CyberSagacity

APPLICATION SECURITY, PROVEN

THE APPSEC REALITY

Modern software organizations run dozens of application security tools across the SDLC. Instead of producing control, they often produce entropy:

- Tens of thousands of findings with inconsistent and often incorrect severity
- High rates of false positives, false negatives, and duplicate findings
- No defensible method to determine which defects actually matter
- No reliable linkage between vulnerabilities, exploitability, business impact, or financial risk

This is not a tooling problem. It is a measurement, control, and intelligence Problem

DESIGNED FOR MODERN SOFTWARE DEVELOPMENT ENVIRONMENTS

As AI, open-source adoption, code reuse, and development velocity continue to increase, application architectures grow more complex and change more frequently. Traditional AppSec approaches struggle to maintain accuracy, coverage, and prioritization at scale.

CyberSagacity provides the control and intelligence layer required for modern software development:

- Measures AppSec tool effectiveness as code volume, reuse, and dependency sprawl expand
- Identifies where inherited, third-party, and generated code introduces material risk, beyond raw findings
- Maintains correct prioritization as applications, architectures, and exposure evolve

CyberSagacity enables development at scale while preserving trustworthy, outcome-driven security decisions.

SATraits™

QUANTIFY ACCURACY. REVEAL COVERAGE. OPTIMIZE TOOLS.

WHAT SATRAITS DOES

SATraits quantitatively measures the effectiveness of your application security tools by analyzing detection accuracy, rates, and coverage.

KEY CAPABILITIES

- Measures real vulnerability detection coverage across AST tools
- Identifies false positives, false negatives, and misclassifications
- Exposes tool overlap and blind spots
- Provides objective performance benchmarks

WHY IT MATTERS

- Eliminates redundant tools and wasted spend
- Improves signal-to-noise for engineering
- Establishes empirical foundation for strategy

OUTCOME

A defensible, measurable foundation for AppSec decisions — based on evidence, not vendor claims.

SATriage™

PRIORITIZE WHAT MATTERS. QUANTIFY REAL RISK.

WHAT SATRIAGE DOES

SATriage transforms raw tool output into a ranked, risk-based remediation plan by correcting severity, modeling exploitability, and quantifying impact.

KEY CAPABILITIES

- Corrects severity, CWE, and exploitability errors
- Ranks vulnerabilities 1-to-N by true risk
- Maps defects to NIST, SSDF, CMMC, PCI, HIPAA
- Quantifies financial loss exposure & remediatio ROI

WHY IT MATTERS

- Engineers focus on the 3–5% of defects that materially reduce risk
- Security teams gain measurable outcomes
- Leadership gains clarity on ROI

OUTCOME

Clear priorities, measurable risk reduction, and provable security impact.

WHY CYBERSAGACITY IS DIFFERENT

Actionable Risk Intelligence

Quantified risk per defect

Ground-Truth Accuracy

Validated findings across tools

Guided Path Prioritization

True 1-to-N fix order

Common Language

One view for every team

CyberSagacity

www.cybersagacity.com

Fix what matters. Ignore what doesn't. Prove the outcome.

Application Security, Proven.