Seceon aiSIEM

Advanced Real-time Threat Monitoring, Detection and Response.

A platform for MSPs/MSSPs to offer efficient, high-margin security services and streamline operations with AI and ML powered detections and automated responses for remediating attacks and breaches.

aiSIEM™ Platform for MSPs/MSSPs

Seceon enables MSPs and MSSPs to reduce cyber threat risks and their security stack complexity while improving their ability to detect and block threats and breaches at scale.

Seceon's aiSIEM platform augments and automates MSP and MSSP security services with our AI and ML powered solutions. It delivers continuous coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds and applications. It is all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis and correlation engines to reliably detect and alert. Today, over 300 plus partners are reselling and running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 7,500 clients.

Engineers and analysts can gain a unified view of user activities, network traffic, anomalous host behaviors, cyber threats, exploits, and attacks using automation, artificial intelligence, advanced correlation, and analytics. aiSIEM simplifies threat containment and risk mitigation, enabling analysts to respond automatically or manually to alerts.

Highlights

GAIN TRUST WITH UNIFIED VISIBILITY AND THREAT INTELLIGENCE CAPABILITIES

Uncover a myriad of threat vectors lurking inside your existing logs,auto-discovered hosts, network, cloud, OT and IoT infrastructure, Seceon aiSIEM combines this telemetry with 360° inference drawn from events, network traffic, packets, identities and behavioral patterns.

REDUCE MEAN TIME TO DETECT AND RESPOND

Considerably shorten Mean-Time-To Detect (MTTD) and Mean-Time-To Response (MTTR) with automated threat detection and remediation in real-time and score them by confidence level and criticality.

EFFORTLESS DEPLOYMENT AND INTEGRATIONS

With just one collector, you can start sending flows and logs and deploy Seceon aiSIEM. Then you can connect your existing technology stack with hundreds of integrations.

CONTINUOUS COMPLIANCE

Ensure compliance 24x7 with Seceon’s audit and reporting capabilities for PCI-DSS, HIPAA, NIST, GDPR and more. Additionally monitor security postures, operations and investigations reporting.

Platform Overview

Ingestion of events, logs, flows, user activity data from almost all sources; identities, networks, endpoints, clouds, and applications.

Contextual enrichment with threat intelligence (40+ sources) combines with vulnerability assessments and historical data.

Behavior baselining and profiling for anomaly detection leveraging Machine Learning and Artificial Intelligence techniques.

Advanced event correlation (on-prem and cloud) and behavioral patterns with AI and Dynamic Threat Models.

Identification of threats based on rules-based policy creation, enforcement and notification for appropriate action and governance

Protection and response based on automated remediation (based on incident triaging and or prebuilt playbooks) and real-time remediation.

Continuous compliance and reporting across several key areas – security, compliance, operations and investigations.

"With Seceon, we have more confidence in our ability to protect our clients, and because it is so efficient, we can offer higher revenue plans without adding overhead."

- Seceon MSSP partner

Supercharge your ability to protect environments with real-time AI and ML powered detection of threats and breaches.

Continuous real-time, automatic, anomaly detection, and behavior analysis of all ingested logs, events, flows combined with identity and application-level data like Microsoft AD, enables Seceon to detect indicators of compromise and threats and apply a confidence and risk score to surface and alert on only the events that matter. You'll lower your mean time to detect (MTTD) and cut the number of false positives your teams may be struggling with.

Finally, an easy-to-use incident response platform designed to make it easy to set and forget automated response playbooks.

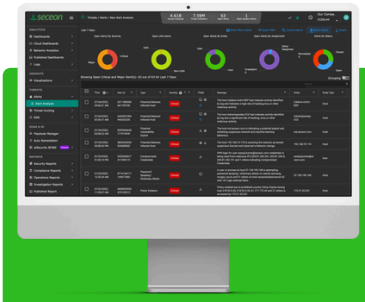
With automated and analyst assisted remediation (blocking, quarantine etc.) based on alert type and severity that provides all of the correlation and situational awareness your teams need will enable you to decrease the mean-time-to-response (MTTR). And with our innovative playbook builder GUI that allows incident responders to seamlessly covert searches and alerts into multi-step playbooks to drive deeper automation.

Launch advanced cybersecurity services with high margins and reduce the risks of cyber threats for your clients - at scale.

With Seceon's multi-tenant, flexible 'best-fit' deployment options, and flexible retention periods, including geographically dispersed deployments, many service providers tell us they have more efficient security operations and higher margins than alternative solutions. Seceon supports hundreds of integrations for EDRs, network log sources, context sources, PSA, ITSM systems, and more. Seceon will rapidly add value to your existing investments. Many of our service provider partners report that they can onboard new customers without the massive amount of hardware that NDR platforms or custom scripting that SOAR platforms require and achieve faster MTTD/MTTR vs legacy store and query SIEMs of the past.

What Advantages do MSPs and MSSPs have with Seceon?

- Comprehensive, unified visibility, threat detection and response with aiSIEM, reducing your team's time to investigate & respond.
- Fast and simplified responses powered by orchestration and automation that leverage AI and ML to reduce MTTD/MTTR without adding overhead.
    - Choose automated responses with included 300+ playbooks (out-of-the-box) that enable automation of response actions for common use cases.
    - Easily create your own automated playbooks for analysts, or take action based on correlated data and transparent detection insights.
- Most vendors require MSPs/MSSPs to buy many solutions like IDS/IPS, TI and VA data, EDR, NDR etc. Seceon's aiSIEM includes these and integrates with your existing investments.
- Gain superior protection with higher threat coverage. Threat coverage with legacy MSSP vendor tools typically ranges from 20-40 %. With Seceon it can go up to 99.9%.
- Seceon partners benefit from mature onboarding processes, automated deployments and training that jumpstarts their service delivery.



ACCURACY, SPEED, PRIORITIZATION

Gain the edge over adversaries and hackers with Seceon's real-time processing of large amounts of data at speed, combined with behavioral anomalies and threat intelligence to arrive at validated and prioritized threat indicators.

FLEXIBILE LICENSING FOR MSPS AND MSSPSS

Harness the power of flexible 'best-fit' cost and licensing through on-premises, cloud or MSP hosted solution spanning multiple sites – data center and branch offices – with multi-tenancy and data segregation at the core of platform architecture.

Learn more about Seceon aiSIEM and

Schedule a Demo www.seceon.com/contact/