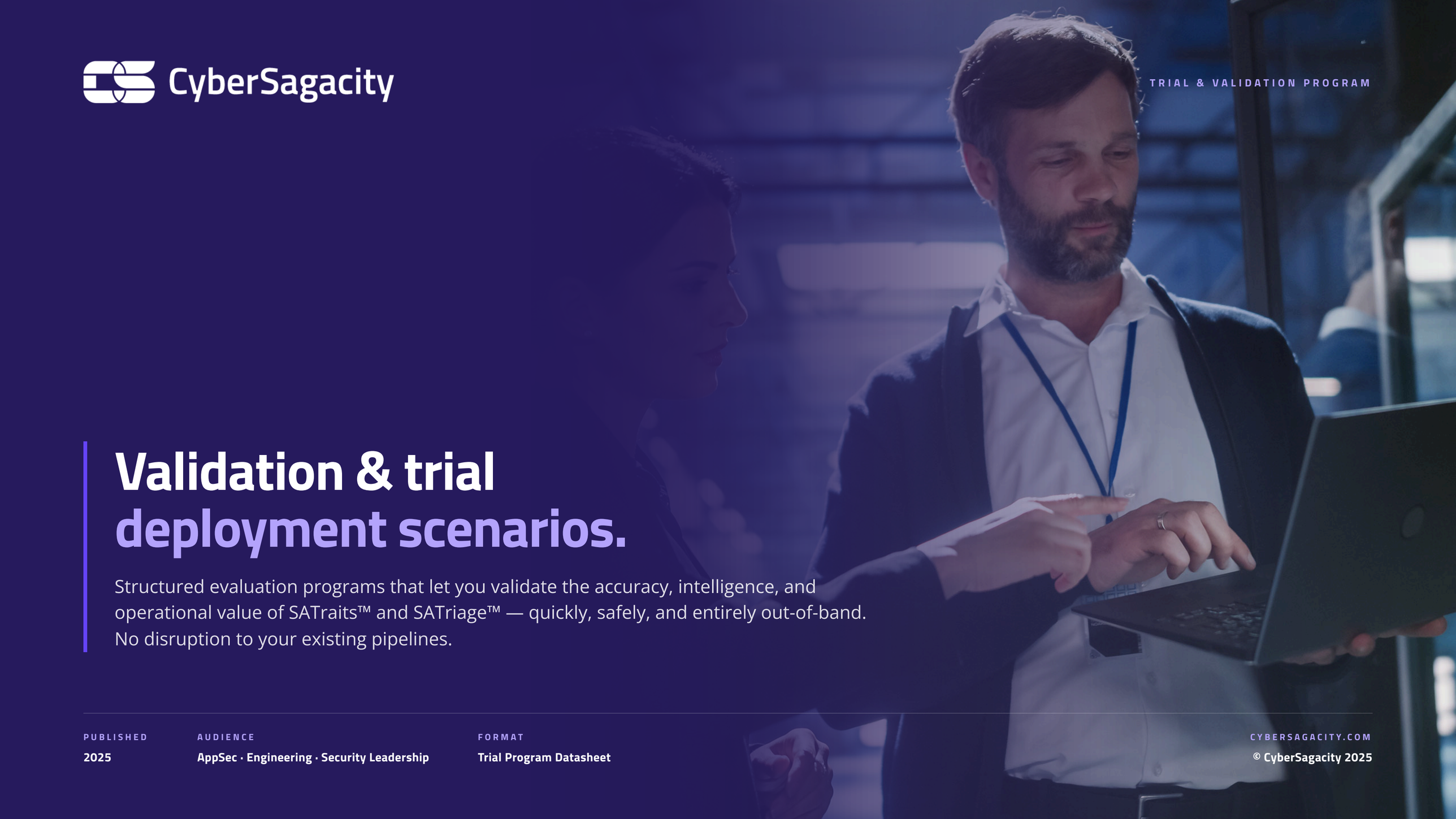
CyberSagacity

TRIAL & VALIDATION PROGRAM



Validation & trial deployment scenarios.

Structured evaluation programs that let you validate the accuracy, intelligence, and operational value of SATraits™ and SATriage™ — quickly, safely, and entirely out-of-band. No disruption to your existing pipelines.

PUBLISHED
2025

AUDIENCE
AppSec · Engineering · Security Leadership

FORMAT
Trial Program Datasheet

CYBERSAGACITY.COM

OVERVIEW

Meet your team where it is — and prove value before committing.

Three structured trials, each meeting customers where they are — whether you run a mature AST program, rely on open-source tooling, or are just beginning your DevSecOps journey.

Every evaluation runs strictly out-of-band, with no disruption to existing development pipelines. Across all scenarios, organizations can quantify measurable improvements in:

- **Defect accuracy** — false positives, false negatives, misclassifications.
- **Tool coverage** and effectiveness across your stack.
- **Prioritization quality** based on exploitability and consequence.
- **Compliance alignment** and governance mapping.
- **Financial-risk reduction** and remediation ROI.
- **AppSec visibility**, decision quality, and operational efficiency.

> **Every trial begins with SATraits™ — then SATriage™ turns coverage into prioritized, defensible decisions.**

EVALUATE USING YOUR EXISTING AST TOOLS

The fastest, least-intrusive path to proof.

You provide defect output from your existing AST tools (SAST, DAST, SCA, MAST, Pentest). We run a combined **SATraits-first, SATriage-second** analysis to surface coverage gaps, accuracy findings, prioritization improvements, and financial implications.

IDEAL FOR Teams already using AST tools we support

TIMELINE **1–2 weeks**

STEP 01

Data ingestion

- Secure transfer via API, CI/CD export, or batch upload
- Short context questionnaire — criticality, architecture, regulatory environment

STEP 02 · SATraits™

Coverage & accuracy assessment

- Benchmarks each tool against a 30-year statistical defect corpus
- Identifies true coverage, blind spots, missed classes, overlap, error rates
- Establishes a quantitative baseline

STEP 03 · SATriage™

Multi-mode analytics

- True-risk prioritization — severity-agnostic 1:n ranking
- Zero-trust / consequence-driven analysis
- Financial-loss & ROI modeling

EVALUATION FOR ORGANIZATIONS WITHOUT EXISTING AST TOOLS

No tooling yet?
We build the baseline.

When no AST tools are in place, CyberSagacity generates a defect dataset using a curated set of vetted open-source scanners (Semgrep OSS, Bandit, OWASP ZAP). From that baseline, SATraits and SATriage deliver coverage insights and prioritization intelligence.

IDEAL FOR Teams early in AppSec maturity or with limited tooling

TIMELINE **4–6 weeks**

STEP 01

Source-code intake & scanning

- Controlled source access, or you run scans internally under guidance
- CyberSagacity executes vetted open-source tools to collect initial defect data

STEP 02 · SATraits™

Coverage & tool-selection assessment

- Determines which AST tools best match your architecture and defect profile
- Quantifies potential coverage lift and accuracy gain per tool
- Produces a data-driven AppSec roadmap

STEP 03 · SATriage™

Multi-mode analysis

- Prioritization, consequence-driven evaluation, and financial modeling
- Same analytic depth as Scenario 1

FULL DEVSECOPS ENVIRONMENT DESIGN & GUIDED PILOT

A tailored AST stack, designed and piloted end-to-end.

IDEAL FOR Organizations building or restructuring a DevSecOps / AppSec program

TIMELINE **8–12 weeks**

STEP 01 · SATraits™

Assessment & tool selection

- Identifies relevant defect classes and patterns in your ecosystem
- Recommends 1–3 AST tools for maximum coverage, minimum overlap

STEP 02

Installation & baseline runs

- Deploy selected tools in a non-production / sandbox environment
- Execute multiple scans; tune configurations for optimal detection

STEP 03 · SATriage™

Analytics & prioritization

- True-risk prioritization, consequence analysis, financial-impact modeling
- Engineer-ready defect lists and executive dashboards

STEP 04

Program & governance design

- Scalable workflow for integrating results into CI/CD
- SLAs, governance controls, compliance alignment, long-term metrics

THREE FLEXIBLE OPTIONS · ONE EVIDENCE-BASED METHOD

Validate your true AppSec posture — rapidly, safely, and without commitment.

- ✔ **Evidence-based visibility** into tool accuracy, coverage, and blind spots.
- ✔ **Correction of false positives & negatives** across your stack.
- ✔ **Prioritization** that reflects real exploitability and business consequence.
- ✔ **Framework mapping** to NIST, PCI, CMMC, HIPAA, and more.
- ✔ **Financial-loss modeling** and ROI-based remediation strategies.
- ✔ **Measurable improvement** in AppSec resilience and decision quality.

IMPORTANT — NON-INTRUSIVE, OUT-OF-BAND BY DESIGN

All scenarios operate strictly out-of-band. CyberSagacity does not integrate into or modify customer CI/CD pipelines until: (1) results are reviewed and validated, (2) the customer selects a deployment model, and (3) a mutually agreed path to integration is defined.

Operational safety, zero workflow disruption, security-by-design from day one.

Learn more at www.cybersagacity.com →