



Seceon aiBAS360

Overview

aiBAS360 is an advanced Breach & Attack Simulation (BAS) platform developed by Seceon to provide continuous, automated threat simulations that emulate real-world cyberattacks. It allows organizations to proactively assess the effectiveness of their security controls and identify gaps across all layers of digital infrastructure.



Key Features

- **Continuous Security Validation** – Real-time assessments instead of periodic testing.
- **Realistic Threat Simulation** – Emulates adversarial TTPs from MITRE ATT&CK.
- **Threat Vectors Simulated** – Phishing, Brute-force attacks (RDP/SSH), Malware infiltration, Lateral movement, Privilege escalation, Data exfiltration.
- **AI-Driven Insights** – Risk scoring, threat prioritization, and automated remediation.
- **Compliance Readiness** – Supports NIST, ISO 27001, PCI-DSS, HIPAA, etc.
- **Seamless Integration** – Unified with aiSIEM and aiXDR platforms.



Global Threat Simulation Examples

1. Lazarus APT (Crypto Theft) – Techniques: T1078, T1190, T1059, T1041
2. Scattered Spider (Retail Ransomware Campaign) – Techniques: T1566, T1219, T1078, T1003
3. Enterprise Honeypots (Brute-Force Attacks) – Techniques: T1110.002, T1110.003
4. APT29 – U.S. Gov Espionage – Techniques: Kerberoasting, LSASS dumping, Pass-the-Ticket



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 Architecture

- Supported OS: Windows (✓), Linux (Upcoming), MAC (Upcoming)
- Deployment: Agent-based installer with Seceon EDR Agent
- Integration Points: aiSIEM, aiXDR, EDR, SOAR, CCE, APE, LTS
- Multi-Tenancy: Tenant-based dashboards and reporting
- Delivery: On-premise, cloud, and hybrid environments



Technical Capabilities

Capability	Details
Automation	Scheduled & trigger-based attack simulation
Real-Time Insights	Dashboard with AI/ML-driven analytics
Visibility	End-to-end kill chain mapping
Custom Dashboards	Tailored views per tenant or business unit
Reporting	PDF/HTML reports, exportable threat drilldown
Licensing	Tiered, usage-based licensing
Compliance Mapping	Supports regulatory reporting across frameworks
Agent Footprint	Lightweight, modular, supports updates & rollback



Beta Innovations

- Installer-Based Setup
- Improved Dashboard Operations
- Multi-Tenant Support
- Roadmap: Full Linux/macOS support, expanded threat library, SOAR integration



Seceon aiBAS360 continuously simulates real-world attacks to validate security posture and prioritize risks with AI-driven insights



Use Cases

- Red Team validation
- Blue Team readiness
- SOC effectiveness measurement
- CISO risk visibility
- Compliance audit trails



Contact & Support

- **Support Portal:** Partner ticketing & documentation
- **Partner Program:** Revenue sharing, certifications, co-marketing
- **Demo & PoC:** Available upon request

Learn more about Seceon



Schedule a Demo

www.seceon.com/contact-us/

