Applying SIEM to monitor IT system and prevent network attack

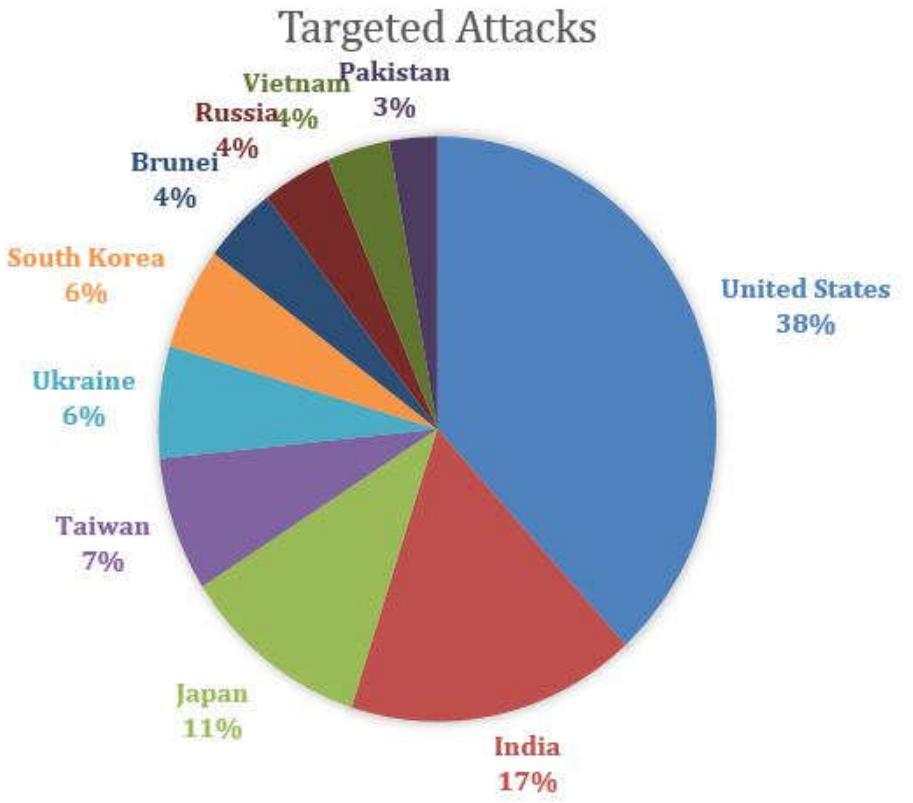
TRUNG TÂM LƯU KÝ CHỨNG KHOÁN VIỆT NAM
VIETNAM SECURITIES DEPOSITORY

21st ACG CrossTraining Seminar

Yogyakarta – Indonesia 2019

Contents

1. Cyber security - Facts and statistic in 2018



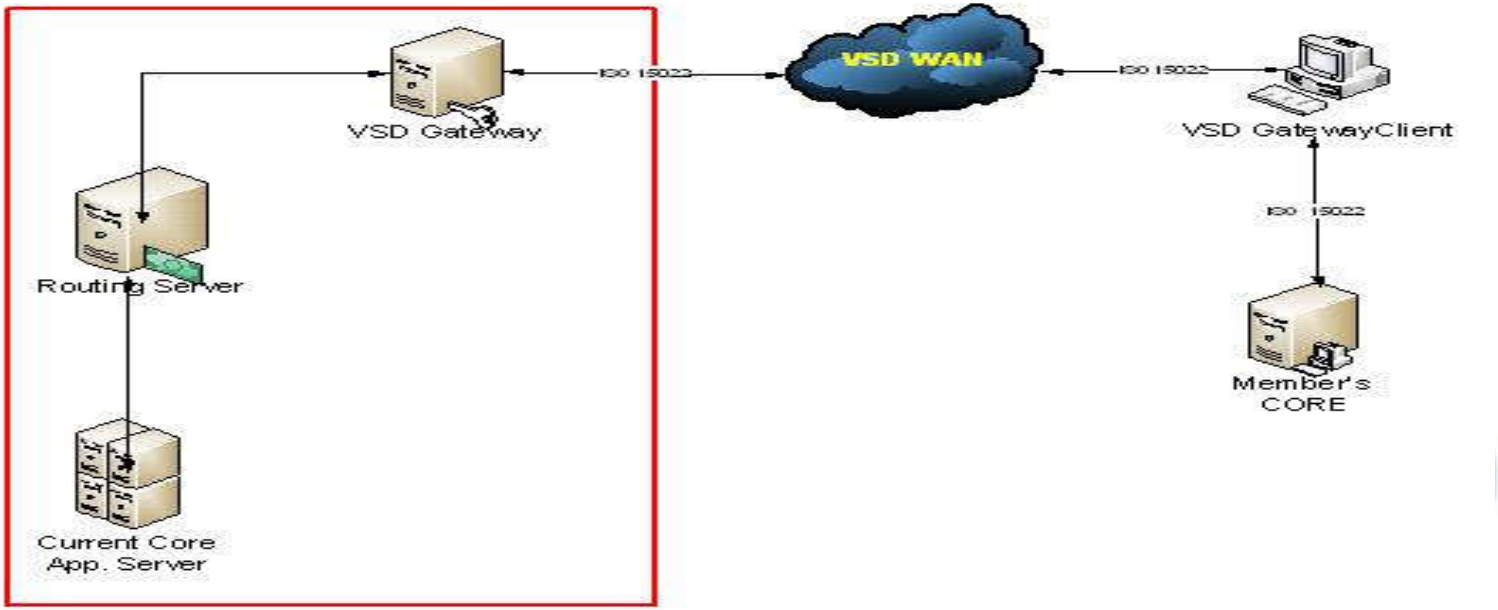
- **The United States is No. 1 target for targeted attacks:** Targeted attacks are often state-sponsored, though some have been by private groups. The U.S. is the No. 1 target (38%), Vietnam (4%).
- **Attackers try to spy, disrupt, identity theft, sabotage, or rob from victims, especially companies in 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.

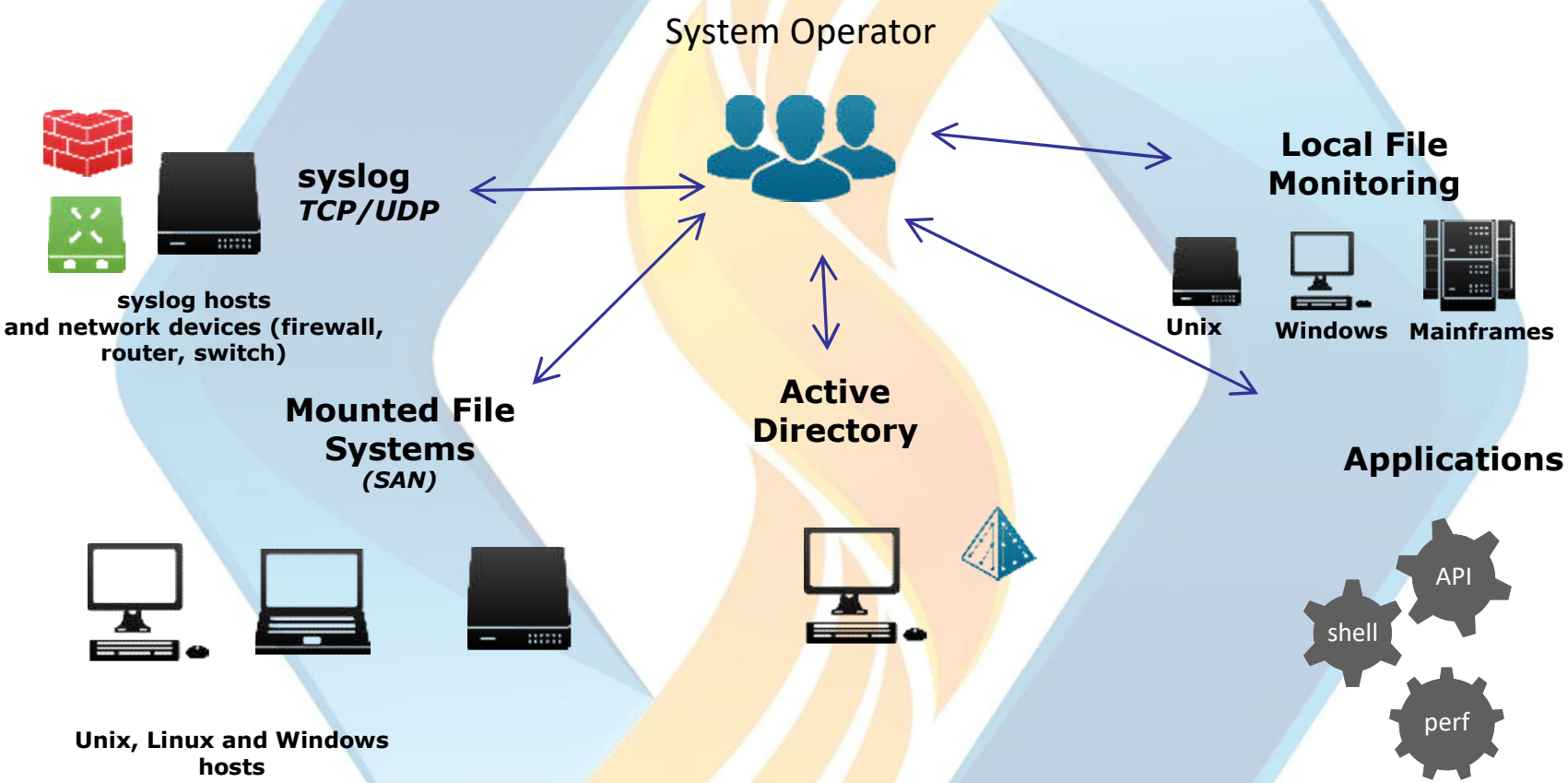
***Source: Internet**

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.

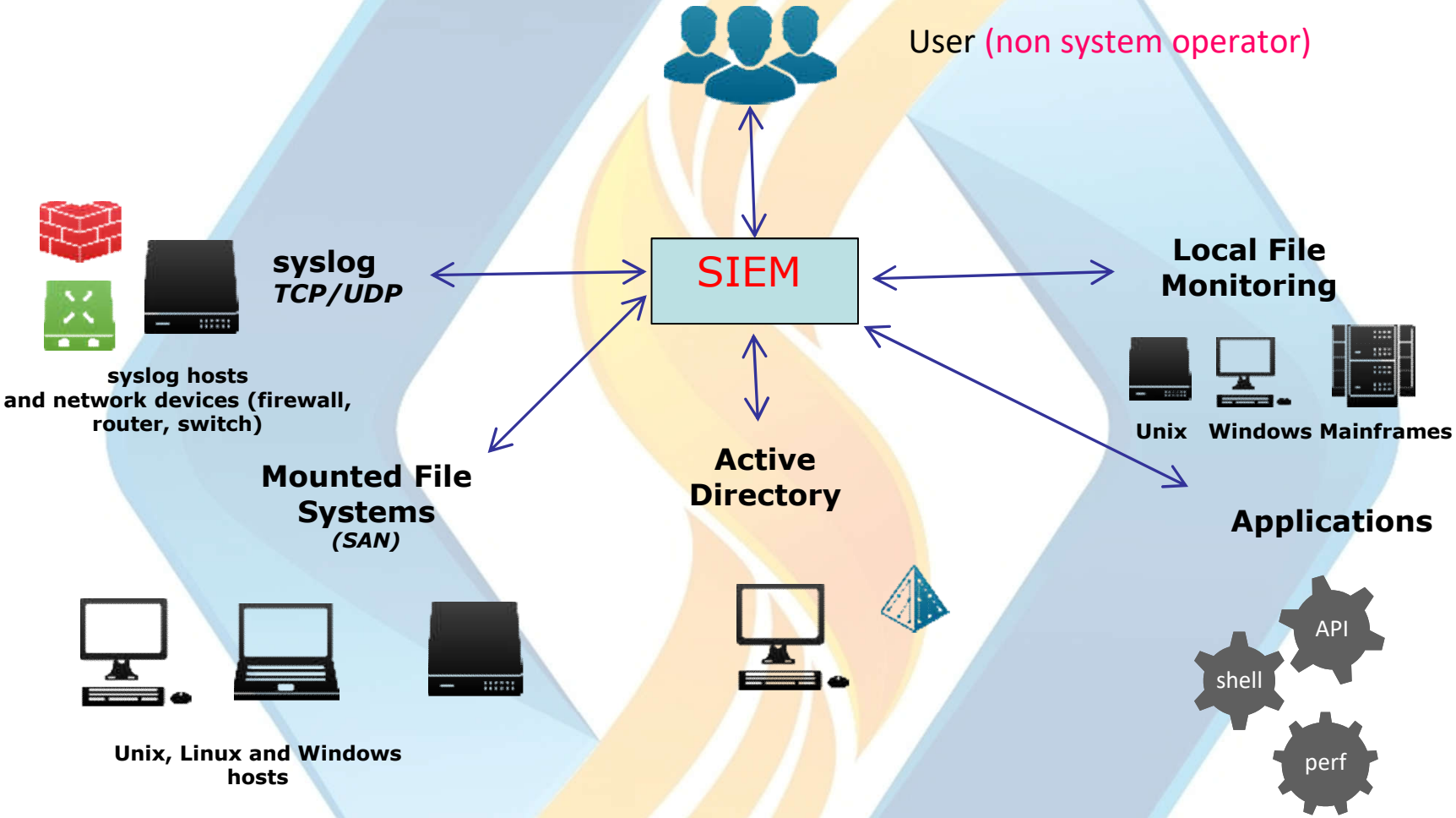
System operator monitor log manually



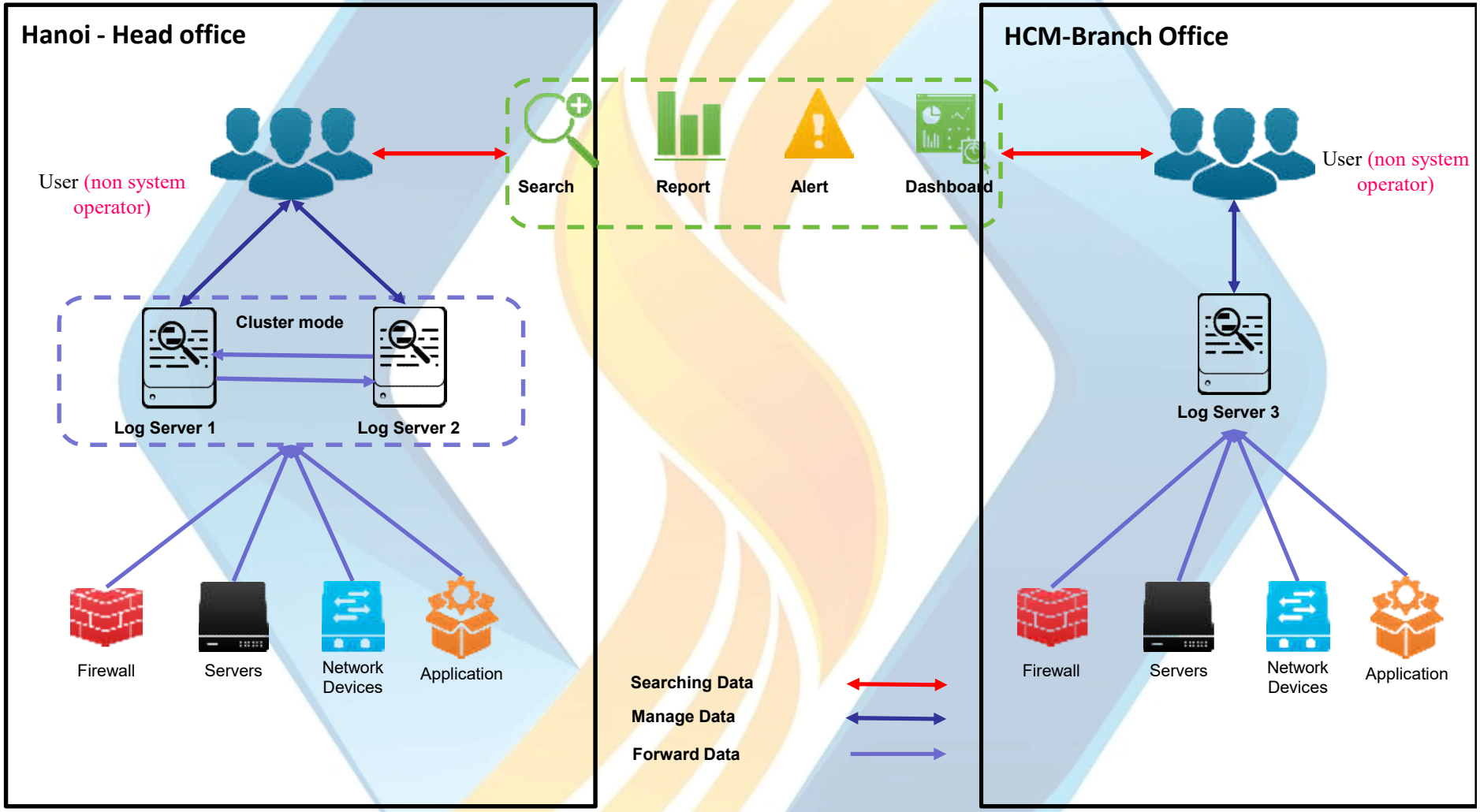
Problems

- 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**

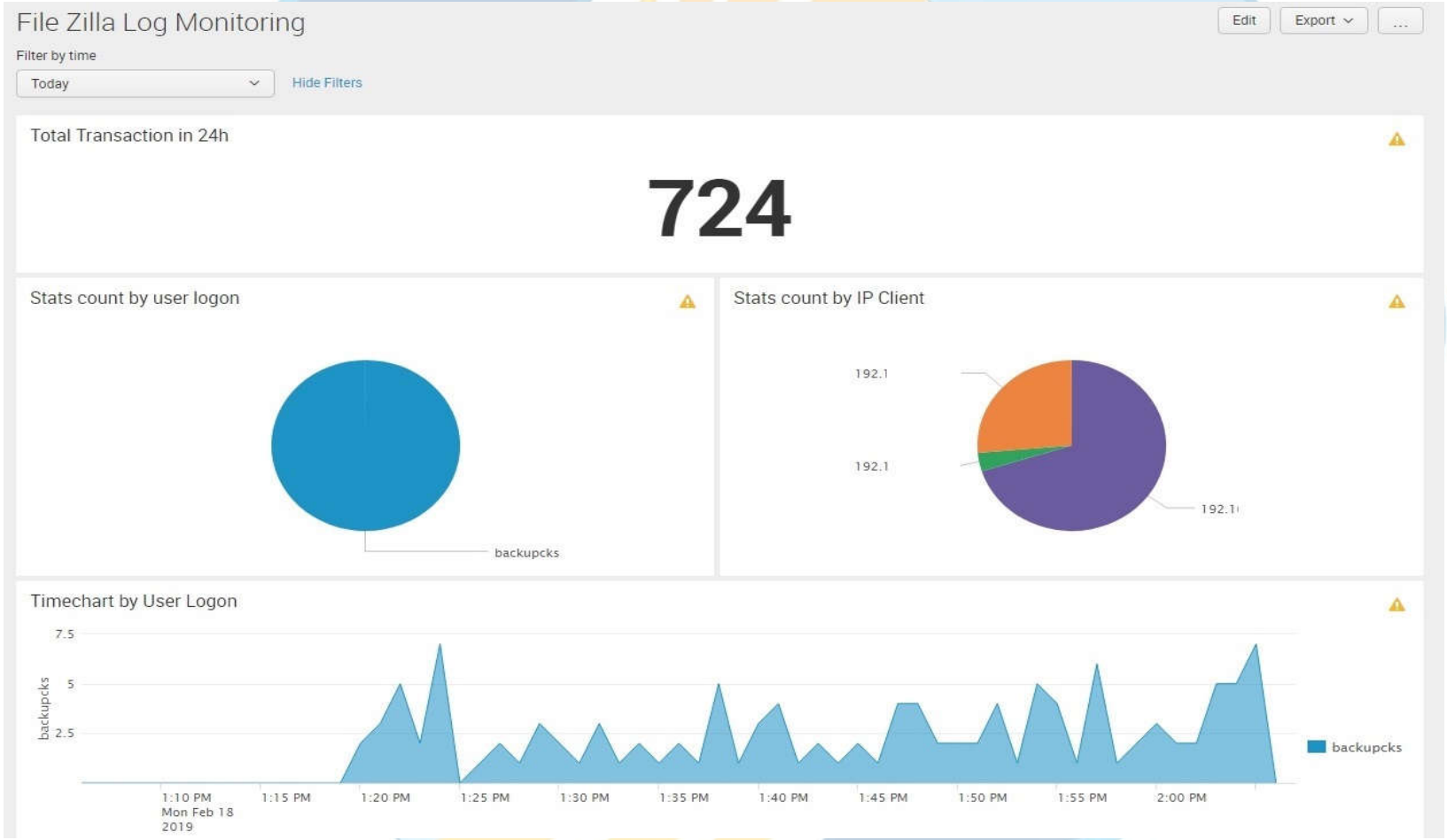
3.Splunk-SIEM in VSD

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

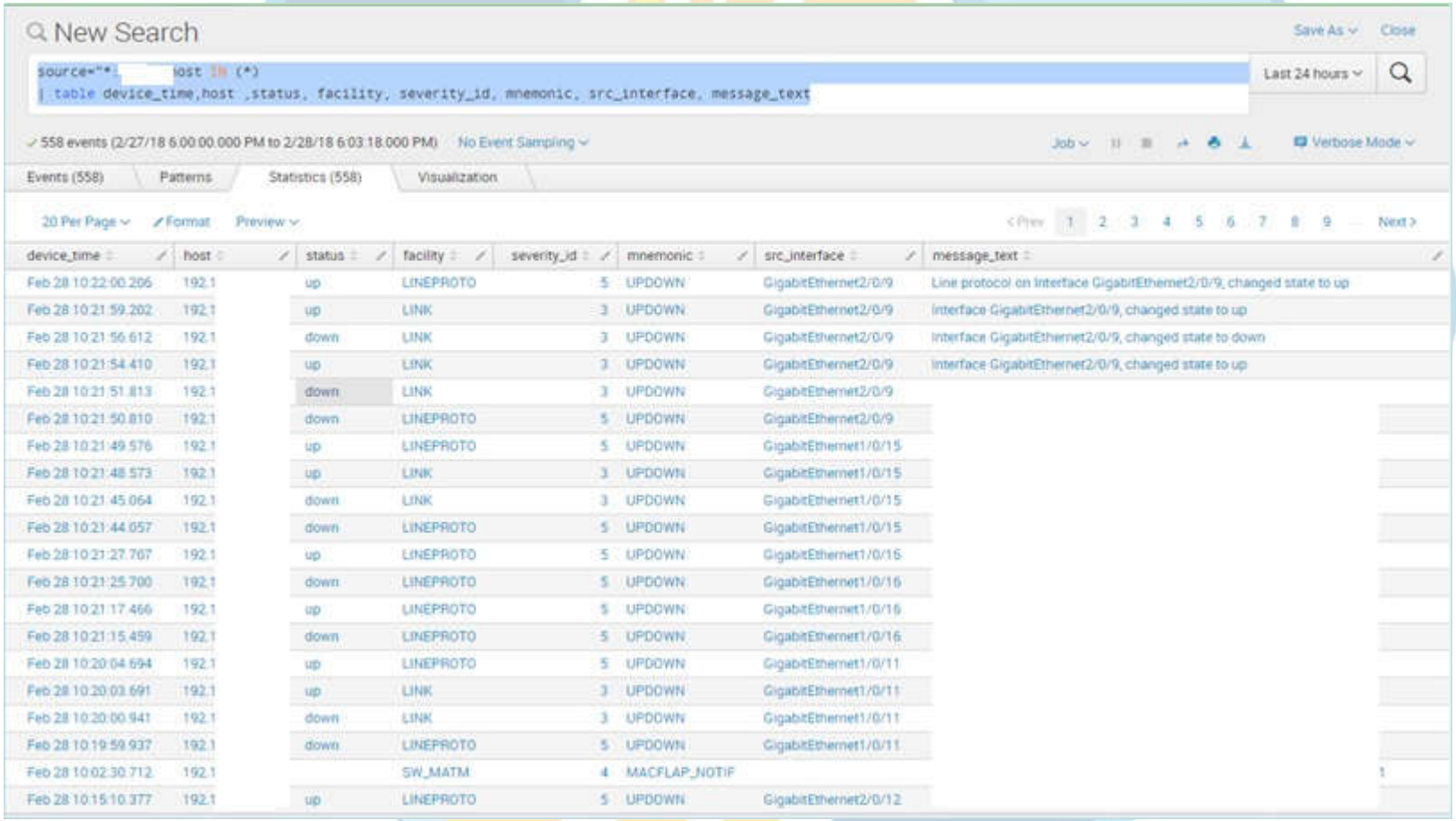
3.Splunk-SIEM in VSD

System health monitoring:



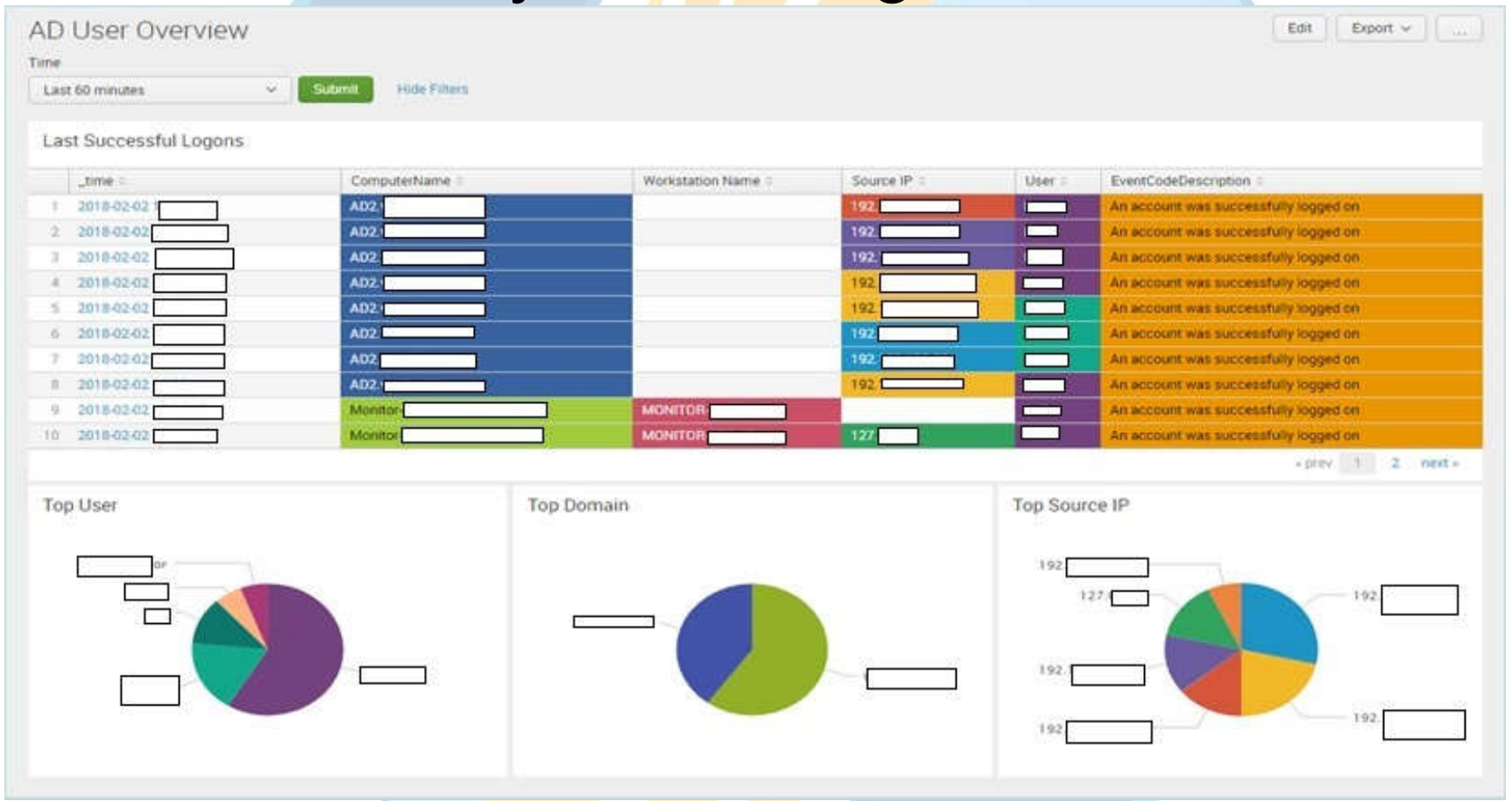
3.Splunk-SIEM in VSD

Network device monitoring:



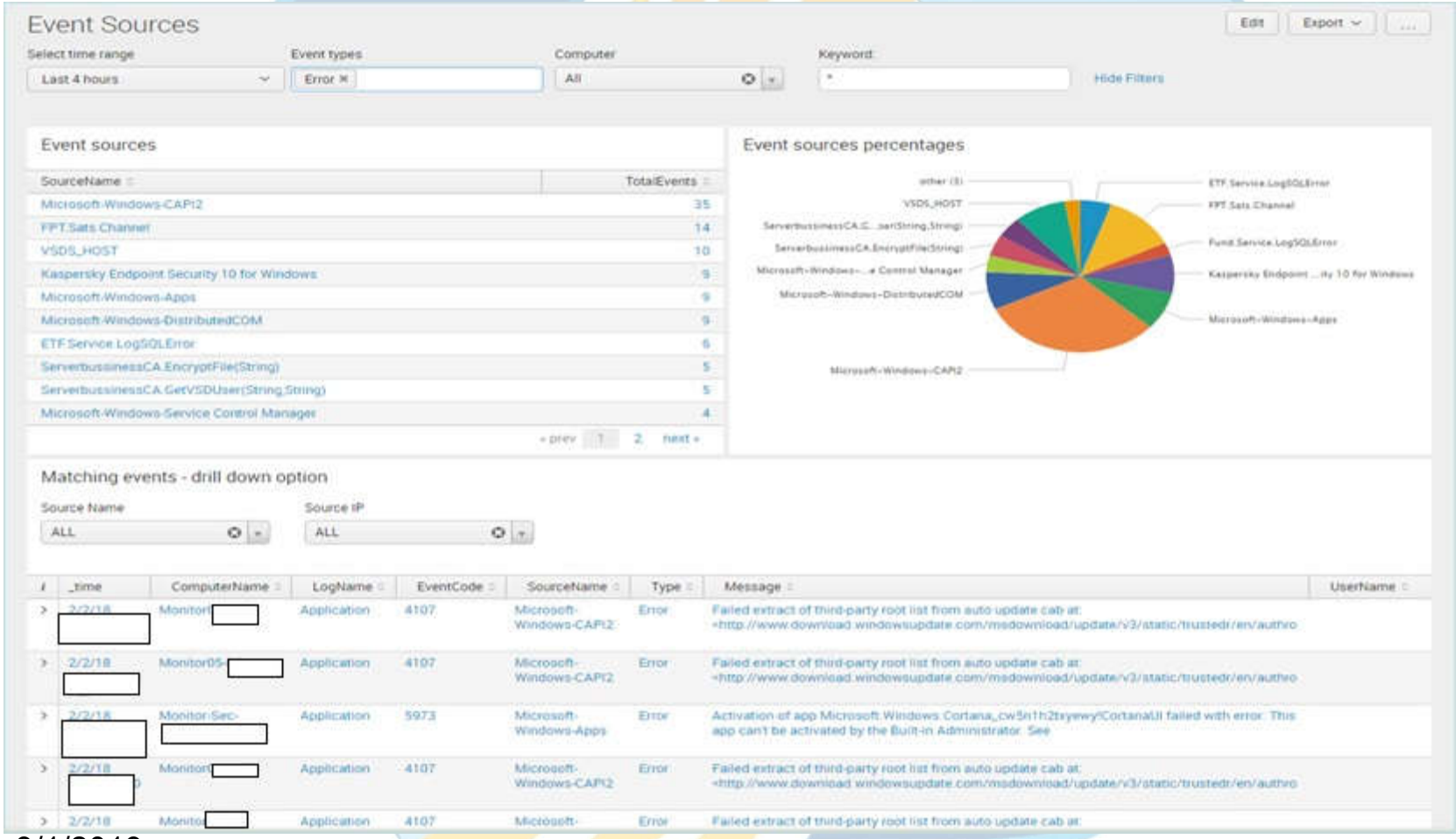
3.Splunk-SIEM in VSD

Active Directory monitoring



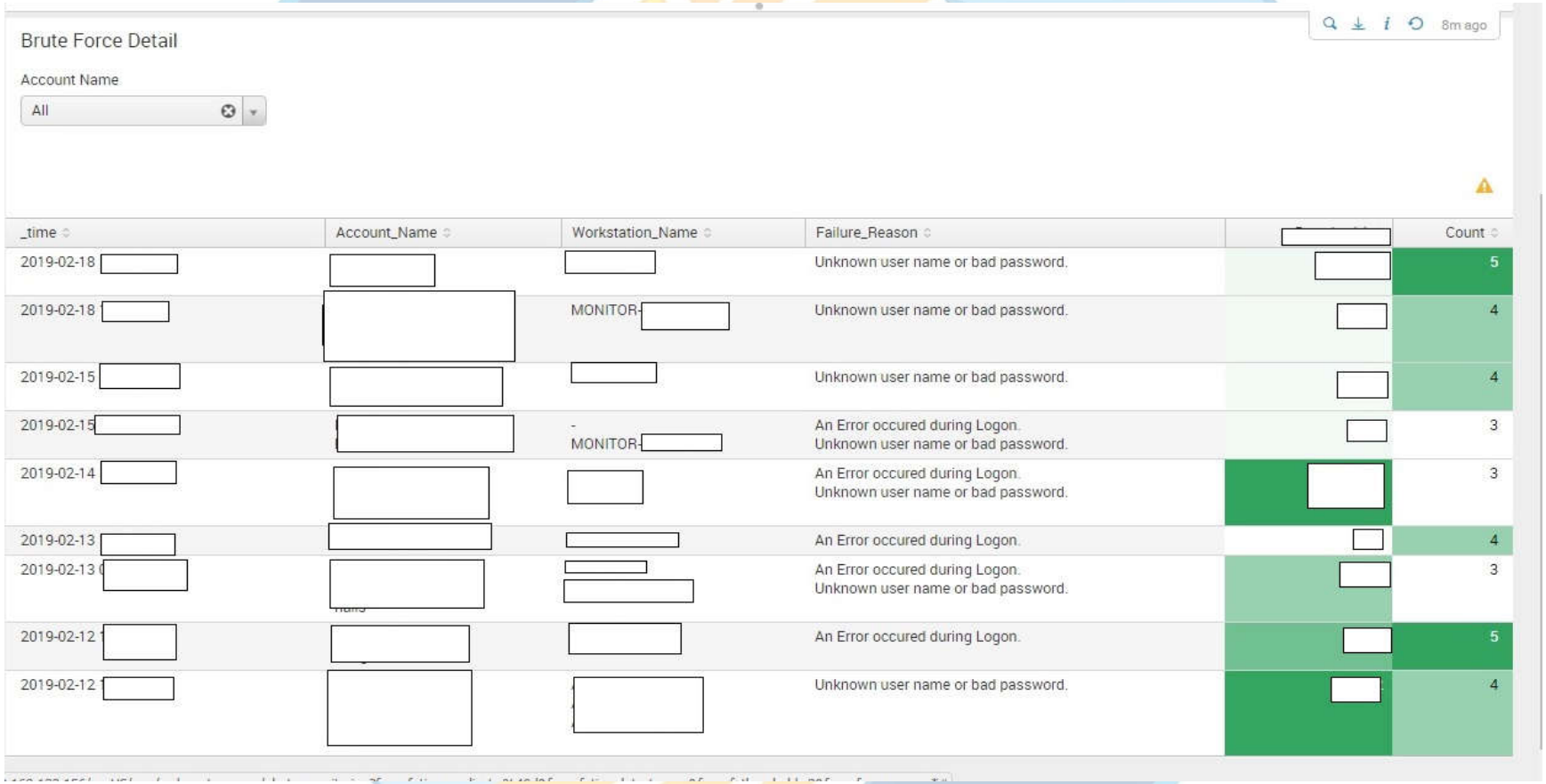
3.Splunk-SIEM in VSD

Application Error Log



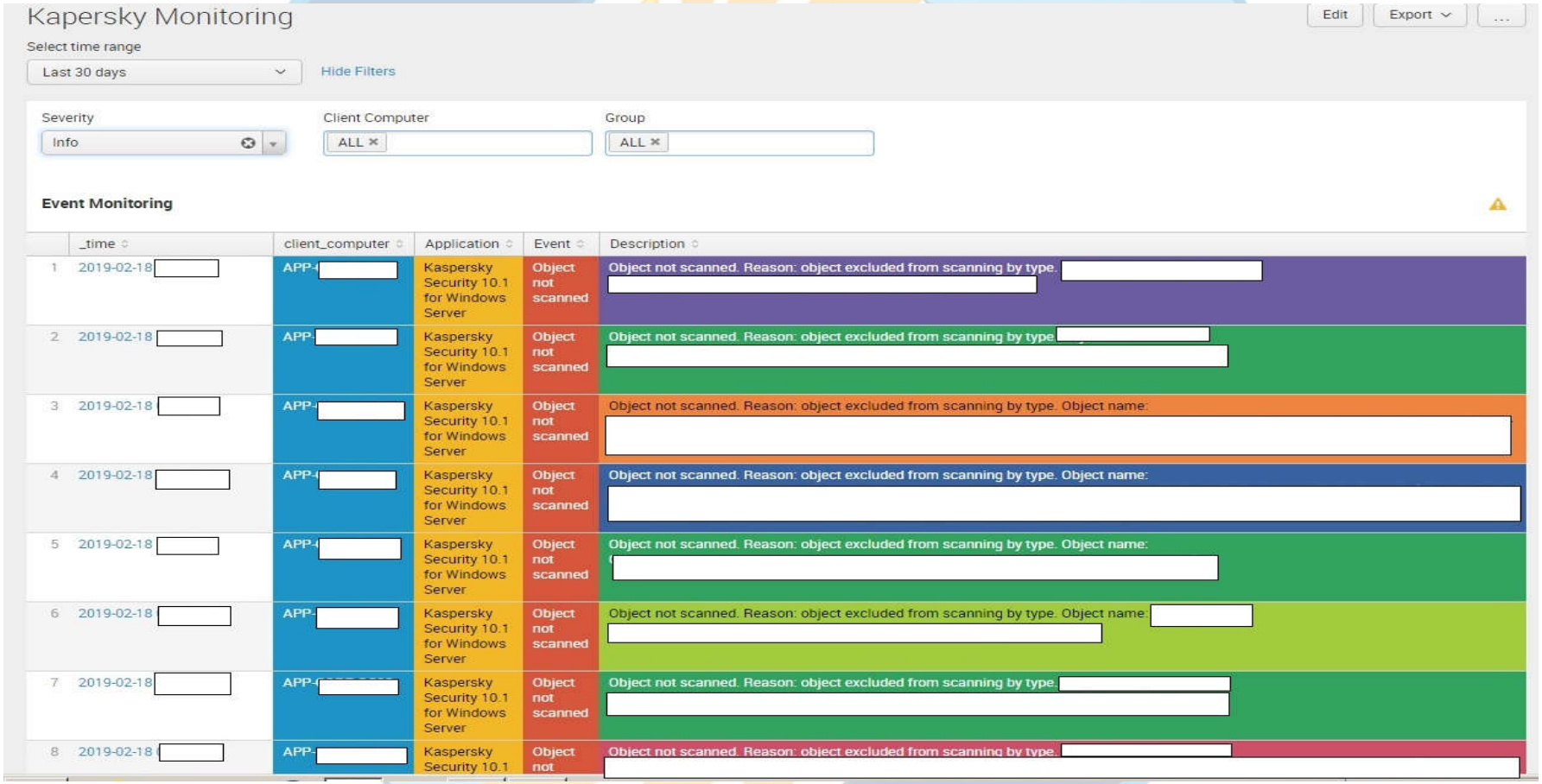
3.Splunk-SIEM in VSD

Brute force attack detection



3.Splunk-SIEM in VSD

Kaspersky antivirus monitoring:



4.Summary

Applying SIEM in VSD:

- Launch: Feb. 2018
- Vendor: Splunk Inc.
- Statistic:

- Avg. Log volume ≈ 9GB/day
- Number of device: 250
- Number of application: 15
- Avg. number of events ≈ 5 million events/day

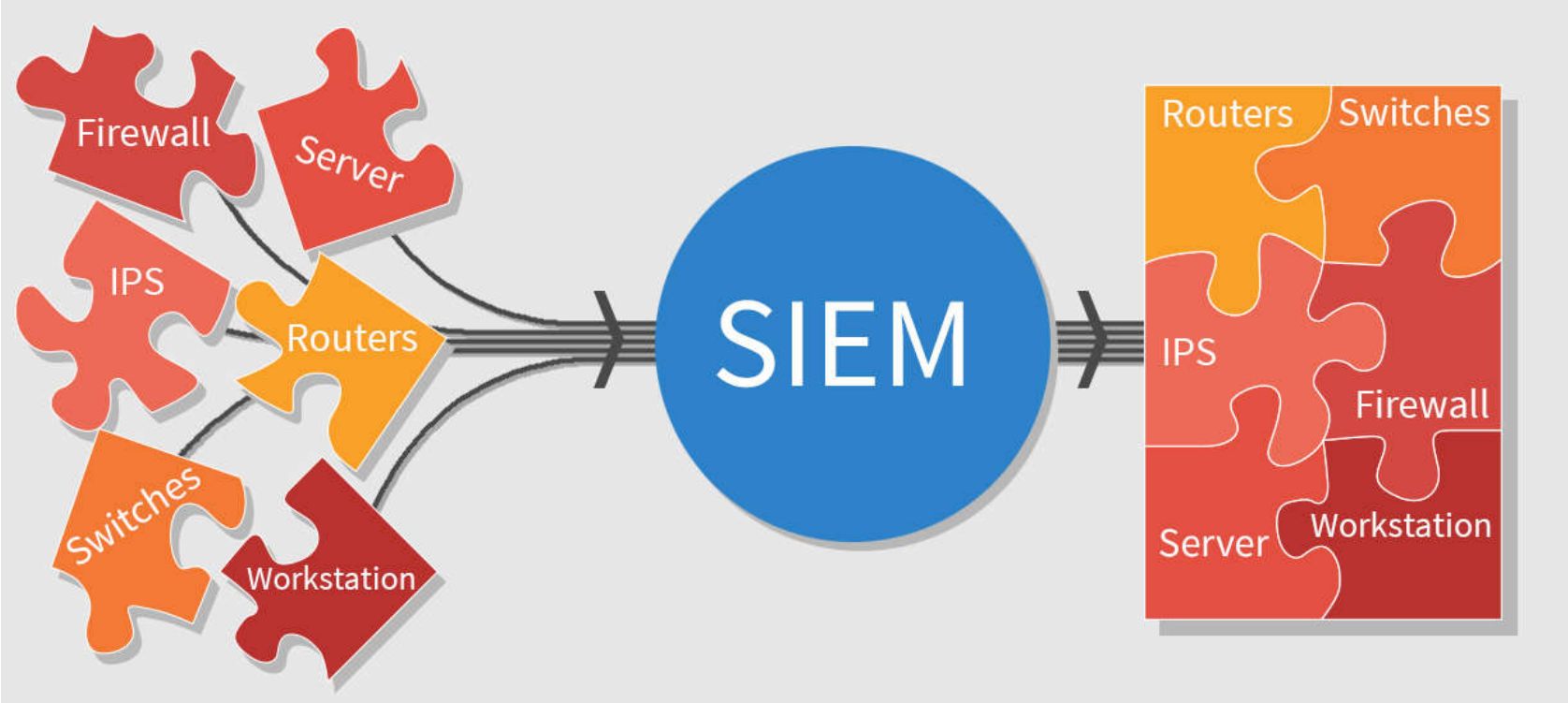
4.Summary

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**


Thank You!