Seceon® aiSIEM™ goes far and above the capabilities of typical SIEM solutions. 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.

Challenges:

- Very complex as it gathers, normalizes, and correlates data from disparate sources
- Operationally very exhausting and challenging especially with growing complexity of threats and new technologies, such as, hybrid cloud
- Responses to threats and incidents are more reactive and need security experts or SMEs for assessments

Solution:

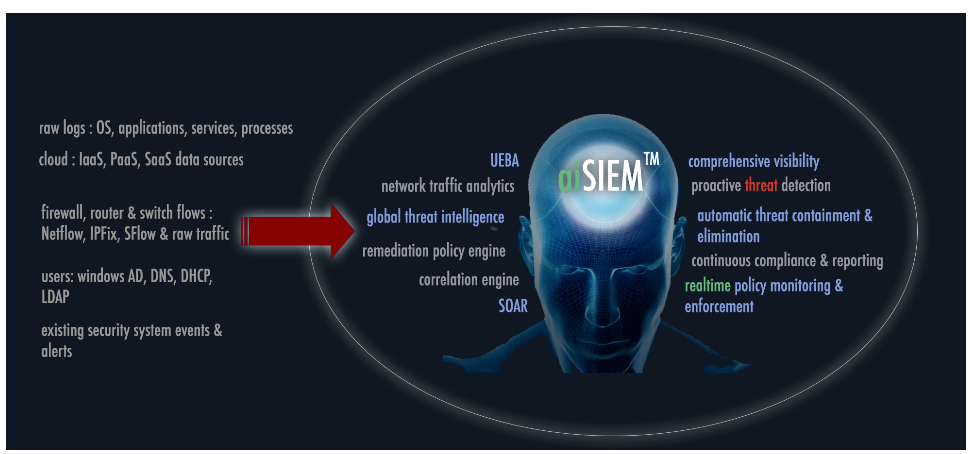
- Ingests raw streaming data and puts it through a fast parallel processing architecture that allows data to be streamed in through memory in real-time
- Uses behavioral analytics generated by an extensive set of dynamic threat models, aided by machine learning, artificial intelligence to detect both known and unknown attacks
- Provides automatic remediation without a need for playbooks on a single platform

Benefits:

- Reduce *Mean-Time-To-Identify* (MTTI) with Proactive Threat Detection
- Reduce *Mean-Time-To-Resolve* (MTTR) with Automatic Threat Remediation
- Continuous Compliance and Risk Monitoring
- Collect everything at a fixed low cost and provide comprehensive visibility of all assets in real-time

Security Information and Event Management (SIEM) has been a critical technology part of an organization's security posture for a long time and does a good job of centralized analysis and reporting by ingesting logs and additional contextual data from different sources. Yet most organizations fail to derive the best value out of SIEM because of its implementation complexity and operational challenges. According to Gartner, no single technology, such as, CLM, UEBA, NTA, SOAR or EDR can replace the entire set of SIEM capabilities. With the adoption of hybrid cloud networks, growing complexity of threat vectors, and a lack of cybersecurity expert talent, businesses today need an improved set of capabilities to complement their SIEM. Furthermore, the volume of security incidents is rapidly growing and has been unmanageable for SOC teams creating a need for end-to-end automation of detection and response. To circumvent the challenges of traditional SIEM, Gartner defines the modern SIEM to work with more than just log data and apply more than simple correlation rules for data analysis. Some of the key capabilities include, large-scale and more robust data collection from cloud and other modern IT data sources, collect & analyze logs and data from networks & endpoints, incorporate threat intelligence feeds for correlation and enrichment, enhanced data analytics beyond rules, fast and scalable search over volumes of raw data and, most importantly, automated response.

Seceon® aiSIEM goes beyond using the log data, simple analysis for correlation of events and applying rules to enhance an organization's security posture. It ingests raw streaming data (Logs, Packets, Flows, Identities) from a variety of sources to provide comprehensive visibility into an organization's security posture at any time.



1.978.923.0040 | www.seceon.com | sales@seceon.com | Seceon Inc., 238 Littleton Road, Westford MA, 01086 | © 2018

Real-time machine learning handles large data volumes in conjunction with contemporary big/fast data frameworks and enables adapting to any environment dynamically for deep data analysis. The complexity is substantially reduced by dynamic threat models and behavioral analytics engines that eliminate need for writing complex rules; complemented with advanced patent-pending correlation engine powered by AI generates meaningful alerts with improved accuracy from scores of threat indicators otherwise analyzed by the security professionals.

"Seceon's machine learning capability has been key to reducing noise and ensuring that critical alerts get the attention they require."

Mark Alayev

Director of Service Delivery, RFA

Additionally, aiSIEM has been designed to support today's enterprise SOC teams as well as MSSPs because of its scalability and distributed architecture. It's laser-like focus on human and machine actionable intelligence produces minimum false positives surfacing only the threats that matter. This empowers the SOC analysts to focus on real incidents and not on a volume of noise, thus improving their efficiency and effectiveness significantly. aiSIEM supports horizontal clustering and has a built-in multi-tenant architecture that can be easily deployed on premise or in cloud to provide managed security services to organizations of any size.

"We've seen the need for years for real-time threat mitigation, especially in the SMB sector. SMBs continue to be the hardest hit and have the most to lose but the least amount of resources."

Ron Culler

Chief Technology Officer, Secure Designs

Most organizations are unable to deal with the increasing number and sophistication of cyber threats because it either takes them too long to identify them or takes too much time to stop them from inflicting damage once breached. Gartner's CARTA approach suggests continuous data analytics is must to constantly assess organization's security posture, provide adaptive access, predict and anticipate threats in real-time and respond to threats that matter in real-time. aiSIEM aligns to the CARTA approach to provide these four major benefits:

Reduce *Mean-Time-To-Identify* (MTTI) with Proactive Threat Detection: aiSIEM proactively detects threats and surfaces them in real-time or near real-time without an agent or alert fatigue. It uses dynamic threat models, machine learning and AI with actionable intelligence combined with proprietary feature engineering for detection of known and unknown threats. It performs threat detection across the cloud, on-premise, and hybrid environments for MSSPs and Enterprises.

Reduce *Mean-Time-To-Resolve* (MTTR) with Automatic Threat Remediation: aiSIEM performs automatic threat containment and elimination in real-time. It also provides clear actionable steps to eliminate the threats that can either be taken automatically by the system at runtime, as per a specific 'configurable' schedule, or manually by the security expert post-analysis.

"I like the OTM architecture, specifically its use of containers and the layered approach. It provides a ton of flexibility in deployment options. SOCs desperately need capabilities they can't find in SIEM tools."

Eric Ogren

Senior Security Analyst, 451 Research

Continuous Compliance and Risk Monitoring: aiSIEM supports organizations' need to adhere to regulatory compliance requirements providing continuous compliance and reporting for HIPAA, GDPR, PCI-DSS, NIST, FINRA and long-term data analytics for security operations and investigation support.

Comprehensive Visibility: Ingests raw streaming data from multiple data sources to provide real-time view of all assets: on-premise/cloud/hybrid and its interactions.

In today's world where data gets stolen within minutes of a breach, requiring analysts to constantly re-write rules leads to unacceptable response time and, more importantly, considerable damage. aiSIEM effectively meets these critical business requirements with an automated approach of producing and applying actionable intelligence for threat containment and elimination in near real-time.