gruve

SOLUTION BRIEF

# AI SOC Managed Service: 24/7 AI-powered security operations

# 01

## Business problem

Building and maintaining an internal 24/7 Security Operations Center requires $2-4 million annually for staffing, technology, and infrastructure—costs that strain budgets while cybersecurity talent shortages make hiring nearly impossible. Organizations with existing SOCs struggle with analyst turnover rates of 30-40%, alert fatigue from investigating thousands of daily alerts, and mean time to respond measured in hours or days rather than minutes.

Traditional managed SOC services provide monitoring but lack the AI-powered automation needed to operate at the speed of modern threats. Basic managed services still rely primarily on human analysts processing alerts manually, creating the same capacity constraints as internal SOCs. Organizations need managed services that leverage AI to deliver faster threat detection, automated investigation, and immediate response—operating at machine speed while maintaining human oversight for critical decisions.

The gap between security requirements and available resources continues widening. Attack timelines compress while defender response times remain static. Compliance requirements intensify while security budgets face constraints. Leadership demands improved security outcomes without proportional budget increases—a challenge only AI-powered managed services can address.

30-40%

analyst turnover rates at organizations with existing SOCs

# 02

## Why now

Cyber threats have fundamentally changed. Adversaries compress attack timelines from days to minutes using AI-powered tools and automated attacks. Manual SOC processes operating on human timescales cannot defend against machine-speed threats. Organizations without AI-powered security operations face exponentially growing risk exposure.

The economics of AI-powered managed SOC services have reached an inflection point. AI automation enables managed security providers to deliver 24/7 coverage with faster response times at costs 40-60% lower than traditional managed services—while exceeding performance of most internal SOCs costing $2-4M annually.

Regulatory frameworks increasingly require 24/7 security monitoring and rapid incident response. SEC cybersecurity disclosure rules, NIS2 Directive, and sector-specific regulations create compliance obligations that organizations cannot meet with 9-5 security operations or slow-responding managed services. AI-powered managed SOCs deliver compliance-ready monitoring, response, and reporting.

The cybersecurity talent shortage shows no improvement trajectory. Organizations cannot build internal SOC capabilities through hiring. Managed services provide immediate access to security expertise, AI agent technology, and operational maturity that would take years and millions to build internally.

Organizations delaying adoption watch competitors deploy AI-powered security operations that detect threats faster, respond more effectively, and operate more efficiently. First-mover advantages in security operations translate directly to reduced breach probability and faster recovery when incidents occur.

40-60%

lower cost with AI automation

# 03

## Solution overview

Gruve's AI SOC Managed Service delivers comprehensive 24/7 security monitoring, threat detection, incident response, and compliance reporting powered by AI agents and delivered by experienced security analysts. We combine autonomous AI investigation capabilities with human expertise to deliver mean time to respond measured in minutes rather than hours—operating at machine speed while maintaining human judgment for critical decisions.

Unlike traditional managed SOC services relying primarily on manual analyst workflows, Gruve leverages AI agents to automate 70-90% of alert triage, investigation, and initial response—enabling our analysts to focus on sophisticated threats, threat hunting, and strategic security improvements. Our hybrid human-AI approach delivers superior outcomes at costs 40-60% below traditional managed services.

| **Gruve's solution components** | **Description** |
|---|---|
| 24/7 AI-powered monitoring | Continuous monitoring across endpoints, network, cloud, applications, and identity systems using AI-enhanced detection algorithms, behavioral analytics, and threat intelligence correlation—delivered through our global SOC operations |
| Automated alert triage & investigation | AI agents automatically process 70-90% of security alerts, performing enrichment, context gathering, root cause analysis, and impact assessment—escalating only validated threats requiring human judgment |
| Rapid incident response | Mean time to respond of 12-15 minutes for priority threats through AI-accelerated investigation and automated containment actions, with 24/7 analyst availability for escalations and complex incidents |
| Proactive threat hunting | Regular threat hunting campaigns leveraging AI recommendations to identify threats bypassing automated detection, with quarterly reports documenting hunting outcomes and security posture improvements |
| Vulnerability management | Continuous vulnerability assessment, risk-based prioritization, patch management coordination, and compensating control recommendations—integrated with threat intelligence for exploit activity |

| Gruve's solution components | Description |
|---|---|
| Compliance reporting | Automated generation of compliance reports for SOC 2, ISO 27001, HIPAA, PCI DSS, GDPR, and sector-specific requirements, including audit trail documentation and incident summaries |
| Security platform management | Ongoing tuning and optimization of SIEM, EDR, firewall, and other security tools, including rule refinement, integration enhancements, and platform upgrades |
| Monthly security briefings | Executive and technical briefings documenting security events, trending analysis, threat landscape updates, and security posture recommendations with leadership-ready reporting |

# 04

## Benefits of Gruve's solution

- **Faster threat detection & response:** Achieve 12-15 minute mean time to respond for priority threats versus hours or days with traditional approaches. AI-powered automation operates at machine speed while maintaining human oversight for critical decisions.
- **Dramatically lower costs:** Access enterprise-grade 24/7 SOC capabilities at 40-60% lower cost than building internal SOC or engaging traditional managed services. Predictable monthly subscription eliminates capital expenses and hiring challenges.
- **Superior coverage:** Gain true 24/7/365 coverage across all time zones without staffing gaps, vacation coverage challenges, or analyst turnover disruption. Our global SOC operations ensure continuous protection.
- **Immediate expertise access:** Leverage team of 300+ certified security professionals including threat hunters, incident responders, malware analysts, and compliance specialists—expertise impossible to build internally.
- **Scalable operations:** Handle 200-300% more alerts without additional costs as AI automation scales effortlessly. Support organization growth without proportional security operations cost increases.
- **Compliance assurance:** Meet regulatory requirements for 24/7 monitoring, rapid response, and comprehensive reporting through automated compliance documentation and audit-ready reports.

# 05

## Service offerings

| Tier | Foundation Managed SOC | Enterprise Managed SOC |
|---|---|---|
| Coverage | Business hours (8×5) with on-call | 24/7/365 global coverage |
| Alert investigation | AI-automated with analyst escalation | Enhanced AI + dedicated analysts |
| Response time SLA | 30 minutes (priority threats) | 12-15 minutes (priority threats) |
| Threat hunting | Quarterly campaigns | Monthly proactive hunting |
| Vulnerability management | Basic assessment | Comprehensive program |
| Platform management | Standard tuning | Advanced optimization |
| Compliance reporting | Standard templates | Custom compliance frameworks |
| Monthly reporting | Executive summary | Detailed technical + executive |
| Account management | Shared AM | Dedicated AM |
| Best for | Mid-market organizations, 24/7 coverage | Enterprise, mission-critical operations |

# 06

## Secure your organization with AI-powered managed SOC

Stop struggling with security analyst shortages, alert fatigue, and slow threat response. Gruve's AI SOC Managed Service delivers enterprise-grade 24/7 security operations at a fraction of internal SOC costs.

Schedule a consultation to discuss your security requirements and receive a customized service proposal. Most engagements begin within 30 days.


**Website:** https://www.gruve.ai/

**Email:** info@gruve.ai