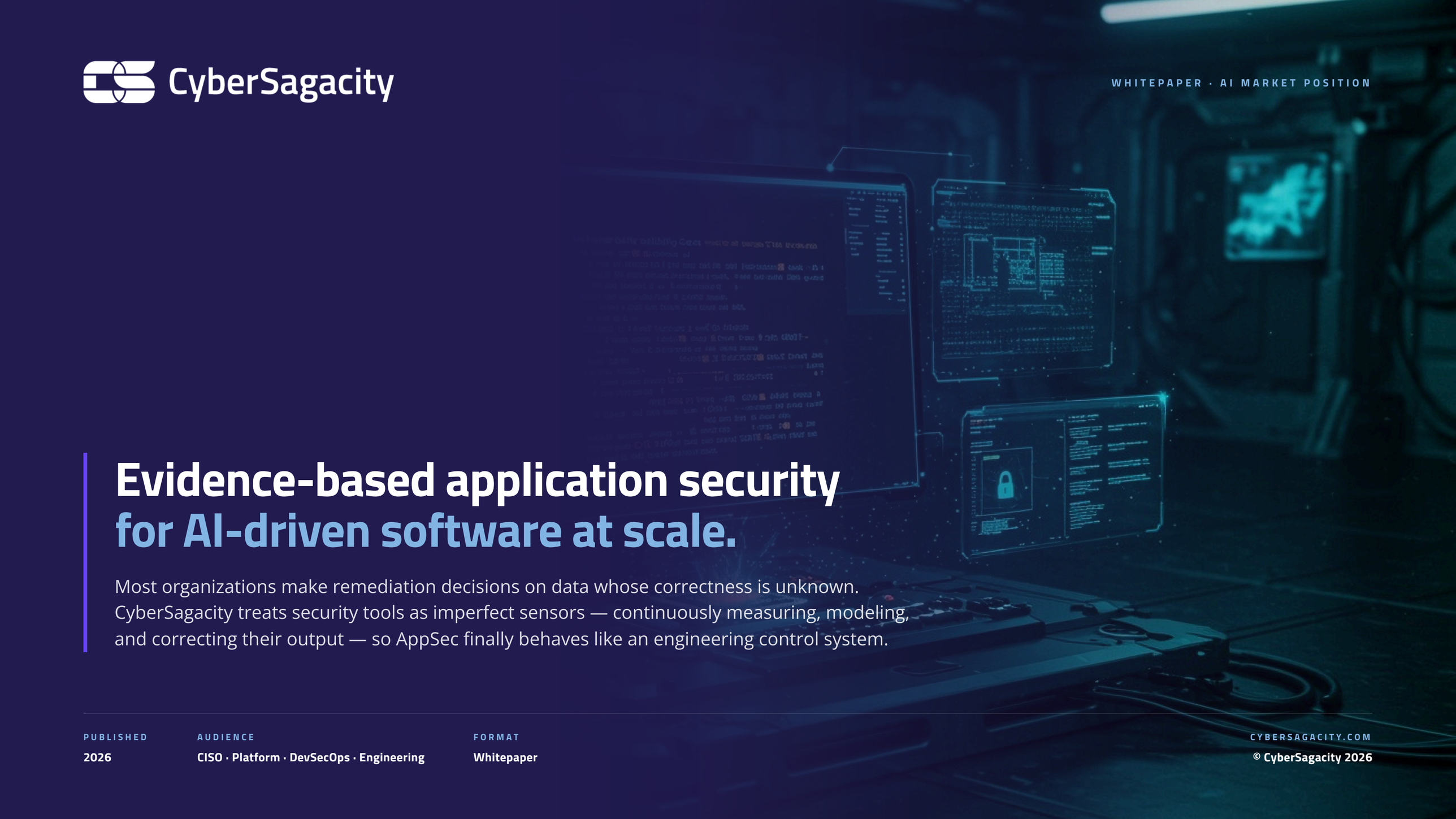
CyberSagacity



Evidence-based application security for AI-driven software at scale.

Most organizations make remediation decisions on data whose correctness is unknown. CyberSagacity treats security tools as imperfect sensors — continuously measuring, modeling, and correcting their output — so AppSec finally behaves like an engineering control system.

PUBLISHED
2026

AUDIENCE
CISO · Platform · DevSecOps · Engineering

FORMAT
Whitepaper

CYBERSAGACITY.COM

EXECUTIVE SUMMARY

Most organizations decide on data whose correctness is unknown.

Tool-generated severity scores are heuristic, inconsistent across vendors, statistically unvalidated, and largely uncorrelated with real exploit behavior.

Yet they're consumed as reliable telemetry — without the basic properties of any production measurement system: accuracy, calibration, known error rates, drift detection, or feedback control.

As AI accelerates code production, the defect amplifies — and **perceived security diverges steadily from actual security**. This is not a tooling problem. It is a control failure.

THE CORE PROBLEM

Security signal with no measurable correctness.

01

Low accuracy

Severity labels and risk scores are largely heuristic, inconsistent across tools, and frequently wrong.

02

No statistical grounding

No measurement of confidence, error rate, false positives, false negatives, or classification drift over time.

03

No exploit or path context

Findings are evaluated in isolation — not by how they combine into real attack paths.

04

No engineering/business alignment

Data isn't mapped to service criticality, revenue impact, regulatory exposure, or operational risk.

Teams chase the wrong issues, real risk accumulates unnoticed, and security becomes theater rather than control.

WE DON'T REPLACE SCANNERS — WE MAKE THEM MEASURABLE

Treat tools as heterogeneous, imperfect sensors.

Rather than assuming tool output is valid, CyberSagacity continuously measures, models, and corrects it:

- Measures classification accuracy, bias, and false positive/negative rates at scale.
- Detects **drift** as rule sets, codebases, and attacker behavior evolve.
- Normalizes and corrects misclassification across tools and versions.
- Correlates findings across services, time, and execution environments.
- Models exploitability and failure propagation in distributed architectures.

APPSEC AS AN ENGINEERING CONTROL SYSTEM

This converts AppSec from alert generation into a monitored, measurable, correctable system — with the properties any control system requires:

Observability **Calibration** **Explainability** **Continuous improvement**

WHAT CYBERSAGACITY DOES

Evidence-based security, not opinion-based.

01

Ground-truth accuracy

Statistically validates classifications against large-scale empirical datasets — detecting misclassification, measuring confidence and uncertainty, and correcting systemic bias across tools and rule sets.

02

Risk that reflects reality

Computes risk from technical exploitability, attack-path formation, asset and service criticality, data sensitivity, and business impact — a ranked, defensible order, not just High/Med/Low.

03

Integration into engineering

Output built for CI/CD pipelines, engineering backlogs, reliability reviews, and board reporting. The goal is not more dashboards — it's better decisions.

It produces data whose correctness can be evaluated, trusted, and acted upon.

WHY THIS MATTERS IN AN AI-ACCELERATED SDLC

Faster development must not mean blind development.

As AI accelerates code generation:

- Defect volume increases faster than human review can scale.
- New defect patterns emerge that tools lag in recognizing.
- Confidence in security posture becomes harder, not easier, to justify.

CyberSagacity provides a stabilizing control layer:

- Measuring what tools miss, mislabel, or misunderstand.
- Keeping security decisions accurate, explainable, and auditable.
- Preserving trust in automated development processes.

THE SHIFT

Scale development velocity — including AI-driven development — without scaling unobserved risk.

VALUE TO A LARGE ENGINEERING ORGANIZATION

Application security as an engineering discipline.

ENGINEERS

Less wasted effort

Fewer false positives, clear and credible prioritization, and reduced wasted effort.

DEVSECOPS & PLATFORM

Defensible posture

Measurable risk reduction, a defensible security posture, and early detection of systemic risk.

THE BUSINESS

Outcomes that count

Lower breach probability, reduced regulatory exposure, and security investment tied to real outcomes.

CONCLUSION

The intelligence layer that makes application security accurate, measurable, and economically rational — so organizations move fast without losing control.