

CASE STUDY

AI Strategy & Roadmap for SOC Optimization

Turning ad-hoc AI exploration into a clear, ROI-driven roadmap for a centralized Security Operations Center.

Client Overview: Centralized SOC Application Onboarding

A large service provider operating a centralized Security Operations Center (SOC) was responsible for onboarding new applications into its monitoring ecosystem. A critical component of this process involved log ingestion and parsing to enable effective monitoring, alerting, and incident response.

Client Situation: Scaling Log Ingestion & Parsing

The organization faced increasing complexity in onboarding applications due to the volume and variability of log data. While processes were functional, they lacked a clear strategic approach to improving efficiency and scalability.

Key challenges included

- Fragmented workflows across onboarding stages with limited end-to-end visibility
- Inconsistent parsing coverage leading to potential monitoring gaps
- Reactive handling of log changes and data inconsistencies
- Limited clarity on where AI could drive the most value within the process

Despite recognizing AI's potential, the organization lacked a structured strategy and roadmap to guide investments and prioritization.



Our Approach: AI Strategy & Roadmap

Positioning

Launching AI without a clear strategy and roadmap often results in stalled initiatives and wasted investment. Our AI Strategy & Roadmap service provided a structured, outcome-driven approach that defines where AI would create the most value, aligning stakeholders on a clear direction, preparing the data foundation, and outlining the steps required to achieve measurable business results.

What We Did

Discover

Identified high-impact AI use cases across the SOC onboarding and log parsing lifecycle

Prioritise

Ranked opportunities based on ROI, feasibility, and speed to value

Align

United stakeholders on a clear AI vision and roadmap for SOC optimization

Measure

Defined measurable success metrics and business outcomes, including onboarding efficiency, data quality, and coverage visibility

Plan

Created a phased roadmap outlining how AI initiatives should evolve over time

Deliverables



AI Strategy Deck

Vision, goals, and roadmap for SOC AI adoption.



Use Case Opportunity Map

AI opportunities across the log parsing lifecycle.



ROI & Value Hypotheses

Quantifying the expected business impact.



Phased AI Roadmap

Aligned to business priorities and readiness.

Outcome

The organization gained a clear, business-aligned AI roadmap focused on measurable results, enabling them to:

- ✓ Focus AI investments on high-value opportunities within SOC operations
- ✓ Build a structured path toward improved efficiency, visibility, and data quality
- ✓ Establish alignment across stakeholders on AI priorities and direction
- ✓ Transition from ad hoc AI exploration to a strategic, ROI-driven approach

Conclusion

By defining a clear AI strategy and roadmap, the service provider established a strong foundation for leveraging AI within SOC operations, ensuring that future investments are targeted, measurable, and aligned with business objectives, rather than driven by experimentation alone.

