

Seceon aiSIEM vs. Competitors: Comprehensive Comparison

Criteria	Seceon aiSIEM	Trend Micro Vision One	FortiSIEM & FortiSOAR	Wazuh SIEM
Core Focus	AI-powered, unified SIEM, SOAR, and UEBA with real-time automated response	XDR-centric, primarily focused on endpoint security	Modular SIEM & SOAR solution, requires separate licensing	Open-source SIEM with endpoint monitoring
AI & Automation	AI-driven threat detection, contextual analysis capabilities, predictive analytics, self-learning models.	AI-enhanced for endpoints, lacks full network AI analytics	Limited AI capabilities, relies on rule-based detection, Forti AI only assist security teams in making better decisions	Basic anomaly detection, requires manual tuning
Threat Detection & Hunting	AI-driven Continuous monitoring with behavioural analytics, AI-powered anomaly detection	Endpoint-focused threat detection, lacks full-stack visibility across the environment	Rule-based detection with SIEM event correlation. It heavily relies on predefined rules and correlation logic to identify and respond to threats	Requires manual rule configuration, lacks AI-driven insights
Incident Response & Automated Remediation	Built-in SOAR automates response and threat containment in real-time	No SOAR. Integration with Third party SOAR. Focus is on XDR. Focuses on endpoints.	Requires FortiSOAR for full automation	Basic incident response, manual effort needed
UEBA (User & Entity Behaviour Analytics)	Advanced UEBA for detecting insider threats, identity analytics, and privilege misuse	Endpoint-centric UEBA, lacks organization-wide behaviour analysis	Part of the FortiSIEM. Requires additional licensing for UEBA	No built-in UEBA

Integration with 3rd-Party Tools	Pre-built connectors for firewalls, IAM, EDR, cloud security, and ticketing systems. Seceon known for deep integration capabilities	Best integrated with Trend Micro ecosystem, limited third-party support or integration	Works best with Fortinet products, limited external tool support or integration capabilities.	Open-source flexibility but requires significant manual programming and setup
Integration with Custom Applications	Open APIs enable seamless integration with custom applications	Limited to Trend Micro-supported applications	API integration possible but requires additional effort	Open-source API integration, requires expertise
Ease of Customization	Highly flexible with customizable dashboards, reports, and correlation rules	Predefined templates, limited customization options	Complex customization requiring professional services. Which is very expensive	Fully customizable, but needs developer expertise being open source.
Handling of Unparsed Logs	AI-driven log parsing, automatic normalization of unstructured data	Limited ability to handle unstructured data/logs	Requires manual log parsing.	Requires configuration and scripting for non-standard logs
Real-Time Monitoring & Threat Intelligence	Continuous monitoring with real-time threat intelligence feeds & holistic approach ensures comprehensive visibility	Endpoint monitoring with delayed correlation	Monitoring based on predefined rules, not real-time	Requires manual setup for real-time insights
Alert Management	Prioritized alerts with AI-driven context and risk scoring	Generates high alert volumes, lacks smart correlation	Generates numerous false positives without strong filtering	Requires manual alert tuning
Dashboard Customization	Fully customizable, role-based dashboards with	Fixed dashboards, limited	Customization possible but complex	Open-source dashboards, but

	advanced visualization	modifications possible		requires developer effort
Scalability & Deployment Flexibility	Scales for SMBs to large enterprises, deployable on-premises, cloud, hybrid	Best suited for enterprises, primarily cloud-based	Scalable but requires separate purchases for different modules	Best for SMBs, lacks enterprise-wide scalability
Cybersecurity Research & Threat Intelligence	Built-in, AI-driven threat intelligence with continuous updates	Leverages Trend Micro's in-house intelligence	FortiGuard feeds available, requires separate licensing	Open-source threat intelligence, requires manual integration
Cost Efficiency	Transparent asset/log-based pricing, low TCO with AI automation	High per-endpoint cost, expensive for enterprises	Modular pricing increases total cost	Open-source but high operational & maintenance costs
Software Licensing & Data Lake Pricing	Simple licensing with data lake included, no hidden costs	Requires additional costs for data storage	Log retention and storage charges apply separately	Free, but requires dedicated infrastructure and skilled maintenance
API Support	Open APIs for seamless integration with security tools and applications	Limited API support outside Trend Micro ecosystem	Requires additional customization for API connectivity	Open-source API, but requires in-house development
Customer Support & Services	24/7 enterprise-grade support, dedicated account managers for every customer	Slow response times for standard users, premium support require	Support available but customer need to choose priority support or premium support subscription	Community support, optional paid support for enterprises