CyberSagacity

POSITIONING BRIEF

Beyond the OWASP Benchmark. Evidence-based AppSec.

The OWASP Benchmark scores tool behavior against synthetic test cases. CyberSagacity measures real-world application risk, accuracy, and business impact. They are not alternatives — they operate at different layers.

PUBLISHED
2025

AUDIENCE
AppSec · Engineering · Security Leadership

FORMAT
Positioning Brief

CYBERSAGACITY.COM

OVERVIEW

Two tools. Two fundamentally different problems.

The OWASP Benchmark evaluates tool behavior against synthetic test cases. CyberSagacity evaluates real-world application risk, accuracy, and business impact.

Both have a place — but they answer different questions, at different layers of an application security program. This brief clarifies scope, design intent, and the methodological differences that separate a lab benchmark from enterprise risk intelligence.

WHAT EACH IS

A synthetic test harness — versus an intelligence platform.

OWASP Benchmark

Open-source SAST test suite · thousands of synthetic, intentionally vulnerable Java snippets

- Synthetic test harness — **not production code**.
- Language-limited (primarily Java).
- Focus: pattern recognition — does a tool find seeded defects.
- Metric: recall / precision against known injected flaws.
- **Strength:** a consistent baseline to tune SAST rule sets.
- **Limit:** no real-world prevalence, exploitability, or financial risk.

CyberSagacity · SATraits™ / SATriage™

Application Security Intelligence across real apps, pipelines & release cycles

- Evidence-based defect validation — **not synthetic scoring**.
- Language-, framework-, and tool-agnostic.
- Focus: accuracy, prioritization, business-risk context, compliance.
- Metric: statistical correlation, probability-of-validity, financial exposure.
- Ingests SAST, DAST, SCA, IAST, MAST, PenTest & cloud tools.
- Guides teams to the defects most likely to be **real and impactful**.

METHODOLOGY CONTRAST

Lab benchmarking vs. enterprise risk intelligence.

	OWASP Benchmark	CyberSagacity · SATraits / SATriage
Purpose	Score SAST tools on synthetic test cases.	Measure real-world accuracy, risk, and business impact.
Data source	Injected flaws in a test harness.	Actual AST outputs + statistical correction + historical defect data.
Scope	Narrow: code-pattern detection.	Broad: technical, operational, regulatory, and financial risk.
Output	Precision / recall.	Validated defects, prioritization, financial-loss modeling, compliance mapping.
Environment	Synthetic.	Real application + pipeline context.
Decision support	Engineering benchmarking.	Enterprise risk, governance, and ROI decisions.

WHY OWASP DOES NOT MEASURE RISK

It measures detection in a lab — not risk exposure in an enterprise.

OWASP evaluates whether a SAST tool “finds a known bug.” It does not evaluate:

- Actual exploitability in production.
- Severity inflation or deflation.
- False negative probability & false positive bias.
- Business impact, loss potential, or compliance exposure.
- Multi-tool correlation & operational prioritization.

The missing middle layer. Today's AST tools — individually or collectively — lack:

- Reliable accuracy (high FP/FN; inconsistent labeling).
- Consistent severity scoring across tools.
- Cross-tool correlation (overlap often **<1%**).
- Business-aligned prioritization.
- Outcome-based risk quantification.

THE STRUCTURAL GAP

Organizations need a corrective intelligence layer that sits above AST tools — one OWASP was never designed to provide.

HOW CYBERSAGACITY PROVIDES THE INTELLIGENCE LAYER OWASP CANNOT

Five things a benchmark can never do.

A

Correct & validate defects

Models trained on 35M+ defects and 60k+ rules flag false positives, false negatives, misclassified severity, duplicates, and overlap across tools.

B

Correlate across tools & context

Ingests SAST, DAST, SCA, MAST, IAST, PenTest & cloud simultaneously; maps to consistent SATraits categories and resolves contradictory dashboards.

C

Prioritize by technical + business impact

Outcome-driven scoring: exploitability, operational impact, data sensitivity, microservice placement, breach patterns, compliance severity, financial loss.

D

Quantify risk in financial terms

Monetary exposure curves per defect and application, remediation ROI, budget optimization, and compliance justification.

E

Align to governance

Maps to NIST SSDF, PCI, HIPAA, CMMC 2.0, FFIEC, FedNow, SOC 2, and ISO 27001 — evidence and auditability no synthetic benchmark offers.

CONCLUSION

Useful for testing tools. Essential for understanding risk.

The OWASP Benchmark is useful for testing tools in isolation. CyberSagacity is essential for understanding risk in production. They are not alternatives — they operate at different layers.

- **OWASP** — a SAST rule-quality test suite.
- **CyberSagacity** — enterprise-wide AppSec intelligence: accuracy, correlation, prioritization, and financial risk modeling.

THE BOTTOM LINE

CyberSagacity solves the problems OWASP was never designed to address.

Learn more at www.cybersagacity.com →