☎ +49 69 506075080
✉ E-mail hello@secaas.it
security-as-a-service.io

SECaaS.IT
eine Marke der XaaS Enterprise GmbH

Product Datasheet PRISM SIEM

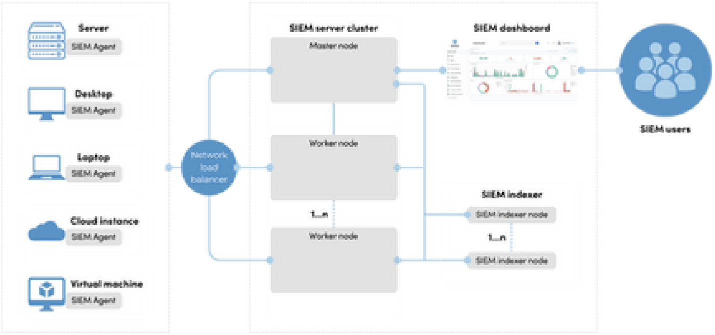
PRISM SIEM

Advanced Security Monitoring & Compliance

1 Introduction

PRISM SIEM is a powerful SIEM solution based on Wazuh, designed for threat detection, log analysis, and compliance monitoring. It can be deployed in on-premises, hybrid cloud environments, or as a Managed Security Service.

2 Architecture



- **Agent: Installed on end devices, servers or cloud instances to record log data and security events.**
- **Manager/Worker: Central management component for processing, analyzing and correlating the data collected.**
- **Indexer: Storage and retrieval of event data.**
- **Dashboard: Visualization and analysis of safety data via a dashboard.**

3 Functionalities

- **Threat detection: Analysis of log data and behavior to identify attacks.**
- **Intrusion Detection System (IDS): Detection of suspicious activity based on signatures and anomalies.**
- **File Integrity Monitoring (FIM): Monitoring and detection of unauthorized changes to files.**
- **Malware Detection: Detection of malware through integration of Virustotal**

- **Threat detection: Analysis of log data and behavior to identify attacks.**
- **Intrusion Detection System (IDS): Detection of suspicious activity based on signatures and anomalies.**
- **File Integrity Monitoring (FIM): Monitoring and detection of unauthorized changes to files.**
- **Malware Detection: Detection of malware through integration of Virustotal**

SECaaS.IT
eine Marke der XaaS Enterprise GmbH

Smart Cybersecurity for Growing Businesses

4 System requirements

Hardware recommendations for a medium-sized environment (~500 endpoints):

- Manager(-Cluster):

CPU	RAM	SSD	🖧
8 vCPUs	16 GB	500 GB SSD	1 Gbps

- Indexer-Cluster:

CPU	RAM	SSD	🖧
16 vCPUs	32 GB	2 TB SSD	10 Gbps

- Dashboard:

CPU	RAM	SSD	🖧
4 vCPUs	8 GB	100 GB SSD	-

5 Scalability

- Use of indexer clusters for load distribution and scaling.
- Horizontal scaling through additional manager instances.
- Support for multi-tenant architectures for managed security services.

6 Scalability

- SSL/TLS encryption between all components.
- Fail-safe indexer through integrated “replica” functions.
- Role-Based Access Control (RBAC) for user and rights management.
- Integration with central identity management such as Keycloak.
- Hardening according to CIS benchmarks.

7 Integrations and extensions

- SIEM-extension: Integration with Splunk, Elastic SIEM or SecurityOnion.
- Security Orchestration & Automation (SOAR): Connection with TheHive/DFIR-IRIS, N8N and Cortex.
- Threat Intelligence: Connection to MISP and other threat feeds.
- Cloud Security: Support for AWS, Azure and Google Cloud with specific agents.

8 Operation and maintenance

- Automatic updates: Setup of unattended upgrades for automatic updates.
- Monitoring: Integration with e.g. Zabbix for performance monitoring.

Backup-Strategy: Regular snapshots of the Indexer database.

9 Compliance and certifications

- Support for GDPR, NIS2, ISO 27001, HIPAA and other regulations.
- Regular audit logs and reporting functionalities.

10 Conclusion

A SIEM solution based on Wazuh offers comprehensive security functions with high flexibility and scalability. Thanks to its open source nature and numerous integration options, PRISM SIEM is suitable for both small companies and large enterprise environments or managed security services.