Solution Brief

AHEAD

AHEAD Managed Security Operations Center (SOC)

AHEAD centralizes monitoring, threat detection, and incident triage, allowing organizations to reduce internal workload and focus on core business operations. By leveraging specialized expertise, automation, and scalable security infrastructure, AHEAD detects threats faster, minimizes downtime, and optimizes overall security operations.

Client Challenges

Building a modern SOC is no easy feat, and the barriers are interconnected:

- Budget limitations and operational complexity make it difficult to staff a SOC on a 24x7x365 basis without driving up cost and overhead. Building a SIEM with limited access to essential data and insufficient data sharing is challenging.
- Expanding technical architectures increase the attack surface and the volume of telemetry — making effective detection and response harder to scale.
- Without an enriched SIEM, there are not enough hours in the day to filter, prioritize, and address alerts for remediation. Security costs balloon and pitfalls increase.

OUR SOLUTIONS

SOC Monitoring & Detection:

The AHEAD Managed SOC ingests and monitors your data and feeds with a goal of detection and triaging of events. We escalate investigated cases that warrant additional review by your teams. Our cases provide an analysis of what was found and details to help you make critical decisions on remediation.

Outcomes: Reduced burden of both the workload of monitoring and the fatigue of triaging alerts.

Automated Threat Response

We work with your security teams to automate response actions to commonly escalated cases, reducing the number of "critical" cases. By identifying common cases, we automate response and reduce focus on recurring cases.

Outcomes: Faster, more efficient, and more predictable responses and a large reduction in MTTR.

Managed Endpoint Detection & Response:

Our experts assume operational ownership of your EDR platform via Elastic or Palo Cortex XSIAM. We manage configurations, policies, and agent health while ensuring endpoint alerts are properly integrated into SOC workflows. AHEAD ensures the platform is tuned for accuracy, reducing noise and false positives so analysts are focused on real threats.

Outcomes: Reduced burden of EDR administration; continuously improving endpoint security posture; relieving internal resources of day-to-day EDR operations, and reduced mean time to detection (MTTD).

How We Engage

We use a structured, outcome-focused approach that helps you adopt AI safely, prove value quickly, and scale with confidence.

Onboarding	Knowledge Transition	Build	Testing & Validation
Account provisioning for SOC engineers, environment preparation, and tool deployment	Configuration reviews, escalation path establishment, and policy, process, and procedure training	Deployment and configuration of SOC tooling, complete process documentation, and 24x7 reporting dashboards	Monitoring burn-in, penetration testing, alert and workflow validation, and steady-state managed SOC operations

Why AHEAD?

Cross-Domain Expertise

Unify security across network, data center, cloud, data, and apps, eliminating silos and tool sprawl.

Elastic SIEM and Cortex XSIAM

Gain unified telemetry, advanced analytics, and detection-as-code vs. just basic log aggregation.

Automation and ML-Driven Ops

Reduce false positives, compress triage time, and achieve market-leading MTTR and automatic resolution rates.

People-Led, Co-Managed Model

Augment your teams with AHEAD's 24x7 Investigation and Response teams, Threat Intelligence and Solution Management, and a dedicated Service Account Manager.

Modular Services

Consume SOC, MDR, vulnerability management, and broader managed security capabilities individually or as a bundled platform.

Work with Us

Contact AHEAD today to schedule a discovery workshop, improve SOC operational efficiency, and fine-tune your security posture.

AHEAD

Accelerate Your Impact

Learn more at
www.ahead.com