử dụng các giao thức phổ biến và tin cậy, sau đó sử dụng tunnel này để đánh cắp dữ liệu từ mạng

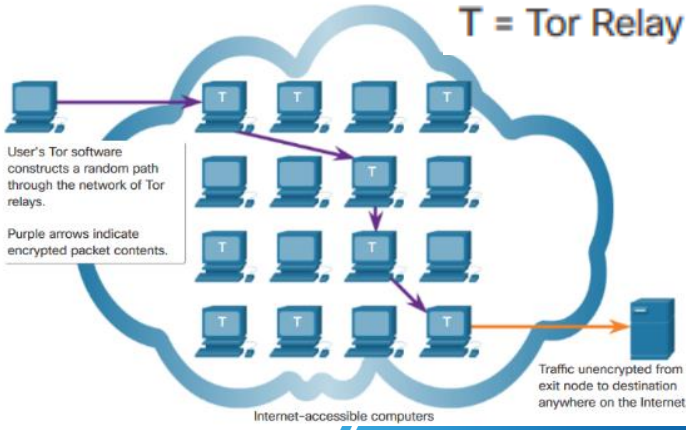
# Mạng Peer-to-Peer và Tor

- **Hoạt động mạng Peer-to-Peer**
  - Có thể phá vỡ biện pháp bảo vệ của tường lửa và thường là phương pháp phổ biến để lây lan malware.
    - 3 dạng ứng dụng Peer-to-Peer: chia sẻ file, chia sẻ processor, và IM (tin nhắn)
    - Các ứng dụng chia sẻ file P2P không nên cho phép hoạt động trong các mạng công ty
- **Tor** là một nền tảng phần mềm và một mạng các host kết nối Peer-to-Peer hoạt động như các router trên mạng Tor
  - Cho phép người dùng truy cập Internet ẩn danh bằng trình duyệt đặc biệt
  - Có thể dùng che giấu danh tính kẻ tấn công và được dùng bởi các tổ chức tội phạm

P2P

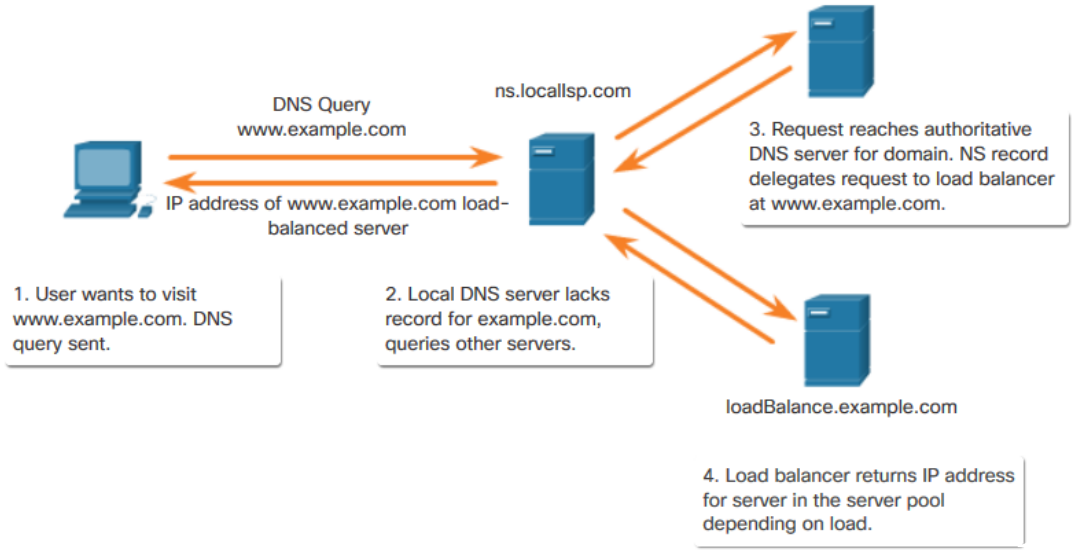


Mạng Tor



# Load Balancing – Cân bằng tải

- Cân bằng tải là hoạt động phân phối lưu lượng mạng giữa các thiết bị hoặc đường mạng để tránh quá tải tài nguyên mạng
  - Một số phương pháp cân bằng tải sử dụng DNS để gửi traffic đến tài nguyên có cùng tên domain nhưng nhiều địa chỉ IP
  - Việc này có thể dẫn đến 1 kết nối Internet có thể được biểu diễn qua nhiều địa chỉ IP trong gói tin các đến
  - Điều này có thể dẫn đến các đặc điểm đáng ngờ trong việc bắt gói tin



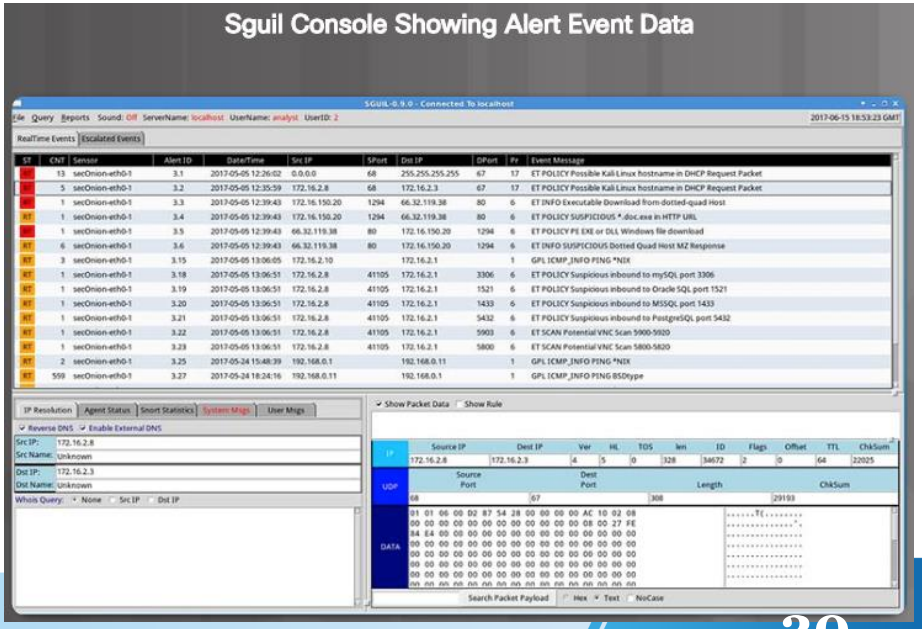
# Các nội dung và Mục tiêu

- 1. Các công nghệ và Giao thức
  - Giải thích cách các công nghệ an ninh ảnh hưởng đến giám sát an ninh
    - Giải thích hoạt động của các giao thức mạng thông dụng trong ngữ cảnh giám sát an ninh
    - Giải thích các công nghệ bảo mật ảnh hưởng như thế nào đến khả năng của các giao thức giám sát mạng thông dụng
- **2. Các file log**
  - **Giải thích về các loại file log được sử dụng trong giám sát an ninh**
    - **Mô tả các kiểu dữ liệu được dùng trong giám sát an ninh**
    - **Mô tả các thành phần có trong file log của thiết bị đầu cuối (end device)**
    - **Mô tả các thành phần có trong file log của thiết bị mạng (network device)**
- 3. Các khái niệm SIEM, SOC

Các loại dữ liệu an ninh

# Dữ liệu Cảnh báo

- Dữ liệu Cảnh báo gồm các gói tin tạo ra từ các IDS/IPS khi có traffic vi phạm chính sách hoặc khớp với dấu hiệu của tấn công
- Một network IDS (NIDS), ví dụ Snort, được cấu hình với các rule để phát hiện tấn công đã biết
- Cảnh báo từ Snort có thể được đọc, tìm kiếm bằng các ứng dụng như **Sguil** (1 phần của bộ công cụ Security Onion)



Log trên thiết bị đầu cuối

# Log của host

- Host-based IDPS (HIDPS) chạy trên các host riêng biệt
  - HIDPS không chỉ phát hiện tấn công mà còn có thể ngăn chặn tấn công khi chạy dưới dạng host-based firewall
  - Tạo ra các log và lưu lại trên host
  - Log trên các host Microsoft Windows có thể xem bằng công cụ Event Viewer
  - **Event Viewer** hiển thị nhiều loại log: Application Logs, System Logs, Setup Logs, và Security Logs.

| Event Type | Description |
|---|---|
| Error | An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged. |
| Warning | An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event. |
| Information | An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts. |
| Success Audit | An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event. |
| Failure Audit | An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event. |

**Các loại log sự kiện trên host Windows**

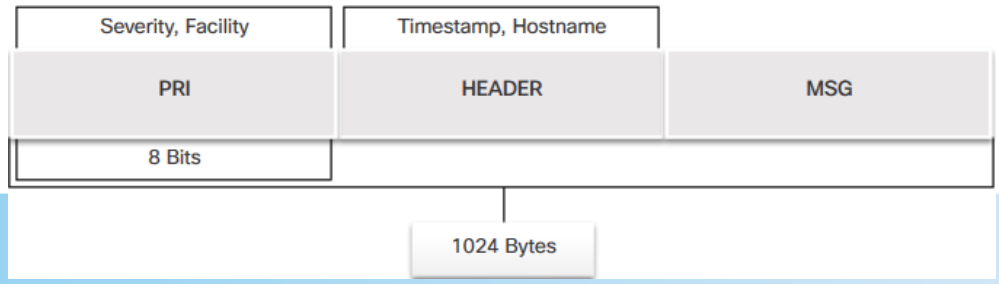
Log trên thiết bị đầu cuối

# Syslog

- Nhiều thiết bị mạng có thể được cấu hình để ghi log các sự kiện và gửi đến server syslog
  - Giao thức dạng Client/Server
  - Gói tin Syslog gồm 3 phần: **PRI** (priority), **HEADER**, và **MSG** (nội dung dạng văn bản)
    - **PRI** gồm 2 phần, **Facility** và **Severity** của thông điệp
      - **Facility** gồm nhiều loại nguồn khác nhau tạo ra thông điệp đó như hệ thống, tiến trình, hoặc ứng dụng để chuyển gói tin đến file log tương ứng
      - **Severity** là 1 giá trị từ 0-7 xác định mức độ nghiêm trọng của thông điệp

<165>1 2019-08-01T15:30:54.001Z ubuntu-box apache 200 20031 - " The Apache Server encountered an error"

PRI HEADER MSG



Log trên thiết bị đầu cuối

# Syslog Priority

## Syslog Severity and Facility

| Integer | Severity |
|---|---|
| 0 | **Emergency**: System is unusable |
| 1 | **Alert**: Action must be taken immediately |
| 2 | **Critical**: Critical conditions |
| 3 | **Error**: Error conditions |
| 4 | **Warning**: Warning conditions |
| 5 | **Notice**: Normal but significant condition |
| 6 | **Informational**: Informational messages |

Priority = (Facility X 8) + Severity

| Integer | Facility |
|---|---|
| 0 | **kern**: Kernel messages |
| 1 | **user**: User-level messages |
| 2 | **mail**: Mail system |
| 3 | **daemon**: System daemons |
| 4 | **auth**: Security/authorization messages |
| 5 | **syslog**: Messages generated internally by Syslogd |
| 6 | **lpr**: Line printer subsystem |
| 7 | **news**: Network news subsystem |
| 8 | **uucp**: Unix-to-Unix copy subsystem |
| 9 | Clock daemon |
| 10 | **authpriv**: Security/authorization messages |
| 11 | **ftp**: FTP daemon |
| 12 | NTP subsystem |
| 13 | Log audit |

Ví dụ:

**PRI = 165**

**165 = 20*8 + 5**

Facility = 20

Severity = 5

>> Xem thêm

Log trên thiết bị đầu cuối

# Log của Server

- Log của Server là một nguồn dữ liệu quan trọng trong giám sát an ninh mạng
  - Server Email và Web có **log truy cập (access)** và **log lỗi (error)**
  - Log của server DNS proxy ghi lại tất cả truy vấn DNS và phản hồi DNS tương ứng trong mạng
  - Log của DNS proxy có thể xác định các host đã truy cập các website nguy hiểm và xác định các tấn công đánh cắp dữ liệu qua DNS hoặc kết nối đến các server CnC của malware

**Apache Access Log**

```
203.0.113.127 â€" dsmith [10/Oct/2016:10:26:57 -0500]
"GET /logo_sm.gif HTTP/1.0â€œ 200
2254 ""http://www.example.com/links.html""
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)
Gecko/20100101 Firefox/47.0"
```

**IIS Access Log**

```
6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3,
198.51.100.10, 80, GET, /home.htm, -, 200, 0, 15321,
159, 15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0;
Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0), -,
http://www.example.com
```

Web Server Logs

# Log truy cập (access) của Apache Webserver

- Log truy cập của Apache Webserver ghi lại các request từ client đến server
  - 2 định dạng log
    - Common log format (CLF)
    - Dạng kết hợp: dạng CLF và thêm một số trường về referrer, user agent

**Apache Access Log Format**

```
203.0.113.127 - dsmith [10/Oct/2016:10:26:57 -0500] "GET /logo_sm.gif
HTTP/1.0" 200 2254 ""http://www.example.com/links.html""
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0"
```

| Field | Name | Description | Example |
|---|---|---|---|
| 1 | Client IP address | IP address of requesting client | 203.0.113.127 |
| 2 | Client identity | Client userid, frequently omitted | - |
| 3 | User ID | User name of authenticated user, if any | dsmith |
| 4 | Timestamp | Date and time of request | [10/Oct/2016:10:26:57 -0500] |
| 5 | Request | Request method and requested resource | GET /logo_sm.gif HTTP/1.0“ |
| 6 | Status Code | HTTP status code | 200 |
| 7 | Size of Response | Bytes returned to client | 2254 |
| 8 | Referrer | Location, if any, from which the client reached the resource | http://www.example.com/links.html |
| 9 | User Agent | Browser used by client | Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0 |

Log trên thiết bị đầu cuối

# Log truy cập (access) của IIS

- Microsoft IIS tạo các log truy cập có thể xem trên server với công cụ Event Viewer

**IIS Access Log Format**

```
6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3, 198.51.100.10, 80, GET,
/home.htm, -, 200, 0, 15321, 159, 15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0;
Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0), -, http://www.example.com
```

| Item | Field | Explanation | Example |
|---|---|---|---|
| Date | date | date on which the activity occurred | 6/14/2016 |
| Time | time | UTC time, at which the activity occurred | 16:22:22 |
| Client IP Address | c-ip | IP address of the client that made the request | 203.0.113.24 |
| User Name | cs-username | authenticated user name | - |
| Service Name and Instance Number | s-sitename | Internet service name and instance number | W3SVC2 |
| Server Name | s-computername | name of the server that generated the log entry | WEB3 |
| Server IP Address | s-ip | IP address of the server | 198.51.100.10 |
| Server Port | s-port | server port for the service | 80 |
| Method | cs-method | requested action (HTTP method) | GET |
| URI Stem | cs-uri-stem | target of the action | /home.htm |
| URI Query | cs-uri-query | the query the client was trying to perform | - |
| HTTP Status | sc-status | HTTP status code | 200 |
| Win32 Status | sc-win32-status | Windows status code | 0 |
| Bytes Sent | sc-bytes | bytes that the server sent | 15321 |
| Bytes Received | cs-bytes | bytes that the server received | 159 |
| Time Taken | time-taken | length of time that the action took, in milliseconds | 15 |
| Protocol Version | cs-version | the protocol version | HTTP/1.1 |
| User Agent | cs(User-Agent) | browser type that the client used | Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0) |
| Cookie | cs(Cookie) | The content of the cookie sent or received, if any | - |
| Referrer | cs(Referrer) | site that provided a link | http://www.example.com |

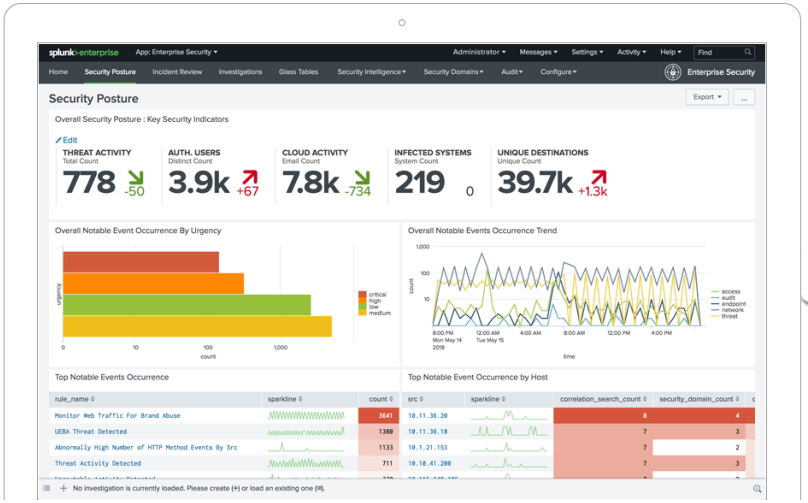
# Các nội dung và Mục tiêu

- 1. Các công nghệ và Giao thức
  - Giải thích cách các công nghệ an ninh ảnh hưởng đến giám sát an ninh.
    - Giải thích hoạt động của các giao thức mạng thông dụng trong ngữ cảnh giám sát an ninh.
    - Giải thích các công nghệ bảo mật ảnh hưởng như thế nào đến khả năng của các giao thức giám sát mạng thông dụng.
- 2. Các file log
  - Giải thích về các loại file log được sử dụng trong giám sát an ninh.
    - Mô tả các kiểu dữ liệu được dùng trong giám sát an ninh.
    - Mô tả các thành phần có trong file log của thiết bị đầu cuối (end device).
    - Mô tả các thành phần có trong file log của thiết bị mạng (network device).
- **3. Các khái niệm SIEM, SOC**

Các khái niệm SIEM, SOC

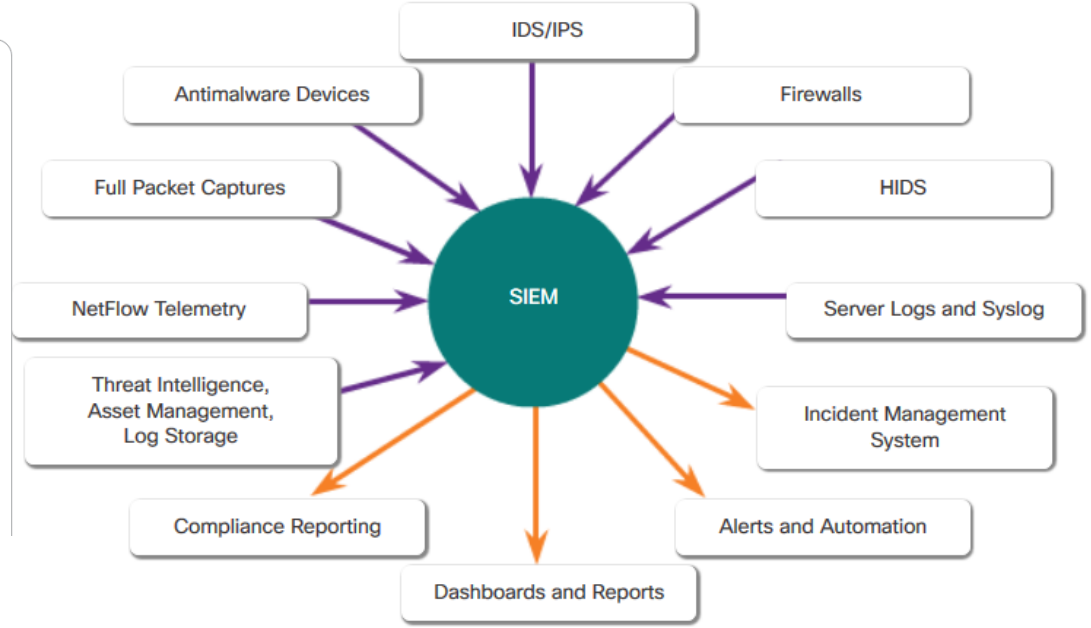
# SIEM và Thu thập log

- Công nghệ Security Information and Event Management (SIEM)
  - Hỗ trợ tạo báo cáo thời gian thực và phân tích dài hạn các sự kiện an ninh
  - Các chức năng: Thu thập log, Chuẩn hoá, Tương quan sự kiện, Tích hợp, Báo cáo, Tuân thủ CNTT
  - Một SIEM phổ biến là **Splunk** *(Video)*




**Splunk**

**Các thành phần của SIEM**

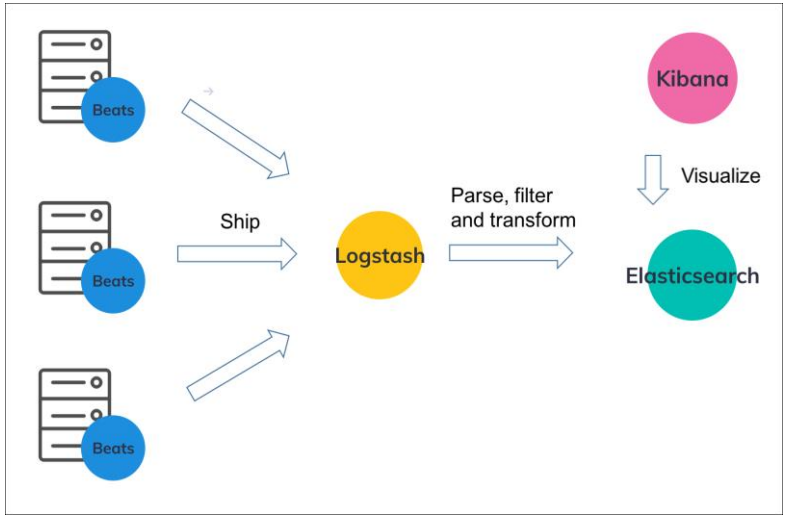


# Top 5 công cụ SIEM

- Hoạt động của **SIEM** và Top 5 công cụ phổ biến
  - https://youtu.be/3JVJy35VdW4

# Nền tảng SIEM mã nguồn mở

- ELK là từ viết tắt của 3 sản phẩm mã nguồn mở của Elastic:
  - **Elasticsearch:** Công cụ tìm kiếm văn bản theo hướng tài liệu
  - **Logstash:** như là 1 bộ tích hợp, thu thập và xử lý dữ liệu từ nhiều nguồn khác nhau trước khi đưa xuống pipeline
  - **Kibana:** Dashboard phân tích và tìm kiếm cho Elasticsearch chạy trên trình duyệt
  - **Beats:** một trong các công cụ chuyển log tốt nhất hiện nay, nhỏ gọn, hỗ trợ mã hoá, có cơ chế khôi phục tốt, đáng tin cậy


Đọc thêm: https://logz.io/blog/filebeat-vs-logstash/

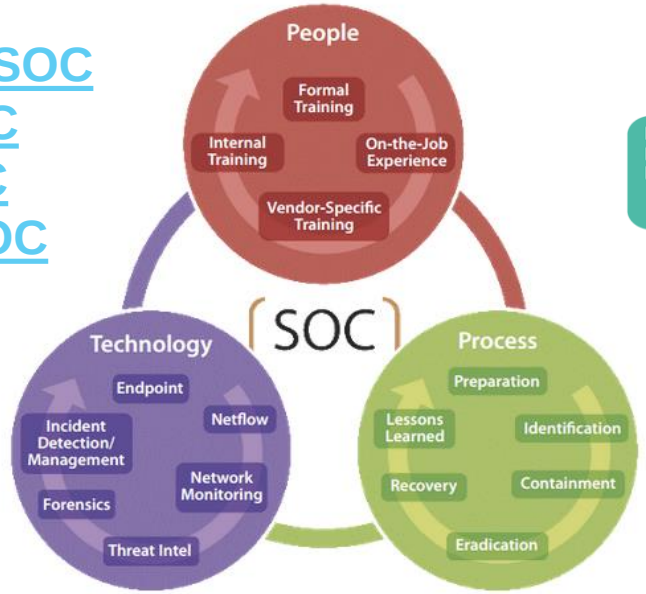
SOC

# Security Operations Center

**SOC** là 1 vị trí trung tâm trong 1 doanh nghiệp, có các chuyên gia, quy trình và công nghệ để liên tục theo dõi và xử lý các vấn đề an ninh: phát hiện, phân tích, đánh giá, báo cáo và phản ứng với các vấn đề an ninh mạng


Video

- From SIEM to SOC
- Running a SOC
- Inside the SOC
- Centurylink SOC



SOC

# SIEM - SOC - NOC

**Q: Điểm khác biệt giữa NOC và SOC?**

- A: **NOC** là viết tắt của **network operations center**. NOC tập trung chủ yếu vào việc giảm thiểu thời gian downtime và đảm bảo các thoả thuận ở mức dịch vụ, trong khi SOC phân tích sâu hơn về các mối đe doạ mạng và các lỗ hổng

**Q: Điểm khác biệt giữa SOC và SIEM?**

- A: SIEM là viết tắt của Security Information and Event Management. SOC là 1 nhóm các chuyên gia và công cụ cùng làm việc chung với nhau và SIEM là một phần công việc họ cần tuân theo

***Tìm hiểu thêm về các giải pháp SIEM, SOC ở Vietnam!***

# Tóm lại…

**Các công nghệ bảo mật** và **các file log** dùng trong giám sát an ninh:

- Một số giao thức thông dụng thường được giám sát như: **syslog, NTP, DNS, HTTP và HTTPS, SMTP, POP3, IMAP, and ICMP**
- Một số công nghệ tường được sử dụng có ảnh hưởng đến việc giám sát an ninh mạng như: **ACLs, NAT và PAT, mã hoá (encryption), tunneling, mạng peer-to-peer, TOR, và load balancing**
- Các thiết bị đầu cuối tạo ra các log. Log của các host Microsoft Windows có thể được xem nội bộ bằng công cụ Event Viewer
- Syslog có các đặc điểm về định dạng gói tin, kiến trúc client-server application và giao thức mạng
- Các server ứng dụng như server mail hay web có lưu trữ log truy cập (access) và log lỗi (error)
- SIEM kết hợp nhiều chức năng của các công cụ quản lý sự kiện an ninh (SEM) và quản lý thông tin an ninh (SIM) để cung cấp cái nhìn toàn diện về mạng của tổ chức
- SOC là một bộ phận chuyên về phân tích traffic và theo dõi các mối đe doạ và tấn công, phát hiện và ngăn chặn các sự cố xảy ra theo thời gian thực

# Câu hỏi/thắc mắc (nếu có)???


# Today end, **See you next week!**