DATA SHEET

Seceon® aiSIEM™ helps organizations to visualize user activity, behavior, applications and flows. It empowers SOC analysts to become more efficient and helps organizations to reduce MTTI and MTTR together providing continuous compliance for the business.

Key Benefits:

Reduce MTTR with Automatic Threat Remediation

- Clear actionable steps to contain and eliminate threats in real-time
- Formalized and automated incident response workflows

Reduce MTTI with Proactive Threat Detection

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

Continuous Compliance and Monitoring

- Reports for regulatory compliance (HIPAA, PCI, NIST, FINRA, GDPR) and investigation support
- Security operations and long-term data analytics

Comprehensive Visibility

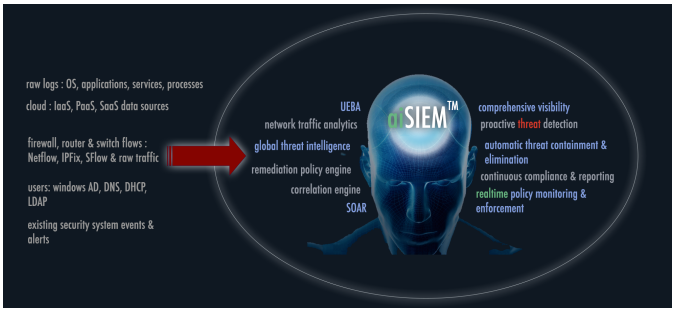
- Ingests raw streaming data (Logs, Packets, Flows, Identities) to provide unparalleled real-time view of all assets and their interactions
- Logically auto discovers and creates asset groups
- Works transparently with encrypted traffic

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

Security Information and Event Management (SIEM) has been part of an organization's security posture for a long time yet most organizations fail to derive the best value out of SIEM because of its implementation complexity and operational challenges. Also, while most SIEMs do a good job of aggregating, indexing and storing logs from different sources for compliance reporting through analysis of historical data, they only ingest half the information required to see most threats and do not understand or analyze the threat indicators. With the adoption of hybrid cloud networks, growing complexity of threat vectors and volume of security incidents, and a lack of cybersecurity expert talent, businesses today need an improved set of capabilities to complement their SIEM.

Seceon® aiSIEM goes beyond using the log data, simple analysis for correlation of events and applying rules for data analysis. The solution uses elastic compute power, dynamic threat models, user and entity behavioral analytics (UEBA), threat intelligence feeds for correlation and enrichment, advanced machine learning (ML), AI with actionable intelligence and proprietary feature engineering and anomaly detection algorithms without a need to establish rules. It includes, large-scale and robust collection and enhanced analysis of logs and data from cloud, endpoints and other IT data sources beyond rules, fast and scalable search over volumes of raw data and, most importantly, automated response to contain and eliminate the threats in real-time. Additionally, it is designed to support enterprise SOC teams and MSSPs because of its scalable and distributed architecture. It integrates with 3rd party ticketing systems and takes over operations of DR site in case of disaster.



Key Features

Behavioral Analytics & Predictive Modeling

- Zero-day malware and Insider attacks

Rapid Deployment with Integrated DevOps Model

- Open and extensible platform (Python, Javascript) with simplified licensing

Contextual Real-time Alerts with Automated Analysis & Correlation

- No rules to define and no thresholds to adjust
- Analyzes data and incorporates threat intelligence feeds for correlation

Data-driven and Agentless solution

- Robust, large-scale data collection from cloud and all data sources
- Streaming platform which scales to billions of events handling per sec

Unified Platform for Ingestion, Storage and Analytics

- Eliminates SILO solutions and gaps

Micro-service/Container Architecture

- Scalable architecture with support for multi-tenancy & data segregation
- Virtualization and Cloud ready

Out-of-the-box Automated Threat Containment and Elimination

- Enhanced data analytics beyond rules with contextual real-time alerts for “threats-that-matter” and automated response

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; creates a baseline based on observed data over a period of time
- 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
- Learns and improves over time while significantly reducing alert volume

Operations Management

- Long Term Storage and Analysis of Raw Logs up to 7 years
- Configurable data retention policies
- Integrates with 3rd party ticketing systems
- Threat intelligence hub
- Takes over operations of DR site in case of disaster
- Regulatory compliance features and reporting
- Scheduled/On-Demand customizable reports
- Web-based User Interface (UI), Customizable dashboards with Drill Down
- Supports well-known authentication services
- Intelligent automation

System Requirements

The two major components of aiSIEM are *Collection and Control Engine* (CCE) and *Analytics and Policy Engine* (APE). CCE resides close to the data sources, whereas, the APE is centralized policy and control engine. CCE securely communicates with APE over SSH channel with 256 bit encryption. aiSIEM solution assures the integrity of the information collected with standard algorithms of robust bit lengths.

For more information and pricing, contact BLTD at sales@bluelabeldist.com