PRISM SIEM Fact Sheet

- **Sales Aids / Arguments**
  - Immediate Entry Points
    - What it means:
      - Sales can address specific problems directly with PRISM SIEM – no lengthy needs analysis required.
    - Typical initial topics:
      - Customer is currently undergoing an audit or ISO certification → PRISM helps immediately with reporting & compliance.
      - Customer has been affected by attacks → PRISM offers rapid detection & forensics.
      - IT department is looking for "easy SOC alternative" → PRISM as an entry point without overhead.
    - Sales formulation:
      - "Let us check in 30 minutes how you can cover your security obligations with PRISM – without infrastructure overhead."
  - Suitable for Clients without Security Teams
    - What it means:
      - PRISM does not require in-house analysts or a Security Operations Center (SOC) – many functions run automatically or can be obtained as a managed service.
    - Customer types:
      - SMEs without IT security resources
      - Public authorities with centralized IT
      - Health IT or start-ups with a focus on product, not IT
    - Features that support this:
      - Automatic threat detection (AI + rules)
      - Playbooks with automatic response
      - Alerting via email, Teams etc.
      - Managed SIEM optional through SECaaS
    - Sales formulation:
      - "Even without a security team, PRISM enables you to detect, document – and ward off – attacks."
  - Fast ROI through Compliance & Security
    - What it means:
      - With PRISM, the customer fulfills legal obligations, avoids fines, and regains transparency & time.
    - Konkrete ROI-Treiber:
      - Relief for internal or external audits (less effort, better quality)
      - Early detection → less damage from attacks
      - Fewer internal resources required → no FTEs for SIEM/SOC
      - Reduction in project costs for ISO 27001, NIS2 implementation
    - Sales formulation:
      - "Instead of 12 months of project, 3 FTEs and expensive effort, PRISM gives you compliance, overview and security in just a few weeks."
  - Open Source = No Core License Fees
    - What it means:
      - PRISM is based on proven open source components (Wazuh, OpenSearch, Kibana). This means that there are no license fees for the basic functions.
    - Vorteile für Kunden:
      - Full cost transparency: operating costs = infrastructure + support – no black box licenses
      - Technological openness: No vendor lock-in, high flexibility
      - Community-supported: Large user base & rapid further development
    - Sales formulation:
      - "You are not investing in license costs, but in concrete security – with full insight into technology and data management."
- **Customer Experiences**
  - Automated and efficient threat detection
  - Lower costs by eliminating physical SOCs
  - Improved compliance & audit readiness
  - Easy to implement and use
- **Pricing**
  - 4 Startups
    - Base: 750 EUR/month
    - Users: 3 included, 470/additional
    - Clients: 15
    - Servers: 5
    - Cloud Security: €300
    - Setup: €750
    - Log retention:
      - 90 days incl.
      - 180 days +€500
      - 270 days +€1,500
  - 4 Growsups
    - Base: €1,500
    - Users: 8 included, €150/additional
    - Clients: 50
    - Servers: 15
    - Setup: €3,000
    - Log retention:
      - 90 days incl.
      - 180 days +€1,500
      - 270 days +€1,500
  - 4 Enterprises
    - Base: €10,000
    - Users: unlimited
    - Clients: 250
    - Servers: 50
    - Setup: on request
    - Log retention:
      - 90 & 180 days incl.
      - 270 days +€5,000
- **Implementation**
  - Planning & Analysis
    - Scope definition, project planning
    - Architecture choice (on-prem, hybrid, cloud)
  - Execution
    - Component installation & configuration
    - Integration with existing systems
  - Operation & Monitoring
    - Auto-updates & continuous monitoring
    - Backup & high availability strategies
    - Regular audits & reporting
- **Advantages**
  - Rapid deployment & cost-efficiency
  - 24/7 monitoring & proactive threat defense
  - Compliance reporting & audit support
  - Reduced staffing through automation
  - Scalable and adaptable
- **Technology & Architecture**
  - Components: Agent, Manager, Indexer, Dashboard
    - Agent:
      - Installed on devices (servers, clients, cloud).
      - Captures log data, detects changes, performs security checks (e.g. FIM, vulnerability detection).
      - → "The eye on site."
    - Manager:
      - Central control unit with rules, correlations, alert logic.
      - → "The brain of PRISM."
    - Indexer:
      - Storage & indexing of all events (OpenSearch/Elasticsearch).
      - → "The database for search & long-term storage."
    - Dashboard:
      - Visualization, configuration, analysis (Kibana/Grafana).
      - → "The cockpit for admins, analysts, auditors."
    - Sales-Argument:
      - "A clearly structured system – with defined roles and maximum transparency."
  - Scalability & Clustering (Elasticsearch / OpenSearch)
    - Elasticsearch / OpenSearch enable distributed storage and parallel processing of large amounts of data.
    - Ideal for high log frequency (>10,000 events/sec) or long retention periods.
    - Indexer clusters can be expanded as required.
    - PRISM can therefore grow – from 10 to 10,000 devices without changing systems.
    - Sales-Argument:
      - "Whether you are a small company or a KRITIS operator – PRISM grows with your requirements."
  - Multi-tenant & container-ready (Kubernetes)
    - Multi-tenant capability:
      - Multi-tenant capable – e.g. for MSPs or groups with multiple locations.
      - Each client only sees its own data, roles and rules.
    - Container-capable (Docker/Kubernetes):
      - PRISM can be flexibly integrated into modern infrastructures – whether as a pod in Kubernetes or containers on Proxmox.
      - Automatic scaling, rollbacks, load balancing possible.
    - Sales-Argument:
      - "One system – many clients, maximum efficiency in operation & operating costs."
  - Cloud & on-premises possible
    - PRISM can be operated both:
      - operated in the cloud (e.g. via AWS, Azure or Google Cloud),
      - as well as on-prem in your own data center or even hybrid.
    - Ideal for GDPR/DSGO-compliant requirements, AirGap zones or IT security guidelines.
    - Sales-Argument:
      - "Whether cloud-native or locally secured – PRISM adapts to your IT strategy."
  - Interfaces: Microsoft 365, Fortinet, Palo Alto, AWS, Syslog
    - Microsoft 365 (M365 Defender, Exchange, Entra):
      - Monitoring and analysis of cloud-based office environments.
    - Fortinet / Palo Alto:
      - Integration via syslog streams – also incl. VPN/firewall logs and IDS/IPS events.
    - AWS CloudTrail & CloudWatch:
      - Log data from S3, EC2, IAM, VPC etc. can be integrated.
    - Syslog, Windows Event Forwarding, REST API:
      - Standard protocols for universal compatibility.
    - Sales-Argument:
      - "PRISM speaks the language of your IT – and integrates seamlessly into your environment."
- **Overview**
  - what is PRISM SIEM?
    - PRISM SIEM is a modular, AI-powered platform for security monitoring and threat detection in IT environments. It is based on open-source technologies (e.g., Wazuh, Elastic Stack) and was specifically developed for companies that need to meet compliance requirements, protect their IT infrastructure, and conserve resources.
    - Key Features at a Glance
      - Real-time monitoring of all security-relevant systems
      - Log analysis & centralized event storage
      - Automated detection of threats & anomalies
      - Playbooks for automated response (SOAR)
      - Compliance dashboards for NIS2, ISO 27001, and more
      - Fully operable on-premises, in the cloud, or as a managed service
    - USP
      - PRISM SIEM combines enterprise-level security, ease of use, and high cost-efficiency – especially suitable for companies without their own SOC.
  - Why is PRISM SIEM indispensable?
    - A SIEM system is the center of modern cyber defense. It enables security-relevant information from a variety of technical systems to be bundled, correlated, and intelligently analyzed.
    - Current challenges addressed by a SIEM:
      - Increasing cyberattacks: Ransomware, phishing, APTs – targeted, fast, often automated
      - Rising regulatory requirements: NIS2, KRITIS regulation, ISO 27001, GDPR – require detection, response, and documentation
      - Complexity of IT landscapes: Multi-cloud, remote work, IoT/OT – SIEM provides visibility
      - Lack of skilled personnel: Manual analysis is barely feasible – PRISM automates detection & response
  - Customer Benefits at a Glance
    - Identify risks before damage occurs
    - Handle cyber incidents in a structured & automated way
    - Pass audits with just a few clicks
    - Monitor and document all security-related processes
- **Target Groups**
  - Startups with fast growth and limited budgets
    - No security teams or specialists
    - Need to meet basic legal standards quickly (e.g., GDPR, ISO light)
    - Need to secure cloud infrastructure & APIs
    - PRISM Advantage: Fast start, low entry cost, compliance assurance
  - Growing companies (Growsups) and established firms
    - Facing first audits or customer requirements
    - Increasing security events & complexity
    - Building internal structures
    - PRISM Advantage: Scalable, team-ready, integration-friendly
  - Hospitals and Critical Infrastructures (KRITIS)
    - Must prove mandatory attack detection (NIS2, IT-SIG 2.0)
    - Often understaffed with high requirements
    - PRISM Advantage: Audit-ready, SOC alternative, BSI-compliant
  - Companies with high compliance requirements (e.g., NIS2, ISO 27001)
    - Must prove mandatory attack detection (NIS2, IT-SIG 2.0)
    - Often understaffed with high requirements
    - PRISM Advantage: Audit-ready, SOC alternative, BSI-compliant
  - IT service providers and cloud providers
    - Must prove mandatory attack detection (NIS2, IT-SIG 2.0)
    - Often understaffed with high requirements
    - PRISM Advantage: Audit-ready, SOC alternative, BSI-compliant
  - Government agencies and public institutions
    - Need transparent security architecture with traceable responses
    - Often federal or decentralized IT structures
    - PRISM Advantage: GDPR-compliant, flexible use, audit-proof
- **Core Functions**
  - Log Management
    - what it does
      - Collects and stores security-relevant events centrally
    - Benefits
      - Full visibility of all security-relevant activities
      - Basis for compliance & forensics
      - No data gaps – no audit risk
    - Sales-Argument
      - "You keep an eye on all security-relevant processes – centrally, audit-proof and accessible at any time."
  - Real-Time Monitoring & Alerting
    - what it does
      - Monitors critical files and configurations for changes
    - Benefits
      - Reaction in seconds instead of days
      - Direct alerts via email, Teams, Slack
      - Visual dashboard with escalation rules
    - Sales-Argument
      - "While others are still looking for what happened, you know what happened – in real time."
  - File Integrity Monitoring (FIM)
    - what it does
      - Analyzes incoming event data continuously and alerts immediately
    - Benefits
      - Detects unauthorized manipulations
      - Important for ISO 27001 & KRITIS
      - Alerts on risky configuration changes
    - Sales-Argument
      - "Your sensitive systems report immediately if someone sneaks in unnoticed."
  - Vulnerability Detection
    - what it does
      - Scans systems for known vulnerabilities
    - Benefits
      - Basis for patch management
      - Significantly reduces attack surface
    - Sales-Argument
      - "Detect vulnerabilities before attackers find them – automatically."
  - Reporting & Compliance (ISO 27001, NIS2, GDPR)
    - what it does
      - Generates customizable reports for audits, management, authorities
    - Benefits
      - Automated templates
      - Verifiable security measures at any time
      - Simple dashboards for CISOs, ISBs, auditors
    - Sales-Argument
      - "You'll pass the next audit with flying colors – PRISM delivers the reports automatically."
  - Threat Intelligence Feeds (e.g. MISP, Virustotal)
    - what it does
      - Compares incoming data with threat databases
    - Benefits
      - Detects known malware, botnets, C&C connections
      - Auto-tagging and alerting
    - Sales-Argument
      - "Your system knows the attackers' tricks – because it works with globally shared knowledge."
  - SOAR / Automation (Playbooks, n8n, TheHive)
    - what it does
      - Automated response to detected threats (block, isolate, inform)
    - Benefits
      - No delay in case of attacks
      - Documented, repeatable reactions
      - Reduced manual effort
    - Sales-Argument
      - "Your system protects itself – without anyone having to stay awake at night."
  - AI-based Anomaly Detection
    - what it does
      - Analyzes patterns in behavior, traffic, system data
    - Benefits
      - Detects zero-day attacks, APTs
      - Protects against insider threats
      - Complements signature-based methods
    - Sales-Argument
      - "The AI recognizes suspicious behavior, even if it has never been seen before."

Presented with xmind