



KNOVATION
SOLUTIONS

Govern Every Identity. Secure Every Line of Code.

BlueFlag Identity Platform powered by
Knovation Solutions

Introduction

Every organisation protects its source code. Few protect the identities creating it.

Artificial Intelligence is transforming software development. AI coding assistants, autonomous development agents, machine identities and automated deployment pipelines are enabling organisations to deliver software faster than ever before.

However, this transformation has created a new and largely invisible attack surface.

Today's Software Development Lifecycle (SDLC) is no longer driven solely by developers. Human identities now operate alongside thousands of service accounts, API keys, deployment tokens, CI/CD pipelines and AI-powered development tools. While organisations have invested heavily in Application Security (AppSec), most still have limited visibility into the identities accessing, modifying and deploying their software.

The result is increased software supply chain risk, growing compliance obligations and a rapidly expanding identity attack surface that traditional security tools were never designed to govern.

Through its partnership with **BlueFlag Security**, **Knovation Solutions** enables African organisations to extend identity governance across the entire Software Development Lifecycle, providing continuous visibility, policy enforcement and risk management for every human, machine and AI identity involved in software delivery.

Business Challenges

Software Development Has Created a New Identity Attack Surface

Modern software development is increasingly automated. Developers collaborate with AI coding assistants, CI/CD pipelines automatically deploy applications, service accounts integrate cloud services, and machine identities interact continuously across development environments. Every one of these identities represents a potential security risk if left unmanaged.

While organisations can often identify vulnerabilities within their code, many cannot answer fundamental governance questions:

- Who has access to our source code?
- Which machine identities can deploy production applications?
- Which AI coding assistants are generating production code?
- Are privileged developer accounts behaving abnormally?
- Can we demonstrate continuous governance for compliance and audit purposes?

Without identity visibility, organisations expose themselves to software supply chain attacks, credential compromise, insider threats and unnecessary operational risk.

Traditional Application Security Stops at the Code

Most organisations already invest in:

- Application Security Testing
- Software Composition Analysis
- Software Supply Chain Security
- DevSecOps automation

These technologies are essential, but they primarily focus on protecting the code itself. They rarely govern the identities responsible for creating, modifying and deploying that code. As AI adoption accelerates, securing code without securing identities leaves a significant governance gap.

Non-Human Identities Are Growing Faster Than Human Developers

Modern development environments contain significantly more non-human identities than human users.

These include:

- Service Accounts
- Personal Access Tokens (PATs)
- API Keys
- Deployment Identities
- CI/CD Service Accounts
- AI Coding Assistants
- Autonomous AI Agents

Without continuous governance, these identities become attractive targets for attackers seeking privileged access to critical development environments.

Governance and Compliance Requirements Continue to Increase

Regulators, customers and executive leadership increasingly expect organisations to demonstrate governance across the entire software delivery process.

Yet collecting audit evidence across multiple repositories, cloud platforms and CI/CD environments remains complex, manual and time-consuming.

Without continuous identity governance, compliance becomes expensive, reactive and difficult to sustain.

Key Capabilities

BlueFlag extends identity governance across the entire Software Development Lifecycle without disrupting developer productivity or existing security investments.

Know Every Identity Across Your SDLC

Continuously discover and classify every identity operating across your development ecosystem, including:

- Human developers
- Service accounts
- Machine identities
- Deployment tokens
- AI coding assistants
- Autonomous AI agents

Gain complete visibility into who and what is interacting with your software development process.

Govern AI-Assisted Development

Treat AI coding assistants as governed identities rather than unmanaged development tools. Apply consistent security policies, monitor AI-generated development activity and maintain oversight as AI becomes embedded within modern software engineering.

Identify Risk Before It Becomes an Incident

Continuously analyse identity behaviour to detect:

- Unusual repository access
- Mass repository cloning
- Privilege abuse
- Credential compromise
- Insider threats
- Suspicious AI activity

Identify anomalous behaviour before it impacts software delivery or business operations.

Enforce Policy Without Slowing Developers

Apply identity governance consistently across:

- Source Code Management
- CI/CD Pipelines

- Cloud Platforms
- Developer Workflows

BlueFlag integrates into existing development environments without requiring agents, code modifications or disruption to developer productivity.

Simplify Continuous Compliance

Automatically generate audit-ready evidence aligned with regulatory, governance and security frameworks. Reduce audit preparation time while improving governance confidence across the SDLC.

Integrate Across Your Existing Security Stack

BlueFlag integrates with more than 60 leading platforms across:

- Source Control
- CI/CD
- Cloud Platforms
- Identity & Access Management
- Security Operations
- AI Development Tools

Protect your existing investments while extending identity visibility across software development.

Business Outcomes

BlueFlag enables organisations to move beyond code security and establish complete identity governance across modern software development.

Gain Complete Identity Visibility

Understand every human, machine and AI identity interacting with your software, not just your developers.

Reduce Software Supply Chain Risk

Identify unmanaged identities, excessive privileges and abnormal behaviour before they become pathways for cyberattack.

Secure AI-Driven Software Development

Adopt AI coding assistants confidently through policy-driven governance, visibility and continuous oversight.

Increase Developer Accountability

Link every code change, deployment and privileged action back to a governed identity, improving traceability and reducing operational risk.

Accelerate Incident Investigation

Quickly determine who accessed what, when and why, reducing investigation time and improving security response.

Reduce Audit Complexity

Automate evidence collection and simplify reporting for governance, compliance and regulatory requirements.

Increase Developer Velocity Without Increasing Risk

Strengthen governance without slowing software delivery or introducing additional operational complexity.

Extend Existing Security Investments

BlueFlag complements existing AppSec, IAM, DevSecOps and Security Operations platforms by adding identity intelligence across the Software Development Lifecycle.

Start with an SDLC Identity Risk Assessment

Most organisations do not know how many identities interact with their software development environment.

An SDLC Identity Risk Assessment provides immediate insight into:

- Every human and non-human identity across your SDLC
- Access to critical repositories and production environments
- Excessive, dormant or unmanaged privileges
- AI development tools operating within your environment
- Identity behaviours that may indicate elevated risk
- Governance and compliance gaps requiring attention

Discover your hidden SDLC identity attack surface, and take the first step toward governing every identity involved in software development.

About Knovation Solutions

Knovation Solutions is a cybersecurity specialist focused on delivering practical, high-impact security architectures for mid-market and enterprise organisations across Africa.

By combining leading technologies with deep operational expertise, **Knovation Solutions** enables businesses to secure their environments with clarity, confidence, and control.

Knovation Solutions:

Website: www.knovation.co.za

Call: +27 83 326 1198

Email: info@knovation.co.za



KNOVATION
SOLUTIONS