

SECURITY
INFORMATION
AND EVENT
MANAGEMENT



INTRODUCTION

A SIEM tool is crucial for organizations to monitor and safeguard their assets and data against cyber threats. SIEM functions by collecting security-related data from various sources, such as logs, network traffic, and other security tools. The collected data is then analyzed using advanced analytics to detect any suspicious activities, potential security breaches, and other security-related events in real-time.

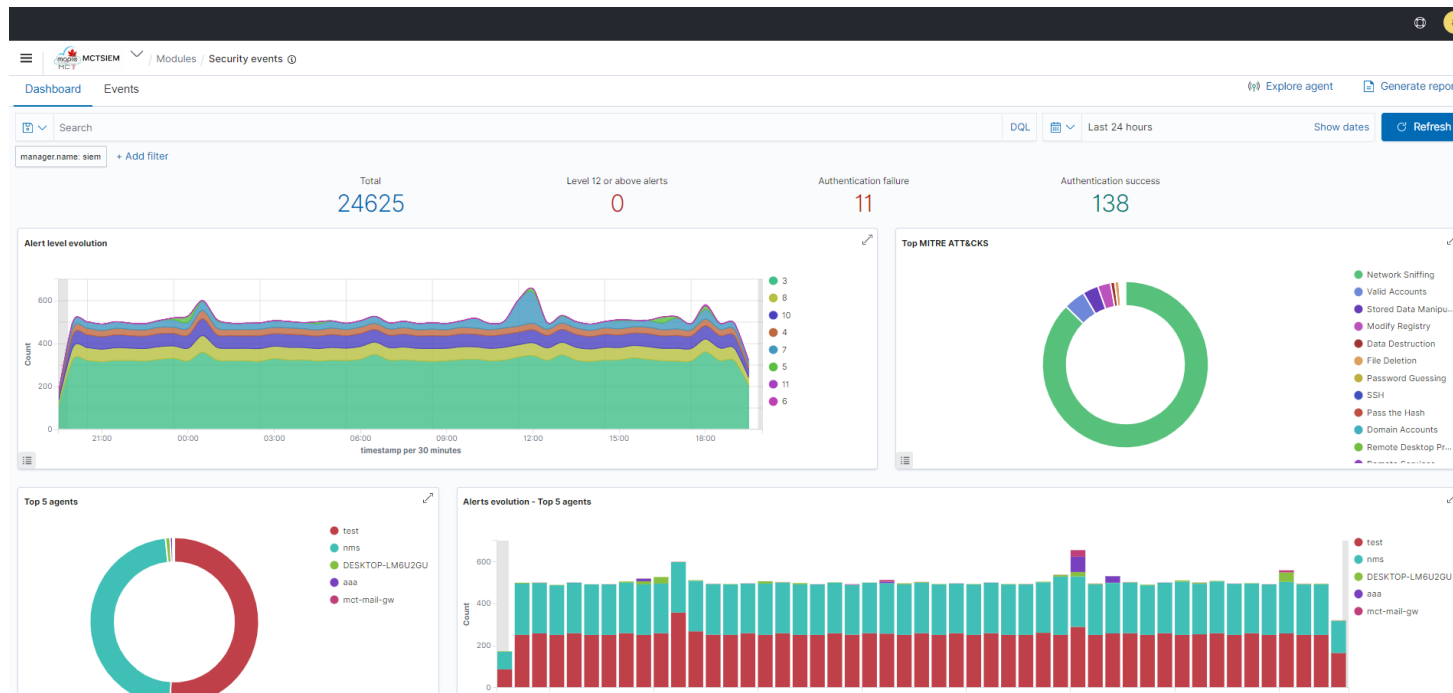
MCTSIEM solution consists of an endpoint security agent, deployed to the monitored systems, and a management server, which collects and analyzes data gathered by the agents providing a data visualization dashboard that allows users to navigate through their security alerts. MCTSIEM also provides agentless monitoring of endpoints with the use of syslog protocol.



INTRODUCTION

MCTSIEM can fetch you the security events in graphical as well as in the log format with the pre-defined and custom rules based on CVEs & threats.

MCTSIEM matches the ruleset present in the SIEM daemon & output the logs of the decoders written for that matching ruleset.



CVE-2016-1585

Details

- Title:** CVE-2016-1585 affects apparmor
- Version:** 2.13.3-7ubuntu5.1
- Last full scan:** May 24, 2023 @ 00:53:20.000
- Updated:** Feb 25, 2021 @ 00:00:00.000
- Name:** apparmor
- Architecture:** amd64
- Last partial scan:** May 24, 2023 @ 01:00:39.000
- References:** [View external references](#)

Recent events

Time	Description	Level	Rule ID
May 22, 2023 @ 18:27:57.597	CVE-2016-1585 affects apparmor	13	23506

Rows per page: 10

MONITORED ELEMENTS



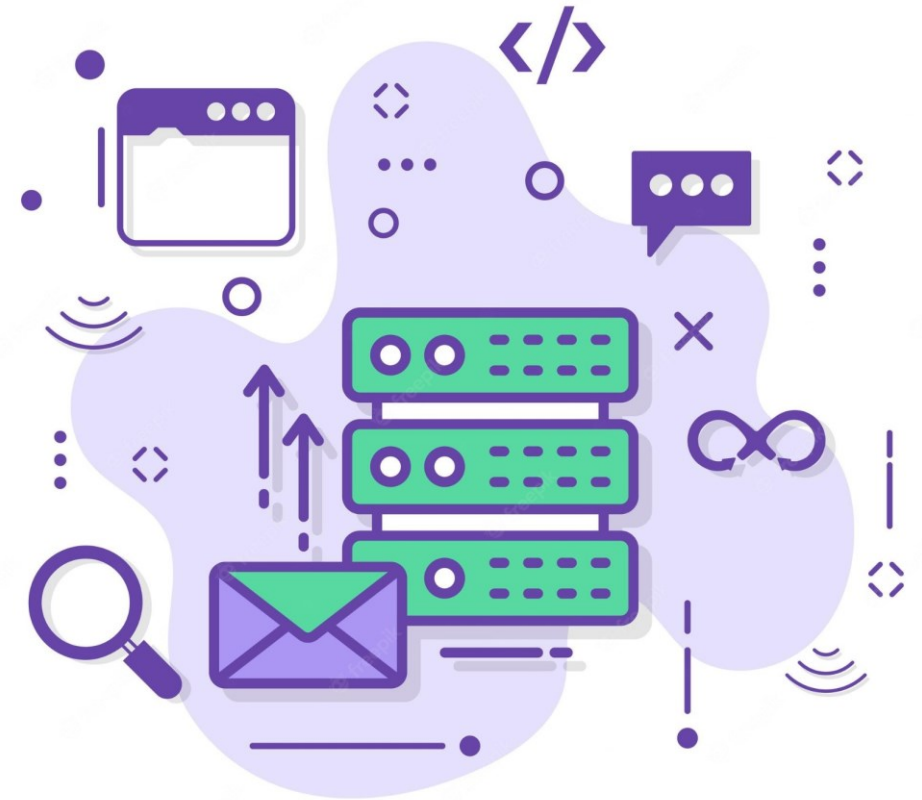
Agentless

MCT SIEM monitors headless device (where agents can't be installed) through syslogs on TCP & UDP. It has a very robust mechanism of detecting the behaviours, anomalies & traffic movement within & outside network devices



Agents Based

Servers, VMs, Operating Systems can be monitored with MCT SIEM Agent based solution. MCT SIEM provides secure tunnel based agent integration on different OS platforms. Agent based solution are available for Windows, Linux, MacOSx



WHY MCT SIEM?

SIEM (Security Information and Event Management) is crucial for organizations due to the growing complexity and sophistication of cyber threats. It provides a centralized platform for collecting, analyzing, and correlating security event data from various sources. SIEM helps organizations detect and respond to security incidents promptly, improving threat visibility and incident response capabilities.

By investing in MCTSIEM solution, organizations benefit from advanced threat detection, real-time monitoring, log management, compliance reporting, and streamlined incident response, ensuring their critical assets are protected from evolving cyber threats effectively and efficiently.





MCT SIEM FEATURES

Log Data Analysis	MCT SIEM assists users by automating log management and analysis to accelerate threat detection. Its intelligent daemon accelerates the process of collecting logs
File Integrity Monitoring	It generates an alert when it detects a change in the file system
Rootkits Detection	MCT SIEM periodically scan its endpoints connected to agents for any kind of anomaly and rootkits detection
Configuration Assessment	It does a posture scanning of the system and maintains a standard configuration through the monitored endpoints
System Inventory	MCT SIEM manages the system inventory of the endpoints along with the processes and network ports open in the system.
Vulnerability Detection & Container Security	MCT SIEM maintains a vulnerability database of latest CVEs and creates a risk report by correlating that list NVTs and also provides a real time results of containers.

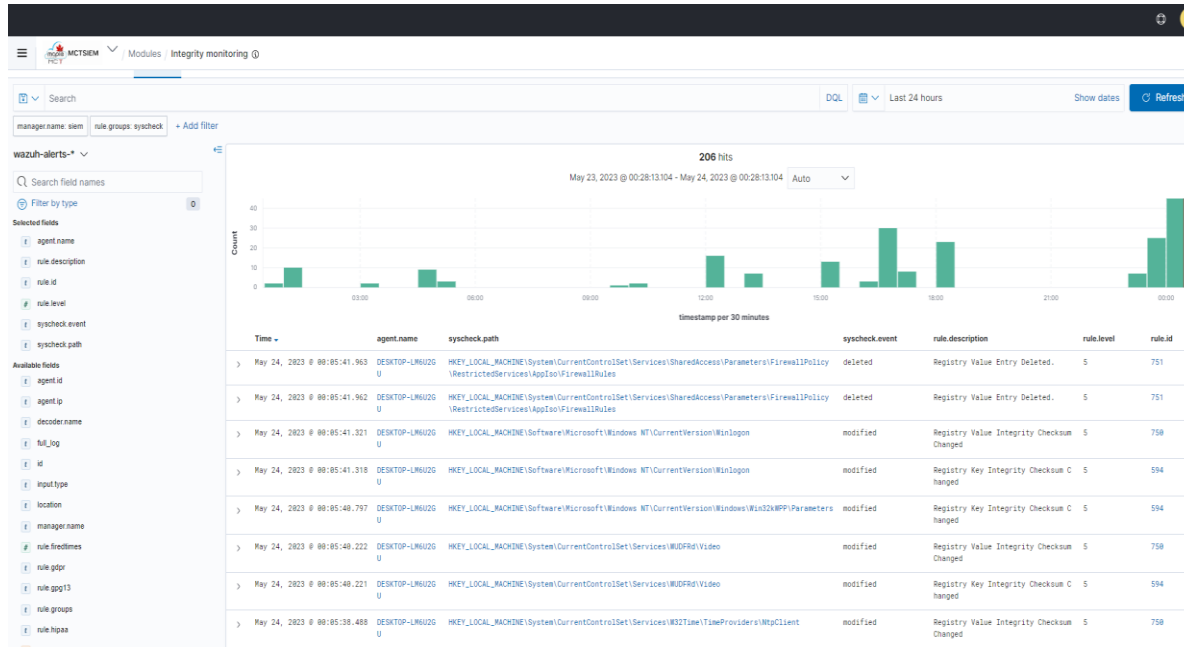
KEY BENEFITS OF MCT SIEM

- Enhanced Threat Protection
- Log Management
- Incident Response
- Real-Time Alerts
- Threat Intelligence
- Compliance Reporting
- Scalability
- Customizable Rules and Policies
- Centralized Visibility
- Data Visualization
- Customized Dashboards



MCT SIEM FLAGSHIP FEATURES

1. Integrity Monitoring – MCT SIEM monitors critical files and directories for unauthorized changes, providing alerts on potential system compromises or tampering.



MCT SIEM FLAGSHIP FEATURES

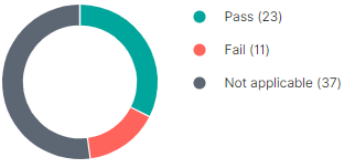
2. Configuration Assessment – MCT SIEM monitors system and application configuration settings to ensure that they are compliant with your policies. Also, custom policies can be created and added with respect to the government guidelines of severity check of configuration.



MCTSIEM / Modules / AD-01 / Security configuration assessment

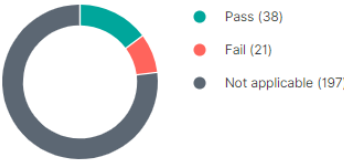
Inventory Events AD-01 (009)

BENCHMARK FOR WINDOWS AUDIT



- Pass (23)
- Fail (11)
- Not applicable (37)

CIS BENCHMARK FOR WINDOWS SERVER 2016



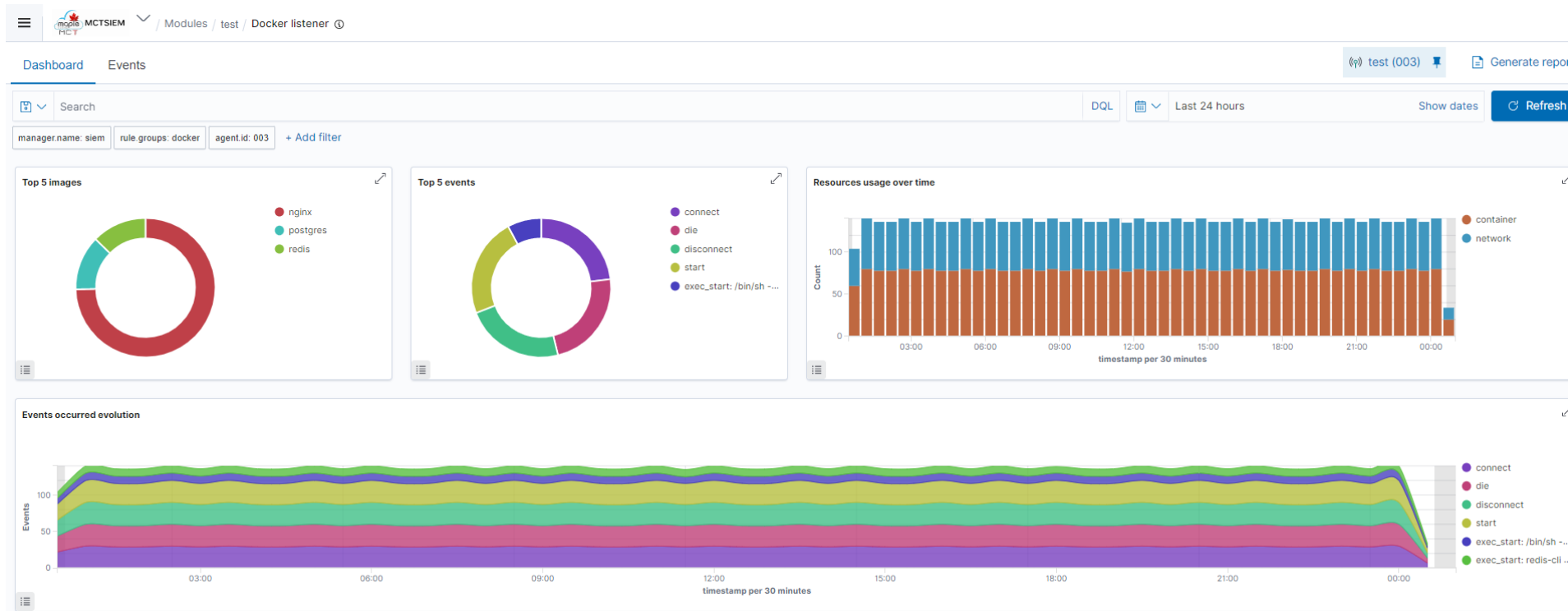
- Pass (38)
- Fail (21)
- Not applicable (197)

Policy	Description	End scan	Pass	Fail	Not applicable	Score
Benchmark for Windows audit	This document provides a way of ensuring the security of the Windows systems.	May 23, 2023 @ 16:41:53.000	23	11	37	67%
CIS Benchmark for Windows Server 2016	This document provides prescriptive guidance for establishing a secure configurati...	May 23, 2023 @ 16:41:50.000	38	21	197	64%

MCT SIEM FLAGSHIP FEATURES



3. Container Security – MCT SIEM also provide the monitoring capabilities of containers like Docker, Kubernetes and container based platform.





MCT SIEM FLAGSHIP FEATURES

4. Vulnerability Detection – MCT SIEM agents check for the updated CVEs in the system through continuously monitoring the endpoints for any vulnerability.

It also offers third party integration for vulnerability detection like virus total

CVE-2023-25584 ×

Details

Title CVE-2023-25584 affects binutils	Name binutils	CVE CVE-2023-25584
Version 2.34-6ubuntu1.4	Architecture amd64	Condition Package unfixed
Last full scan May 23, 2023 @ 18:49:19.000	Last partial scan May 24, 2023 @ 00:41:36.000	Published Feb 15, 2023 @ 00:00:00.000
Updated -	References View external references	

Recent events 1 hits

Search DQL [v] Last 7 days Show dates Refresh

+ Add filter

Time ↓	Description	Level	Rule ID	Status
> May 22, 2023 @ 18:28:05.621	CVE-2023-25584 affects binutils	7	23504	Active

MCTSIEM Modules | test | Vulnerabilities

Inventory Events test (003)

SEVERITY

- Critical (8)
- High (209)
- Medium (100)
- Low (22)

DETAILS

Critical	High	Medium	Low
8	209	100	22

Last full scan: May 23, 2023 @ 18:49:19.000
Last partial scan: May 24, 2023 @ 00:41:36.000

SUMMARY

- vim (42)
- vim-common (42)
- vim-runtime (42)
- vim-liny (42)

Vulnerabilities (339) Export formatted

Filter or search

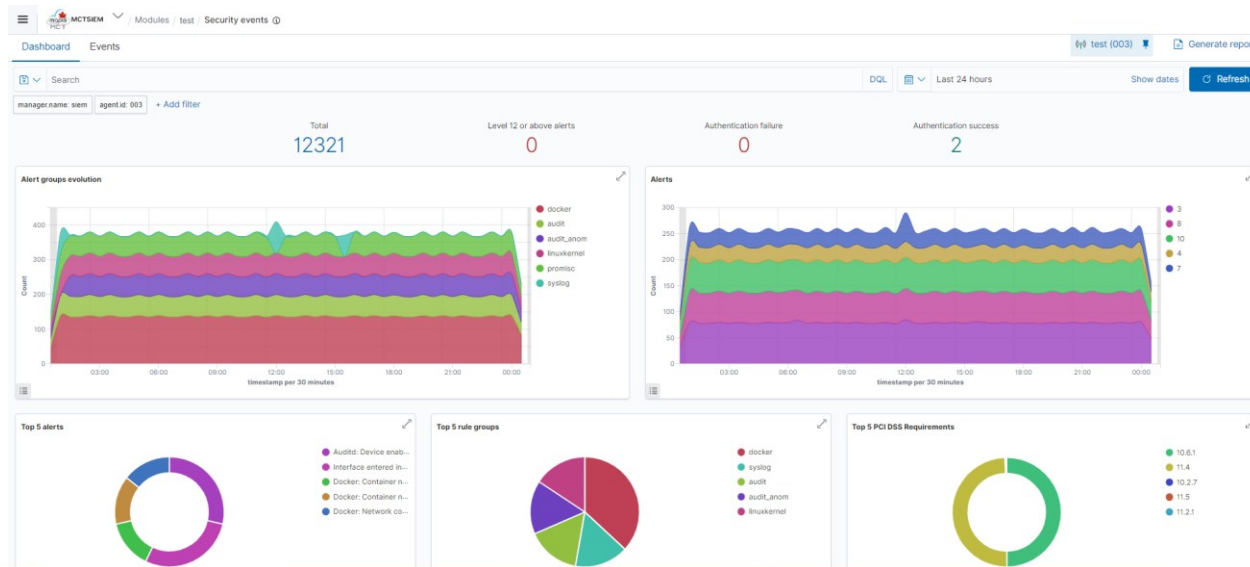
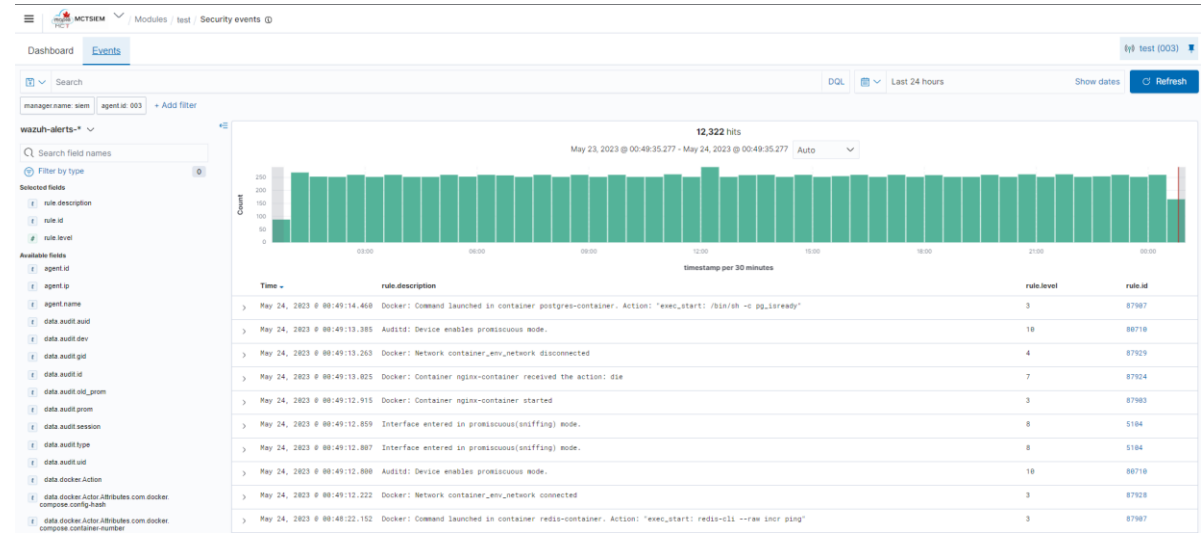
Name ↑	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
apparmor	2.13.3-7ubuntu5.1	amd64	Critical	CVE-2016-1585	7.5	9.8	May 22, 2023 @ 18:27:57.000
appport	2.20.11-0ubuntu27.26	all	Low	CVE-2022-28653	0	0	May 22, 2023 @ 18:28:16.000
binutils	2.34-6ubuntu1.4	amd64	Medium	CVE-2023-25584	0	0	May 22, 2023 @ 18:28:05.000
binutils	2.34-6ubuntu1.4	amd64	Medium	CVE-2023-25585	0	0	May 22, 2023 @ 18:28:06.000
binutils	2.34-6ubuntu1.4	amd64	Medium	CVE-2023-25588	0	0	May 22, 2023 @ 18:28:07.000
binutils	2.34-6ubuntu1.4	amd64	High	CVE-2021-45078	6.8	7.8	May 22, 2023 @ 18:28:15.000
binutils-common	2.34-6ubuntu1.4	amd64	Medium	CVE-2023-25584	0	0	May 22, 2023 @ 18:28:05.000
binutils-common	2.34-6ubuntu1.4	amd64	Medium	CVE-2023-25585	0	0	May 22, 2023 @ 18:28:06.000
binutils-common	2.34-6ubuntu1.4	amd64	Medium	CVE-2023-25588	0	0	May 22, 2023 @ 18:28:07.000
binutils-common	2.34-6ubuntu1.4	amd64	High	CVE-2021-45078	6.8	7.8	May 22, 2023 @ 18:28:15.000



MCT SIEM FLAGSHIP FEATURES

5. Security Events – MCT SIEM collects, aggregate, index and analyze security data, helping organizations detect intrusions, threats and behavioral anomalies.

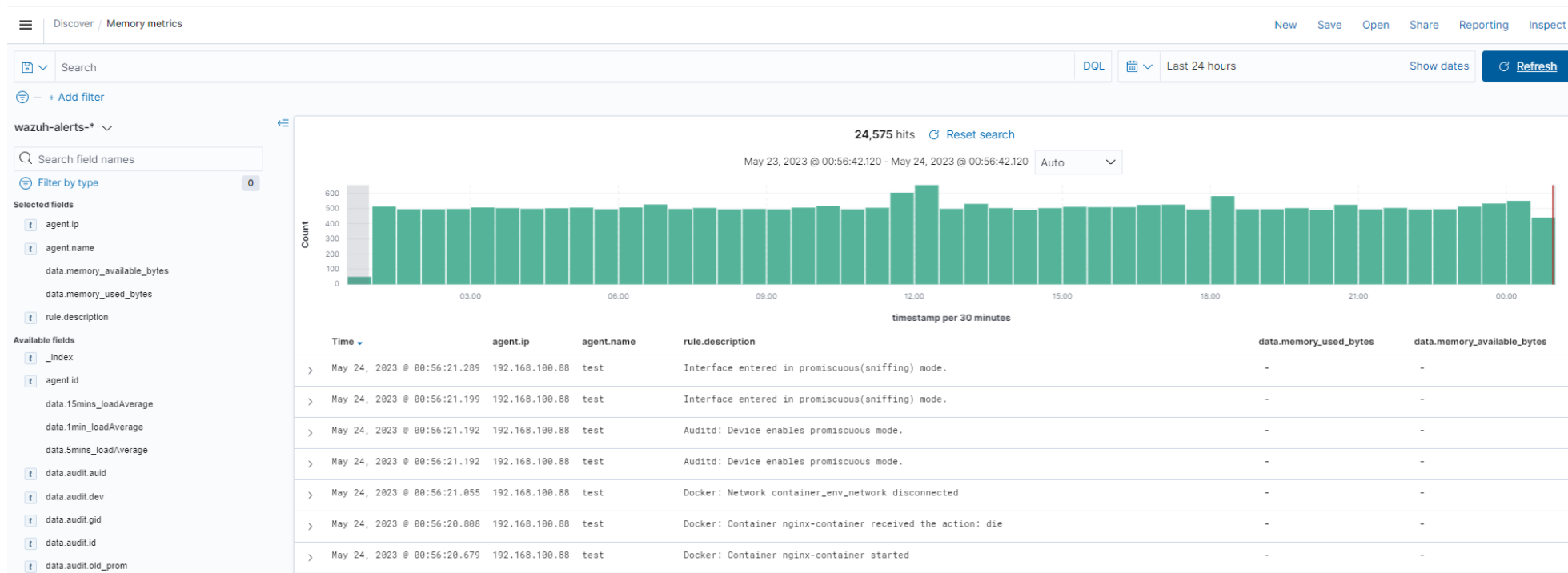
Security Events tab provides detailed security event trail of the network devices and servers and can be visualized in MCT SIEM





MCT SIEM FLAGSHIP FEATURES

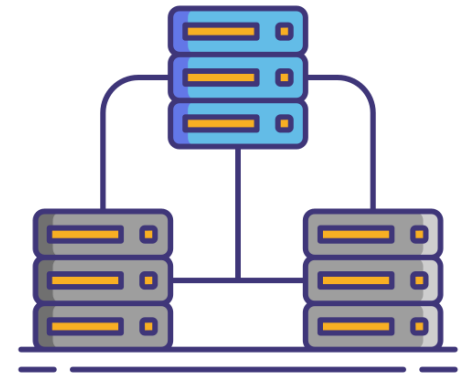
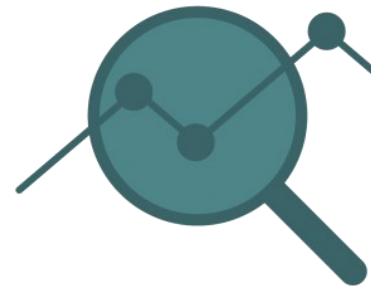
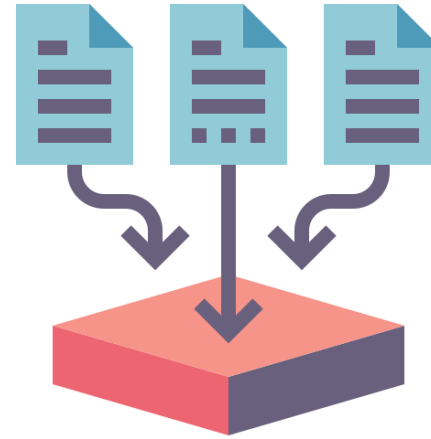
6. Centralized Syslog Server – MCT SIEM, in addition to its SIEM capabilities, can function as a central syslog server. With MCT SIEM as the central syslog server, organizations can consolidate and manage logs from various devices and systems in a centralized location. Syslog server feature allows for the collection, storage, and analysis of syslog data, enabling organizations to monitor and analyze logs for security events, compliance, and troubleshooting purposes. By serving as a central syslog server, MCT SIEM enhances log management efficiency, simplifies log aggregation, and provides a unified view of log data, empowering organizations to gain valuable insights and improve their overall security posture.



COMPONENTS OF SIEM SOLUTIONS

SIEM (Security Information and Event Management) solutions are designed to collect, analyze, and correlate security-related data from various sources in real-time, to detect and respond to security incidents. The main components of a SIEM solution are:

- **Data Collection:** This component collects data from various sources, such as servers, network devices, endpoints, and applications. It includes agents, adapters, and log collectors that capture and forward the data to the SIEM system.
- **Data Normalization:** The data collected from various sources is in different formats, which makes it difficult to analyze and correlate. The data normalization component converts the data into a standardized format that can be easily analyzed and correlated.
- **Event Correlation:** This component correlates security-related events from different sources to identify potential security threats. The correlation engine analyzes the data to identify patterns, anomalies, and trends that could indicate a security breach.



COMPONENTS OF SIEM SOLUTIONS

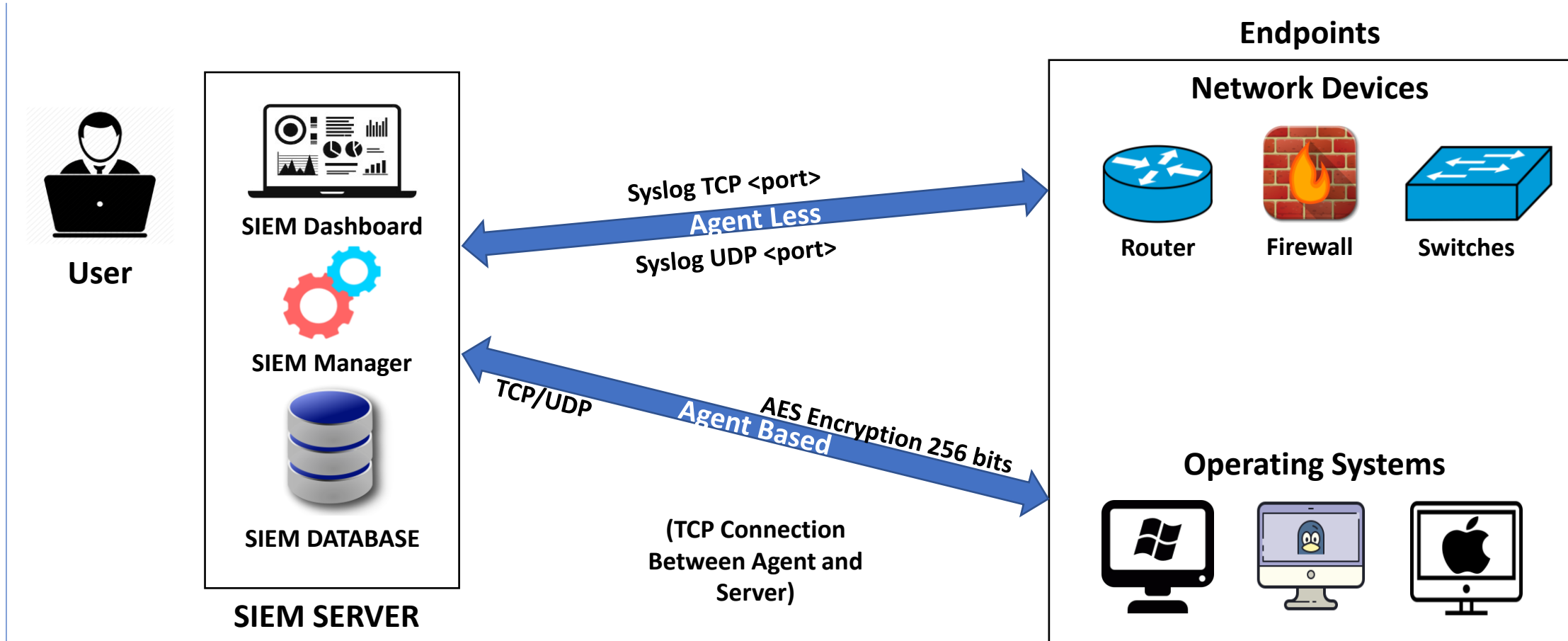
- **Alerting:** The alerting component generates alerts and notifications based on the rules and policies set by the security team. The alerts can be sent via email, SMS, or other communication channels, to inform the security team about potential security incidents.
- **Reporting and Analytics:** This component provides dashboards, reports, and visualizations to help security teams monitor and analyze security-related data. It also enables the team to identify trends, patterns, and anomalies that could indicate potential security threats.
- **Incident Response:** The incident response component provides a set of tools and procedures to investigate and respond to security incidents. It includes workflows, playbooks, and automated response actions that help security teams quickly respond to security incidents.

- **Compliance Management:** The compliance management component helps organizations comply with industry standards, regulations, and policies. It provides a set of predefined rules and policies that can be customized to meet specific compliance requirements.

Overall, the SIEM solution is a complex system that combines various components to provide a comprehensive security monitoring and incident response platform.

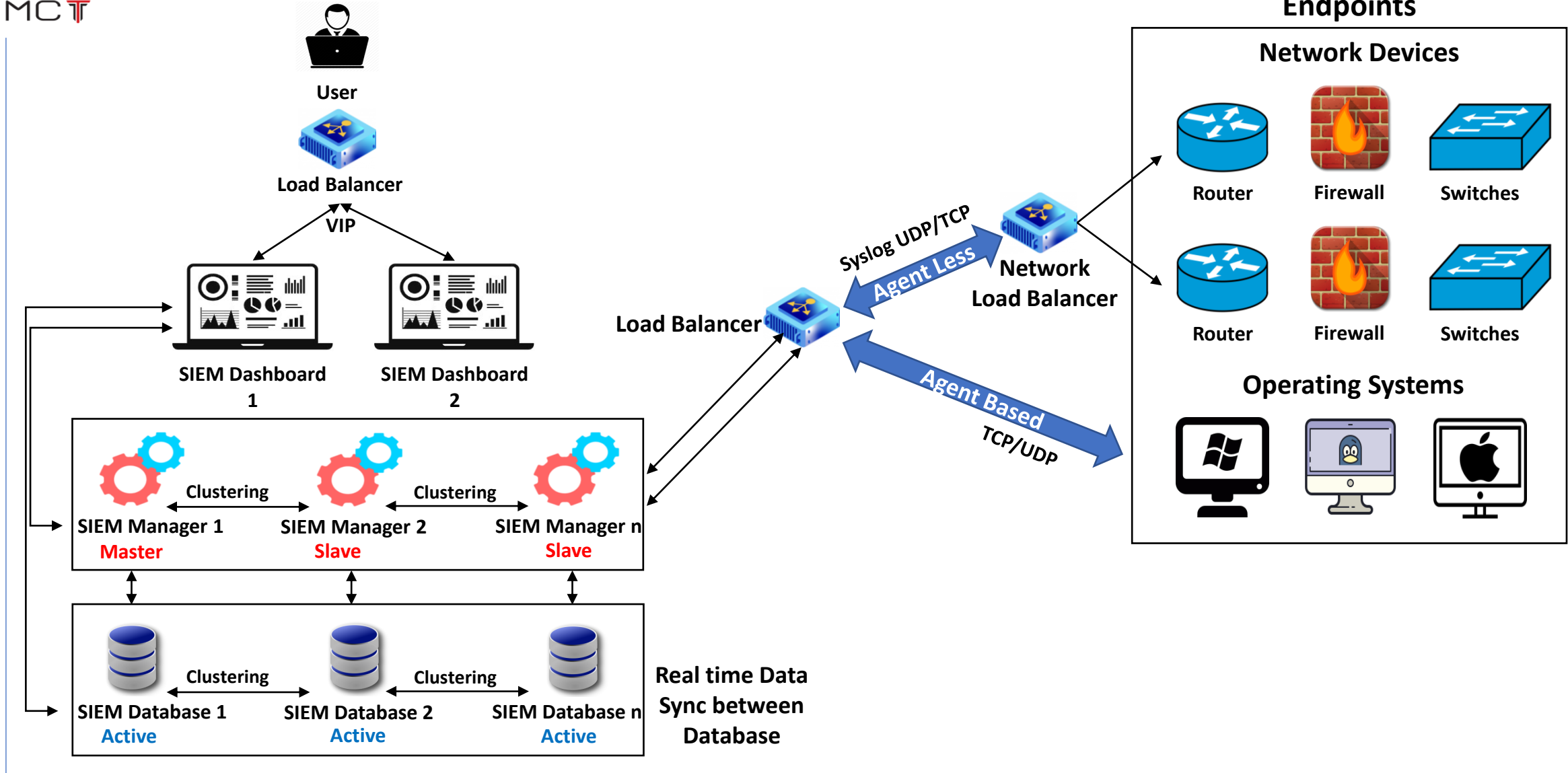


MCT SIEM STANDALONE ARCHITECTURE





MCT SIEM DISTRIBUTED ARCHITECTURE





THANKS!

DO YOU HAVE ANY
QUESTIONS?

fly@maplecloudtechnologies.com

+918178803636

www.maplecloudtechnologies.com