

Why CyberSagacity will replace ASOC and ASPM.

ASOC and ASPM added integration and visibility — but inherited the weaknesses of the tools they orchestrate. A new model for Application Security Intelligence: validated data, quantified risk, and ROI you can prove.

EXECUTIVE SUMMARY

The AppSec industry has reached a tipping point.

Despite billions spent on Application Security Testing, organizations remain overwhelmed by flawed scan data, false positives, blind spots, and metrics disconnected from real business risk.

ASOC and ASPM platforms were built to add integration and visibility — but they fundamentally inherit the weaknesses of the tools they orchestrate, accepting unverified scan results as truth and producing dashboards without confidence.

CyberSagacity was built to break that cycle — replacing aggregation with precision analytics, so organizations can trust their data, prioritize what matters, and justify every AppSec dollar with evidence.



INTRODUCTION

Orchestration and posture management inherit the data problem they sit on.

Application Security Testing is foundational to modern software development — yet the tools and processes that support it have not kept pace with the scale, complexity, or business impact of modern software risk.

ASOC and ASPM were created to bridge gaps and add visibility. But they share one fundamental limitation: they rely on the availability, accuracy, and quality of the underlying AST scan data.

The result is predictable: **noise instead of insight**, high cost with little verified value, and a continued inability to prioritize and quantify real-world risk.

CyberSagacity does not accept scan output as truth. It transforms raw scan data into validated, prioritized, business-aligned intelligence.

ASOC · APPLICATION SECURITY ORCHESTRATION & CORRELATION

Built to integrate and automate AST tools — not to verify them.

ASOC tools integrate, orchestrate, and automate the execution of SAST, DAST, SCA, and related AST tools, normalizing and correlating results across scanning products to reduce workflow friction.

Strengths	Key Limitations
<ul style="list-style-type: none"> • Unifies and manages outputs from SAST, DAST, SCA, and other scanning tools. • Consolidates and deduplicates findings to reduce manual triage. • Automates workflow steps across development pipelines and security processes. • Improves operational efficiency and remediation responsiveness. 	<ul style="list-style-type: none"> ○ Garbage in = garbage out: accepts tool results as-is and does not verify accuracy. ○ No data correction: false positives, false negatives, and labeling inconsistencies remain. ○ Limited risk context: workflow efficiency improves, but meaningful risk insight does not. ○ Added complexity: orchestration layers without better foundational signal quality.

ASOC improves throughput and logistics — but not confidence, accuracy, or risk outcomes.

ASPM · APPLICATION SECURITY POSTURE MANAGEMENT

Visibility and governance across the stack — but not correctness.

ASPM expands beyond orchestration to provide governance and visibility across security activities, tools, and software assets, helping organizations track their overall posture over time.

Strengths	Key Limitations
<ul style="list-style-type: none"> ● Centralized visibility across applications, teams, and AST tools. ● Maps vulnerabilities to business units, compliance controls, and policies. ● Detects systemic gaps in coverage, process, and tool utilization. ● Supports governance, inventory, and executive reporting needs. 	<ul style="list-style-type: none"> ○ Dependent on scanner accuracy: correlates data without correcting flaws in it. ○ High operational overhead: needs substantial integration and process maturity. ○ More management layers: adds dashboards, not reliability or validated risk reduction. ○ No ROI or real risk quantification: lacks actuarial and financial modeling.

ASPM improves visibility and governance — but not correctness, prioritization, or economic justification.

THE SATRAITS™ / SATRIAGE™ PLATFORM

CyberSagacity addresses the core data problem itself — not just the workflow on top of it.



Corrects the core data problem

Statistically normalizes, validates, and corrects AST results — eliminating noise, duplication, and misclassification to make the data trustworthy.



Precision analytics, not just correlation

Identifies false positives, false negatives, mislabeled severity, coverage gaps, and tool blind spots — revealing which scanners work and where they fail.



Risk-based prioritization with business context

Ranks defects by probabilistic exploitability and likely consequence — not generic severity labels — focusing remediation on real-world likelihood and impact.



Regulatory & financial relevance

Maps each defect to compliance controls (NIST, PCI DSS, CMMC, HIPAA) and computes financial loss exposure — letting leadership quantify value and justify investment.



Flexible, tool-agnostic, efficient

Works seamlessly with existing CI/CD pipelines, tool stacks, and workflows — acting as an intelligence layer and system of record, not a replacement.

COMPETITIVE LANDSCAPE

Where orchestration and posture stop, intelligence begins.

Capability	ASOC	ASPM	CyberSagacity
Orchestration & workflow automation	✓	✓	✓
Unified visibility & governance	×	✓	✓
Data validation & correction	×	×	✓
False positive / negative detection	×	×	✓
Tool accuracy & coverage analytics	×	×	✓
Risk-based prioritization by probability	×	×	✓
Compliance mapping	LIMITED	✓	✓ AUTOMATED
ROI / financial risk modeling	×	×	✓
Minimal added complexity	×	×	✓

WHY SATRAITS™ / SATRIAGE™ OUTPERFORM ASOC & ASPM

Not another dashboard layer — the first AppSec intelligence system.

CyberSagacity transforms raw scan output into validated evidence and quantifiable risk insight — for engineers, security leaders, and executives alike. It delivers what ASOC and ASPM cannot:

- **Ground-truth accuracy** across all defects and all tools.
- **Statistical validation** of every finding and tool.
- **Business-aware prioritization** based on probability and impact.
- **Compliance-linked reporting** without manual mapping.
- **ROI modeling** and financial justification for every activity.

ASOC makes AppSec faster.

ASPM makes AppSec more visible.

**CyberSagacity makes AppSec measurable, accurate,
and profitable.**

THE DISTINCTION

Aggregating more scan data no longer solves the problem. Organizations need evidence — validated, prioritized, contextualized, and economically justified.

SUMMARY

From more scan data to trusted evidence.

The industry has reached a point where simply aggregating more scan data no longer solves the problem.

CyberSagacity's SATraits™ and SATriage™ platform was purpose-built to deliver the outcome organizations actually need — making application security **measurable, actionable, and financially justifiable**. It turns raw data into trusted evidence that drives real risk reduction, compliance alignment, and ROI across every AppSec investment.

THE NEW STANDARD

Trust your data. Prioritize what matters. Prove the ROI of every AppSec dollar.

[Learn more at www.cybersagacity.com](https://www.cybersagacity.com) →