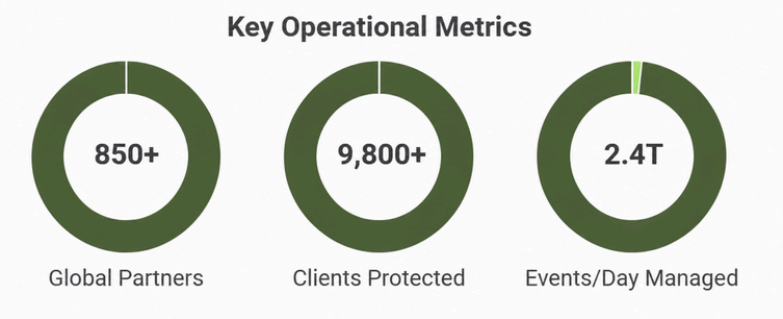
seceon
SECURITY FOR EONS

Open Threat Management Platform

PARTNER-FIRST COMPANY - WE DON'T COMPETE WITH OUR PARTNERS

Unified AI-Powered Cybersecurity Platform

Seceon's Open Threat Management (OTM) Platform delivers unified, AI-powered security operations through a single, integrated platform consolidating SIEM, XDR, SOAR, NDR, UEBA, and OT security. Purpose-built for MSPs, MSSPs, and enterprises, eliminating tool sprawl and delivering superior threat detection.



Core Platform Capabilities:

1. **aiSIEM** - Machine learning-based event correlation and behavioral analytics
2. **aiXDR-PMax** - Unified detection and response for endpoints, networks, and cloud workloads
3. **SOAR 4.0** - Automated orchestration with 100+ prebuilt playbooks, guardrails, and 3,000+ integrations
4. **UEBA** - User and Entity Behavior Analytics to catch insider threats and identity misuse
5. **aiSecOT360** - Visibility, segmentation, and risk management for OT/ICS environments
6. **aiCompliance CMX360 -** Evidence automation across 50+ frameworks, including NIS2, DORA and GDPR
7. **aiSecurityScore360** - 0–1000 posture scoring with fixes ranked by risk reduction
8. **NDR** - Advanced network threat detection with DPI, NetFlow telemetry, anomalies, and lateral movement visibility.
9. **SERA AI & AutoSOC** – AI assistant and multi-agent investigation with evidence-scored verdicts
10. **aiSecurity UIDGuard360 -** Identity threat detection for credential abuse, privilege escalation and directory attacks

Highlights

CUT ALERT NOISE BY 93.9%

At an MSSP partner running 209 customer environments, daily triage queues dropped from 6,447 alerts to 393 in 15 days.

RESOLVE 70% OF INCIDENTS AUTOMATICALLY

Guarded SOAR playbooks resolve 70% of incidents without analyst intervention, with automated response in under 90 seconds.

AI THAT SHOWS ITS EVIDENCE

With SERA AutoSOC, AI agents debate each case, code scores the verdict, and cases with missing data stay open instead of closing.

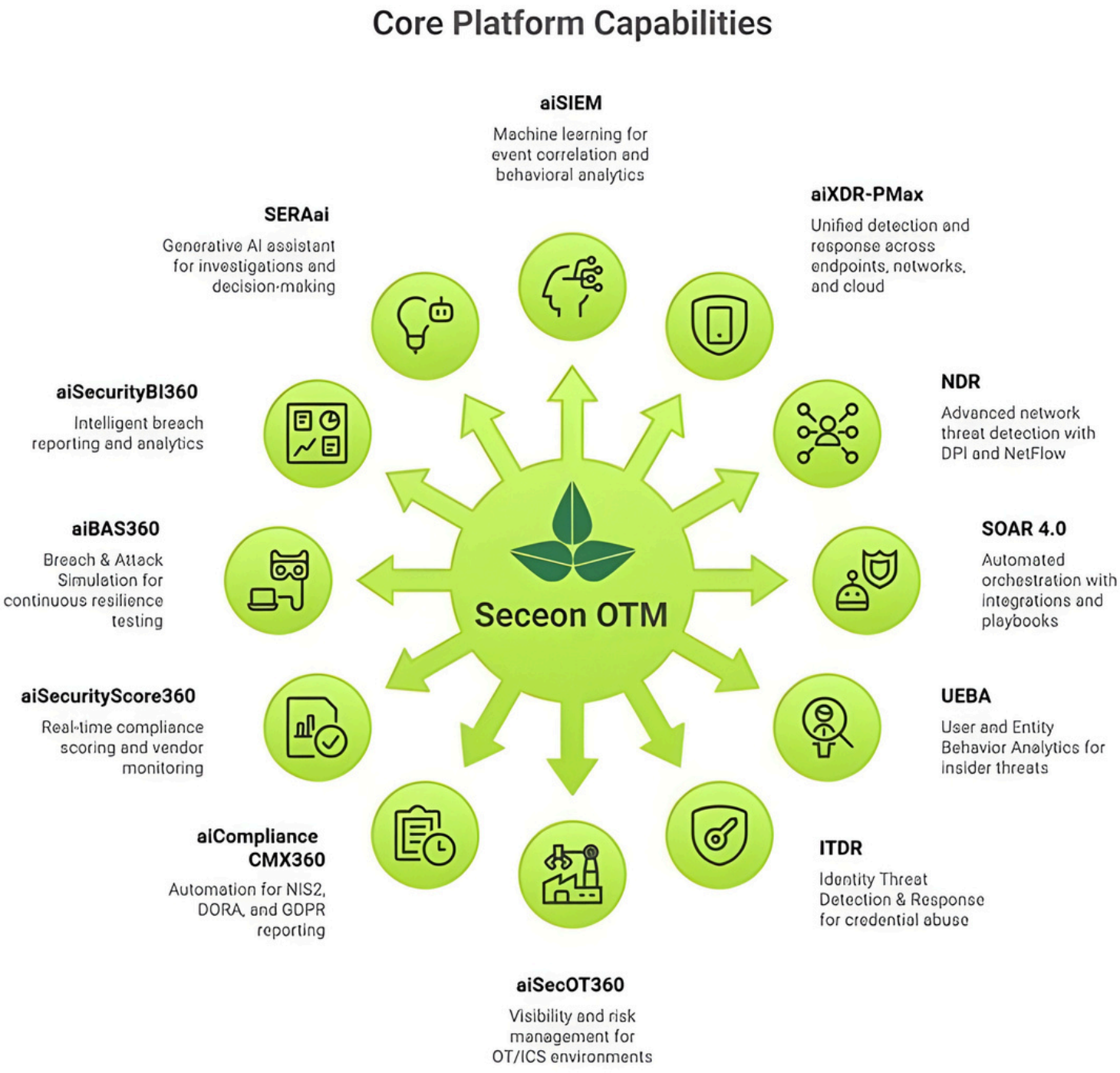
DEPLOY ANYWHERE IN HOURS

Install in about 5 hours on premises, in sovereign or public cloud, hybrid or air-gapped, with full functionality within 2 weeks.

PREDICTABLE COST AT ANY SCALE

Asset-based licensing with no per-GB or per-EPS fees, and multi-tier multi-tenancy for MSSPs.

9. **aiBAS360** - Breach & Attack Simulation to test resilience continuously
10. **aiSecurityBI360** - Intelligent breach reporting, analytics, and executive dashboards
11. **SERAai** – Generative AI assistant that accelerates investigations and decision-making
12. **ITDR** - Identity Threat Detection & Response for credential abuse, privilege escalation, and directory attacks



Market Validation

- **Measured noise reduction:** 93.9% fewer false alarms across 209 MSSP customer environments.
- **Independent assurance:** SOC 2 Type II report and ISO/IEC 27001 certification.
- **Tested coverage:** All 14 tactics and 295 techniques in MITRE ATT&CK v20.0.

Key Platform Differentiators

Feature	Description
Multi-Tier Multi-Tenancy	Enables Master MSSP operations
Unified Architecture	Single data format
False Positive Reduction	95% reduction via AI
MTTD & MTTR	Sub-5 minute detection/response
Automated Response	70% automated response
Asset-Based Licensing	Predictable pricing
Rapid Deployment	5-hour install, 2-week functionality
Single-Analyst Operations	3-5x productivity gains
Unified IT/OT/Cloud	No visibility gaps
Cost Reduction	47-58% cost reduction

Quantified Business Impact:

Seceon's unified AI-driven platform delivers measurable business value through **cost optimization, operational efficiency, and compliance automation**. By replacing multiple tools with a single integrated system, organizations achieve up to **58% licensing savings**, **84% lower integration costs**, and **70% reduction in SOC expenses**. Advanced automation drives **3–5× analyst productivity**, **95% fewer false positives**, and **sub-5-minute detection and response times**. With built-in frameworks like **SOC 2, ISO 27001, NIST, HIPAA, and PCI-DSS**, Seceon enables **90% automated reporting** and **faster audit readiness**, helping enterprises realize **full ROI within 6–9 months** and annual savings of up to **$4.2 million** while strengthening overall security posture.

Quantified Business Impact

$ Cost Optimization

- **47-58% Licensing Savings:** One platform, fewer tools.
- **84% Integration Savings:** No custom connectors.
- **70% SOC Cost Cut:** Automated workflows.
- **Predictable Pricing:** Asset-based model.

Operational Efficiency

- **3-5× Productivity:** Unified interface + automation.
- **95% Fewer False Positives:** AI-driven correlation.
- **<5 Min MTTD:** Real-time detection.
- **70% Auto Response:** Instant incident resolution.

Security Effectiveness

- **Zero Correlation Gaps:** Unified data across all domains
- **Complete Attack Chains:** Seamless event correlation
- **Real-Time Threat Intel:** 70+ integrated sources
- **Behavioral Analytics:** ML-powered UEBA

Compliance Automation

- **90% Auto Reporting:** Framework-ready outputs.
- **2 Hrs vs 2 Weeks:** Rapid audit prep.
- **91% Faster Cycles:** Automated evidence.
- **Multi-Framework:** SOC2, ISO27001, NIST, HIPAA, PCI-DSS.

🎯 ROI Summary

Organizations achieve **full ROI within 6-9 months** through combined cost savings and efficiency gains. Platform delivers **$2.5M-$4.2M annual savings** for mid-to-large enterprises vs. multi-vendor approaches, enabling **5x faster incident response** and **70% reduction in security team overhead**.

Platform Architecture:

Seceon's platform is built on a **modern microservices architecture** engineered for scalability, speed, and resilience. It leverages **Docker containers** for flexible deployment, **Apache Kafka** for high-volume event streaming (2.4T+ events/day), and **Apache Spark** for real-time analytics processing over **250PB/day** with **2M+ operations per second**.

Its **three-tier design CCE (Collection & Enrichment)**, **APE (AI/ML Processing & Correlation)**, and **LTS (Long-Term Storage & Forensics)** ensures seamless data flow from ingestion to analysis and compliance retention.

With **3000+ pre-built integrations**, Seceon connects effortlessly to leading tools across **security (Palo Alto, Fortinet, CrowdStrike)**, **cloud (AWS, Azure, GCP, O365)**, and **identity & ITSM platforms (Active Directory, Okta, ServiceNow, Jira)** delivering unified visibility and zero data silos.

Platform Architecture

Microservices Design

- Docker Containers: Scalable deployment
- Apache Kafka: Event streaming (2.4 T/day)
- Apache Spark: Real-time analytics
- Indexing: OpenSearch
- Persistence: Cassandra

Three-Tier Architecture

- CCE: Data ingestion (3000+ connectors), normalization, enrichment
- APE: Stream processing, AI/ML, correlation, policy
- LTS: 7-year retention, forensics, compliance

🎯 Integration: 3000+ Pre-Built Connectors:

Security: Firewalls (Palo Alto, Cisco, Fortinet), EDR (CrowdStrike, SentinelOne, Defender), SIEM (Splunk, QRadar), Vulnerability (Nessus, Qualys) | Cloud & Identity: AWS, Azure, GCP, O365, Active Directory, Azure AD, Okta, ServiceNow, Jira



Comprehensive Platform Features

Seceon's unified platform delivers end-to-end security intelligence across **SIEM, XDR, SOAR, and OT/ICS** domains. **aiSIEM** provides AI-driven analytics, real-time correlation, and 95% false-positive reduction with 7-year forensic retention and built-in compliance for **SOC 2, ISO 27001, NIST, HIPAA, and PCI-DSS**.

aiXDR extends unified detection and response across IT, OT, Cloud, and Identity—enabling cross-domain threat correlation, automated remediation (70%), and full forensic traceability.

SOAR 4.0 accelerates response with **Generative AI playbooks**, **3000+ integrations**, and self-learning orchestration that executes actions in under 5 seconds.

For **NDR and OT Security, aiSecOT360** delivers passive visibility across Purdue levels 0 to 5 and **117+** industrial protocol profiles, with evidence for NERC CIP and IEC 62443.

Performance Specifications		
Metric	**Specification**	**Impact**
Event Processing	2.4 Trillion/day	Enterprise-scale capacity
Processing Speed	150M events/second	Real-time with sub-second latency
Document Indexing	50 TB/day	Comprehensive forensics
Database Ops	400K ops/second	High-performance persistence

Metric	Specification	Impact
Availability	99.9% uptime	Enterprise reliability
False Positives	95% reduction	vs. traditional SIEM
MTTD	Sub-5 minutes	Automated identification
MTTR	Sub-5 minutes	Automated response
Automation	70% incidents	Fully automated



Unified Data Format — Purpose-Built Architecture

Seceon's platform is **purpose-built from the ground up**, not stitched together from acquired or disconnected tools. At its core lies the **Seceon Event Format (SEF)** - a unified, lossless data model that powers **seamless data flow, real-time correlation, and consistent analytics** across SIEM, XDR, SOAR, and Compliance. Unlike multi-product platforms that rely on several data formats and fragile connectors, SEF stitches pre- and post-NAT tuples, extracts real client addresses and applies defined defaults, so every source indexes cleanly.

This unified design eliminates correlation gaps, enhances visibility, and enables automated responses across IT, OT, and Cloud environments. The result: **3-5x greater analyst productivity**, **90% less integration effort**, and a simplified, high-performance security ecosystem that delivers precision, speed, and scalability from a single platform.

Unified Data Format: Purpose-Built Architecture

❌ "Kludged Together" Platforms

- AI-driven analytics, 95% false positive reduction
- Real-time multi-dimensional correlation
- ML-powered UEBA for users/entities/devices
- 70+ threat intelligence sources
- SOC2, ISO27001, NIST, HIPAA, PCI-DSS compliance
- 7-year retention with forensic search

✅ Seceon's Unified Format

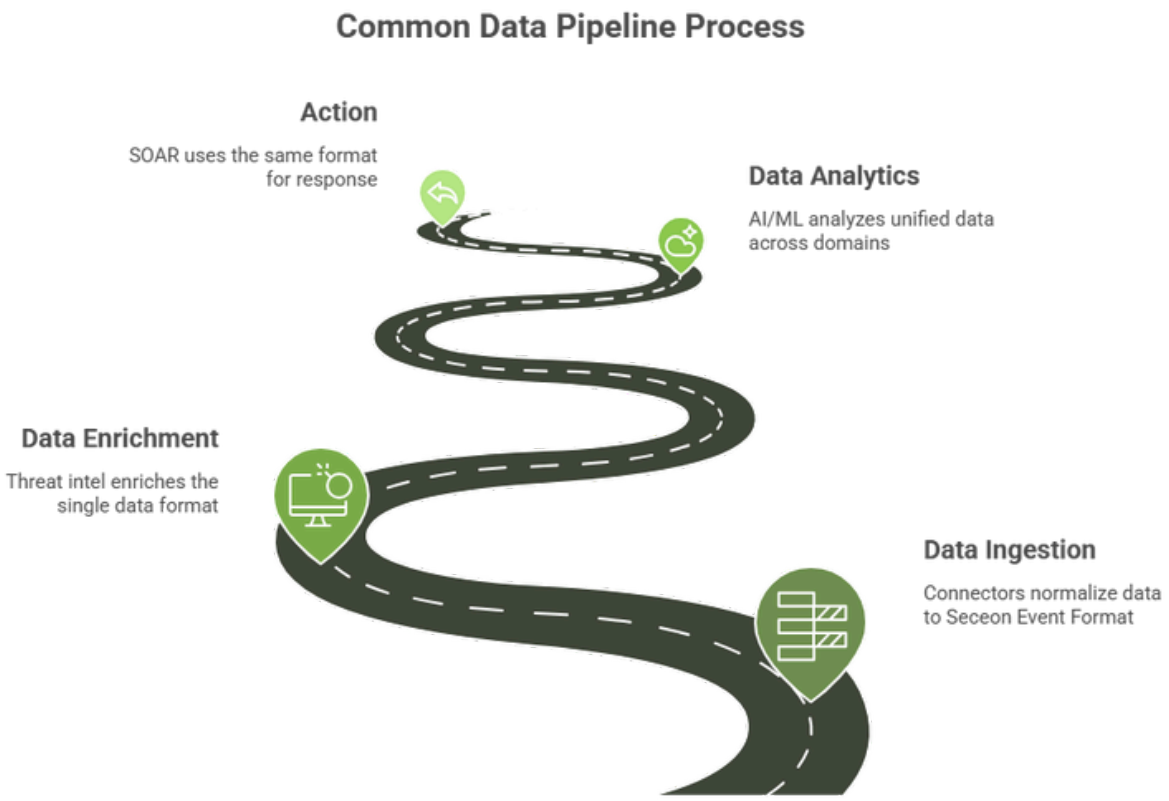
- Single Event Format at ingestion
- Data flows natively across all capabilities
- Perfect fidelity, no information loss
- Real-time correlation across all domains
- Single, consistent UX across platform
- Store once, use everywhere
- One data model to understand
- Unified API for integrations

Common Data Pipeline

Seceon's **Common Data Pipeline** ensures seamless, end-to-end data flow across the entire security lifecycle from collection to automated response - all powered by the **Seceon Event Format (SEF)** for consistent, lossless data handling.

- **Ingestion:** 3000+ connectors normalize logs, flows, and events into the unified Seceon Event Format.
- **Enrichment:** Contextual threat intelligence and metadata are automatically added for deeper insight.
- **Analytics:** Advanced AI/ML models analyze unified data across IT, OT, Cloud, and Identity domains in real time.
- **Action:** SOAR 4.0 executes automated, context-aware responses using the same consistent data format.

One seamless pipeline from data to decision to action, ensuring accuracy, speed, and full visibility across the enterprise.



Flexible Deployment Options

Seceon offers deployment flexibility to fit any operational or compliance requirement on-premises, in a sovereign or public cloud, hybrid, or air-gapped.

- **On-Premises:** Full data control, FIPS 140-3-validated cryptography, and air-gapped support, including data-diode topologies, for regulated or critical environments.
- **Cloud (SaaS):** Rapid deployment with auto-scaling, global reach, and minimal overhead, ideal for MSSPs and distributed enterprises.
- **Hybrid:** Combine on-prem data control with cloud analytics for scalability and compliance-driven flexibility.

Deploy anywhere. Protect everywhere with the same unified AI-driven platform.

Flexible Deployment Options		
Model	**Features**	**Use Cases**
On-Premises	Complete data control, compliance with data residency, customizable hardware, air-gapped support	Regulated industries, government, critical infrastructure, data sovereignty
Cloud (SaaS)	Rapid deployment (hours), automatic scaling, global availability, reduced overhead	MSPs/MSSPs, distributed enterprises, rapid deployment, multi-site operations
Hybrid	Critical data on-premises with cloud analytics, distributed processing, flexible flow	Multi-site enterprises, compliance + cloud benefits, gradual migration



Compliance & Certifications

Seceon simplifies governance and audit readiness with automated evidence collection across 50+ frameworks, including SOC 2, ISO 27001, NIST CSF 2.0, NIST SP 800-53, HIPAA, PCI DSS v4.0, NERC CIP, GDPR, DORA, CMMC 2.0, and FISMA. Seceon itself holds a SOC 2 Type II report and ISO/IEC 27001 certification.

Its built-in compliance engine delivers **90% automated reporting**—reducing preparation time from **2 weeks to just 2 hours**—while maintaining **complete audit trails**, **7-year log retention**, and **real-time compliance monitoring**.

Pre-built dashboards, automated control validation, and multi-framework support enable organizations to maintain continuous compliance across all operational and geographic environments with zero manual overhead.

Compliance & Certifications

Automated Frameworks

- SOC 2 Type II: 90% automated reporting
- ISO 27001: Information security management
- NIST CSF: Identify, Protect, Detect, Respond, Recover
- HIPAA: Healthcare data protection
- PCI-DSS: Payment card security
- NERC CIP: Critical infrastructure
- GDPR: European data privacy
- FISMA: Federal security

Key Features

- 90% automated reporting: 2 hrs vs. 2 weeks
- Complete audit trails and chain of custody
- 7-year log retention with forensic search
- Automated evidence collection
- Real-time compliance monitoring
- Pre-built compliance dashboards
- Automated control validation
- Multi-framework simultaneous support

MSSP Features – Multi-Tier Multi-Tenancy (MTMT)

Seceon's platform is purpose-built for **Managed Security Service Providers (MSSPs)** to scale efficiently through a **true Multi-Tier, Multi-Tenant (MTMT) architecture**. It empowers **Master MSSPs** to manage multiple regional or sub-MSSPs within a single environment ensuring **complete data isolation**, **customized AI/ML threat models**, and **independent operations** for every tenant.

- **Master MSSP Enablement:** Seamlessly manage global, regional, and sub-MSSP structures under one unified platform.
- **Data Isolation:** Every query, index and cache key is tenant-scoped, keeping each customer's data strictly segregated.
- **Per-Tenant AI/ML:** Dedicated behavioral models adapt to each environment for precise threat detection.
- **White-Label Capability:** Deliver branded, high-margin security services with full customization.
- **Centralized Management:** Operate through a unified "single pane of glass" for total visibility and control.
- **Horizontal Scalability:** Effortlessly onboard new tenants without duplication or downtime.
- **Role-Based Access:** Granular permissions for admins, analysts, and end customers.
- **Custom Policy Management:** Configure unique security and compliance policies per tenant with ease.

Seceon's MTMT architecture gives MSSPs the power to scale and differentiate: one MSSP partner alone runs 209 customer environments on a single platform.



Partner Success Team

Seceon's **Partner Success Team** is dedicated to empowering MSSPs and partners with end-to-end technical, operational, and business support. Offering 24×7 follow-the-sun assistance from engineering teams in the USA, EMEA, and APAC with guaranteed SLAs, the team provides dedicated engineers, **regular health checks**, and **performance optimization** to ensure seamless operations. Partners benefit from **implementation guidance**, **architecture consulting**, **custom integration development**, and **continuous software updates** for peak efficiency. In addition,

Seceon delivers **training and certification programs**, **capacity planning**, and **advanced threat-hunting services**, helping partners enhance service quality, expand capabilities, and maximize profitability through a trusted, long-term collaboration.

Partner Success Team

24x7 Technical & Professional Support

- Guaranteed SLAs with priority response
- Dedicated support engineers
- Regular health checks
- Performance optimization
- Software updates & patches
- Capacity planning assistance
- Implementation & deployment
- Architecture design consulting
- Custom integration development
- Training & certification programs
- Managed security services options
- Advanced threat hunting services

About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI- and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 850 partners, Seceon supports more than 9,800 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/



© 2026 Seceon Inc. All rights reserved. aiSIEM and aiXDR are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.