

Applying SIEM to monitor IT system and prevent network attack



TRUNG TÂM LƯU KÝ CHỨNG KHOÁN VIỆT NAM
VIETNAM SECURITIES DEPOSITORY

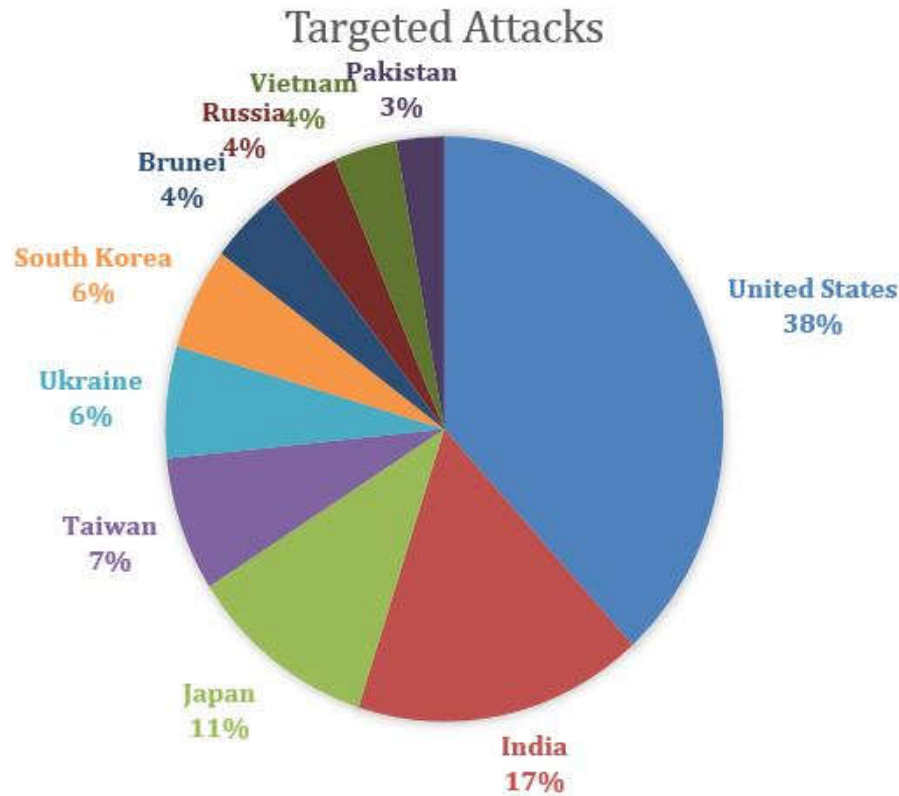
21st ACG CrossTraining Seminar

Yogyakarta – Indonesia 2019

Contents

- 1** Cyber security-facts and statistics 2018
- 2** VSD IT System & SIEM requirements
- 3** SIEM in VSD
- 4** Summary

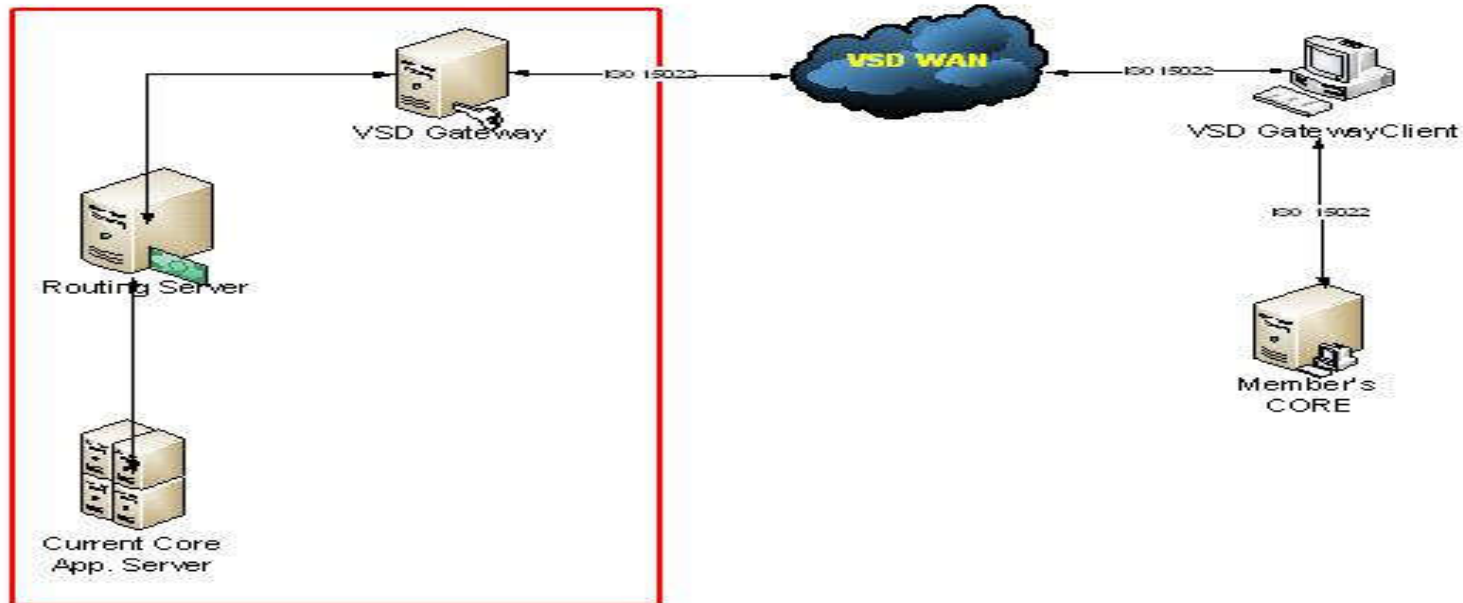
1. Cyber security - Facts and statistic in 2018



- **The United States is No. 1 target for targeted attacks:** Targeted attacks are often state-sponsored, though some have been by private groups. The U.S. is the No. 1 target (38%), Vietnam (4%).
- **Attackers try to spy, disrupt, identity theft, sabotage, or rob from victims, especially companies in finance sector.**
 - Vietnam is one of most favorite targets for attacker!
 - VSD, a company in finance sector pays special attention to invest in improving security for the system by investing network firewall, database firewall, establishing and monitoring system operations procedure and enhancing the awareness of business user and expertise of system operators.

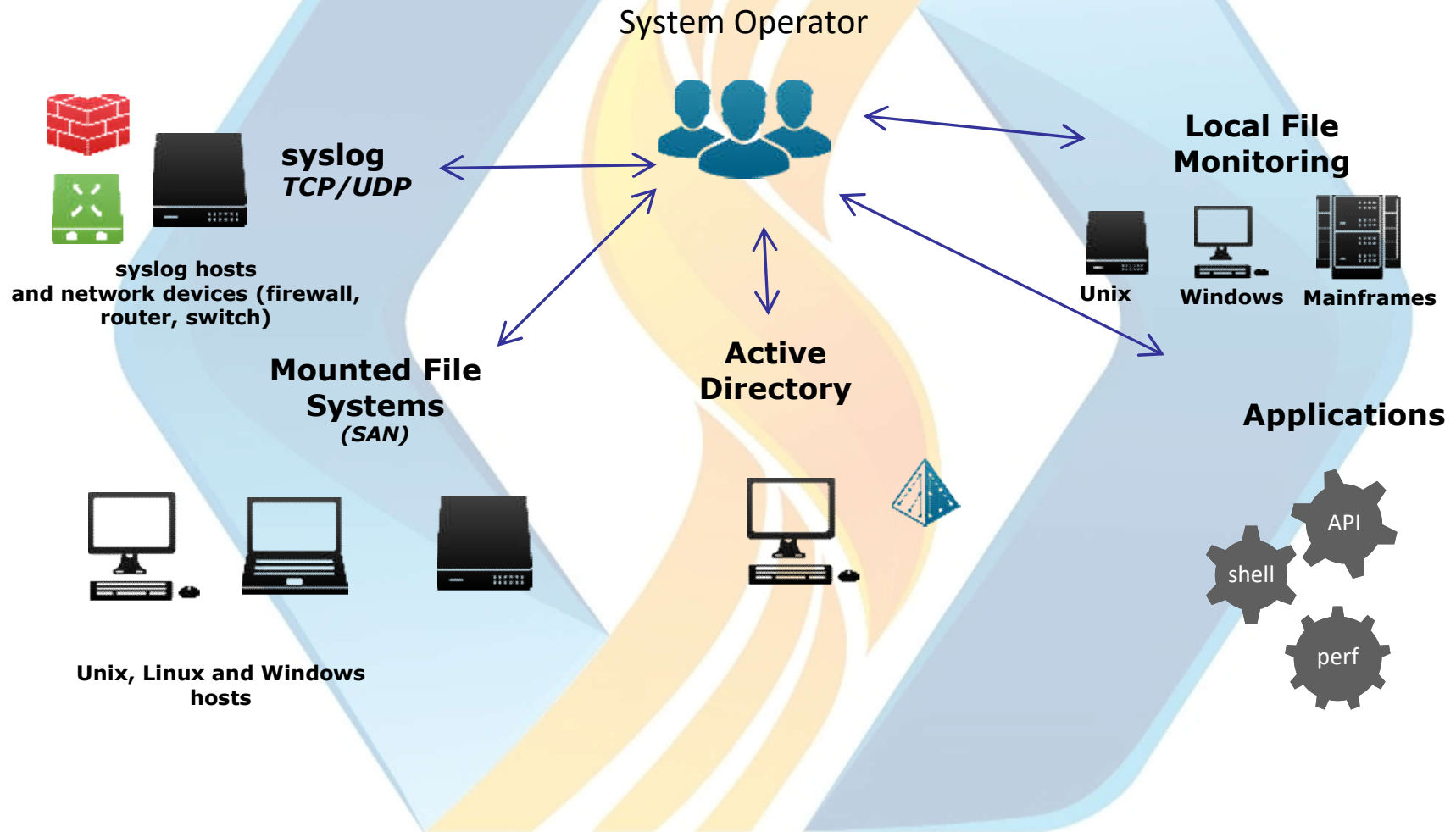
*Source: Internet

VSD IT connecting mechanism and milestone



- **Before July 1, 2015 :** Depository Member (DM) connect to VSD via Terminal
- **July 1, 2015 :** DM connect to VSD via STP system using ISO 15022 Message format (10 DMs connected at that time, now: 48 DMs online incl. securities companies and custodian bank, another DMs still via Terminal).
- **August 1, 2017:** Cash payment for government bond transactions through the State Bank of Viet Nam
- **August 10, 2017:** Go-live derivatives market (Clearing member, settlement bank connect to VSD via STP)
- **Until now, VSD has online connection with:** stock exchanges, settlement banks (cash- and derivatives market), state bank of vietnam, securities companies, custodian banks.

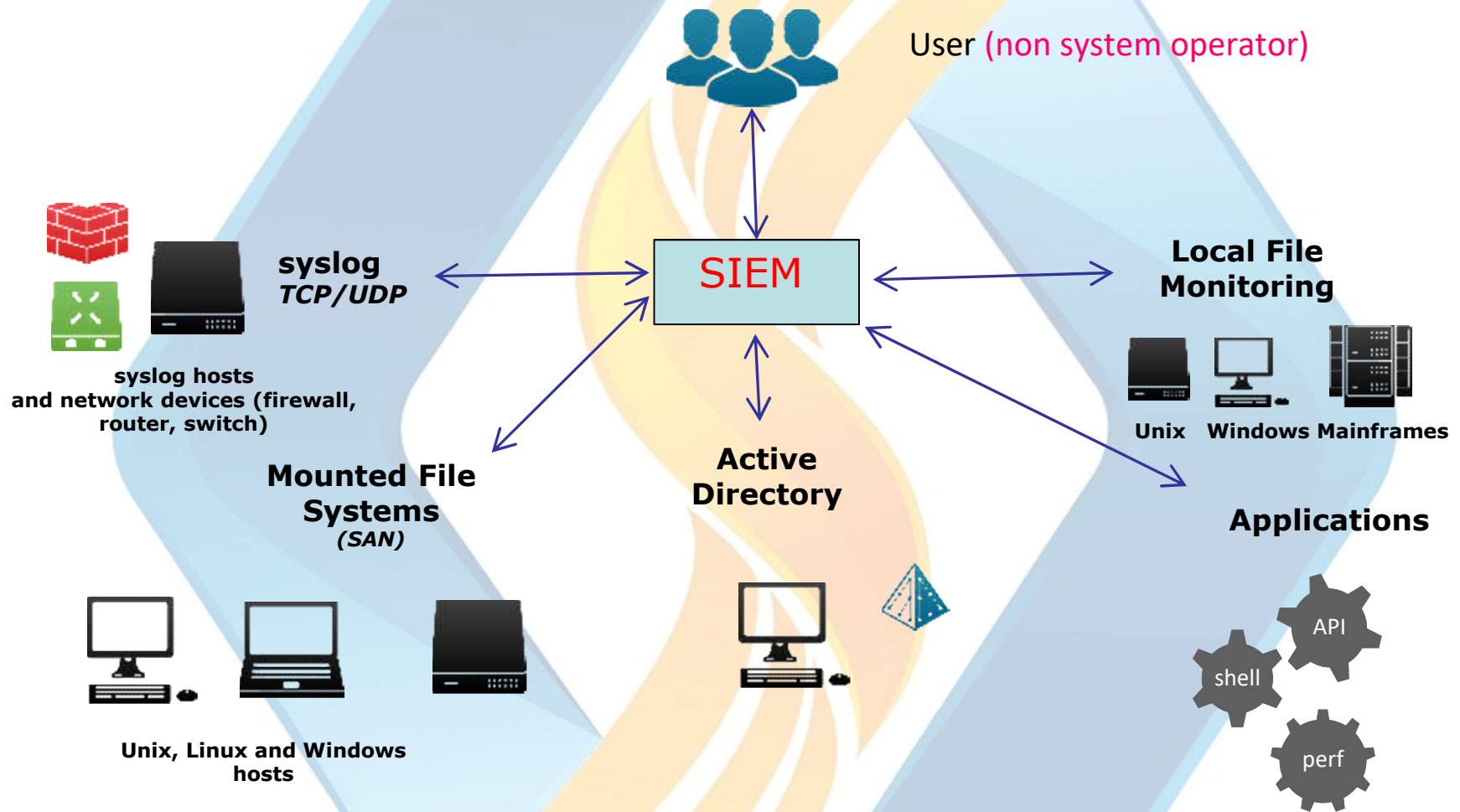
System operator monitor log manually



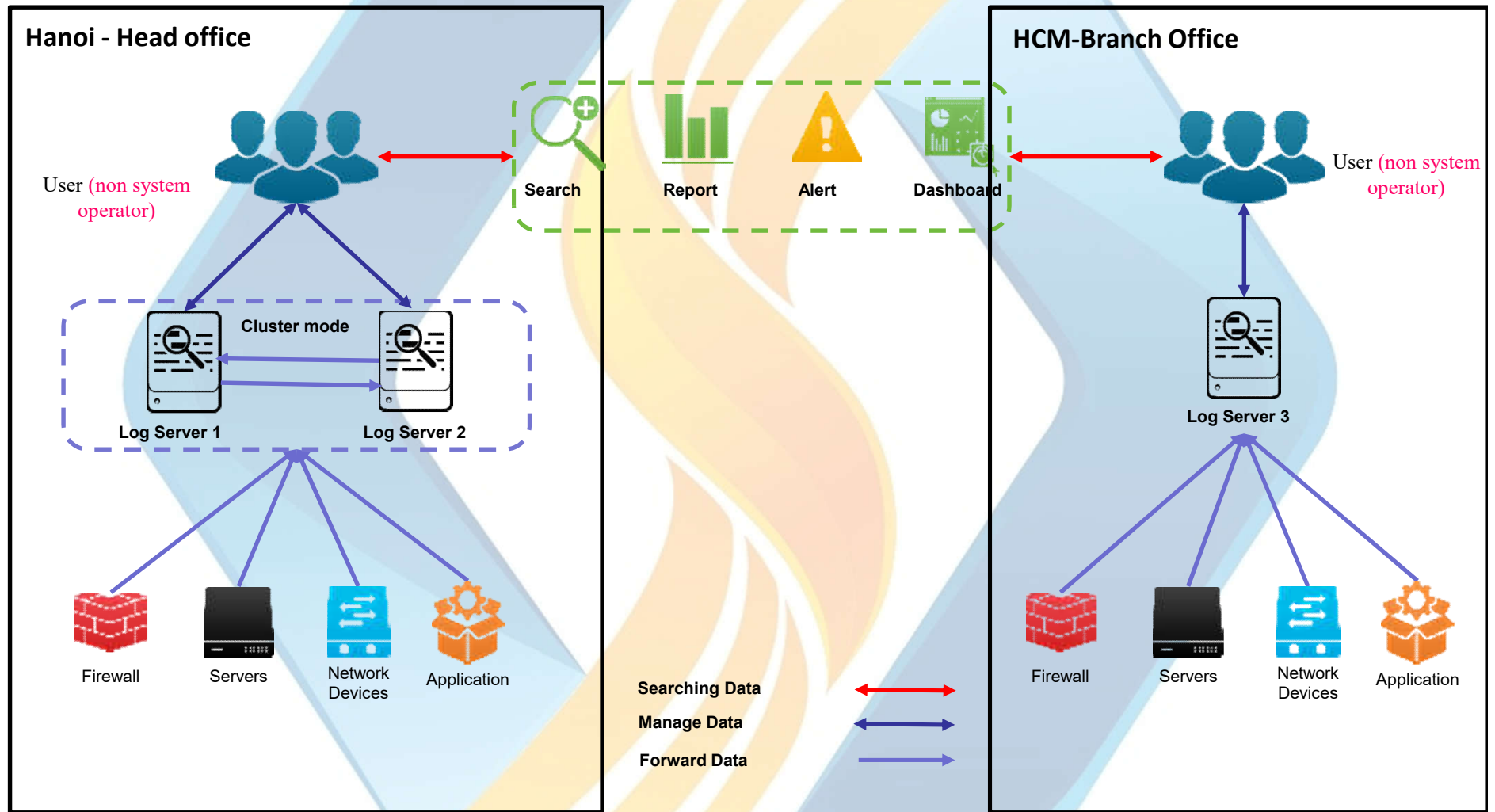
Problems

- Numbers of system operator for monitoring system log
- Deep analyzing system log for detecting network attack needs well-qualified system operator with expertise.
- System operator must logon to each system/device for manual correlating log procedure when incident occurs for tracing hacker's activities.
- Alert for "possible" system attack only on single device, no forensic based on correlating log between different device/system (Firewall/IPS log, Router/Switch log, Application Log, OS Log)

SIEM instead of system operator



SIEM to monitor IT system and prevent network attack



What is SIEM?

- **SIEM - security information and event management**
- *“The underlying principles of every SIEM system is to aggregate relevant data from multiple sources. For example, when a potential issue is detected, a SIEM might log additional information, generate an alert and instruct other security controls to stop an activity’s progress”(*)*

*Source: Internet

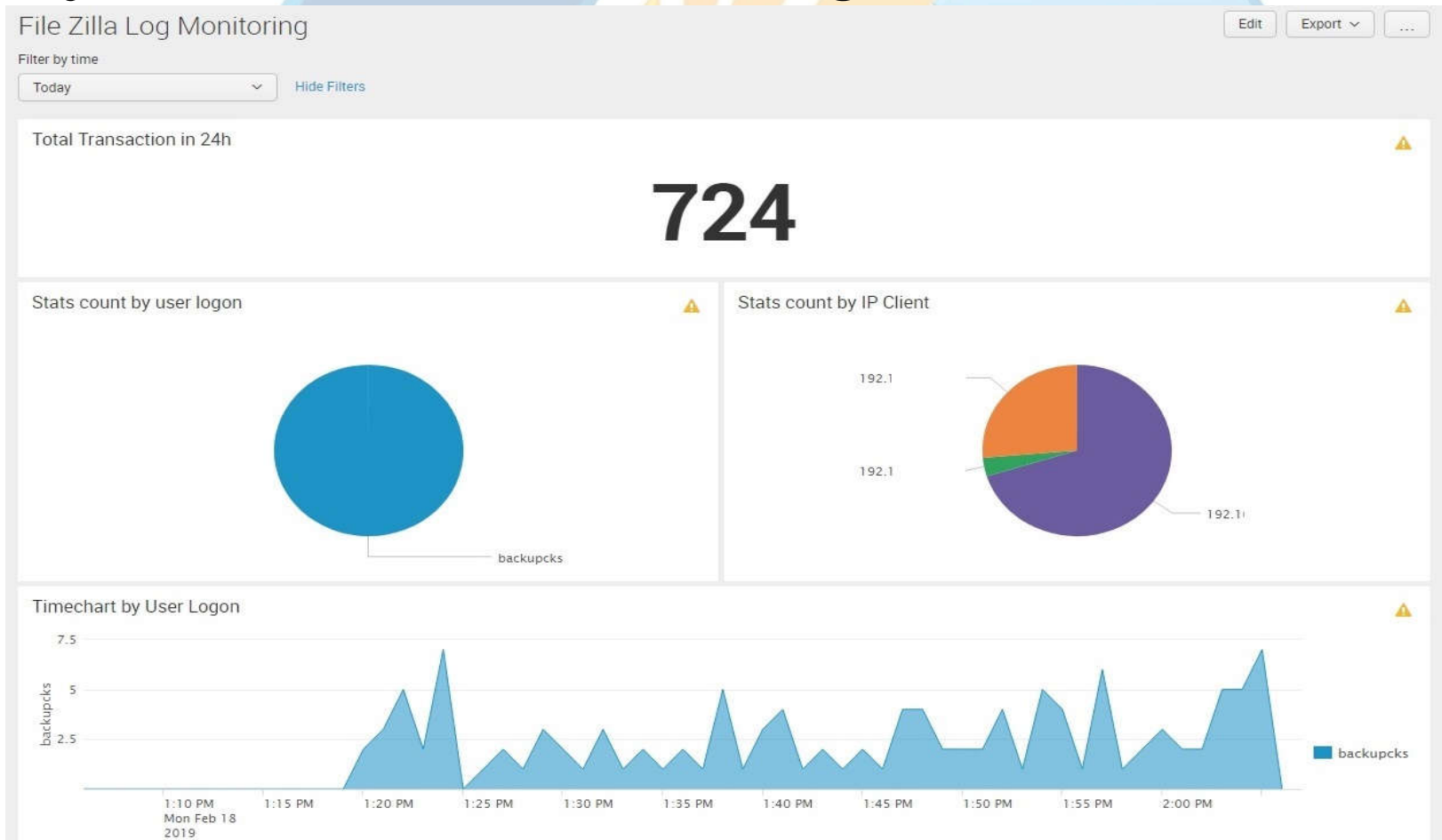
3.Splunk-SIEM in VSD

Scope:

- Network device (Router, Switch,..) log
- Network firewall log
- Database firewall log
- Server and workstation (Unix, Linux, Windows,...) log
- Active Directory log
- Database log
- Antivirus log
- Business application log

3.Splunk-SIEM in VSD

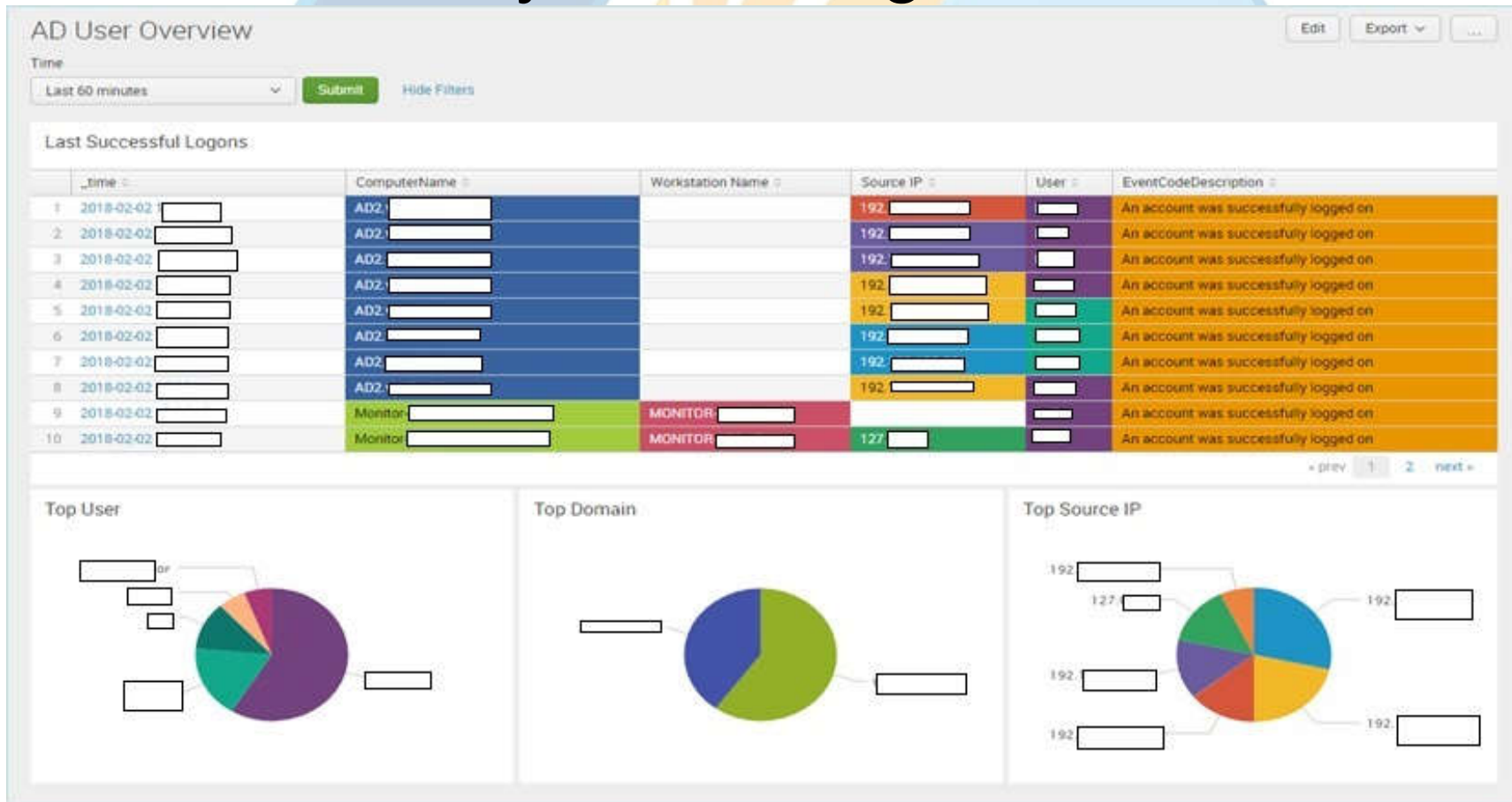
System health monitoring:



3/1/2019

3.Splunk-SIEM in VSD

Active Directory monitoring



3.Splunk-SIEM in VSD

Application Error Log

The screenshot displays the Splunk SIEM interface for 'Event Sources'. The top navigation bar includes 'Event Sources', 'Edit', 'Export', and a menu icon. Below the navigation bar, there are filters for 'Select time range' (Last 4 hours), 'Event types' (Error X), 'Computer' (All), and 'Keyword' (*). A 'Hide Filters' button is also present.

The main content area is divided into two sections:

- Event sources:** A table listing various source names and their total event counts.
- Event sources percentages:** A pie chart showing the distribution of events across different source categories.

Below these sections is a 'Matching events - drill down option' area with filters for 'Source Name' (ALL) and 'Source IP' (ALL).

The bottom section shows a table of matching events with columns for time, computer name, log name, event code, source name, type, message, and user name.

| # | _time | ComputerName | LogName | EventCode | SourceName | Type | Message | UserName |
|---|--------|--------------|-------------|-----------|-------------------------|-------|---|----------|
| > | 2/2/18 | Monitor | Application | 4107 | Microsoft-Windows-CAP12 | Error | Failed extract of third-party root list from auto update cab at: -http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/autho | |
| > | 2/2/18 | Monitor05 | Application | 4107 | Microsoft-Windows-CAP12 | Error | Failed extract of third-party root list from auto update cab at: -http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/autho | |
| > | 2/2/18 | Monitor/Sec- | Application | 5973 | Microsoft-Windows-Apps | Error | Activation of app Microsoft.Windows.Cortana_cw5n1h2txyewy\CortanaUI failed with error. This app can't be activated by the Built-in Administrator. See | |
| > | 2/2/18 | Monitor | Application | 4107 | Microsoft-Windows-CAP12 | Error | Failed extract of third-party root list from auto update cab at: -http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/autho | |
| > | 2/2/18 | Monitor | Application | 4107 | Microsoft- | Error | Failed extract of third-party root list from auto update cab at: | |

3.Splunk-SIEM in VSD

Brute force attack detection

Brute Force Detail 8m ago

Account Name: All

| _time | Account_Name | Workstation_Name | Failure_Reason | Count |
|------------|--------------|------------------|--|-------|
| 2019-02-18 | | | Unknown user name or bad password. | 5 |
| 2019-02-18 | | MONITOR- | Unknown user name or bad password. | 4 |
| 2019-02-15 | | | Unknown user name or bad password. | 4 |
| 2019-02-15 | | - MONITOR- | An Error occured during Logon. Unknown user name or bad password. | 3 |
| 2019-02-14 | | | An Error occured during Logon. Unknown user name or bad password. | 3 |
| 2019-02-13 | | | An Error occured during Logon. | 4 |
| 2019-02-13 | | | An Error occured during Logon. Unknown user name or bad password. | 3 |
| 2019-02-12 | | | An Error occured during Logon. | 5 |
| 2019-02-12 | | | Unknown user name or bad password. | 4 |

3.Splunk-SIEM in VSD

Kaspersky antivirus monitoring:

Kaspersky Monitoring Edit Export ...

Select time range
Last 30 days Hide Filters

Severity: Info Client Computer: ALL Group: ALL

Event Monitoring

| | _time | client_computer | Application | Event | Description |
|---|------------|-----------------|--|--------------------|---|
| 1 | 2019-02-18 | APP- | Kaspersky Security 10.1 for Windows Server | Object not scanned | Object not scanned. Reason: object excluded from scanning by type. |
| 2 | 2019-02-18 | APP- | Kaspersky Security 10.1 for Windows Server | Object not scanned | Object not scanned. Reason: object excluded from scanning by type. |
| 3 | 2019-02-18 | APP- | Kaspersky Security 10.1 for Windows Server | Object not scanned | Object not scanned. Reason: object excluded from scanning by type. Object name: |
| 4 | 2019-02-18 | APP- | Kaspersky Security 10.1 for Windows Server | Object not scanned | Object not scanned. Reason: object excluded from scanning by type. Object name: |
| 5 | 2019-02-18 | APP- | Kaspersky Security 10.1 for Windows Server | Object not scanned | Object not scanned. Reason: object excluded from scanning by type. Object name: |
| 6 | 2019-02-18 | APP- | Kaspersky Security 10.1 for Windows Server | Object not scanned | Object not scanned. Reason: object excluded from scanning by type. Object name: |
| 7 | 2019-02-18 | APP- | Kaspersky Security 10.1 for Windows Server | Object not scanned | Object not scanned. Reason: object excluded from scanning by type. |
| 8 | 2019-02-18 | APP- | Kaspersky Security 10.1 | Object not scanned | Object not scanned. Reason: object excluded from scanning by type. |

4. Summary

Applying SIEM in VSD:

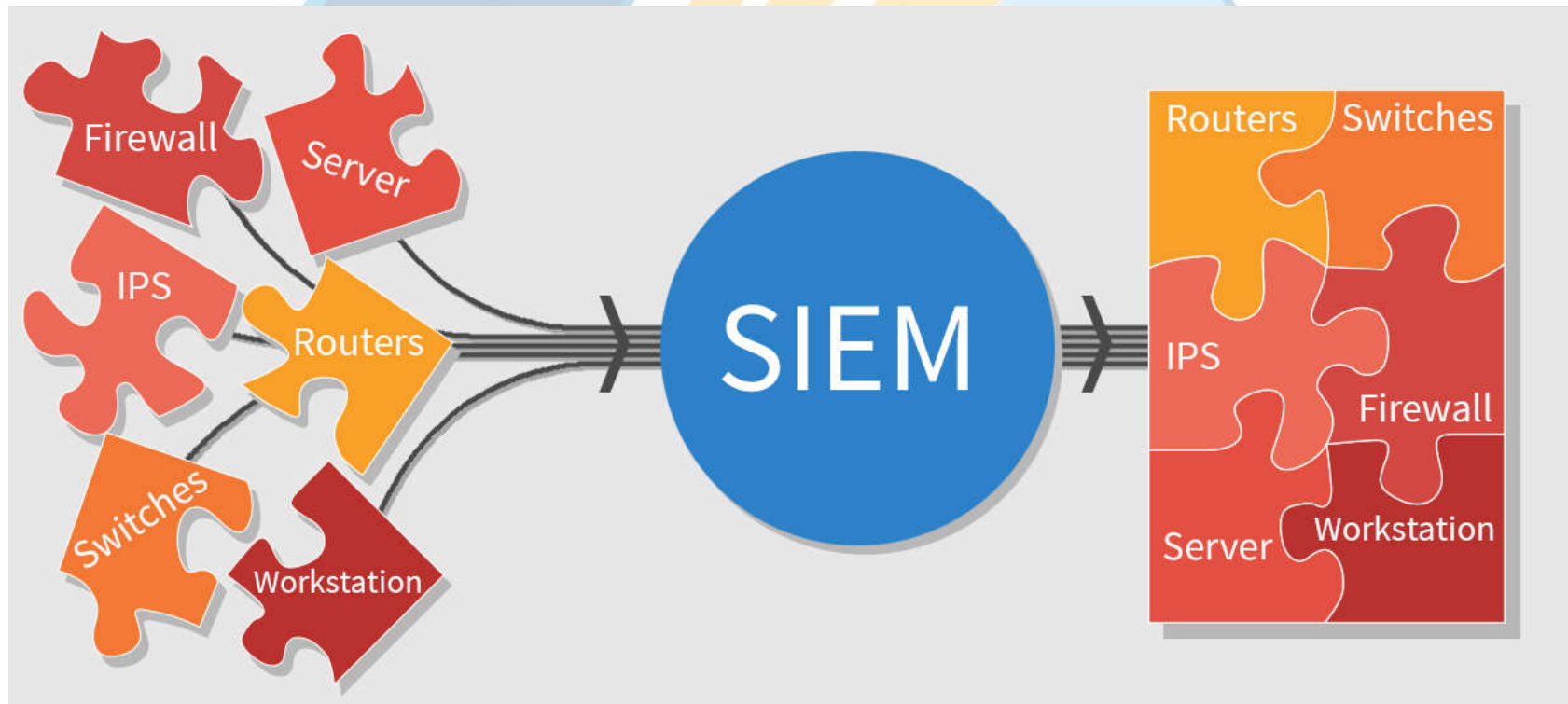
- Launch: Feb. 2018
- Vendor: Splunk Inc.
- Statistic:
 - Avg. Log volume \approx 9GB/day
 - Number of device: 250
 - Number of application: 15
 - Avg. number of events \approx 5 million events/day

4. Summary

Applying SIEM in VSD:

- Benefit:
 - Real-time alert for “possible” system attack
 - Real-time alert for system failure
 - Log correlation between different system device, application.
 - Minimizing investigation time when problems occurs related to security or system failure (30%)

SIEM



Correlating partial system components into a complete system picture.

*Source: Internet

