BlueFlag Security

SDLC SECURITY RISK ASSESSMENT · SOLUTION BRIEF · JULY 2026

SDLC Security Risk Assessment

Govern WHO — and WHAT — ships your code. See every identity in 48 hours. Free.

Your SDLC is a network of identities — developers, contractors, service accounts, and now AI coding assistants and autonomous agents committing code alongside them. **90% of SDLC attacks now originate at identity, not code** — a surface your SAST, SCA and ASPM tools were never built to see. Our free, no-obligation assessment makes every identity, AI tool and access path visible in 48 hours.

COMMITMENT	SETUP	FINDINGS	SCOPE
Free	**<30 min**	**48 hours**	**Humans · NHIs · AI**
No obligation — one point of contact to review findings	Read-only API — no agent, no code changes, zero dev friction	Prioritised, board-ready report of your real SDLC exposure	Every identity that can touch your code — AI agents included

Assessment scope and timings are BlueFlag-standard for supported SCM and CI/CD platforms.

WHY NOW

Most organisations are operating blind — AI just widened the blind spot

Traditional scanners look at **code**. The exposure that leads to real incidents lives in **identities** — dormant contractor accounts, stale credentials, over-privileged tokens, and now AI assistants and autonomous agents committing code and holding credentials with no inventory, approval or named owner. The assessment answers what boards and auditors now ask: who — and what — can access, modify and ship the software that runs your business?

THE GAP

What your current stack shows vs. what the assessment reveals

WHAT YOU SEE TODAY

- Code vulnerabilities from scanners (SAST / SCA)
- Cloud posture and runtime alerts
- The identities your IAM already knows about

Necessary — but silent on the identities, AI tools and access paths actually shipping your code.

WHAT THE ASSESSMENT REVEALS

- Hidden access paths, stale credentials & forgotten accounts
- Shadow AI tools — attributed to the individuals using them
- Over-privileged humans, machines & AI agents, by actual usage
- Toxic combinations across identities, tools and code

75% **of SDLC risk your existing stack was never built to see.** SAST, SCA and ASPM scan code. The assessment shows you the other 75% — identity, AI and behavioural exposure that only an identity-centric platform can surface.

WHAT'S IN YOUR REPORT

Six domains. One 48-hour assessment report.

Here's what you'll find waiting for you when the report lands — organised the way security leaders actually put it to work.

1 Govern AI in your SDLC

- A full inventory of every AI coding tool in use — Copilot, Claude, Cursor, Codex & more
- Sanctioned vs. shadow AI, each tool attributed to an individual
- Every AI agent listed as an identity with a named owner
- Which developers and teams use each AI agent, and how extensively

WHY IT MATTERS

AI's footprint — visible, governed, enforced.

2 Stop insider threats & IP loss

- A full roster of internal developers, contractors and vendors with access
- Over-privileged identities, ranked by actual usage
- Risky behaviours flagged: bypassed branch protections, unauthorized merges
- Anomalous clone, exfiltration and credential-abuse events surfaced

WHY IT MATTERS

Threats caught before damage, not after.

3 Govern the non-human workforce

- A count of hidden service accounts uncovered
- A list of stale tokens, API keys and long-lived credentials
- Dormant and orphaned machine identities, flagged
- NHIs mapped to owners and the pipelines they serve

WHY IT MATTERS

Every NHI accounted for and right-sized.

4 Harden SDLC posture

- A full catalogue of repositories, CI/CD pipelines and build systems
- Exposed secrets and critical vulnerabilities flagged in code and IaC
- Repos lacking signed commits, branch protection or mandatory review, listed
- Ownership and maintenance gaps documented

WHY IT MATTERS

Toolchain posture that stays fixed.

5 Automate compliance

- Separation-of-duties and least-privilege gaps documented
- AI-only pull requests bypassing human review, flagged
- A readiness scorecard: NIST SSDF and ISO 27001
- Findings mapped to evidence auditors accept

WHY IT MATTERS

Audit prep becomes on-demand reports.

6 Secure the software in every deal

- An SDLC maturity and risk score to support valuation
- Developer, contractor and advisor access findings
- Anomalous repository activity flagged, pre- and post-close
- An IP exposure summary for diligence

WHY IT MATTERS

Diligence tells the price — we protect the value.

EASE OF DEPLOYMENT

Live in under 30 minutes — no agents, no code changes

BlueFlag connects like a SIEM, not a security agent. Read-only APIs plug into the SCM, CI/CD and identity tools you already run — nothing installed on a developer machine, nothing added to your build pipeline, nothing for developers to notice.

1 CONNECT <30 min

Read-only API connection to your SCM, CI/CD and registries — one point of contact, zero developer friction.

2 DISCOVER

Every human, non-human and AI identity inventoried into one identity graph with behavioural baselines.

3 ANALYSE

Toxic combinations, over-privilege, shadow AI and exposure points correlated across identity, toolchain and code.

4 REPORT 48 h

A prioritised findings report reviewed with you — clear actions, ranked by risk, ready to execute.

No agent · No code changes · Support for multiple SDLC tools · Deployed this week

WHAT YOU'LL WALK AWAY WITH

Five outcomes from your risk assessment report

Not a list of alerts — the assessment hands you these five deliverables directly, in 48 hours, at no cost.

01

Visibility into risks in your development environment

A single, attributable inventory of every developer, contractor, AI tool and identity that can touch your code.

02

Visibility into your non-human & AI workforce

Every service account, bot and AI agent mapped and risk-scored alongside your human developers, not left out of the picture.

03

A compliance-ready evidence base

Findings pre-mapped to NIST SSDF, ISO 27001 and SOC 2 — evidence, not just observations.

04

A prioritised, risk-ranked action list

Findings your team can execute against immediately — reviewed with a single point of contact, not left in a PDF.

05

A data-backed business case for governance

Evidence-backed rationale for closing the 75% of SDLC risk that SAST, SCA, ASPM and IAM tools were never built to cover.

WHAT CUSTOMERS TYPICALLY SEE

The first report, in practice

TYPICAL FINDING	EXAMPLE	WHY IT MATTERS
Dormant contractor access	Accounts still active months after project end.	Forgotten access is the quietest path to your source code.
Shadow AI, attributed	Unsanctioned AI coding tools in daily use, mapped to individuals.	The AI inventory conversation starts with facts, not guesses.
Over-privileged CI tokens	Long-lived pipeline credentials with production reach.	One leaked token shouldn't equal one shipped backdoor.
AI-only pull requests	Agent-authored changes merged without human review.	Provenance and review gaps become audit findings — or incidents.
Orphaned critical repos	Sensitive repositories with no accountable owner.	Unowned code is ungoverned code.

Illustrative findings — representative of typical first assessments, anonymised.

WHAT SETS US APART

Why this can't come from your existing stack

SAST, SCA, ASPM and IAM tools each see one slice of the SDLC. None of them was built to unify identity, AI, behaviour and code into a single, governed picture — which is exactly the gap BlueFlag closes.

Identity-first SDLC security	Built around the real source of 90% of SDLC attacks: human, machine and AI identities — not just the code they produce.
AI-aware by design	The only assessment that treats every AI coding tool and autonomous agent as a first-class, attributed identity.
Toxic interaction detection	Dangerous combinations across identities, tools and code that no single-domain scanner — SAST, SCA, ASPM or IAM — can see on its own.
Actionable insights, fast	Prioritised, board-ready findings in 48 hours, reviewed with one point of contact — not weeks of manual audit prep.
Unified risk visibility	One identity graph across humans, NHIs, AI agents, tools and code — the 75% of SDLC risk your current stack was never built to cover.
Seamless & developer-friendly	No agents. No friction. Read-only APIs that work where you already build.

PROVEN AT ENTERPRISE SCALE

2,500+
developer identities governed in production at a global FinTech

300+
audit hours saved per year at a FinTech scaleup

40%+
CI tool licence savings at a global CX / SaaS leader

THE BOTTOM LINE

"You can't reduce risk you can't see. In 48 hours, the assessment shows you every identity — human, machine and AI — that can reach your code, what each one can touch, and where to act first."

BlueFlag Security · SDLC Security Risk Assessment

Take the first step toward visibility and control.

Request your complimentary risk assessment today.

www.blueflagsecurity.com