cycode

Cycode Solution Overview

Software Supply Chain Attacks Are on the Rise

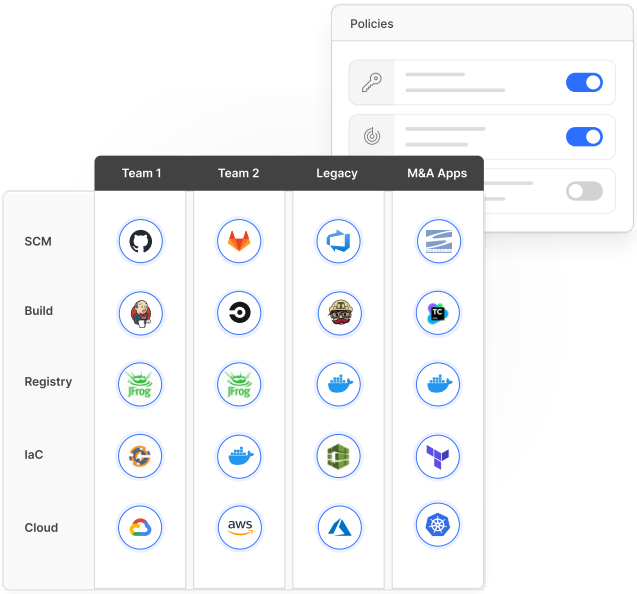
Software supply chain attacks are rapidly increasing. These are breaches, such as SolarWinds and Kaseya, that compromise the development teams, tools, and processes involved in building, packaging, and deploying applications. According to Gartner, "By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."

The rise in SSC 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 existing 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 need tools capable of defending their software development tools, users, and processes.

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, and software composition analysis—to close specific attack types and vectors that could result in SDLC compromise, thus reducing the likelihood of a breach.

Correlate Data Across Appsec Siloes

Each phase of the SDLC has its own tooling, such as SCMs in the implementation 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 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 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 tracks code integrity, user activity, and events across the SDLC to prioritize risk, find anomalies, and prevent code tampering.

Implement Continuous SDLC Compliance

Understanding how one's software development practices and SDLC security posture align with compliance frameworks can be a difficult, highly manual, extremely time-consuming undertaking. Fixing violations, implementing the required security controls, and generating evidence for attestation to auditors adds even more complexity and requires more effort.

Cycode provides security teams with the ability to easily understand their SDLC's compliance posture and how it maps against specific compliance frameworks. With centralized policy management, users can efficiently implement security controls that align their SDLC with regulatory requirements and generate evidence for attestation.

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, Cycode is able to obtain better results than could be achieved with individual tools, thus greatly reducing the risk of compromise or breach.

Our platform offers several distinct use cases, including:

Source Control and CI/CD Security

Harden DevOps tools and infrastructure by centrally managing governance and security policies.

Hardcoded Secrets Detection

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

Code Tampering Prevention

A comprehensive solution combining integrity verification, anomaly detection, critical code monitoring, & governance.

Infrastructure as Code Security

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

Source Code Leakage Detection

Identify suspicious behavior and detect proprietary code exposures.

Continuous SDLC Compliance

Easily assess, improve, and attest to the compliance posture of modern software delivery pipelines.

Learn more at cycode.com