CyberSagacity

ARTIFACT № 1 · POSITIONING PAPER

AI & APPLICATION SECURITY

# AI is accelerating application security risk.

CyberSagacity enables secure AI development through validated security telemetry — turning fragmented findings into decision-grade intelligence for the leaders who answer for it.


PUBLISHED
April 2026

AUDIENCE
CISO · AppSec · Engineering Leadership

READING TIME
8 minutes

EXECUTIVE SUMMARY

# Application security risk is scaling faster than organizations can evaluate and manage it.

AI-generated code is transforming software development — dramatically increasing speed, scale, and accessibility. Modern environments now routinely use open source, large language models, code assistants, and automated refactoring tools at a pace that far exceeds traditional workflows.

AI systems do not inherently produce secure code. They replicate patterns from training data — often including insecure implementations, outdated libraries, intentional vulnerabilities, and flawed architectural assumptions. The result is a new class of risk: rapidly increasing volumes of code, hidden non-obvious vulnerabilities, misaligned severity and exploitability signals, and expanding attack surfaces across APIs, microservices, and distributed systems.

## What is required is not more security tools. It is better intelligence.

CyberSagacity introduces an **Application Security Telemetry Intelligence Layer** that works alongside AI and development workflows to validate, normalize, and prioritize security signals before they drive decisions, automation, or remediation.

THE DIFFERENTIATOR

In an environment where AI is accelerating both innovation and risk, the differentiator is no longer how much security data you have — but how much of it you can trust.

THE REALITY

# Software is being built faster than it can be secured.

AI-assisted development is the most significant productivity shift since cloud computing. But speed without assurance creates structural risk.

## 01 Code volume amplifies risk

AI enables larger codebases, more complex architectures, increased reuse of components, and rapid expansion of APIs and microservices. More code does not just increase functionality — it increases the probability and density of exploitable defects.

## 02 AI “slop” introduces high-impact defects

AI-generated code rarely fails syntactically. Instead it introduces:

- Misapplied design patterns and library use
- Hidden logic flaws and injection pathways
- Insecure default configurations

## 03 AI lacks security and business context

AI coding engines are pattern imitators, not security optimizers. They do not understand exploitability in real-world environments, account for compliance requirements, model business or financial exposure, or evaluate architectural risk.

## 04 “Good enough” creates systemic risk

AI-generated code often appears correct and well-structured, producing reduced scrutiny, over-reliance on automation, and the assumption that working code is secure code. False confidence is one of the most critical risks introduced by AI-driven development.

BACKGROUND · THE CORE PROBLEM

# AI amplifies the quality of the data it consumes.

AI does not solve the AppSec problem. It amplifies it.

If security telemetry is noisy, misclassified, incomplete, or lacking context, then AI-driven remediation, prioritization, and automation will fix the wrong issues, ignore real exposure, scale incorrect decisions, and increase technical debt.

## AI will either scale clarity — or confusion.

**Modern AppSec stacks are built around detection, orchestration, and visualization:**

- **AST** tools detect defects · **ASOC** platforms coordinate workflows · **ASPM** tools visualize posture · **RBVM** platforms reprioritize vulnerabilities

All of these systems depend on one thing: **security telemetry**. Yet that telemetry is frequently inconsistent across tools, duplicated and conflicting, misaligned with exploitability, and lacking business context.

A NEW ARCHITECTURAL LAYER

Application Security Telemetry Intelligence — validating defect accuracy, identifying tool bias and coverage gaps, normalizing findings by exploitability and policy, and producing decision-grade telemetry.

CYBERSAGACITY'S ROLE

# From raw findings to defensible intelligence.

CyberSagacity transforms fragmented AppSec data into a trusted foundation for decision-making and automation.

### Signal validation

Eliminate false positives and correct misclassification before they propagate downstream.

### Coverage intelligence

Identify blind spots and optimize tool effectiveness across your AppSec stack.

### Risk normalization

Align findings to exploitability, business impact, and policy — not vendor severity defaults.

### Decision-grade outputs

Provide structured, defensible intelligence for leadership and automation alike.

**WITHOUT CYBERSAGACITY**

- AI amplifies noisy, inconsistent signals
- Developers fix low-value or incorrect findings
- Critical vulnerabilities remain hidden
- Security becomes a bottleneck — or an illusion

**WITH CYBERSAGACITY**

- AI operates on validated, high-integrity telemetry
- Remediation focuses on true exposure
- Developer effort aligns with actual risk reduction
- Security becomes faster, more accurate, and measurable

STRATEGIC IMPACT

# The choice in front of every regulated organization.

Organizations that rely on unvalidated telemetry will scale uncertainty, inefficiency, and exposure. Those that establish a foundation of validated, decision-grade intelligence will move faster, operate more efficiently, and reduce real risk with confidence.

**AI WITHOUT VALIDATED TELEMETRY**

- Increased security noise
- Rising technical debt
- Misaligned remediation effort
- Reduced confidence in security decisions

**AI WITH CYBERSAGACITY**

- Faster, safer software delivery
- Measurable risk reduction
- Improved engineering productivity
- Defensible, board-level security insight

> **The future of AppSec is not more detection. It is decision-grade intelligence built on validated telemetry.**

TAKE THE NEXT STEP

# Make your AppSec data audit-defensible.

If AI is accelerating your development, it is accelerating your risk surface in equal measure. The organizations that out-deliver and out-defend in the next 18 months are the ones building on validated, decision-grade telemetry today.

See how CyberSagacity establishes that foundation in your environment.

LEARN MORE

**www.cybersagacity.com**



INFO@CYBERSAGACITY.COM