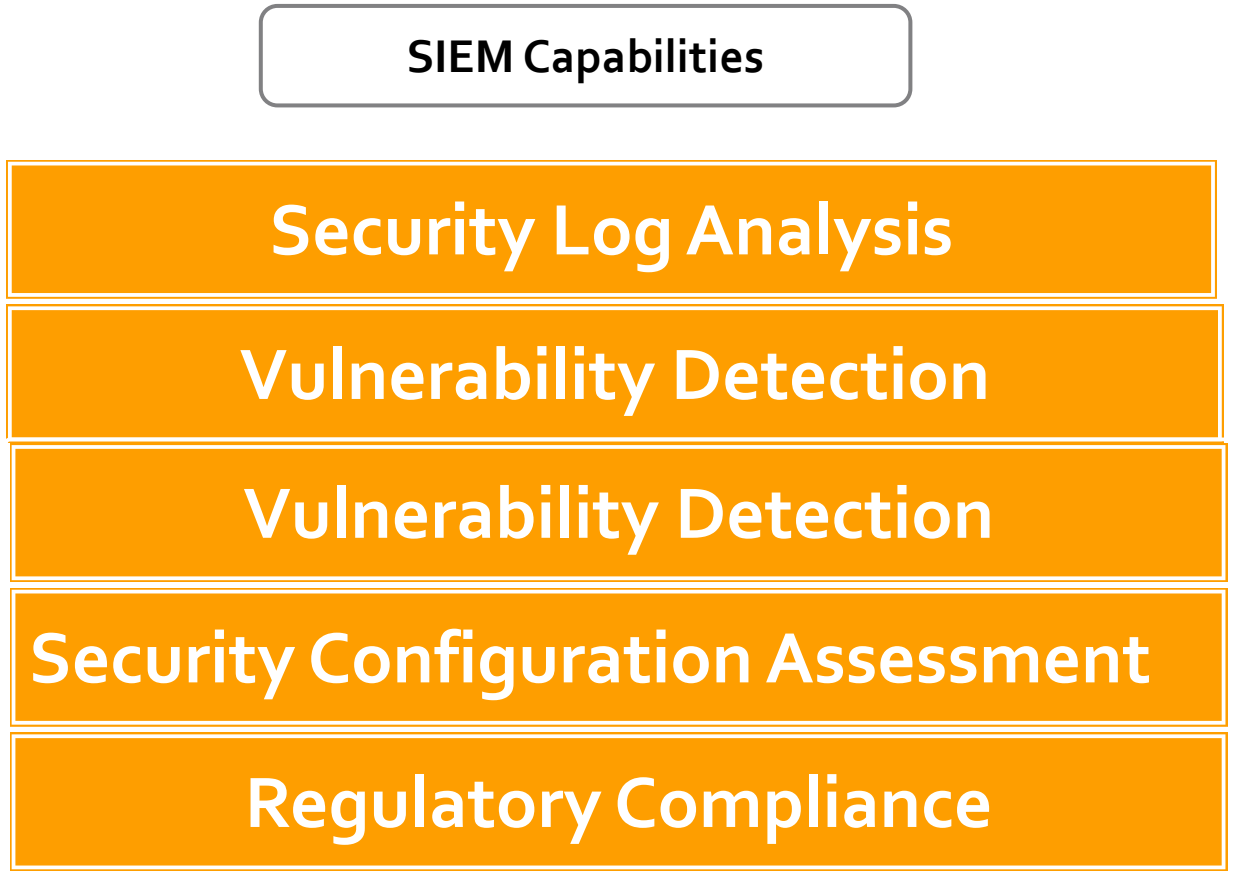
A plenarily integrated SIEM solution And it's Deployment.

Md. Rashedul Hasan
E-mail: rashedul.engr@gmail.com
Dhaka, Bangladesh

SIEM & it's Capabilities

SIEM solution is an essential piece of a security operations center (SOC) toolkit.
SIEM solutions collect data from across an organization's security architecture and alert about attacks, enabling rapid detection and response to threats.



Why Wazuh SIEM?

Wazuh is a free and open source security platform that unifies XDR and SIEM capabilities. It protects workloads across on-premises, virtualized, containerized, and cloud-based environments. Wazuh helps organizations and individuals to protect their data assets against security threats.

Some of the more common use cases of the Wazuh solution-

- Intrusion detection
- Log data analysis
- File integrity monitoring
- Anomaly and Malware detection
- Vulnerability detection
- VirusTotal integration
- Configuration assessment
- Incident response
- Regulatory compliance (NIST, PCIDSS, GDPR, NIST, TSC and HIPAA)
- IT Hygiene
- Cloud security
- Containers security
- Posture Management
- Workload Protection

Integrations

- Microsoft 365 and Microsoft 365 Defender
- Malware Detection with Virultotal with Active Response
- Malware Detection with Yara with Active Response
- SSH brute-force detection with Active Response
- Monitoring malicious command using aduitd
- Suricata integration for IDS
- Building IOCs file threat intelligence
- LimeRAT detection with active response
- Thehive integration for incident response
- Cortex Integration with Thehive for observable analysis

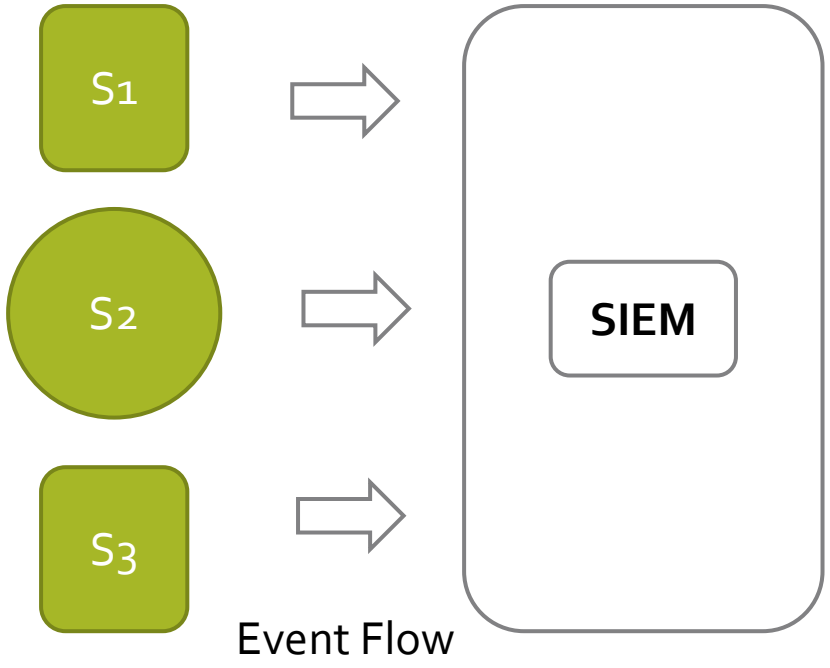
WAZUH SIEM Deployment

Wazuh can be deployed in two ways:

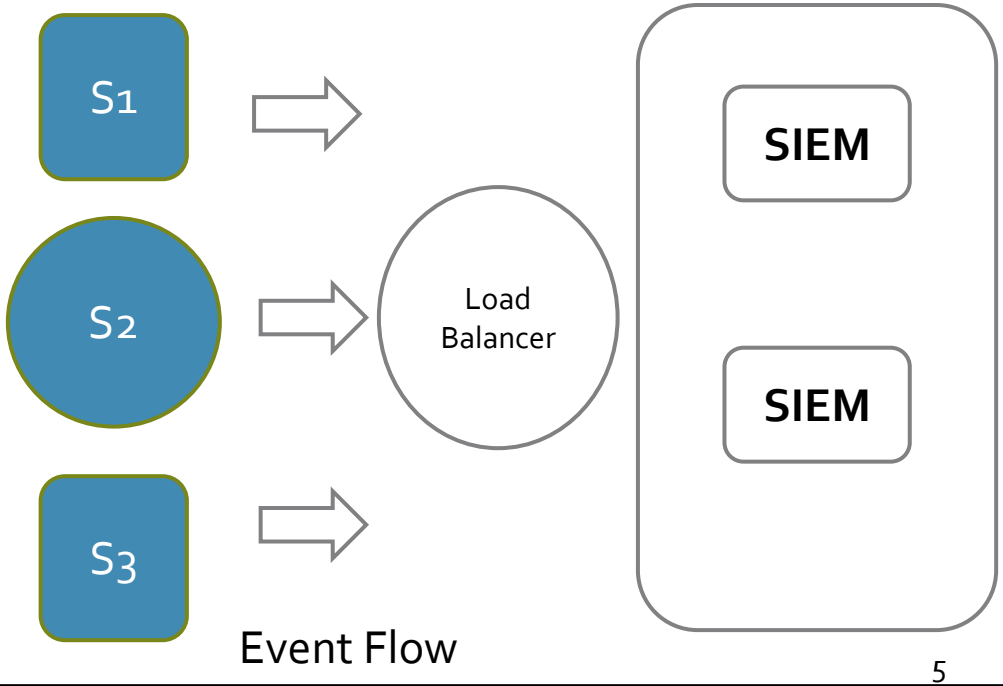
- **All In One**: Wazuh Server and ELK Stack are installed and configured on the same system.

- **Distributed**: Each component is setup on a seperate Server.

- **Standalone SIEM Deployment**



- **SIEM Cluster Deployment**



Preparing for the Installation

- **Operating System:**

Wazuh can be installed on various operating systems, including CentOS, Debian, Ubuntu, Windows, and macOS.

- **Hardware Specifications:**

Hardware requirements highly depend on the number of protected endpoints and cloud workloads.

- **Software Dependencies:**

Wazuh requires several software components, including **Elastic Stack**, **Filebeat**, and **Wazuh Manager**.

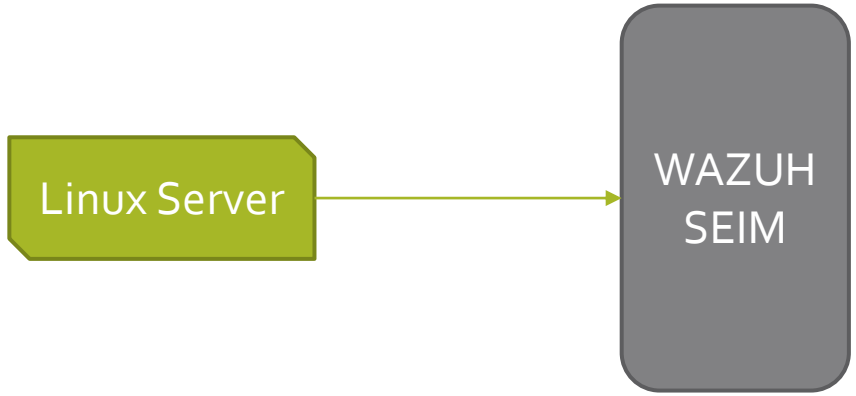
Elastic Stack is a set of open-source tools for data processing and analysis, including Elasticsearch, Logstash, and Kibana.

Filebeat is a lightweight agent that collects log data from different sources and forward it to Elasticsearch.

Wazuh Manager is the central component of the Wazuh architecture, which receives data from the Wazuh Agents and processes it to generate alerts and notifications.

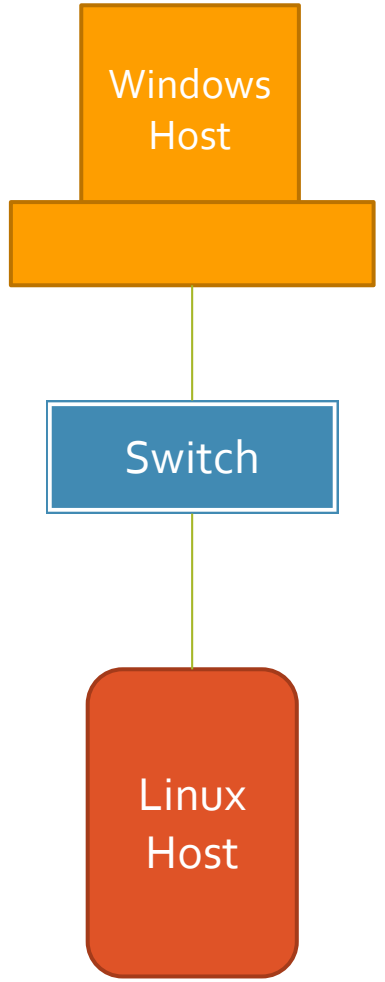
Step-by-Step Installation

- **Step 1:** Set Up Wazuh Server
  - Install **Wazuh**
  - Install **Wazuh Manager**
  - Install **Elasticsearch**
  - Install **Filebeat**
  - Install **Kibana**



Step-by-Step Installation (Cont.)

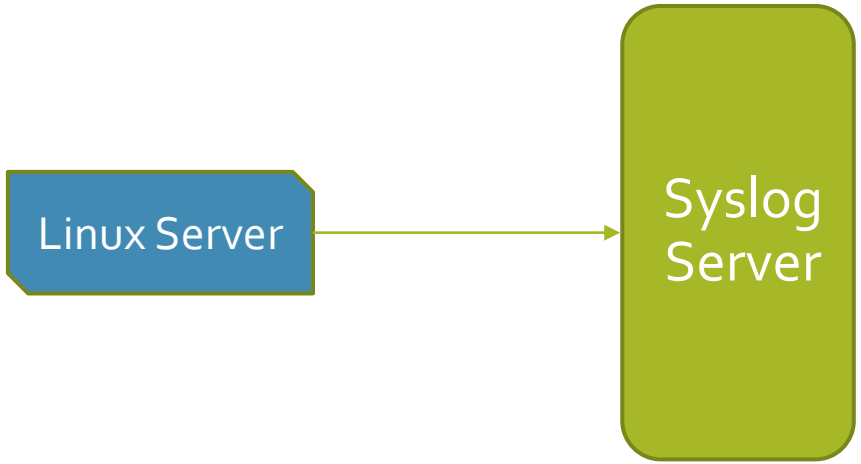
- **Step 2:** Install and Configure **Wazuh Agents**
  - Configure Windows Agent into **Windows Host**
  - Configure Windows Agent into **Linux Host**



Step-by-Step Installation (Cont.)

Step 3: Install and Configure **Syslog Server**

- Configure **Linux Server** as a Syslog Server
- Configure Wazuh Agent into this Syslog Server

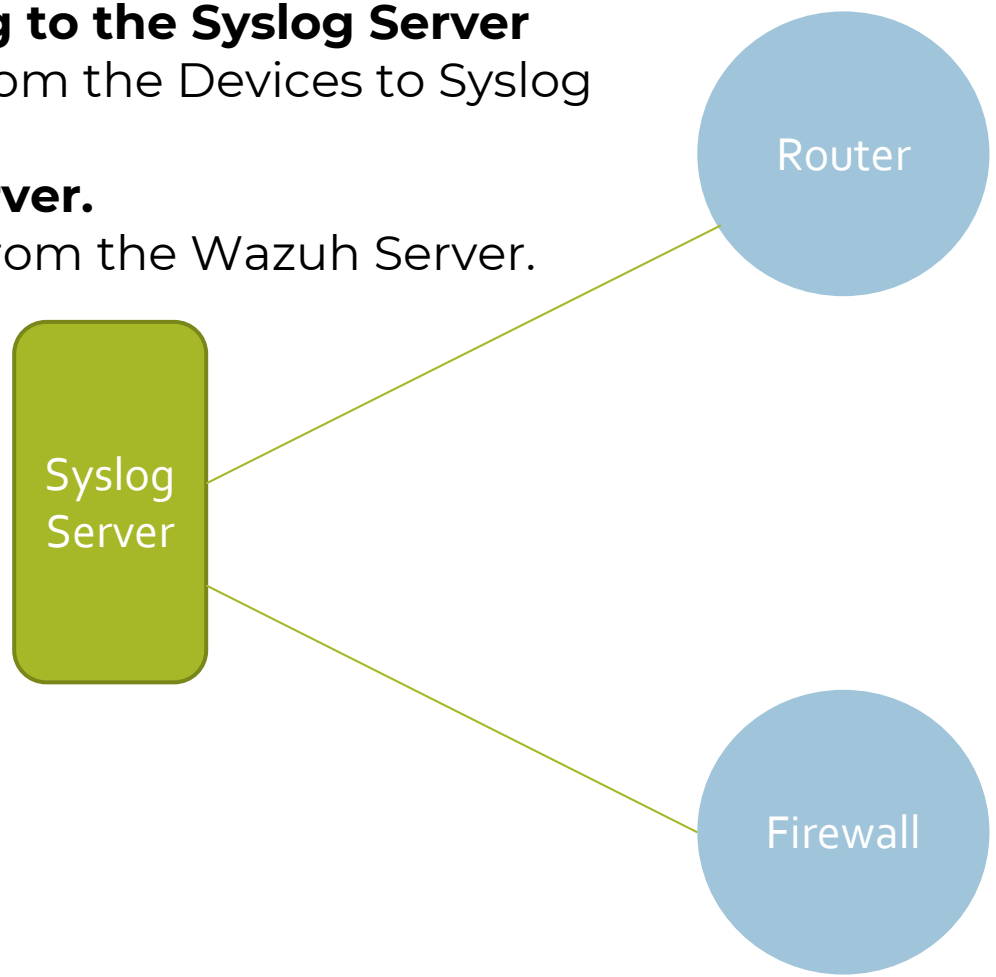


Step-by-Step Installation (Cont.)

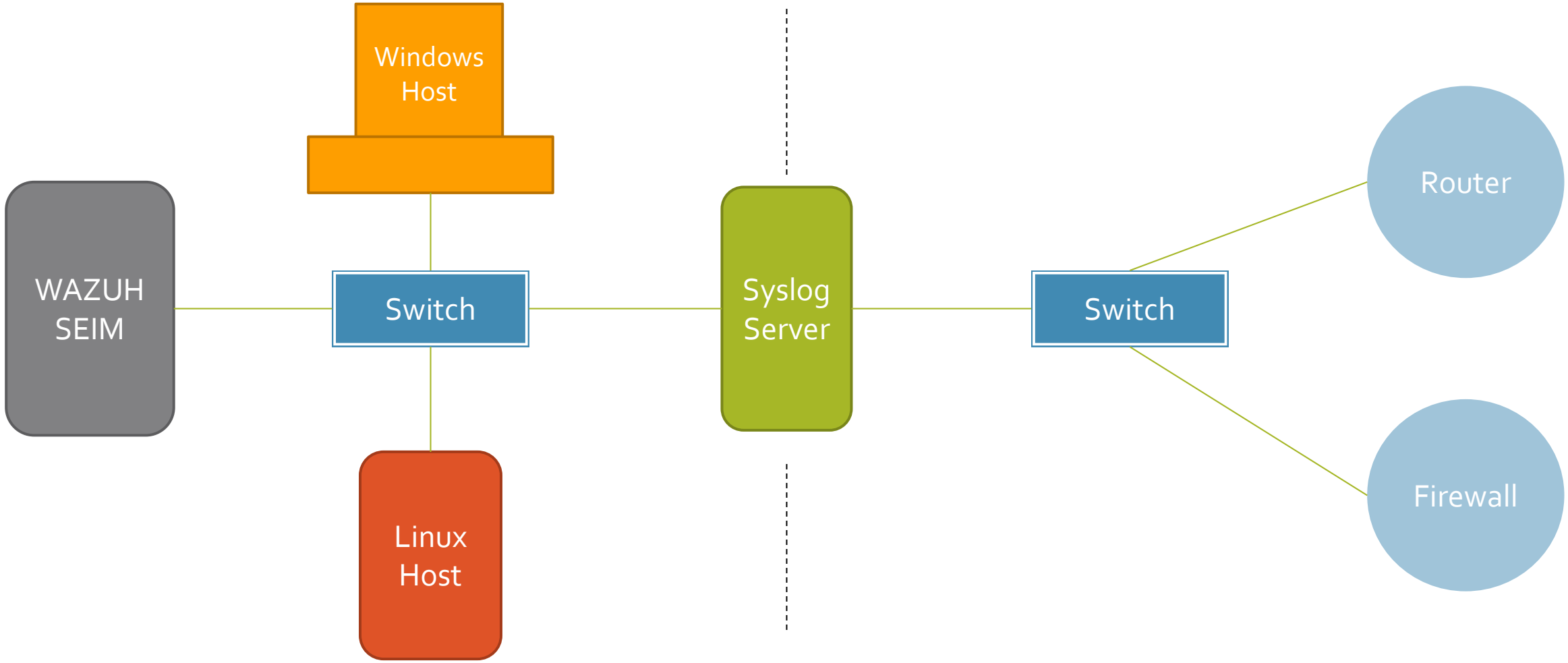
Step 4: Configure Network Devices to Send the Log to the Syslog Server

- Set the Destination Address to Send the Log from the Devices to Syslog Server.
- Check the Incoming Logs From the **Syslog Server.**
- Configure **Wazuh Server** to Receive the Log From the Wazuh Server.
- Check the Incoming Logs for Syslog Server

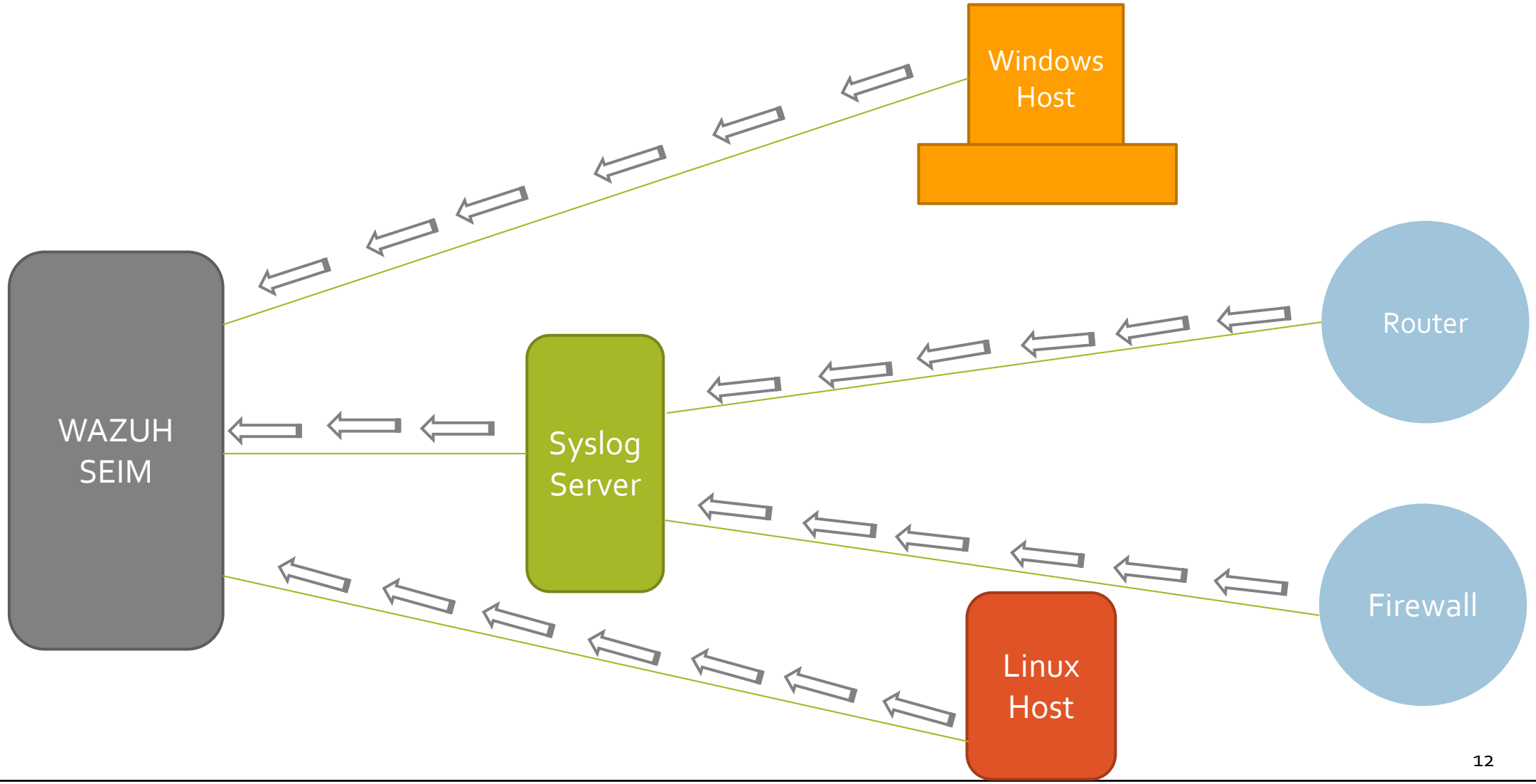
Step 5: Configure Security Event Collection
Step 6: Enable Real-time Monitoring and Alerting
Step 7: Perform Regular Log Analysis and Incident Investigation
Step 8: Continuously Enhance Security Posture



Complete Diagram with Wazuh SIEM



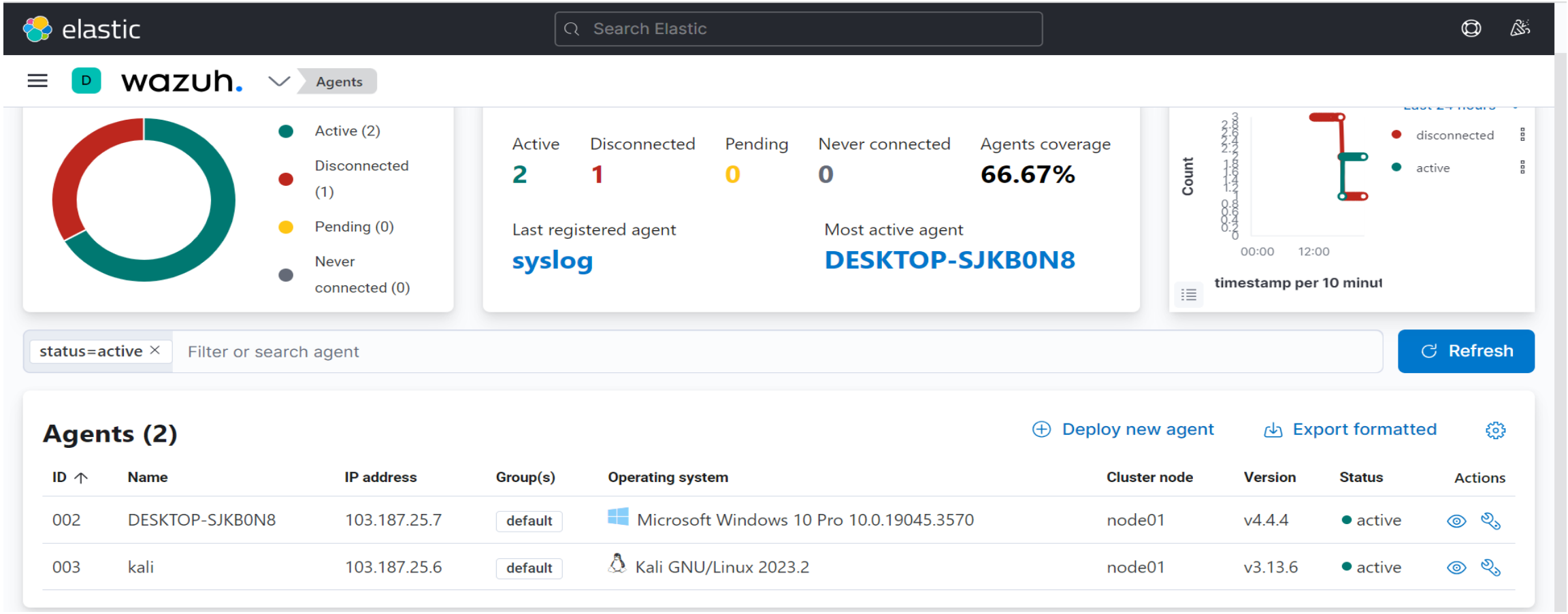
Data Flow between Wazuh and connected devices.



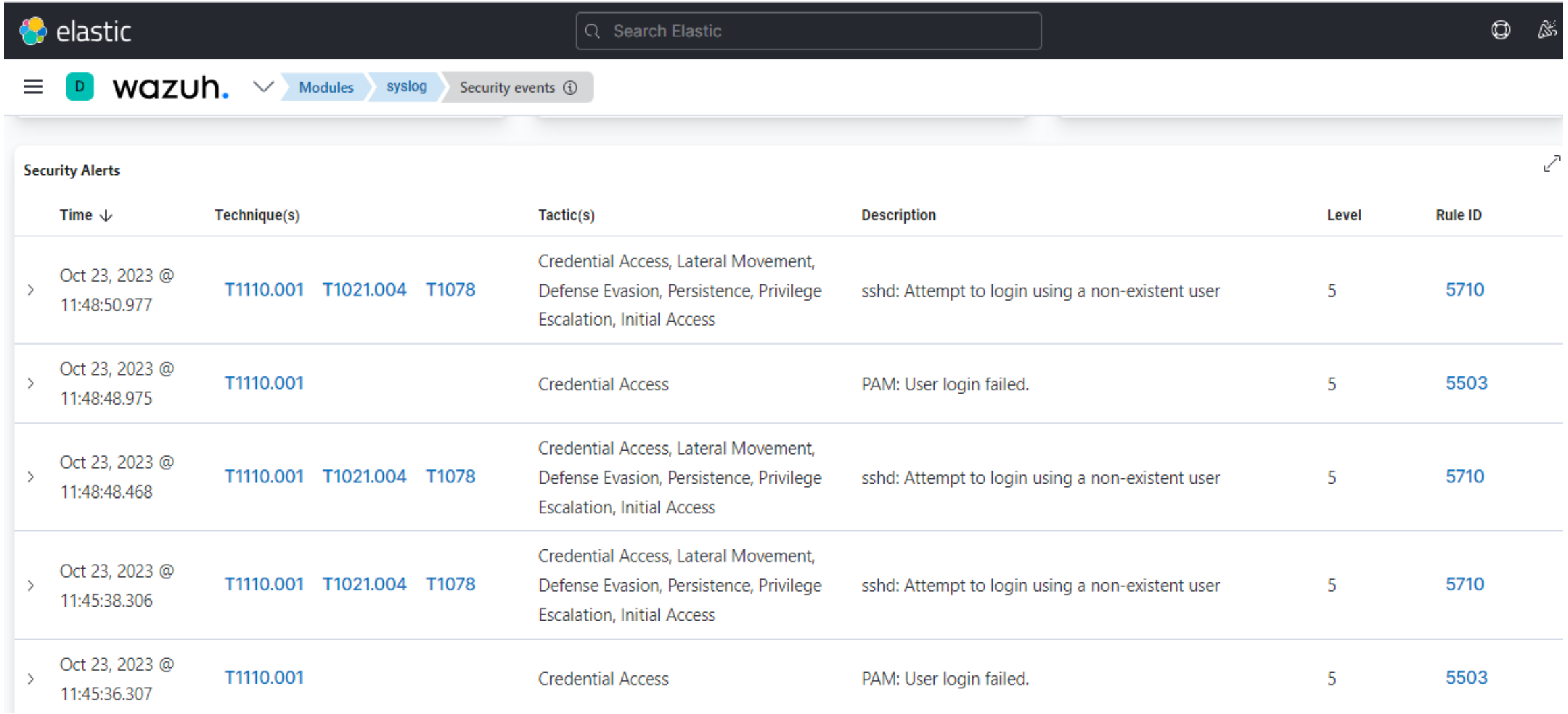
Wazuh SIEM Demo

Agents overview

All configured Host (Agent) is showing into the Agents List with Active, Disconnected, Pending Never Connected List.



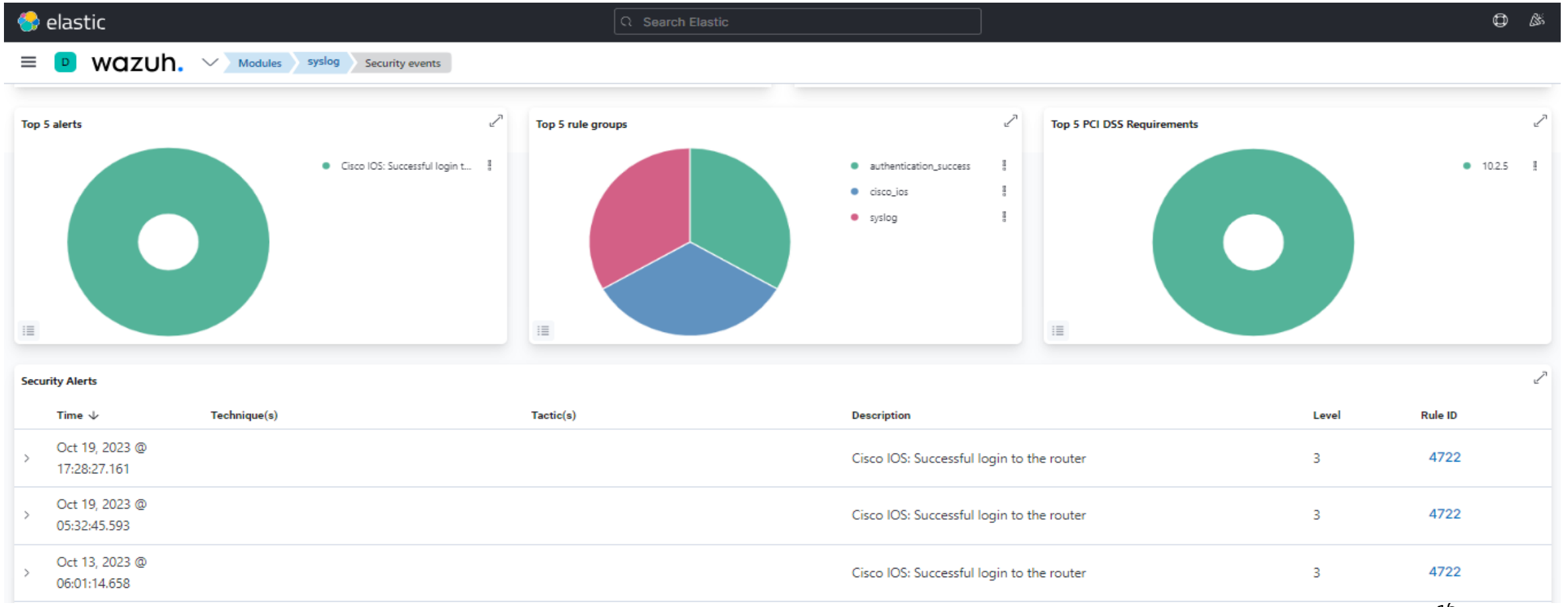
Security Events Monitoring (Failed Login Attempts)



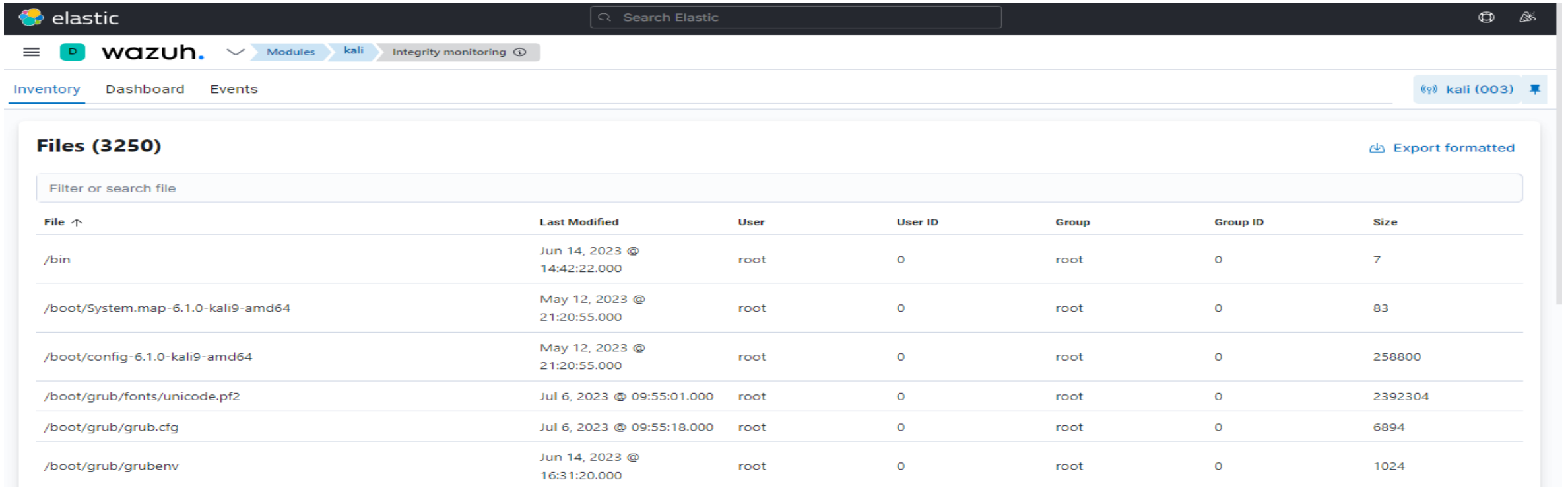
Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Oct 23, 2023 @ 11:48:50.977	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710
Oct 23, 2023 @ 11:48:48.975	T1110.001	Credential Access	PAM: User login failed.	5	5503
Oct 23, 2023 @ 11:48:48.468	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710
Oct 23, 2023 @ 11:45:38.306	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710
Oct 23, 2023 @ 11:45:36.307	T1110.001	Credential Access	PAM: User login failed.	5	5503

Security Events Monitoring (Successful Login Attempts)

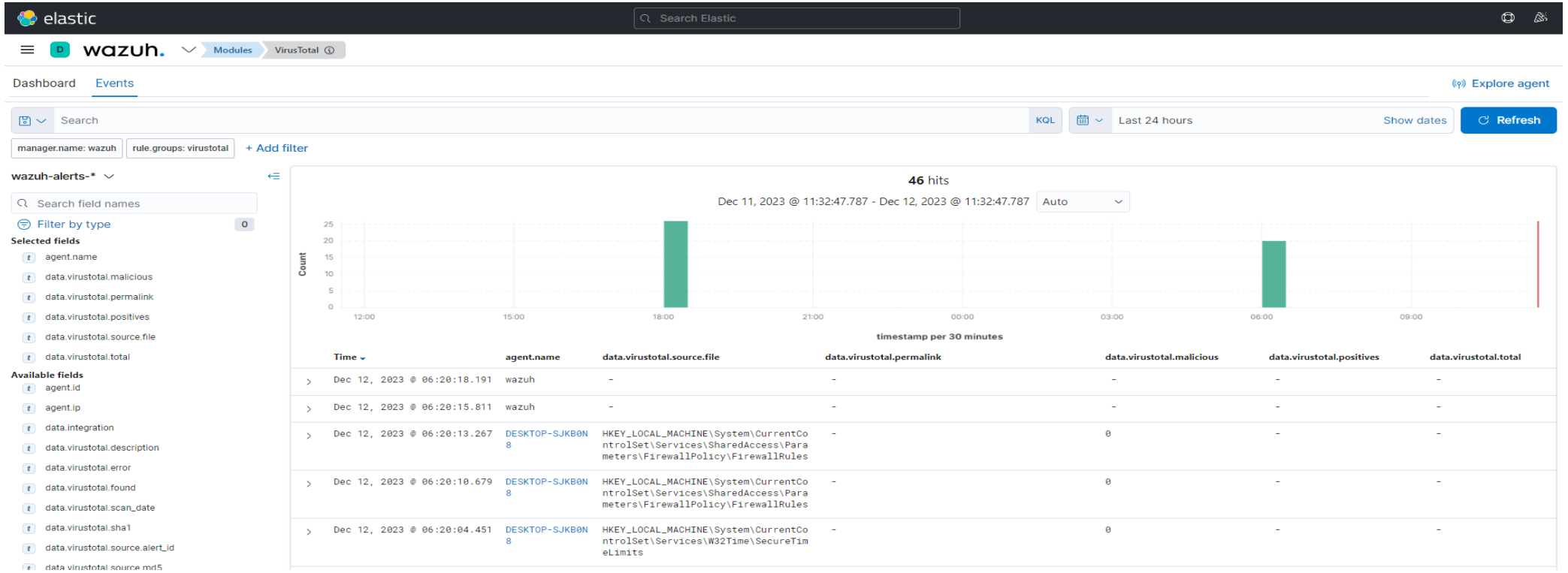


File Integrity Monitoring Dashboard



- Identifying changes in context, permissions, ownership & attribute
- Graph view of modified, added and deleted files over time
- Use case of detecting threat
- Use case of regulatory compliance like ISO 27001, NIST 800-53

VirusTotal Integration



- Real Time Virus and malware detection
- Effective way of inspecting monitored files for malicious content
- Manager & Endpoint both needs manual integration remediation

VULNERABILITY DETECTION:

- Discover vulnerabilities of OS and applications installed on the monitored endpoints and matches to CVE & CVSS
- Automatic vulnerability detection and assessment
- External vulnerability feeds indexed by National Vulnerability Database (NVD), Canonical, Debian, Red Hat, Arch Linux Advisories Security (ALAS), Microsoft.

Office 365 Integration:

- Event Severity Graph
- Phishing and Malware Information
- User Activity Information

MITRE ARR&CK

- Review MITRE ATT&CK techniques in environment mapped to problem reports
- MITRE tactics and their associated techniques
- Alert evolution by Graph

Security Configuration Assesment:

- Scan to detect misconfiguration and exposures, based on CIS controls
- Recommends remediation action

Container Security:

- Providing Comprehensive visibility into container resources
- Capability to audit Kubernetes Infrastructure


THANK YOU!