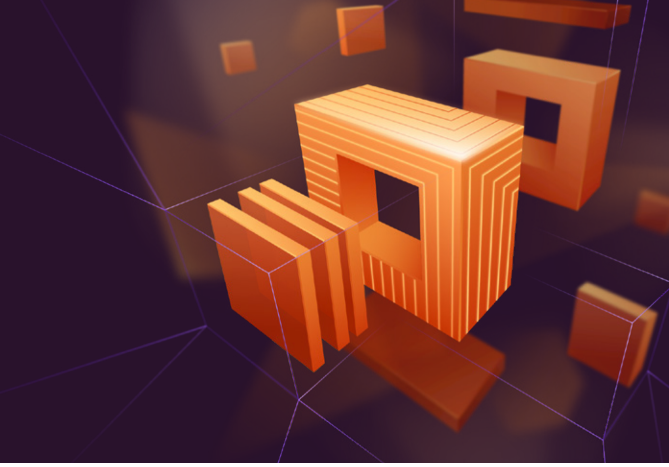
Source Code Leakage Detection

SOLUTION BRIEF



Source code is the foundation of a software company's intellectual property. If it leaks and falls into the hands of malicious actors, the repercussions can be devastating. Not only is a company's IP at risk, but attackers can use source code to identify vulnerable routes and libraries to further exploit an application. Code leaks also expose business logic, which can be leveraged against other applications. Source code leaks sometimes even expose sensitive data such as customer account information or hardcoded secrets. The damage to an organization's reputation from a code leak can have a real impact on their bottom line.

One challenge in preventing code leaks is that even minor mistakes can lead to public exposure. For example, Git systems are designed so that developers bring their personal account to work on corporate projects. Many developers set their personal repositories to public to share their work. If a developer accidentally saves their work to the wrong repository, proprietary code could be made public.

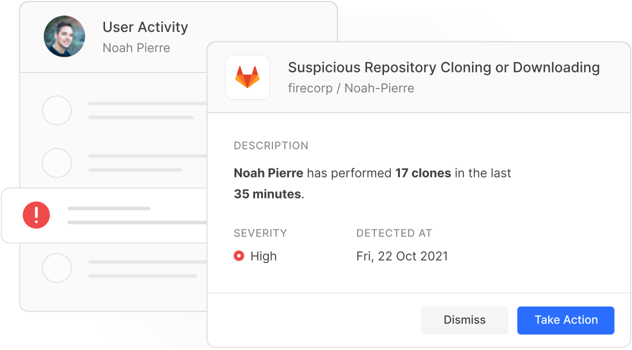
Cycode prevents code leakage and reduces damage should a leak occur. If a leak occurs, Cycode quickly gets it off the web to minimize exposure and decrease the likelihood that a leak develops into a breach.

Prevent Code Leakage

Because the impact of code leakage can be devastating, organizations must prevent them whenever possible. Implementing proper governance and least privilege policies is a first step in limiting who can access code. Organizations must also monitor for anomalous or suspicious user activity that can be a predictor of a code leak risk. Small changes in user behavior might not be concerning on their own, but multiple changes to typical behavior could signal that something is amiss. Equipped with this information, security teams can keep intellectual property safe.

Cycode enables users to implement consistent governance and least privilege policies organization-wide. The fewer people who have access to code, the less likely that it is accidentally or intentionally exposed.

To further prevent code leakage, Cycode detects anomalous activity involving source code. Cycode first learns the normal behavior of an organization's software development environment, including typical user activity, repository access patterns, and more. Cycode automatically identifies suspicious activity, which may either cause or be the precursor to a leak—such as cloned repositories, privately forked repositories, and excessive downloading—and sends an alert so potential harm can be avoided.



User Activity
Noah Pierre

Suspicious Repository Cloning or Downloading
firecorp / Noah-Pierre

DESCRIPTION

Noah Pierre has performed **17 clones** in the last **35 minutes.**

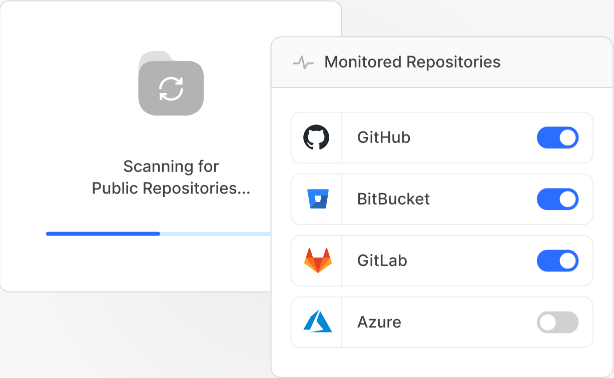
SEVERITY
● High

DETECTED AT
Fri, 22 Oct 2021

Reduce Business and Security Risks

Code leaks have consequences that impact business operations. This includes exposing intellectual property and trade secrets or tipping off competitors to product roadmaps and feature announcements. Leaks also have security implications. Attackers frequently search code leaks for hardcoded secrets or attack vectors to exploit, both of which can lead to further breaches. A complete code leakage solution reduces the damage that a code leak could cause, including the likelihood that it develops into a breach.

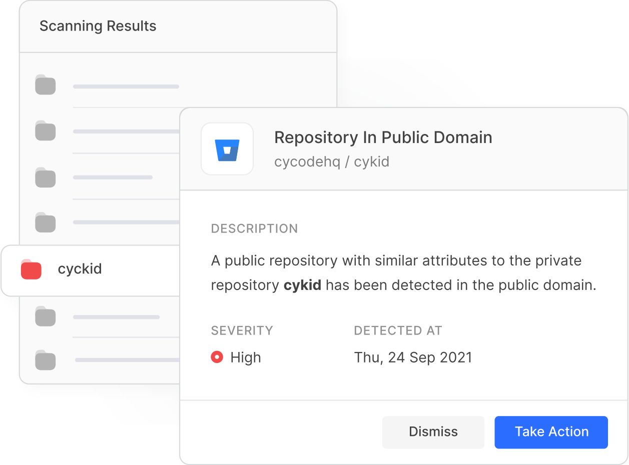
Cycode reduces the risk of code leakage using a number of integrated techniques. This includes scanning for and mitigating hardcoded secrets and misconfigurations in IaC templates. Code leaks involving hardcoded secrets could give attackers a direct pathway into an organization's systems or environments. They also significantly expand attack surfaces, which makes the software supply chain even more difficult to defend. IaC templates are often leaked alongside proprietary code. If an IaC template falls into the wrong hands, malicious actors could look for insecure configurations that could be exploited and used to breach the organization.



Minimize the Impact of Exposure

Private source code appearing in public repos—whether by accident or as the result of a breach—is shockingly common. GitHub has reported a 248% increase in Digital Millennium Copyright Act (DMCA) takedown requests from 2017 to 2021. Organizations need to be vigilant to prevent exposure so that malicious actors don't have an opportunity to do harm.

To proactively identify a leak, Cycode fingerprints proprietary repositories then continuously monitors public repositories and code sharing sites for repository identifiers in the wild, including names and keywords, which might indicate a leak. If proprietary code appears on a public site, Cycode automatically sends an alert via email, Slack, or an incident management system so the code can be removed immediately. By reducing the time that code is publicly exposed, Cycode reduces the likelihood of it falling into the wrong hands, minimizing the impact of a code leak.



A public repository with similar attributes to the private repository **cykid** has been detected in the public domain.

SEVERITY: High

DETECTED AT: Thu, 24 Sep 2021

Complete Software Supply Chain Security

Cycode helps customers find source code leaks, prevent new leaks, and reduce the risk of exposure should a leak occur. This holistic approach to software supply chain security reduces organizations' overall risk of code leakage.

While preventing code leakage is critical, 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 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