Operationalizing AI in Security

AI can improve speed, consistency, visibility, and decision support across security operations, but technology alone does not create better outcomes. Organizations that get the most value from AI are usually the ones that do the foundational work early: understanding the problem, strengthening the operating model, and defining how AI will function across the broader security environment.

This is not a wait-and-see moment. Security leaders cannot afford to spend the next year watching how others use AI. The better path is to move now with discipline: build the right foundation, identify where AI can create operational value, and integrate it in ways that strengthen operations, support human judgment, and align with the organization's governance expectations.

A Practical 5-Part Model

1. Assess the Current State
Start by evaluating the problem to be solved. Review the workflows involved, current performance gaps, documentation quality, decision points, system dependencies, and adjacent stakeholders. The goal is to understand whether the challenge is truly a technology issue, a process issue, an integration issue, or some combination of the three.

2. Strengthen the Operating Foundation
Before introducing AI, review and update the surrounding processes and procedures. This includes escalation paths, documentation standards, governance expectations, operating rhythms, and the policies that shape how work is performed. AI delivers the greatest value when it is built on a sound operational base.

3. Define the Integration Model
Determine where AI fits across the broader security environment. Consider how it may affect intake, investigations, reporting, intelligence, training, Legal, HR, Compliance, and executive decision support. The value of AI is rarely limited to one isolated task. It is often greatest when AI supports connected workflows across systems and functions. This is also the stage where organizations should evaluate and choose the AI solution that best fits the use case, operating model, integration requirements, and governance expectations.

4. Test with Humans in the Loop
Pilot use cases in structured phases with users across different levels of technical comfort and security expertise. This helps refine workflows, thresholds, usability, training needs, and escalation expectations while preserving the role of human judgment in decision-making.

5. Implement with Governance and Iteration
Roll out in stages, build in clear guardrails, monitor performance, and adjust based on user behavior, operational results, and enterprise risk considerations. Governance should not be added later. It should be part of the operating model from the start.

Turning AI Strategy Into Operational Value

What This Approach Helps Organizations Do

A disciplined approach to AI in security helps organizations move beyond experimentation and toward practical, sustainable results. Rather than treating AI as a standalone solution or a quick technology fix, this approach helps leaders evaluate where AI can genuinely improve outcomes, where foundational work is still needed, and how to introduce new capabilities without creating unnecessary operational, legal, or governance risk.

By taking this path, organizations can:

- Clarify where AI can create real operational value
- Improve readiness before investing in tools
- Reduce implementation friction and avoid unintended gaps
- Preserve human oversight and decision quality
- Strengthen integration across workflows, systems, and stakeholder groups
- Build a more defensible, scalable, and business-aligned capability

In other words, this approach helps organizations make better decisions before deployment, implement more effectively, and build AI-enabled security programs that are positioned to deliver value over time.

The Key Principle:

AI delivers the greatest value when paired with strong security foundations, clear workflows, and practical governance.

Organizations that get the most value from AI are not necessarily the ones that move first. They are the ones that build the right foundation, identify the right use cases, and operationalize AI with discipline.

MEET THE CSA EXPERT

Matthew Logan, Senior Advisor, CSA

Matthew Logan is a Senior Advisor specializing in AI-enabled security advisory services. He brings nearly 20 years of experience leading work across enterprise investigations, asset protection strategy, intelligence, and operations within large, complex organizations. His background includes aligning security, investigations, and operational risk programs with broader business strategy, governance, and execution.

About CSA's Approach

CSA helps organizations evaluate where AI can support security operations, investigations, intelligence, and related business functions in a practical, governed, and business-aligned way. Our focus is not on adopting technology for its own sake, but on helping clients build AI-enabled security capabilities that are operationally sound, strategically aligned, and positioned for long-term value.