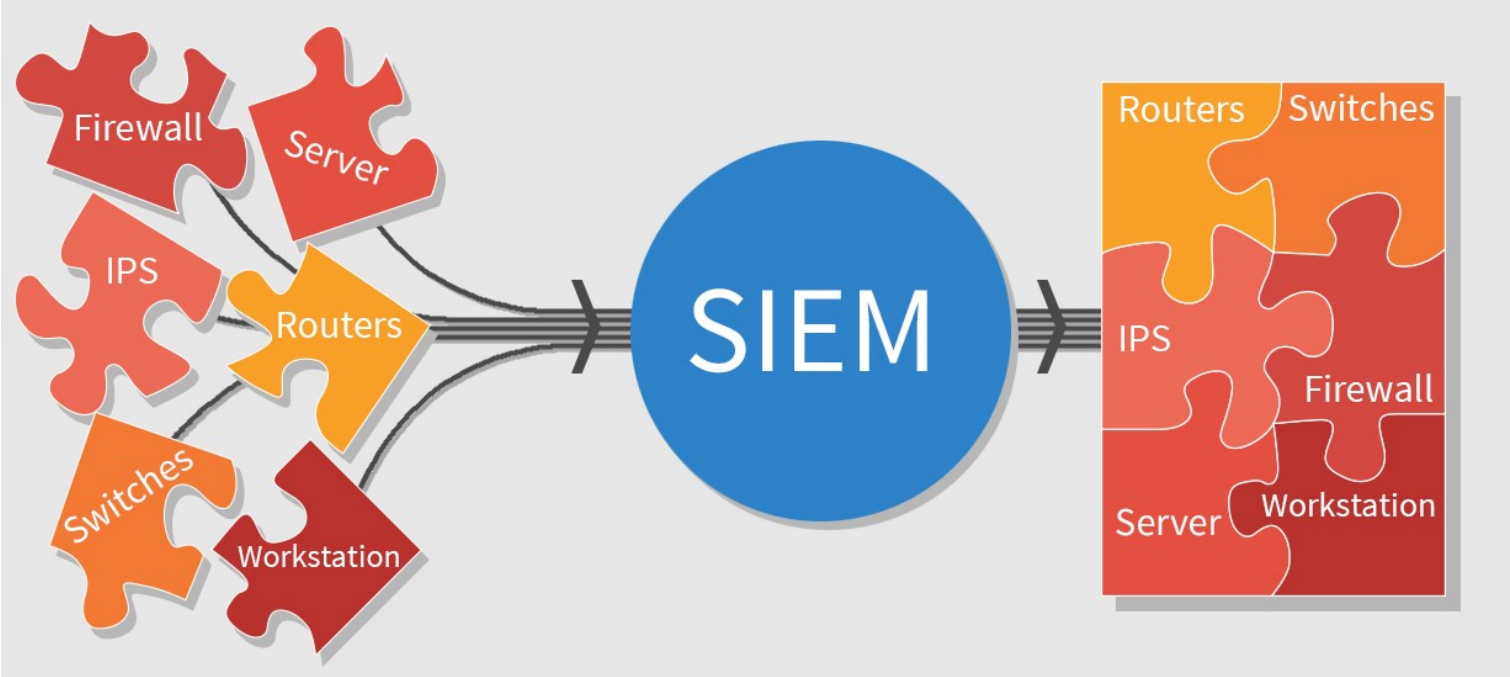
Chương 4.
Hệ thống giám sát an ninh mạng

4. Hệ thống quản lý sự kiện và giám sát an ninh mạng SIEM

- SIEM: Security Information and Event Management
- SIEM là giải pháp thực hiện việc giám sát sự kiện an toàn thông tin cho hệ thống.
- Quản lí sự kiện an ninh (SEM) và quản lí thông tin an ninh (SIM)

4. Hệ thống SIEM

- Tiến trình:



4. Hệ thống SIEM

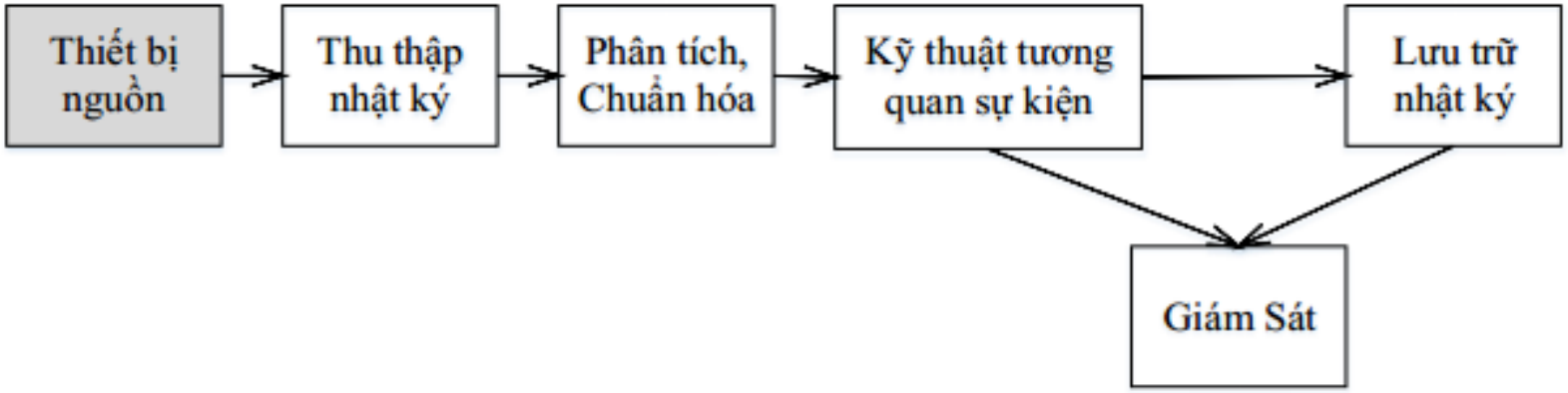
- SIEM cung cấp:
  - Quản lý nhật ký:
    - Quản lý nhật ký (Log) là chìa khóa đầu tiên cho các giải pháp SIEM.
    - Thu thập nhật ký từ các thiết bị và ứng dụng trong hệ thống
    - Phân tích nhật ký
    - Lưu trữ nhật ký
    - Nhật ký được lưu trữ bao lâu?
    - Những loại nhật ký nào được lưu trữ?

4. Hệ thống SIEM

- SIEM cung cấp:
  - Tương quan liên kết sự kiện:
    - Liên kết các bản ghi nhật ký với nhau để tương quan chúng
    - Tìm ra dấu hiệu tấn công

4. Hệ thống SIEM

- Kiến trúc:



4. Hệ thống SIEM

1. Kỹ thuật thu thập:

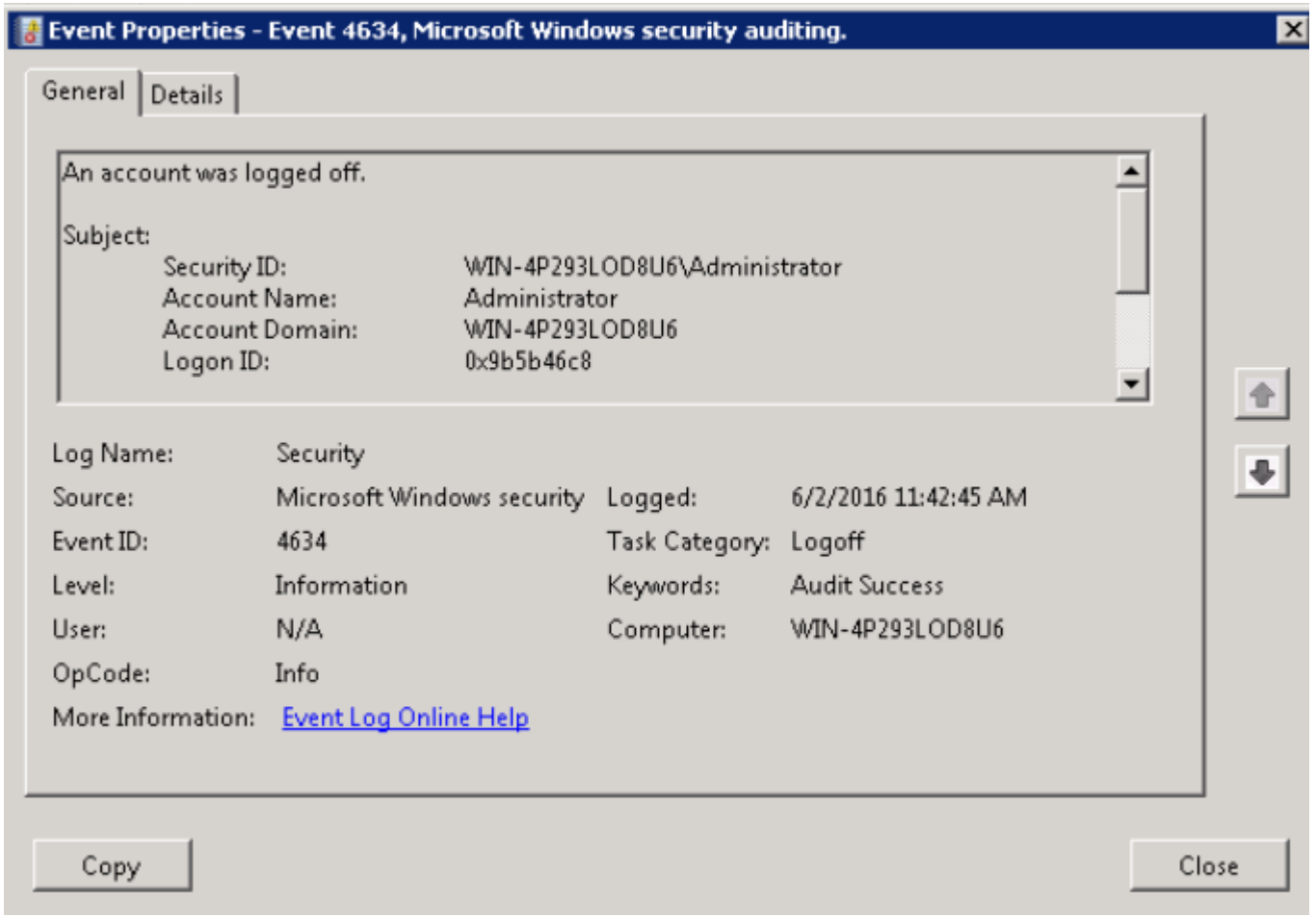
- **Push log:** Các bản ghi nhật ký sẽ được các thiết bị nguồn gửi về SIEM.
- **Pull log:** Các bản ghi nhật ký sẽ được SIEM đi tới và lấy về.

4. Hệ thống SIEM

2. Phân tích, chuẩn hóa:

- Tất cả các bản ghi lúc đầu thu về đang ở định dạng gốc ban đầu.
- Việc thay đổi tất cả các loại bản ghi nhật ký khác nhau thành các bản ghi có cùng một định dạng duy nhất được gọi là chuẩn hóa
- Việc chuẩn hóa các bản ghi nhật ký giúp cho SIEM có thể thống nhất các bản ghi nhật ký, nhanh chóng phân tích cũng như tương quan sự kiện an ninh sau này.

4.2 Phân tích và chuẩn hóa log



4.2 Phân tích và chuẩn hóa log

- Log trên Linux

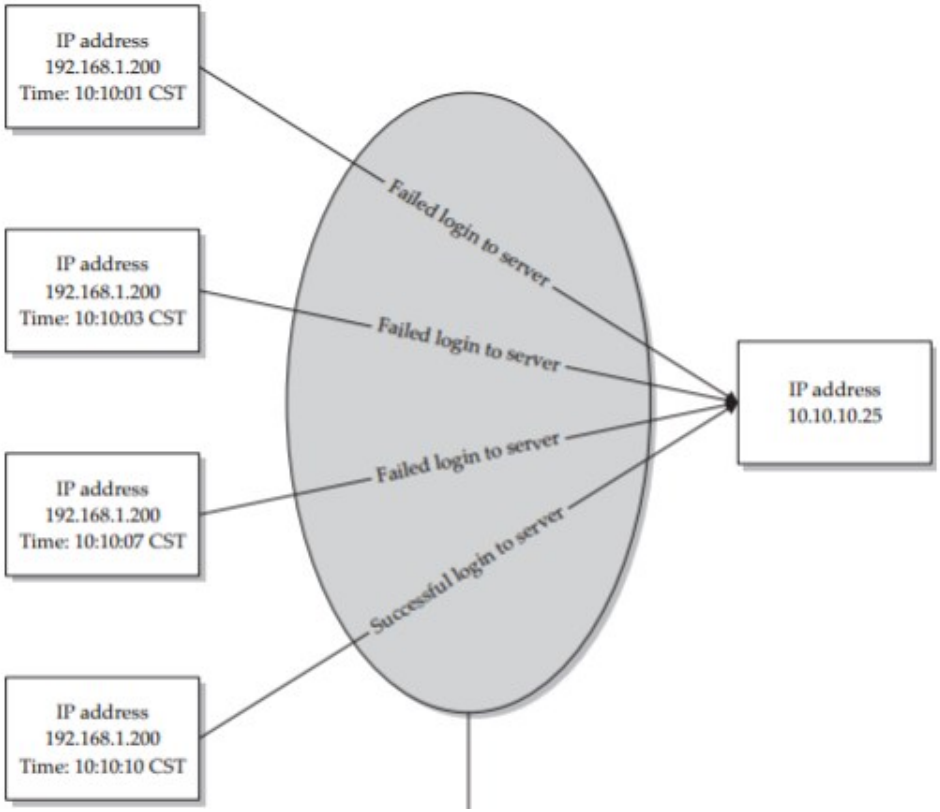
```
Jun  2 21:43:11 izviet sshd[8243]: Accepted password for root from 113.23.48.104 port 28979 ssh2
Jun  2 21:43:11 izviet sshd[8243]: pam_unix(sshd:session): session opened for user root by (uid=0)
```

4.2 Phân tích và chuẩn hóa log

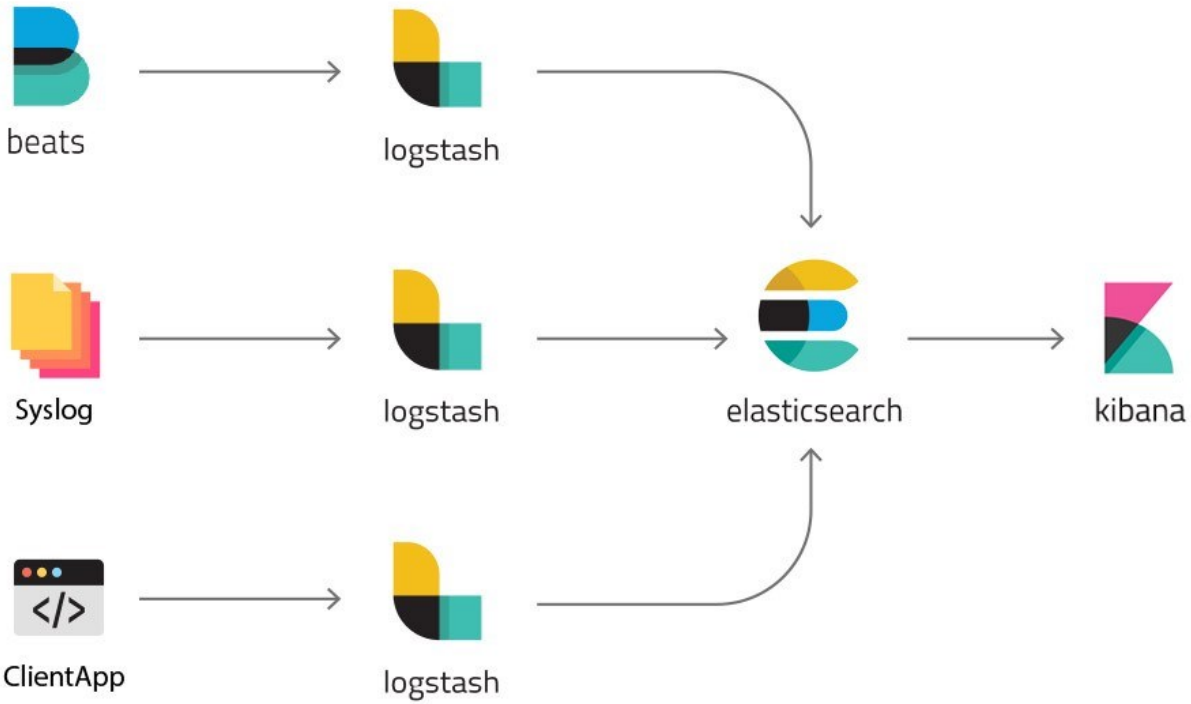
- Sau khi SIEM chuẩn hóa:

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	OTX	SOURCE IP	DEST IP
2016-06-02 21:45:03	AlienVault HIDS: SSHD authentication success.	0	AlienVault HIDS-authentication_success	vuat8b	N/A	113.23.48.104:28979	WebServer
2016-06-02 21:43:16	AlienVault HIDS: Successful login during non-business hours.	0	AlienVault HIDS-login_time	vuat8b	N/A	113.23.48.104:47152	WindowsServer

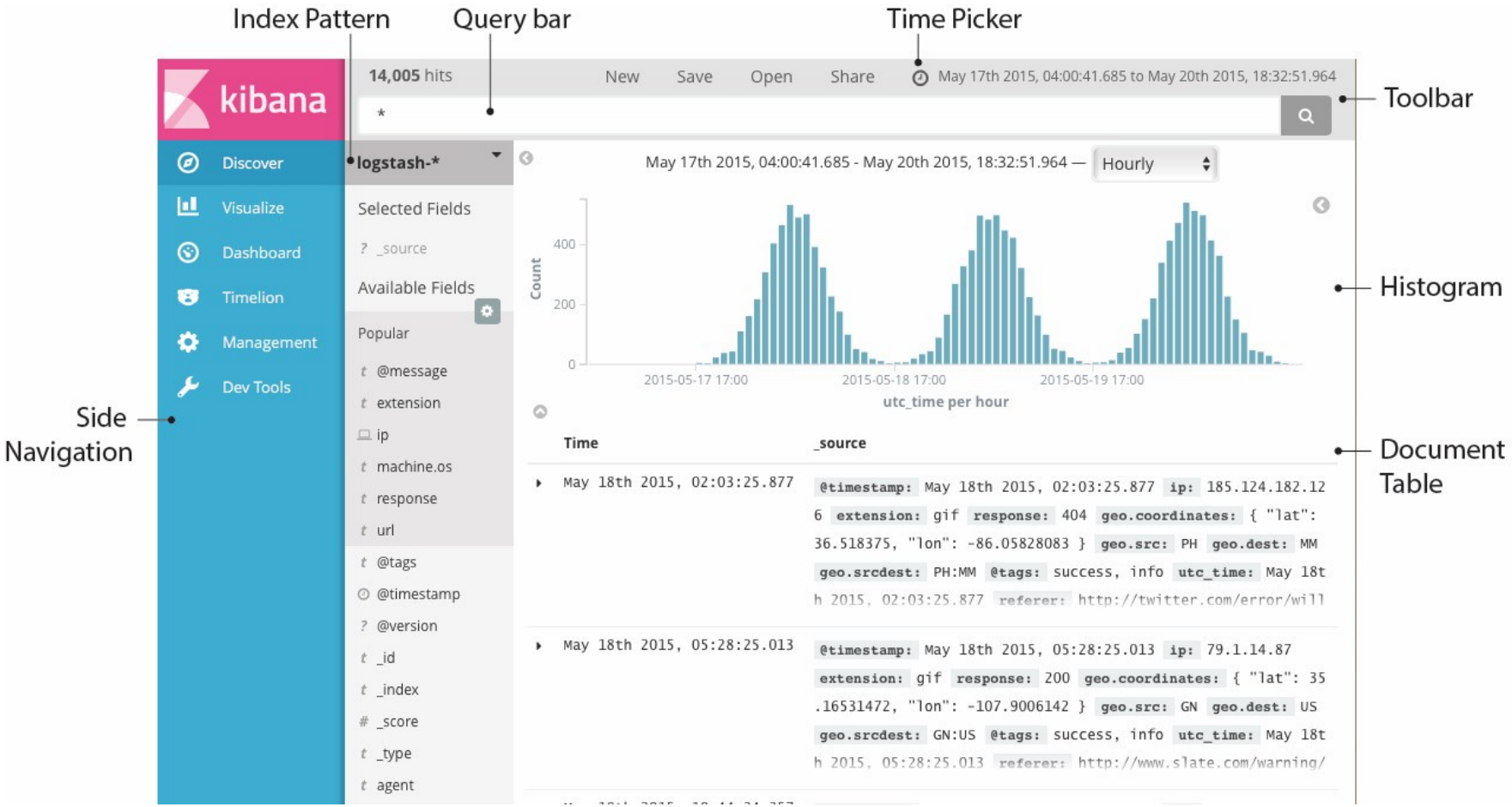
4.3 Kỹ thuật tương quan sự kiện



Một số sản phẩm:


beats
logstash
Syslog
logstash
elasticsearch
kibana
ClientApp
logstash


splunk>
Log Files
Configurations
Messages
Alerts
Metrics
Scripts
Changes
Tickets
Sensors
Security
APP
Custom Applications
Networks
Databases
Servers
Smartphones and Devices
VM
Virtual Machines
Web Services


Index Pattern
Query bar
Time Picker
kibana
14,005 hits
New
Save
Open
Share
May 17th 2015, 04:00:41.685 to May 20th 2015, 18:32:51.964
Toolbar
*
Discover
Visualize
Dashboard
Timelion
Management
Dev Tools
logstash-*
Selected Fields
? _source
Available Fields
Popular
t @message
t extension
ip
t machine.os
t response
t url
t @tags
@timestamp
? @version
t _id
t _index
_score
t _type
t agent
May 17th 2015, 04:00:41.685 - May 20th 2015, 18:32:51.964 —
Hourly
Count
400
200
0
2015-05-17 17:00
2015-05-18 17:00
2015-05-19 17:00
utc_time per hour
Histogram
Side Navigation
Time
_source
May 18th 2015, 02:03:25.877
@timestamp: May 18th 2015, 02:03:25.877 ip: 185.124.182.126 extension: gif response: 404 geo.coordinates: { "lat": 36.518375, "lon": -86.05828083 } geo.src: PH geo.dest: MM geo.srcdest: PH:MM @tags: success, info utc_time: May 18th 2015, 02:03:25.877 referer: http://twitter.com/error/will
May 18th 2015, 05:28:25.013
@timestamp: May 18th 2015, 05:28:25.013 ip: 79.1.14.87 extension: gif response: 200 geo.coordinates: { "lat": 35.16531472, "lon": -107.9006142 } geo.src: GN geo.dest: US geo.srcdest: GN:US @tags: success, info utc_time: May 18th 2015, 05:28:25.013 referer: http://www.slate.com/warning/
Document Table

Một số sản phẩm SIEM:

- Thương mại: EMC enVision, Cisco MARS, Q1Labs, eIQ Networks, AlienVault, Trigeo Network
- Syslog-NG, Metalog, Msyslog, Sysklogd, Sysklogd-sql, Snare, Logcaster, InTrust, LogLogic.
- SEC (Simple Event Correlator), OSSIM (Open Source SIEM), Plixer International Scrutinizer, flow analyzer, Fluke Networks, NetFlow Tracker