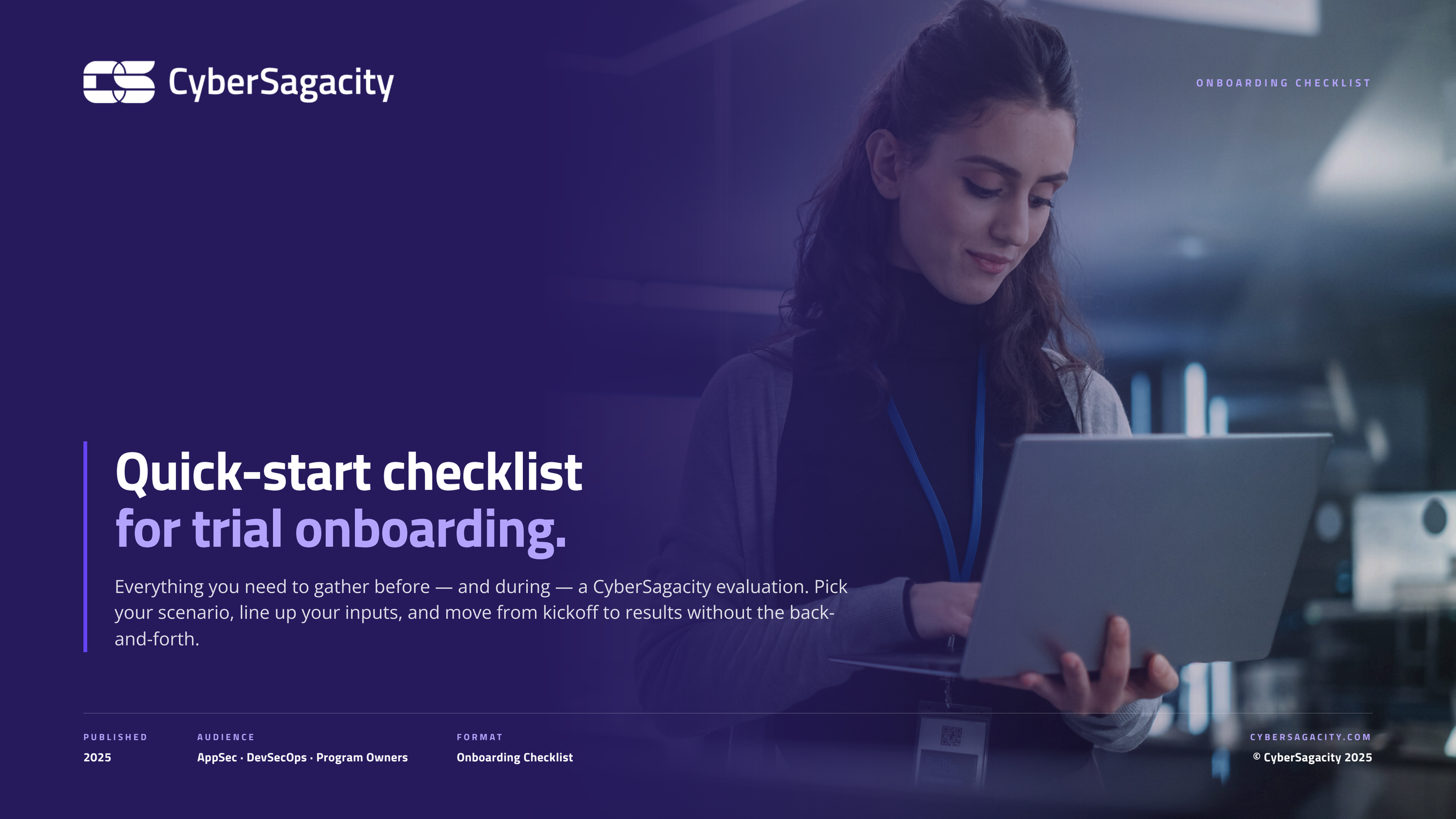
CyberSagacity



Quick-start checklist for trial onboarding.

Everything you need to gather before — and during — a CyberSagacity evaluation. Pick your scenario, line up your inputs, and move from kickoff to results without the back-and-forth.

PUBLISHED
2025

AUDIENCE
AppSec · DevSecOps · Program Owners

FORMAT
Onboarding Checklist

GET READY IN FOUR STEPS — THEN PICK YOUR TRACK

Line up your inputs before kickoff.

BEFORE YOU BEGIN

- [ ] Select which **trial scenario** applies (Existing AST / No Tools / Full Pilot)
- [ ] Identify **1–3 applications** to include in the evaluation
- [ ] Complete the short **application-context questionnaire**
- [ ] Establish a **secure file-exchange method** (API, S3, share, or upload)

TRACK A

Scenario 1 — Existing AST Tools

- [ ] Export defect results from SAST, DAST, SCA, MAST, or Pentest tools
- [ ] Provide scan configuration files *(optional, but helpful)*
- [ ] Supply metadata: languages, frameworks, CI/CD location, criticality
- [ ] Deliver output files to CyberSagacity
- [ ] Receive SATraits coverage report
- [ ] Review SATriage prioritization & consequence-based results

TRACK B

Scenario 2 — No AST Tools

- [ ] Provide controlled source-code access, **or** run scans internally using our instructions
- [ ] Confirm approved open-source scanners (Semgrep OSS, Bandit, ZAP)
- [ ] Supply scanning output to CyberSagacity
- [ ] Review SATraits coverage & tool-selection recommendations
- [ ] Review SATriage prioritization results

TRACK C

Scenario 3 — Full DevSecOps Pilot

- [ ] Identify codebases and environments for sandbox testing
- [ ] Provide access for temporary AST tool installation (or self-host)
- [ ] Run initial scans to generate baseline defect data
- [ ] Participate in tool tuning and configuration adjustments
- [ ] Review SATraits tool-evaluation & coverage analysis
- [ ] Review SATriage analytics, prioritization & workflow recommendations
- [ ] Receive guidance for CI/CD integration *(optional)*