gruve

SOLUTION BRIEF

AI-driven SOC services

Transform traditional SOC operations by embedding AI Agents into every layer.

01

Executive summary

Modern cyber threats demand speed, precision, and continuous adaptation. Our AI-Driven SOC transforms traditional operations by embedding AI Agents into every layer of the SOC—working as digital team members delivering real-time threat detection, response automation, and intelligence-driven security outcomes.

02

Current challenges in today’s SOCs

Enterprises managing modern cyber operations face several growing challenges:

- **Alert overload & fatigue:** Human analysts are overwhelmed with volume, leading to delays in response.
- **Talent shortage & skill gaps:** Difficulty hiring skilled L1, L2, and threat-hunting experts.
- **Slow response times:** Manual triage, investigation, and correlation cause delays.
- Increasing threat sophistication: AI-powered attacks, fast-moving malware, and identity attacks.
- **Fragmented tooling:** Multiple SIEM, SOAR, EDR, and cloud platforms without unified automation.
- **Pressure from regulators:** Need for traceable, explainable security operations with provable governance.
- **Rising operational costs:** Traditional SOC models scale costs linearly with analysts. Shape

03

Our solution: AI-driven SOC (AI Agents as digital analysts)

We deliver a complete transformation of your SOC by integrating AI Agents that perform analyst duties across the entire lifecycle of threat detection, investigation, response, and reporting:

- **AI-driven SOC implementation:** Deploy AI agents for automatic triage, investigation, threat hunting, intel enrichment, vulnerability prioritization, and SOAR-based automated response across a modern AI-enabled security stack.
- **AI-enhanced SOC operations:** Provide 24/7 AI-assisted SOC operations with real-time detection, AI-led investigations, automated responses, continuous tuning, and proactive threat hunting.
- **AI SOC maturity assessment:** Evaluate current SOC processes, tooling, automation readiness, and AI adoption to produce modernization score, AI roadmap, automation priorities, and next-gen SIEM migration plan

An AI-driven hybrid SOC where 60–80% of repetitive security operations are automated, enabling faster detection, reduced false positives, and improved analyst efficiency and decision-making.

04

What we cover in AI-driven SOC

This section outlines the scope of what is covered in our AI-Driven SOC offering. Key items:

- **AI-powered threat detection:** We strengthen your detection capabilities with ML-based UEBA, insider threat detection, malware/ransomware activity detection, fraud & account compromise, advanced SIEM correlation, and adversary behaviour modelling to identify threats with higher accuracy and lower noise.
- **AI-driven incident response:** Our AI systems perform rapid root-cause analysis, intelligent response decisioning, and automated containment actions to reduce MTTR and minimize business impact.
- **Threat intelligence automation:** We automate IOC analysis, campaign attribution, and threat scoring to provide real-time, context-rich intelligence that enhances detection and response workflows.
- **AI-enhanced governance & reporting:** We deliver explainable AI-driven decisions, regulator-ready audit trails, compliance monitoring (SOC2, ISO 27001, PCI, etc.), and automated daily/weekly reports to simplify compliance and strengthen oversight.
- **AI-based vulnerability & risk management:** Our platform correlates VA scan data, scores and prioritizes risks, and recommends optimal patch strategies to reduce exposure proactively.
- **SOC modernization consulting:** We guide your transition to a next-gen SIEM, build your SOAR automation roadmap, and modernize detection engineering to align your SOC with AI-driven best practices.

05

Why AI-driven SOC

What benefits the client gets from engaging this service, including:

- **Higher SOC maturity:** AI Agents elevate your operations into a modern, proactive, intelligence-driven SOC with stronger detection, automation, and visibility.
- **Faster detection & response:** Organizations achieve up to an 80% reduction in manual triage effort, a 50–60% drop in MTTR, and real-time threat containment powered by SOAR automation.
- **Lower analyst workload:** AI handles repetitive tasks, including correlation, enrichment, and reporting, allowing analysts to focus on higher-value investigations and strategic improvements.
- **Stronger security posture:** AI-driven correlation, behavioural analytics, and continuous monitoring enhance threat visibility, identify risks early, ensure automated compliance, and continuously improve detection accuracy.
- **Reduced false positives:** AI intelligently enriches, and correlates alerts, applies context-aware scoring, and auto-learns from feedback—delivering high-confidence alerts and significantly reducing false positives.
- **Cost optimization:** AI agents scale SOC operations efficiently, enabling higher throughput and capability expansion, also helps to increase the productivity and efficiency without increasing headcount.

06

Why Gruve

We deliver measurable improvements across your security operations, including faster MTTD and MTTR, significant false-positive reduction, and enhanced analyst efficiency through intelligent automation and AI-driven processes:

- **AI-native MSSP expertise:** Our approach blends deep cybersecurity knowledge with advanced AI engineering, scalable data pipelines, and years of experience supporting regulated industries such as BFSI, Healthcare, Government, and Critical Infrastructure.
- **AI Agents purpose-built for SOC workflows:** Our AI agents are custom-trained on MITRE ATT&CK, detection-engineering playbooks, investigation workflows, threat-intelligence frameworks, vulnerability-scoring logic, and SOAR response guidelines—ensuring decision-quality actions at every step of the SOC lifecycle.
- **Human + AI co-managed SOC:** Your analysts gain an AI teammate that works instantly, never fatigues, maintains full consistency, and scales effortlessly without requiring additional hiring—enabling a more resilient, efficient, and future-ready SOC.

07

Kickstart delivery methodology

Sr No	Phase	Purpose	Key activities	Outcomes
1	AI-SOC discovery & requirements workshop	Product overview, understand current SOC maturity, tooling, processes, gaps, and AI adoption readiness	Stakeholder discussions, environment discovery, SOC maturity scoring, tool mapping (SIEM/SOAR/EDR/Cloud), AI-readiness assessment, success criteria definition	Modernization baseline, AI-SOC readiness score, requirements document, transformation roadmap
2	AI-driven SOC design (architecture & automation blueprint)	Design the AI-enabled SOC architecture, workflow automations, AI Agents, and integration strategy	Build AI-SOC architecture diagrams, design data flows, define AI agent roles (triage, investigation, intel, response), define automation use cases, map MITRE ATT&CK coverage	AI-SOC design document, automation blueprint, detection-engineering templates, success KPIs
3	AI Agent deployment & SOC integration	Deploy AI Agents across SIEM, SOAR, EDR, cloud, threat intel pipelines for real-time automation	Configure AI agent connections, deploy models, integrate SIEM/SOAR/UEBA, enable threat intel automation, baseline ingestion, connect to customer workflows	AI-enabled SOC stack deployed, integrated AI agents, operational automation workflows
4	Use case automation & AI playbook engineering	Transform manual SOC processes into automated AI-driven workflows	Build automation playbooks, tune AI decision models, implement L1/L2 triage workflows, run pilot investigations, validate outputs with real data, continuous tuning	Validated automated use cases, stable AI playbooks, improved detection and response accuracy
5	Knowledge transfer, AI governance & operations training	Ensure the customer can operate, govern, and scale the AI-Driven SOC	Hands-on training, AI governance workshops, best practices, runbooks, explainability training, operational checklists, Q&A	Customer can operate & govern AI-SOC, maintain playbooks, tune models; complete documentation
6	30-day AI performance review & SOC optimization	Assess performance, tune AI agents, refine automations, plan scale-up	Review MTTD/MTTR improvements, false-positive reduction, SOC productivity metrics, conduct improvement workshop, update configs/ runbooks	AI-SOC improvement report, optimization plan, roadmap for expansion & next-gen SIEM migration

About Gruve

Gruve partners with leading enterprises to transform data into measurable business impact. Our team brings deep expertise in enterprise data architecture, AI and analytics strategy, cloud modernization, and organizational change. We combine technical rigor with business acumen, ensuring recommendations are both architecturally sound and executable within your organizational constraints. With proven success across financial services, healthcare, manufacturing, and technology sectors, Gruve delivers data and AI solutions that drive growth, efficiency, and competitive advantage.

Contact Gruve to see a live demo and map your audit workflow to continuous monitoring.

Email: sales@gruve.ai
Web: www.gruve.ai