cycode

Cycode Platform Overview

COMPLETE SOFTWARE SUPPLY CHAIN SECURITY

Software Supply Chain Attacks Are on the Rise

Software supply chain (SSC) attacks, like SolarWinds and Kaseya, are increasingly common. According to Gartner, "By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."

The rise in these attacks is the result of attackers shifting their targets from fortified production apps to the development tools and infrastructure that are used to build those applications. This is the path of least resistance for attackers because traditional AppSec solutions focus on securing application code or production applications but leave the software delivery pipeline itself unprotected. In order to avoid falling victim to SSC attacks, security teams must balance their AppSec investments to include protecting code as well as defending their software development tools, users, and processes.

Find Vulnerabilities Across the Entire SDLC

Software vulnerabilities can exist across the entire software development lifecycle (SDLC)—in custom code, open source libraries, components brought in during the build process, in infrastructure as code (IaC), containers, and more. Cycode offers complete end-to-end software vulnerability identification on a single platform with context from the entire SDLC. Cycode is unique in its ability to perform software composition analysis on both software and pipeline components and to pinpoint vulnerable dependency locations in production environments, which identify a myriad of new attack vectors and dramatically reduce remediation times.

Correlate Data Across AppSec Siloes

Each phase of the SDLC has its own tooling, such as SCMs in the coding phase, build tools in the testing phase, container registries in the deployment phase, and cloud providers in the runtime or maintenance phase—all of which form natural data barriers. Security is similarly segmented with traditional AppSec tools like SAST, SCA, WAF, etc., all running in different siloes. This makes it difficult to obtain a complete view of a software supply chain and its risks.

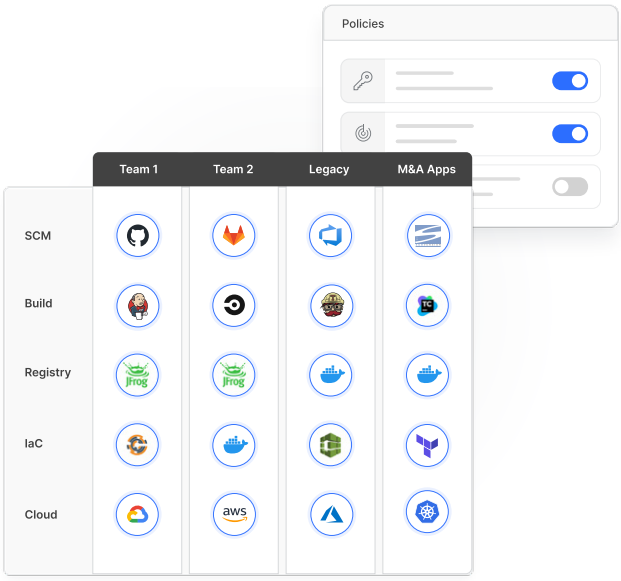
Cycode centralizes your AppSec tooling by offering cutting-edge SAST, NextGen SCA, and pipeline security capabilities on a single platform that integrates with DevOps tools and infrastructure providers to obtain a complete view of the SDLC, including tools, settings, activity, security issues, and more. Armed with a comprehensive view of a software delivery pipeline, Cycode's Knowledge Graph is able to prioritize and orchestrate remediation efforts—using information like production exploitability—from a single, centralized workbench.

Harden SDLC Tooling

The DevOps approach to software development has brought with it an increase in tooling, including source control management systems (SCMs), build tools, container registries, infrastructure as code tools, cloud providers, and more. These tools represent an expanded

attack surface. Failure to implement consistent and effective security controls across this tooling provides attackers with an easy entry point into the SDLC.

Cycode enables organizations to centrally manage and implement consistent security policies—such as least privilege, branch protection rules, security build rules, etc.— across all their DevOps tools and infrastructure. This hardens software delivery pipelines against attack and helps enforce the concept of defense in depth across the SDLC.



Defend the SDLC from Every Angle

Cloud application security starts from the pipeline. The interconnected tooling and automated processes of DevOps make it easier for attackers to move throughout the SDLC after initial compromise. Once attackers have breached a single system, automated pipelines make it easy for them to move laterally across the SDLC and to compromise other parts of the environment such as production applications. The Cycode platform uses a series of complementary, purpose-built security techniques—such as hardcoded secret detection, code tampering prevention, infrastructure as code security, code leakage detection, SAST, and software composition analysis—to close specific attack types and vectors that could result in SDLC compromise, thus reducing the likelihood of a breach.

Complete Software Supply Chain Security

Cycode provides visibility, security, and integrity across the SDLC using a number of complementary solutions. By addressing software supply chain attacks using multiple tools and techniques from a single platform, Cycode is able to offer better results and lower AppSec tooling costs than could be achieved with individual tools.

Our platform offers several distinct use cases, including:

Hardcoded Secrets Detection
Find existing secrets across your entire SDLC and block new secrets in pull requests.

Source Code Leakage Detection
Identify suspicious behavior and detect proprietary code exposures.

NextGen Software Composition Analysis (SCA)
Find vulnerable dependencies in open source and other pipeline components.

Source Control and CI/CD Security
Harden DevOps tools and infrastructure by centrally managing governance and security policies.

Static Application Security Testing (SAST)
Zero in on vulnerabilities in custom developed code.

Code Tampering Prevention
Prevent tampering by combining integrity verification, anomaly detection, critical code monitoring, & governance.

Container Scanning
Scan containers for vulnerable dependencies.

Infrastructure as Code Security
Prevent cloud misconfigurations and apply security standards to infrastructure as code.

Learn More at cycode.com