PRISM SIEM Hintergrunddokument

Einleitung

Sicherheitsvorfälle in IT-Systemen nehmen in Anzahl und Komplexität stetig zu. Unternehmen jeder Größe und Branche stehen vor der Herausforderung, ihre IT-Infrastruktur vor Cyberangriffen zu schützen und gleichzeitig gesetzlichen Anforderungen gerecht zu werden. Hier kommen SIEM-Systeme (Security Information and Event Management) ins Spiel. Dieses Dokument bietet einen umfassenden Überblick über die Funktionsweise, Einsatzmöglichkeiten und Mehrwerte von SIEM-Systemen sowie eine detaillierte Beschreibung der PRISM SIEM Lösung von SECaaS.IT.

Was ist ein SIEM-System?

Ein SIEM-System (Security Information and Event Management) ist eine IT-Sicherheitslösung, die sicherheitsrelevante Ereignisse und Informationen in Echtzeit sammelt, korreliert und analysiert. Ziel ist es, Bedrohungen frühzeitig zu erkennen, Sicherheitsvorfälle zu analysieren und die Einhaltung gesetzlicher Vorschriften sicherzustellen.

Kernfunktionen eines SIEM-Systems

1. **Log Management:**
    - Sammlung, Speicherung und Analyse von Protokolldaten aus Betriebssystemen, Anwendungen, Firewalls und Netzwerken.
    - Grundlage für Korrelation und Rückverfolgung von Sicherheitsvorfällen.
2. **Echtzeitüberwachung (Real-Time Monitoring):**
    - Permanente Überwachung sicherheitsrelevanter Aktivitäten.
    - Erkennung von Mustern, die auf Insider-Bedrohungen, Malware oder unautorisierte Zugriffe hinweisen.
3. **Korrelationsanalyse:**
    - Verknüpft Ereignisse aus verschiedenen Quellen zu einem Gesamtbild.
    - Unterstützt die Identifikation komplexer Angriffe, z. B. APTs (Advanced Persistent Threats).
4. **Alarmierung & Reaktion:**
    - Definierte Regeln lösen automatisierte Alarme aus.
    - Eskalationspfade und automatische Reaktionen (z. B. Blockierung von IP-Adressen, Quarantäne von Geräten).
5. **Reporting & Compliance:**
    - Standardisierte Berichte für interne Audits und externe Prüfungen.
    - Unterstützung bei regulatorischen Anforderungen (DSGVO, NIS2, ISO 27001, HIPAA, TISAX etc.).
6. **Threat Intelligence Feeds:**
    - Integration mit MISP, VirusTotal & Co. für tagesaktuelle Bedrohungsdaten.
    - Vergleich interner Events mit bekannten IOC (Indicators of Compromise).

7. **SOAR-Funktionalitäten (Security Orchestration, Automation and Response):**
    - Playbooks zur automatisierten Reaktion auf erkannte Bedrohungen.
    - Integration mit Tools wie TheHive, Cortex oder n8n zur Workflow-Automatisierung.
8. **File Integrity Monitoring (FIM):**
    - Erkennung unerlaubter Änderungen an sensiblen Dateien oder Konfigurationen.
    - Besonders wichtig in kritischen Systemen oder bei der Einhaltung von Compliance-Vorgaben.

Typische Einsatzbereiche

- **Health IT & KRITIS:** Absicherung von Patienten- und Betriebsdaten in Krankenhäusern.
- **Finanzwesen:** Überwachung sensitiver Systeme zur Betrugsprävention und Einhaltung regulatorischer Vorgaben.
- **Industrie 4.0:** Schutz von Produktionsnetzwerken und SCADA-Systemen.
- **Behörden & Verwaltung:** Transparente Sicherheitsarchitektur zur Einhaltung von Datenschutzgesetzen.

Mehrwert für den Vertrieb – Argumente für den Verkauf

- **Sofortige Einstiegspunkte:** PRISM SIEM bietet definierte Pakete für Startups, Mittelstand und Großunternehmen.
- **Klare Compliance-Vorteile:** Unterstützt direkt beim Nachweis der Erfüllung gesetzlicher Anforderungen.
- **Kalkulierbares Preismodell:** Transparente Lizenzierung, skalierbar je nach Größe.
- **Schnelle Inbetriebnahme:** Erste Ergebnisse oft innerhalb weniger Tage sichtbar.
- **Managed Option:** Verkauf auch an Kunden ohne eigenes Security-Team möglich.

PRISM SIEM im Detail – Technische Highlights

Komponentenübersicht

- **Agent:** Überwacht Hosts (Server, Clients) und sendet Daten an den Manager.
- **Manager:** Zentrale Regelverwaltung, Korrelation, Alert-Generierung.
- **Indexer:** (basiert meist auf OpenSearch/Elasticsearch) speichert und indexiert Log-Daten.
- **Dashboard:** Weboberfläche für Analysen, Dashboards und Reporting (z. B. Kibana).

Basis-Funktionalitäten

- **Log-Management:** Sammlung und Auswertung von System- und Applikationslogs.
- **File Integrity Monitoring (FIM):** Erkennt Manipulationen an Dateien/Konfigurationen.
- **Vulnerability Detection:** Identifikation potenzieller Schwachstellen auf Hosts.
- **Compliance-Modul:** Vorbereitende Maßnahmen für Berichte bzgl. ISO 27001, B3S, PCI-DSS, GDPR.

Erweiterte Merkmale (optional)

- **Threat Feeds:** Integration externer Bedrohungsdatenbanken wie MISP, Virustotal (ggf. Zusatzkosten).
- **SOAR-Funktionen:** Automatisierte Incident-Response-Workflows durch Integration mit n8n, TheHive, Cortex.
- **Full Network IDS/IPS:** Erweiterbar mit Tools wie Suricata oder Zeek.
- **Multi-Tenant-Architektur:** Für Service Provider oder große Unternehmensgruppen.

Architektur & Skalierung

- Horizontal skalierbar durch zusätzliche Manager/Indexer-Knoten
- Cloud-Ready (Azure, AWS, GCP), On-Premises und Hybrid einsetzbar
- Clusterbetrieb für hohe Datenmengen (Elastic-Stack für dedizierte Logging-Plattformen)

Implementierungsprozess (Kurzüberblick)

1. **Planung & Architektur:** Ressourcenplanung, Sicherheitskonzept, ggf. Hochverfügbarkeitsstrategie
2. **Installation & Konfiguration:** Basisinstallation aller Komponenten, Regelbasis, Datenquellenanbindung
3. **Tests & Feintuning:** Regelanalyse, Alerting-Optimierung, ggf. Integration von Threat Intelligence
4. **Betrieb & Weiterentwicklung:** Regelmäßige Aktualisierung der Komponenten und Regeln, optional als Managed Service

Vertriebsargumente – Vorteile für den Kunden

- **Open-Source-Basis:** Keine Lizenzkosten für Basissystem, große Community
- **Funktionsvielfalt:** Host-basierte Intrusion Detection, Log-Analyse, Compliance-Unterstützung
- **Schneller Einstieg:** Schnelle Implementierung möglich
- **Skalierbarkeit:** Geeignet für kleine IT-Teams bis hin zu SOC-Umgebungen
- **Sicherheitsgewinn:** Frühzeitige Erkennung, automatische Reaktion, umfassende Auswertung
- **Kostenersparnis:** Alternative zu teuren physischen SOCs
- **Compliance:** Unterstützt gezielt ISO 27001, NIS2, DSGVO, PCI-DSS, KRITIS-Anforderungen
- **Modularer Aufbau:** Skalierbare Architektur mit Agent, Manager, Indexer und Dashboard.

- **Konnektoren & Integrationen:** Kompatibilität mit gängigen Lösungen wie Microsoft 365, Fortinet, Palo Alto, AWS CloudTrail, Syslog, Suricata, Zeek.
- **Verschlüsselung & Zugriffsschutz:** TLS-Verschlüsselung aller Datenverbindungen, RBAC (Role-Based Access Control), Keycloak-Integration für SSO.
- **Visualisierung:** Leistungsstarke Dashboards mit Kibana/Grafana für technisches Monitoring und Management-Berichte.
- **Automatisierte Backups:** Snapshot-Funktion für Indexdaten.
- **Containerisierung & Kubernetes-Support:** Für größere Umgebungen – skalierbar im Clusterbetrieb.

Fazit

PRISM SIEM vereint technologische Tiefe mit anwenderfreundlicher Umsetzung. Für Vertriebsteams bietet es ein flexibles, leistungsfähiges Produkt mit klaren Mehrwerten für unterschiedliche Kundensegmente. Ob Mittelstand mit hohem Schutzbedarf oder Großkunde mit 24/7 Anforderungen – PRISM SIEM liefert.

Für detailliertere Beratung oder Produktdemos steht das SECaaS-Team jederzeit zur Verfügung.

Kontakt: hello@secaas.it | https://security-as-a-service.io

PRISM SIEM Background Document

Introduction

Security incidents in IT systems are steadily increasing in both number and complexity. Organizations of all sizes and industries face the challenge of protecting their IT infrastructure against cyber threats while also meeting regulatory requirements. This is where SIEM systems (Security Information and Event Management) come into play. This document provides a comprehensive overview of the functionality, use cases, and benefits of SIEM systems, along with a detailed description of the PRISM SIEM solution by SECaaS.IT.

What is a SIEM System?

A SIEM system (Security Information and Event Management) is a cybersecurity solution that collects, correlates, and analyzes security-relevant events and information in real time. The goal is to detect threats early, analyze security incidents, and ensure compliance with regulatory requirements.

Core Functions of a SIEM System

1. **Log Management:**
   - Collection, storage, and analysis of log data from operating systems, applications, firewalls, and networks.
   - Foundation for correlation and forensic analysis of security incidents.
2. **Real-Time Monitoring:**
   - Continuous monitoring of security-relevant activities.
   - Detection of patterns indicating insider threats, malware, or unauthorized access.
3. **Correlation Analysis:**
   - Links events from different sources into a comprehensive picture.
   - Supports identification of complex attacks such as APTs (Advanced Persistent Threats).
4. **Alerting & Response:**
   - Predefined rules trigger automated alerts.
   - Escalation paths and automatic responses (e.g., IP blocking, device quarantine).
5. **Reporting & Compliance:**
   - Standardized reports for internal audits and external assessments.
   - Supports regulatory compliance (GDPR, NIS2, ISO 27001, HIPAA, TISAX, etc.).
6. **Threat Intelligence Feeds:**
   - Integration with MISP, VirusTotal, and others for up-to-date threat intelligence.
   - Compare internal events against known Indicators of Compromise (IOC).
7. **SOAR Capabilities (Security Orchestration, Automation, and Response):**
   - Playbooks for automated response to detected threats.
   - Integration with tools such as TheHive, Cortex, or n8n for workflow automation.
8. **File Integrity Monitoring (FIM):**

    - Detects unauthorized changes to sensitive files or configurations.
    - Particularly important in critical systems or for compliance purposes.

Typical Use Cases

- **Healthcare & Critical Infrastructure:** Protecting patient and operational data in hospitals.
- **Finance:** Monitoring sensitive systems for fraud prevention and regulatory compliance.
- **Industry 4.0:** Securing production networks and SCADA systems.
- **Public Sector:** Transparent security architecture for data protection compliance.

Value for Sales – Selling Points

- **Quick Entry Points:** PRISM SIEM offers predefined packages for startups, SMBs, and enterprises.
- **Clear Compliance Benefits:** Directly supports proving compliance with regulatory standards.
- **Predictable Pricing Model:** Transparent licensing, scalable by size.
- **Fast Deployment:** First results often visible within a few days.
- **Managed Option:** Also suitable for customers without internal security teams.

PRISM SIEM in Detail – Technical Highlights

Component Overview

- **Agent:** Monitors hosts (servers, clients) and sends data to the manager.
- **Manager:** Central rule engine, correlation, and alert generation.
- **Indexer:** (typically based on OpenSearch/Elasticsearch) stores and indexes log data.
- **Dashboard:** Web interface for analysis, dashboards, and reporting (e.g., Kibana).

Core Features

- **Log Management:** Collection and analysis of system and application logs.
- **File Integrity Monitoring (FIM):** Detects unauthorized file/configuration changes.
- **Vulnerability Detection:** Identifies potential host vulnerabilities.
- **Compliance Module:** Prepares reports aligned with ISO 27001, B3S, PCI-DSS, GDPR.

Advanced Features (Optional)

- **Threat Feeds:** Integration with threat intelligence sources such as MISP, VirusTotal (additional cost possible).

- **SOAR Functions:** Automated incident response workflows via n8n, TheHive, Cortex.
- **Full Network IDS/IPS:** Extendable with tools like Suricata or Zeek.
- **Multi-Tenant Architecture:** Ideal for service providers or enterprise groups.

Architecture & Scalability

- Horizontally scalable via additional manager/indexer nodes.
- Cloud-ready (Azure, AWS, GCP), on-premises, or hybrid deployments.
- Cluster operation for large-scale data (Elastic Stack for dedicated logging infrastructure).

Implementation Process (Overview)

1. **Planning & Architecture:** Resource planning, security concept, HA strategy if needed.
2. **Installation & Configuration:** Setup of all components, rule base, data source integration.
3. **Testing & Tuning:** Rule analysis, alert optimization, optional threat intelligence integration.
4. **Operation & Evolution:** Continuous updates and optimization, optional managed service.

Sales Arguments – Key Benefits for Clients

- **Open Source Foundation:** No licensing costs for the core system, strong community.
- **Feature-Rich:** Host-based IDS, log analysis, compliance support.
- **Fast Time-to-Value:** Quick implementation possible.
- **Scalability:** Suitable for small IT teams up to full SOC environments.
- **Security Gain:** Early detection, automated response, comprehensive visibility.
- **Cost Efficiency:** Alternative to expensive physical SOCs.
- **Compliance Ready:** Supports ISO 27001, NIS2, GDPR, PCI-DSS, KRITIS.
- **Modular Design:** Scalable architecture with Agent, Manager, Indexer, and Dashboard.
- **Connectors & Integrations:** Compatible with Microsoft 365, Fortinet, Palo Alto, AWS CloudTrail, Syslog, Suricata, Zeek.
- **Encryption & Access Control:** TLS encryption, RBAC, Keycloak integration for SSO.
- **Visualization:** Powerful dashboards using Kibana/Grafana for monitoring and reporting.
- **Automated Backups:** Snapshot functionality for index data.
- **Container & Kubernetes Support:** Cluster-ready for larger environments.

Conclusion

PRISM SIEM combines deep technology with user-friendly execution. For sales teams, it’s a flexible and powerful product with clear value propositions for different customer segments. Whether for a growing SMB or a 24/7 enterprise environment – PRISM SIEM delivers.

For more details or product demos, contact the SECaaS team.

Contact: hello@secaas.it | https://security-as-a-service.io