PRISM SIEM Fact Sheet

Überblick

- was ist PRISM SIEM?
  - PRISM SIEM ist eine modulare, KI-gestützte Plattform zur Sicherheitsüberwachung und Bedrohungserkennung in IT-Umgebungen. Sie basiert auf Open-Source-Technologien (z.B. Wazuh, Elastic Stack) und wurde speziell für Unternehmen entwickelt, die Compliance-Anforderungen erfüllen, ihre IT-Infrastruktur schützen und gleichzeitig Ressourcen schonen möchten.
  - Funktionen im Überblick
    - Echtzeit-Überwachung aller sicherheitsrelevanten Systeme
    - Log-Analyse & zentrale Ereignisspeicherung
    - Automatisierte Erkennung von Bedrohungen & Anomalien
    - Playbooks für automatisierte Reaktionen (SOAR)
    - Compliance-Dashboards für NIS2, ISO 27001 u.v.m.
    - Vollständig betreibbar On-Prem, in der Cloud oder als Managed Service
  - USP
    - PRISM SIEM vereint Enterprise-Security, einfache Bedienung und hohe Kosteneffizienz – besonders geeignet für Unternehmen ohne eigenes SOC.
- Warum is PRISM SIEM unverzichtbar?
  - Ein SIEM-System ist das Zentrum moderner Cybersicherheit. Es ermöglicht, aus einer Vielzahl technischer Systeme sicherheitsrelevante Informationen zu bündeln, zu korrelieren und intelligent auszuwerten.
  - Aktuelle Herausforderungen, auf die ein SIEM reagiert:
    - Zunehmende Cyberangriffe: Ransomware, Phishing, APTs – gezielt, schnell und teils automatisiert.
    - Steigende regulatorische Anforderungen: NIS2, KRITIS-Verordnung, ISO 27001, DSGVO – fordern Angriffserkennung, Reaktionsfähigkeit & Dokumentation.
    - Komplexität der IT-Landschaft: Multi-Cloud, Remote Work, IoT/OT machen Schutz schwierig – SIEM bringt Sichtbarkeit.
    - Mangel an Fachpersonal: Manuelle Analysen sind kaum mehr machbar – PRISM automatisiert Detection & Response.
- Kundennutzen auf einen Blick
  - Risiken erkennen, bevor Schaden entsteht
  - Cyber-Vorfälle strukturiert & automatisiert behandeln
  - Audits mit wenigen Klicks bestehen
  - Sicherheitsrelevante Vorgänge überblicken und belegen

Zielgruppen

- Startups mit schnellem Wachstumsphasen und begrenztem Budget
  - Haben keine Security-Teams oder Spezialisten
  - Wollen schnell gesetzliche Mindeststandards erfüllen (z.B. DSGVO, ISO light)
  - Müssen Ihre Cloud-Infrastruktur & APIs absichern
  - PRISM Vorteil: Schneller Start, niedrige Einstiegskosten, Compliance-Absicherung
- Wachsende Unternehmen (Growups) und etablierte Firmen
  - Stehen kurz vor ersten Audits oder Kundenanforderungen
  - Security-Events nehmen zu – IT wird komplexer
  - Aufbau interner Strukturen läuft – sie brauchen Tools, die mitwachsen
  - PRISM Vorteil: Skalierbar, teamfähig, integrationsstark
- Krankenhäuser und Kritische Infrastrukturen (KRITIS)
  - Müssen gesetzlich vorgeschriebene Angriffserkennung nachweisen (NIS2, IT-SIG 2.0)
  - Personalmangel ist oft groß, gleichzeitig sind die Anforderungen hoch
  - PRISM Vorteil: Sofort Audit-ready, SOC-Alternative, BSI-tauglich
- Unternehmen mit hohen Compliance-Anforderungen (z.B. NIS2, ISO 27001)
  - Müssen gesetzlich vorgeschriebene Angriffserkennung nachweisen (NIS2, IT-SIG 2.0)
  - Personalmangel ist oft groß, gleichzeitig sind die Anforderungen hoch
  - PRISM Vorteil: Sofort Audit-ready, SOC-Alternative, BSI-tauglich
- IT-Dienstleister und Cloud-Anbieter
  - Müssen gesetzlich vorgeschriebene Angriffserkennung nachweisen (NIS2, IT-SIG 2.0)
  - Personalmangel ist oft groß, gleichzeitig sind die Anforderungen hoch
  - PRISM Vorteil: Sofort Audit-ready, SOC-Alternative, BSI-tauglich
- Behörden und öffentliche Einrichtungen
  - Brauchen transparente Sicherheitsarchitektur mit nachvollziehbarer Reaktion auf Angriffe
  - Oft föderale oder dezentrale IT-Strukturen – PRISM unterstützt das
  - PRISM Vorteil: DSGVO-konform, flexibel einsetzbar, revisionssicher

Kernfunktionen

- Log Management
  - Was es macht: Sammelt und speichert sicherheitsrelevante Ereignisse (z.B. Login-Versuche, Systemveränderungen, Netzwerkaktivitäten) aus verschiedenen Quellen zentral.
  - Nutzen
    - Vollständige Sicht auf alle sicherheitsrelevanten Aktivitäten
    - Basis für Compliance-Dokumentation & Forensik
    - Keine Datenlücken – kein Risiko bei Audits
  - Sales-Argument: „Sie behalten alle sicherheitsrelevanten Vorgänge im Blick – zentral, revisionssicher und jederzeit abrufbar."
- Echtzeit-Überwachung & Alarmierung
  - Was es macht: Analysiert laufend eingehende Ereignisdaten und meldet verdächtige Aktivitäten sofort.
  - Nutzen
    - Reaktion innerhalb von Sekunden statt Tagen
    - Direkte Alarmierung per Mail, Teams, Slack etc.
    - Klare Eskalationsregeln und visuelle Darstellung im Dashboard
  - Sales-Argument: „Während andere noch suchen, was passiert ist, wissen Sie es längst – in Echtzeit."
- File Integrity Monitoring (FIM)
  - Was es macht: Überwacht kritische Dateien und Konfigurationen (z.B. AD, Registry, Policies) auf Änderungen.
  - Nutzen
    - Erkennt unautorisierte Manipulationen sofort
    - Wichtig für ISO 27001 & KRITIS (Schutz der Integrität)
    - Alarmiert bei gefährlichen Konfigurationsänderungen (z.B. in Firewalls)
  - Sales-Argument: „Ihre sensiblen Systeme melden sofort, wenn sich jemand unbemerkt hineinschleicht."
- Vulnerability Detection
  - Was es macht: Scannt Systeme auf bekannte Schwachstellen und gleicht diese mit Sicherheitsdatenbanken ab.
  - Nutzen
    - Frühzeitige Identifikation gefährdeter Systeme
    - Basis für Patch-Management
    - Reduziert Angriffsfläche deutlich
  - Sales-Argument: „Erkennen Sie Schwachstellen, bevor Angreifer sie finden – ganz automatisch."
- Reporting & Compliance (ISO 27001, NIS2, GDPR)
  - Was es macht: Erstellt anpassbare Berichte für Audits, Management, Aufsichtsbehörden.
  - Nutzen
    - Automatisierte Vorlagen für ISO, NIS2, BSI etc.
    - Jederzeit nachweisbare Sicherheitsmaßnahmen
    - Einfaches Dashboard für CISO, ISB oder Prüfer
  - Sales-Argument: „Sie bestehen das nächste Audit mit Links – PRISM liefert die Berichte automatisch."
- Threat Intelligence Feeds (z.B. MISP, Virustotal)
  - Was es macht: Gleicht eingehende Daten mit externen Bedrohungsdatenbanken ab.
  - Nutzen
    - Erkennt bekannte Malware, Botnets, Command&Control-Verbindungen
    - Permanente Aktualisierung durch globale Threat Feeds
    - Automatische Markierung und Alarmierung bei Treffer
  - Sales-Argument: „Ihr System kennt die Tricks der Angreifer – weil es mit weltweit gebündeltem Wissen arbeitet."
- SOAR / Automatisierung (Playbooks, n8n, Thehive)
  - Was es macht: Reagiert automatisiert auf erkannte Bedrohungen – z.B. durch Blockieren, Isolieren oder Informieren.
  - Nutzen
    - Keine Zeitverluste bei Angriffen
    - Reproduzierbare, dokumentierte Reaktionen
    - Weniger manuelle Eingriffe → Entlastung der IT
  - Sales-Argument: „Ihr System schützt sich selbst – ohne dass nachts jemand wach bleiben muss."
- Anomalieerkennung durch KI
  - Was es macht: Analysiert Muster im Nutzerverhalten, im Netzwerkverkehr und in Systemdaten, um „ungewöhnliches" Verhalten zu erkennen.
  - Nutzen
    - Erkennung von Zero-Day-Angriffen und APTs
    - Schutz vor internem Missbrauch („Insider Threats")
    - Ergänzt klassische Signatur-basierte Methoden
  - Sales-Argument: „Die KI erkennt verdächtiges Verhalten, auch wenn es noch nie zuvor gesehen wurde."

Vertriebshilfen / Argumente

- Sofortige Einstiegspunkte für Vertrieb
  - Was es bedeutet: Vertrieb kann mit PRISM SIEM direkt konkrete Probleme adressieren – keine langwierige Bedarfsanalyse nötig.
  - Typische Einstiegsthemen
    - Kunden hat gerade Audit oder ISO-Zertifizierung vor sich. → PRISM hilft sofort mit Reporting & Compliance.
    - Kunde wurde von Angriffen betroffen. → PRISM bietet schnelle Erkennung & Forensik.
    - IT-Abteilung sucht nach „leichter SOC-Alternative" → PRISM als Einstieg ohne Overhead.
  - Vertriebsformulierung: „Lassen Sie uns in 30 Minuten prüfen, wie Sie mit PRISM Ihre Security-Pflichten abdecken können – ohne Infrastrukturaufwand."
- Geeignet für Kunden ohne Security-Team
  - Was es bedeutet: PRISM benötigt keine internen Analysten oder ein Security Operations Center (SOC) – viele Funktionen laufen automatisiert oder können als Managed Service bezogen werden.
  - Kundentypen
    - KMU ohne IT-Security-Ressourcen
    - Behörden mit zentraler IT
    - Health-IT oder Startups mit Fokus auf Produkt, nicht IT
  - Features, die das unterstützen
    - Automatische Bedrohungserkennung (KI + Regeln)
    - Playbooks mit automatischer Reaktion
    - Alerterung per Mail, Teams etc.
    - Managed SIEM optional durch SECwo5.
  - Vertriebsformulierung: „Auch ohne Security-Team sind Sie mit PRISM in der Lage, Angriffe zu erkennen, zu dokumentieren – und abzuwehren."
- Schneller ROI durch Compliance & Sicherheit
  - Was es bedeutet: Hilft PRISM erfüllt der Kunde gesetzliche Pflichten, vermeidet Bußgelder, und gewinnt Transparenz & Zeit zurück.
  - Konkrete ROI-Treiber
    - Entlastung bei internen oder externen Audits (weniger Aufwand, bessere Qualität)
    - Frühzeitige Erkennung → weniger Schaden durch Angriffe
    - Weniger interne Ressourcen nötig → keine FTEs für SIEM/SOC
    - Reduktion von Projektkosten bei ISO 27001, NIS2-Umsetzung
  - Vertriebsformulierung: „Statt 12 Monate Projekt, 5 FTEs und teuren Aufwand bekommen Sie mit PRISM innerhalb weniger Wochen Compliance, Überblick und Sicherheit."
- Open-Source-Basis = keine Lizenzkosten im Kernsystem
  - Was es bedeutet: PRISM baut auf bewährten Open-Source-Komponenten auf (Wazuh, OpenSearch, Kibana). Dadurch fallen keine Lizenzgebühren für die Grundfunktionen an.
  - Vorteile für Kunden
    - Volle Kostentransparenz: Betriebskosten = Infrastruktur + Support – keine Blackbox-Lizenzen
    - Technologische Offenheit: Kein Vendor-Lock-in, hohe Flexibilität
    - Community-gestützt: Große Nutzerbasis & schnelle Weiterentwicklung
  - Vertriebsformulierung: „Sie investieren nicht in Lizenzkosten, sondern in konkrete Sicherheit – mit vollem Einblick in Technologie und Datenhaltung."

Kundenerfahrungen

- Automatisierte und effiziente Bedrohungserkennung
- Geringere Kosten durch Verzicht auf physische SOCs
- Verbesserte Compliance und Auditfähigkeit
- Einfache Implementierung und Nutzung

Pricing

- Basispreis
  - Startups: 750 EUR/Monat
  - Growups: 1.500 EUR/Monat
  - Enterprises: 10.000 EUR/Monat
- Log Speicher (90 Tage inklusive)
  - Startups
    - 90 Tage inklusive
    - 180 Tage +500 EUR
    - 270 Tage +1.500 EUR
  - Growups
    - 90 Tage inklusive
    - 180 Tage +1.500 EUR
    - 270 Tage +1.500 EUR
  - Enterprises
    - 90 Tage inklusive
    - 180 Tage inklusive
    - 270 Tage +5.000 EUR
- Anzahl Nutzer
  - Startups
    - 5 inklusive, weitere 70 EUR/Nutzer
  - Growups
    - 8 inklusive, weitere 150 EUR/Nutzer
  - Enterprises
    - unbegrenzt inklusive
- Anzahl Clients
  - Startups: 15
  - Growups: 50
  - Enterprises: 250
- Anzahl Server
  - Startups: 5
  - Growups: 15
  - Enterprises: 50
- Cloud Security: 500 EUR/Monat
- Einrichtungskosten
  - Startups: 750 EUR
  - Growups: 3.000 EUR
  - Enterprises: nach Anfrage

Implementierung

- Planung und Analyse
  - Definition des Scopes und Projektplanung
  - Auswahl der passenden Architektur (On-Premises, Hybrid, Cloud)
- Umsetzung
  - Installation und Konfiguration der Komponenten (Agent, Manager, Indexer, Dashboard)
  - Integration mit bestehenden Systemen und Sicherheitslösungen
- Betrieb und Überwachung
  - Automatisierte Updates und kontinuierliche Überwachung
  - Backup-Strategien und Hochverfügbarkeitslösungen
  - Regelmäßige Audits und Berichte

Vorteile

- Schnell einsatzbereit und kosteneffizient
- 24/7 Überwachung und proaktive Bedrohungsabwehr
- Compliance-konforme Berichterstellung und Audit-Funktionen
- Reduzierung von Personalaufwand durch Automatisierung
- Flexibel skalierbar und an verschiedene Unternehmensgrößen anpassbar

Technologie & Architektur

- Komponenten: Agent, Manager, Indexer, Dashboard
  - Agent
    - Installiert auf Endgeräten (Server, Clients, Cloud-Instanzen).
    - Erfasst Logdaten, erkennt Veränderungen, führt Sicherheitschecks aus (z.B. FIM, Vulnerability Detection).
    - → „Das Auge vor Ort."
  - Manager
    - Zentrale Steuerungseinheit. Hier laufen Regeln, Korrelationen und Alarmierungslogiken.
    - → „Das Gehirn von PRISM."
  - Indexer
    - Speicherung und Indexierung aller Sicherheits-Events – meist auf Basis von OpenSearch oder Elasticsearch.
    - → „Die Datenbank für Suche, Auswertung und Langzeitspeicherung."
  - Dashboard
    - Benutzeroberfläche zur Visualisierung, Konfiguration und Analyse. Basierend auf Kibana oder Grafana.
    - → „Das Cockpit für Admins, Analysten und Auditoren."
  - Sales-Argument: „Ein klar strukturiertes System – mit definierten Rollen und maximaler Transparenz."
- Skalierbarkeit & Clusterfähigkeit (Elasticsearch / OpenSearch)
  - Elasticsearch / OpenSearch ermöglichen verteilte Speicherung und parallele Verarbeitung großer Datenmengen.
  - Ideal bei hoher Logfrequenz (>10.000 Events/sec) oder langem Aufbewahrungszeitraum.
  - Indexer-Cluster können beliebig erweitert werden.
  - PRISM ist dadurch wachstumsfähig – von 10 auf 10.000 Geräte ohne Systemwechsel.
  - Sales-Argument: „Ob kleines Unternehmen oder KRITIS-Betreiber – PRISM wächst mit Ihren Anforderungen mit."
- Multi-Tenant & Container-Ready (Kubernetes)
  - Multi-Tenant-Fähigkeit
    - Mandantenfähig – z.B. für MSPs oder Konzerne mit mehreren Standorten.
    - Jeder Mandant sieht nur seine Daten, Rollen und Regeln.
  - Container-fähig (Docker/Kubernetes)
    - PRISM lässt sich flexibel in moderne Infrastrukturen einfügen – ob als Pod in Kubernetes oder Container auf Proxmox.
  - Sales-Argument
    - Automatisches Skalieren, Rollbacks, Load Balancing möglich.
    - „Ein System – viele Mandanten, höchste Effizienz in Betrieb & Betriebskosten."
- Cloud- & On-Premises möglich
  - PRISM kann sowohl
    - in der Cloud betrieben werden (z.B. über AWS, Azure oder Google Cloud),
    - als auch On-Prem im eigenen Rechenzentrum oder sogar hybrid.
  - Ideal bei DSGVO/DSG-konformen Anforderungen, Air-Gap-Zonen oder IT-Sicherheitsrichtlinien.
  - Sales-Argument: „Ob Cloud-native oder lokal abgesichert – PRISM passt sich Ihrer IT-Strategie an."
- Schnittstellen: Microsoft 365, Fortinet, Palo Alto, AWS, Syslog
  - Microsoft 365 (M365 Defender, Exchange, Entra)
    - Überwachung und Analyse cloudbasierter Office-Umgebungen.
  - Fortinet / Palo Alto
    - Integration per Syslog-Streams – auch inkl. VPN-/Firewall-Logs und IDS/IPS-Events.
  - AWS CloudTrail & CloudWatch
    - Logdaten aus S3, EC2, IAM, VPC etc. integrierbar.
  - Syslog, Windows Event Forwarding, REST API
    - Standardprotokolle für universelle Kompatibilität.
  - Sales-Argument
    - „PRISM spricht die Sprache Ihrer IT – und integriert sich reibungslos in Ihre Umgebung."

Presented with xmind