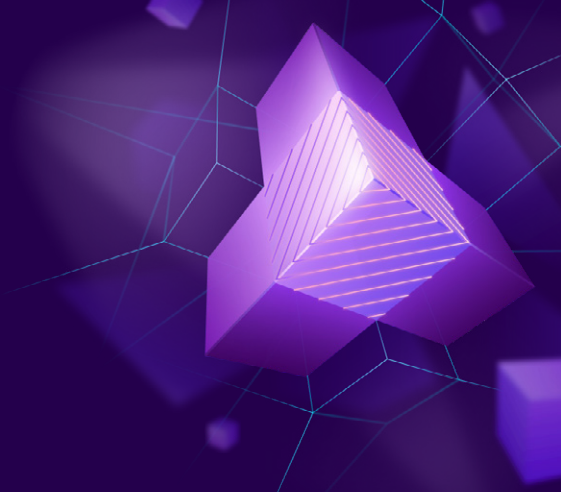
cycode

Source Control and CI/CD Security

SOLUTION BRIEF



Manage Governance of Source Control and CI/CD Security Policies Across All DevOps Tools

As DevOps tool chains become more sophisticated, the need to manage policies across the entire SDLC is now more critical than ever. Over the last decade, application development has experienced staggering innovation, which has brought with it an equal amount of complexity. Organizations embracing DevOps methodologies have adopted technologies like containers, Kubernetes, Infrastructure as Code (IaC), and microservices architectures. This wave of innovation has delivered exponential gains in efficiency for engineering teams. It also has created serious security risk.

Attackers have taken notice of this trend and shifted their focus from production applications to the DevOps tools and infrastructure that make up the modern software delivery pipeline. Once hackers gain a foothold in a software delivery pipeline, they can easily move laterally to steal secrets, adjust cloud configurations, and even insert and push malicious code into production. This problem is only getting worse. According to Gartner, the number of software supply chain attacks is expected to triple by 2025.

Modern DevOps toolchains continue to grow larger and more complex. Organizations often have multiple teams using different tools, and acquisitions bring with them additional teams and even more tools, all of which are typically configured for efficiency, not security. Security leaders face a pressing need to manage security policies across diverse ecosystems. The entire SDLC needs to be hardened to protect against supply chain attacks. Security teams need an easy way to ensure that proper security controls like least privilege, separation of duties, and branch protection are enforced in a centralized and uniform way across all tooling in the SDLC.

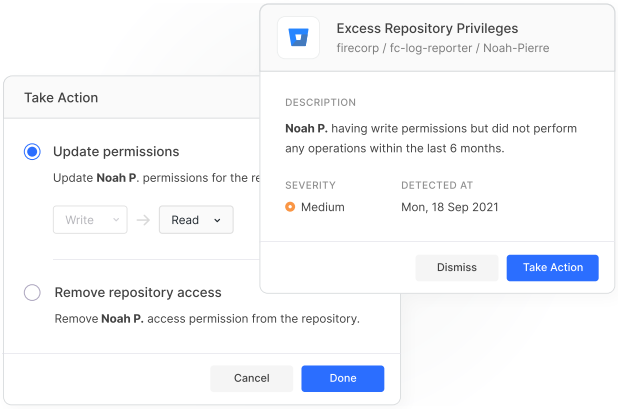
Consistent security and governance is the foundation of software supply chain security. Cycode applies and enforces consistent governance and security policies across all engineering teams and tools to provide complete visibility and a hardened security posture. By normalizing configuration across all SDLC tooling, security teams can focus on policies rather than just implementation details.

Enforce Least Privilege

Least privilege policies are one of the most important security layers because enforcing this reduces the risk of all security issues. Developers often have over-provisioned access to their organization's environment based on the possibility that they might someday need a system or resource to do their job. Attackers and malicious insiders take advantage of these expansive access privileges to move laterally across systems to leak code, tamper with code, or worse. Auditing for excess privilege slows attackers down by forcing attackers to compromise the right account rather than just any account.

Cycode automatically audits and enforces least privilege policies by removing excess and unused privileges on developers' accounts, such as access to repositories, read vs. write, and user vs. admin rights. This lessens the impact of a compromised account by reducing access to code that could be leaked or tampered with. When security policy violations are identified, Cycode's workflow automation engine can be used to

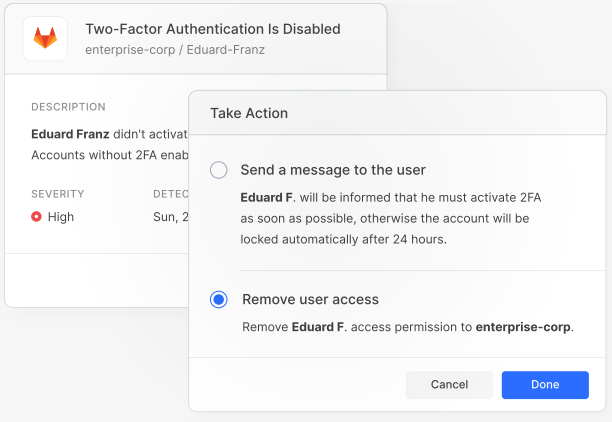
automatically notify AppSec teams, open a ticket, or implement policy changes in the relevant tool, such as revoking user access. Finally, Cycode ensures separation of duties across roles, tools, and teams, which is a core component of many compliance requirements, such as SOC 2 Type II, PCI-DSS, and others.



Harden Authentication

Attackers are targeting developers and using compromised developer accounts as an entry point into organizations' software development pipeline. Modern development teams use a wide range of tools. Because each has different default settings and security options, enforcing consistent authentication policies across all these tools is both difficult and time consuming.

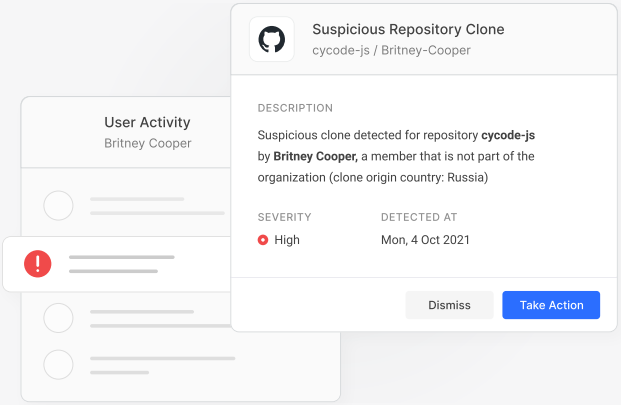
Cycode hardens authentication by integrating with DevOps tools and infrastructure to enforce strong authentication policies such as multi-factor authentication and single sign-on. This helps verify that each user is who they claim to be. Strong authentication makes it much more difficult for attackers to gain access to developer accounts, thereby lowering the risk that a compromised account is used to infiltrate the software development pipeline.



Detect Anomalous Activity

Insider threats are incredibly damaging and notoriously hard to detect because they don't set off traditional security detection mechanisms. With an insider threat, the attacker is already on the network or has gained access to SDLC tools and thus passed many security controls. Moreover, malicious insiders often know where the valuables are and can avoid detection by using legitimate credentials, known machines, and provisioned access privileges.

Cycode identifies these threats and others by learning how users normally interact with tools in the SDLC. Cycode then automatically detects high-risk deviations from the learned baselines of the users involved, such as cloning code from unknown locations or cloning excessive repos within a short period of time. By identifying suspicious and anomalous activity in an environment, Cycode helps find insider threats in the SDLC before they reach the point of a breach.



Monitor Security Controls for Change

Software delivery pipelines are about continuous improvement. These improvements come via changes that occur both in new feature code as well as in updates in the tools that make up development pipelines. Security controls are used to harden these systems, and organizations need to know when any changes are made. Without appropriate rules in place about how these changes occur, code may be tampered with, code may be updated without permission, or systems may end up vulnerable or insecure.

Cycode helps securely manage change in each facet and

phase of the SDLC to prevent unintentional security control changes:

Branch Protection

Enforce compliance through key branch protection rules such as peer review, commit signing, disallowing forced pushes, and hardcoded secrets detected.

Build Rules

Ensure security and integrity by enforcing security rules for every build, such as confirming signed files match the commit, scanning for IaC misconfigurations, hardcoded secrets, and more.

Security Updates

Monitor for critical security updates to on-premises deployments of key DevOps tools to prevent pipeline breaches by known vulnerabilities.

Ensuring change happens in a secure and sanctioned way reduces the risk of unauthorized changes to code, build tools, IaC code, and more that may result in a breach.

Orchestrate AppSec Across the SDLC

Cycode offers a series of complementary security tools that mitigate security issues from different angles. This reduces breaches by focusing on how threats combine into actual risk factors rather than just vulnerabilities. For example, when combined with hardcoded secret detection or file integrity verification, strong authentication and least privilege policies significantly reduce the risks of breaches via secret exposure or code tampering.

Pre-Built Integrations for DevOps Tools

Enabling each development team to choose the best tools for their environments means that enterprises end up with many overlapping DevOps tools. Cycode offers a wide range of pre-built integrations that deploy in 2-3 clicks and less than one minute, delivering immediate value and allowing maximum agility as customers' SDLCs change over time.

Complete Software Supply Chain Security

Cycode integrates with all software delivery pipeline tools and infrastructure providers to enforce consistent governance and security policies, providing complete visibility and hardened security posture. Though managing governance of source control and CI/CD security policies across all DevOps tools is essential, it is only one step in protecting the software supply chain. To truly reduce risk, organizations need a comprehensive solution that covers the entire SDLC.

Cycode is the only end-to-end software supply chain security solution that provides visibility, security, and integrity across all phases of the SDLC. In addition to governance, Cycode provides complete software supply chain security that helps teams manage hardcoded secrets, IaC misconfigurations, code leaks, and more. Cycode's patented Knowledge Graph tracks code integrity, user activity, and events across the SDLC to find anomalies and prevent code tampering so that organizations can be sure their supply chain is completely covered.

While consistent security and governance is the foundation of software supply chain security, organizations need to protect the entire development pipeline. Cycode offers a complete solution that secures infrastructure at each phase of the SDLC to protect against software supply chain attacks.

Cycode is a complete software supply chain security solution that provides visibility, security, and integrity across all phases of the SDLC. Cycode integrates with DevOps tools and infrastructure providers, hardens their security postures by implementing consistent governance, and reduces the risk of breaches with a series of scanning engines that look for issues like hardcoded secrets, infrastructure as code misconfigurations, code leaks and more. Cycode's knowledge graph tracks code integrity, user activity, and events across the SDLC to prioritize risk, find anomalies, and prevent code tampering.

More solution briefs at Cycode.com