DATA SHEET

Seceon® aiNBAD™ empowers Enterprise and MSSP SOC teams to proactively detect zero day and unseen variants of known threats instantly with its award-winning ML and AI technologies' behavior and anomaly detection engines in real-time. The Seceon® OTM platform of aiNBAD further empowers the SOC analysts to become more efficient and helps organizations to significantly reduce MTTI and MTTR.

Key Benefits:

Real-Time Network Behavior Analysis

- aiNBAD begins to learn and analyze your network behavior for anomaly detection with no wait
- SOC-centric actionable intelligence will show the specific anomaly location and recommend actions
- Differentiates the threat classes, such as, Zero Day, DDoS, Malware, Ransomware for quick action
- Complete transparency on the threat scoring for effective threat resolution
- Only surfaces threats that matter for effective operational throughput
- Allows SOCs to cover more threats through Machine learning and AI based automation and analytics.
- Risk mitigation with full automation
- On demand comprehensive view of security posture
- Variety of reports with meaningful KPI's
- Complete Audit trail
- Alert Management workflow with integrated notification
- Automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts
- Enhanced Flows per second with validated supported hardware

Automatic Threat Remediation

- Clear actionable steps to contain and eliminate threats in real-time
- Formalized and automated incident response workflows; no specialized playbooks to be written
- Out-of-the-box and customized remediation with various security tools like SIEM, APT, Security Analytics/Forensics, WAF, IDS/IPS, Mail Security, Web Security, ADC

Traditionally organizations deploy many of the perimeter and endpoint devices to protect the corresponding segments of the infrastructure from known and signature-based threats. Such protection must be complemented to protect against the breaches in the network that sits in-between perimeter and endpoint devices from the continuing evolution of threat vectors and surfaces that attackers employ. aiNBAD caters exactly to this problem by building a cohesive multi-layered security posture to combat the modern known and unknown threats and ensure the security of critical information accessed by the network. 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 biggest concern for enterprises is protection of data of all forms, 95 percent of attacks exfiltrate or corrupt data within a few hours of the breach—hardly enough time for smart humans to react!

Seceon® aiNBAD built upon its Open Threat Management (OTM) Platform enables organizations to detect both known signature based and evolving not-yet-seen cyber threats quickly, and to stop them as they happen, preventing the infliction of extensive corporate damage. The platform moves away from static rules-based threat detection and instead 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 pre-defined or static rules.

Ponemon Institute's Megatrend survey published in 2018 confirms that the importance of Artificial Intelligence (AI) in Cyber Defense is growing at the fastest pace followed by Threat Intelligence Feeds and Analytics. Seceon aiNBAD delivers the best in breed of these three technologies to instantly detect and contain threats that cannot be detected by other means.

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

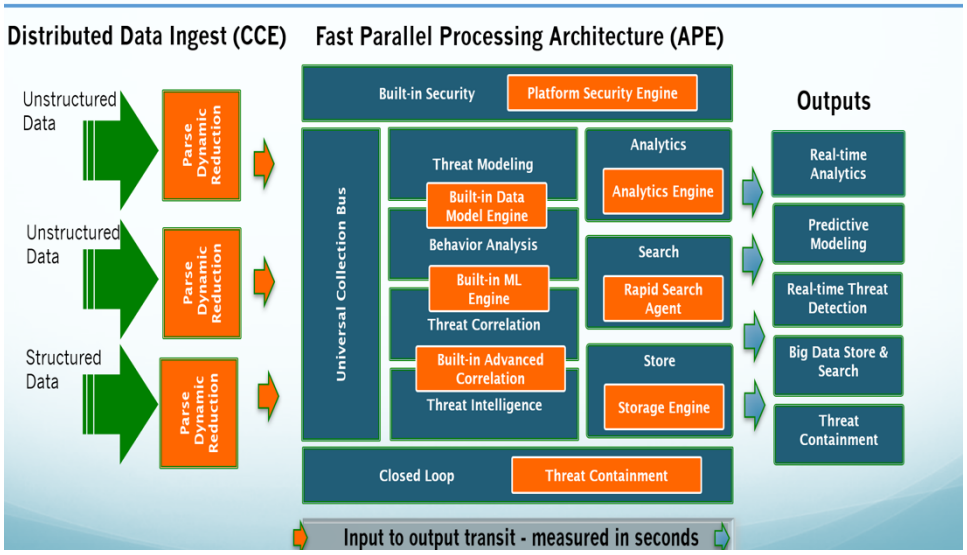
Continuous Monitoring and Reporting

- 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

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

Seceon® OTM Platform: How it works?



Key Attack and Alert Types

Zero Day	Data Exfiltration	Worm	Policy Violation (Whitelist, Country)	Trojan Activity
Volumetric DDoS	Amplification DDoS	ICMP DDoS	TCP SYN DDoS	Potential Data Raid
Malware Infected Host	Potential Vulnerability Exploit	Spank Attack	Botnets in the Network	

System Requirements

Seceon Analytics and Policy Engine (APE)	**Seceon** Collection and Control Engine (CCE)
Physical, Virtual, Cloud based	Physical, Virtual, Cloud-based
Linux OS: CentOS 7.x (ask for supported versions)	Linux OS: CentOS 7.x (ask for supported versions)
128GB RAM	4GB RAM minimum (16GB preferred)
32-core CPU minimum (56 cores preferred)	4-CPU core minimum (8-CPU cores preferred)
6-480GB SSD minimum (8-960GB SSD preferred); RAID-5 recommended	150GB Hard disk

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