DATA SHEET

Seceon® Open Threat Management Platform empowers Enterprise and MSSP SOC teams to orchestrate and analyze operational security data, manage threats and vulnerabilities, and respond to security incidents threats in real-time.

Key Benefits:

Automatic Threat Remediation

- Clear actionable steps to contain and eliminate threats in real-time
- Formalized and automated incident response workflows
- Out-of-the-box and customized remediation with various security tools like SIEM, APT, Security Analytics/Forensics, EDR, Sandboxes, WAF, IDS/IPS, Mail Security, Web Security, ADC

Proactive Threat Detection

- Proactively detects threats that matter and surfaces them in near real-time or real-time without agent or alert fatigue
- Performs threat detection across multi-cloud, on-premise, and hybrid environments for MSSPs and Enterprises
- Complete integration with Incident management tools

Continuous Monitoring and Reporting

- Ingests raw streaming data (Logs, Packets, Flows, Identities) to provide unparalleled real-time view of all assets and their interactions
- Definition get translated into data stream processing topologies for efficient correlation

Comprehensive Visibility

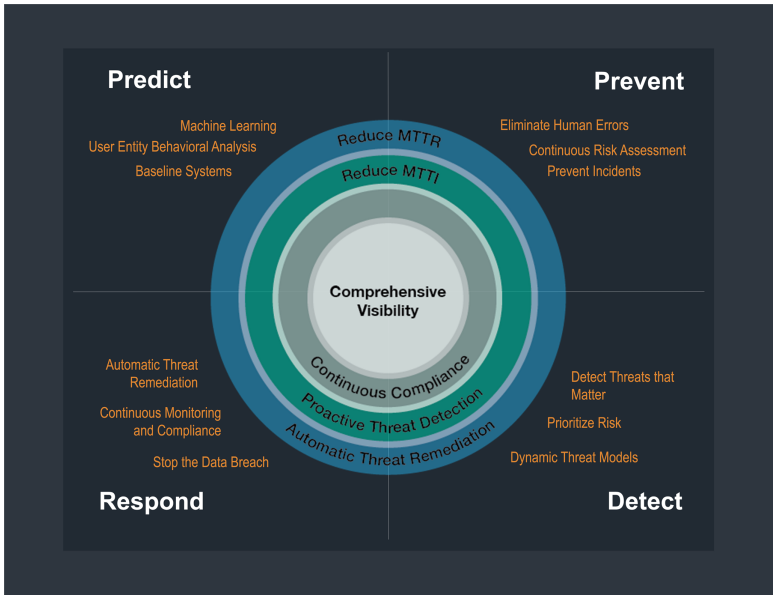
- Logically auto discovers and creates asset groups
- Works transparently with encrypted traffic

Flexible and Scalable Deployment

- Solution available for on-premise with single or multiple sites, in the cloud or hybrid deployment
- Scalable architecture with full support for multi-tenancy and data segregation

Traditionally organizations build a cohesive multi-layered security posture to combat the threats and ensure the security of information. Cybersecurity technologies deployed in today's enterprise are built on a fundamental hypothesis – smart humans must use an array of advanced security tools from different vendors that were not built to communicate with each other seamlessly, analyze data and provide correlation from multiple sources, automatically identify a threat and then mitigate it. The problem is that 95 percent of attacks exfiltrate or corrupt data within a few hours of the breach - hardly enough time for smart humans to react!

Seceon® Open Threat Management (OTM) Platform enables organizations to detect cyber threats quickly, and to stop them as they happen, preventing the infliction of extensive corporate damage. The platform uses elastic compute power, dynamic threat models, behavioral analytics, advanced machine learning, AI with actionable intelligence with proprietary feature engineering and anomaly detection algorithms without a need to establish rules.



Key Features

Behavioral Analytics & Predictive Modeling • Zero-day malware and Insider attacks	**Data-driven and Agentless solution**
Contextual Real-time Alerts with Automated Analysis & Correlation • No rules to define and no thresholds to adjust • Learns and improves over time while significantly reducing alert volume	**Rapid Deployment with Integrated DevOps Model**
Unified Platform for Ingestion, Storage and Analytics (SoC in Box) • Eliminates SILO solutions and gaps	**Micro-service/Container Architecture** • Virtualization and Cloud ready
Out-of-the-box Automated Threat Containment and Elimination • Configurable parameter, supports perimeter firewalls, Microsoft AD	**Real-time Stream Processing and Big-Data Engine** • Out-of-the box scalability, redundancy with clustering support
Machines Learning and AI with Actionable Intelligence • Cognitive abilities are built using non-stop, real-time unsupervised and semi-supervised learning • Executes a suite of general anomaly and threat specific algorithms and intelligently decays outdated experiences • AI Engine automates analysis, minimizes false positives, improves accuracy, and delivers real-time performance	**Dynamic Threat Models** • Automate the task of writing rules in order to detect real threat issues from plethora of threat indicators • Threat models are based on patented technology where rules are all preconfigured and they adjust dynamically
Operations Management • Evidence collection and journaling • Threat intelligence hub • Customizable reports generation • Open and extensible platform (Python, Javascript)	• Comprehensive SLA tracking and metrics • Regulatory compliance features and reporting • Intelligent automation • Collaborative investigation

For more information and pricing, please contact Seceon at sales@seceon.com