cycode

Continuous Compliance Across the SDLC

SOLUTION BRIEF

The modern DevOps approach to software development has clear advantages over past approaches, when it comes to efficiency and productivity. However, DevOps methodology is also more complicated than prior approaches. It involves a high degree of automation and orchestration across the software development life cycle (SDLC). In fact, a single software delivery pipeline used by a single engineering team often includes a half dozen tools like source control management systems, build tools, Infrastructure as Code tools, container registries, cloud providers and more. As a result, understanding how one's software development practices and 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 effort. Finally, to compound the issue, auditors who are typically non-technical, may struggle to understand the evidence provided by their AppSec peers. This can lead to miscommunication, delays, and inefficiency in the audit process.

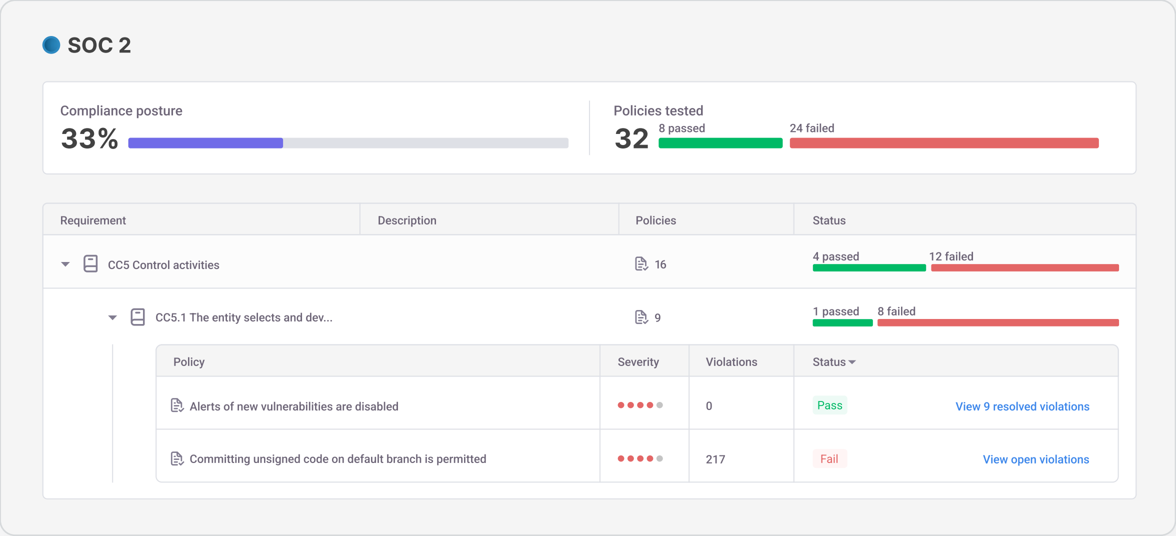
Security teams need the ability to easily understand their compliance posture against the specific frameworks to which they are beholden. They must be able to easily identify and close gaps which may hinder their compliance efforts. Finally, they must be able to quickly and easily generate evidence for auditors in a format which auditors can understand.

Easily Understand AppSec Compliance Postures Across the SDLC

Today’s DevOps tools and infrastructure are usually tested, purchased, and implemented by engineering. This puts AppSec teams in a situation where they may lack basic visibility into the tools being used, the activity occurring in them, and the security policies that govern them. Thus compared to other parts of a security program, it can be very challenging for AppSec teams to understand how their organization’s posture stacks up against specific compliance regulation requirements like SOC 2 Type 2, PCI-DSS, or ISO 27001.

Cycode is built on top of a graph database known as the Knowledge Graph, that provides a comprehensive view of an organization's software delivery pipeline, including the user privileges, activity, configurations, and security controls of each tool. An extensive library of pre-built security policies then compares the requirements of a specific framework against customers’ development environments to find compliance violations. As customers implement changes to address policy violations within their environment, Cycode reflects those changes to provide an always-ready compliance snapshot.

This realtime feedback about software delivery pipeline compliance status greatly reduces the time and effort needed to achieve compliance.



SOC 2

Compliance posture
33%

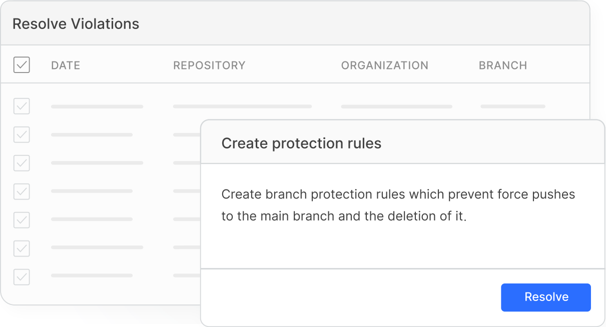
Policies tested
32 8 passed 24 failed

Requirement	Description	Policies	Status
CC5 Control activities		16	4 passed 12 failed
CC5.1 The entity selects and dev...		9	1 passed 8 failed

Policy	Severity	Violations	Status
Alerts of new vulnerabilities are disabled	●●●●○	0	Pass View 9 resolved violations
Committing unsigned code on default branch is permitted	●●●●○	217	Fail View open violations

Efficiently Remediate Violations & Implement Controls

Determining how an organization's posture is misaligned with compliance framework's requirements is only half the battle. In order to pass an audit, security teams must also fix the discovered violations and implement any missing security controls. In modern SDLCs, installing the requisite security controls can be a lengthy, time consuming process that spans many systems and processes.



Resolve Violations

□	DATE	REPOSITORY	ORGANIZATION	BRANCH

Create protection rules

Create branch protection rules which prevent force pushes to the main branch and the deletion of it.

Cycode helps AppSec teams efficiently take the steps needed to adhere to compliance requirements by providing fix suggestions, and in some cases automatically apply code fixes or policy corrections, across your entire SDLC, from a single, centralized user interface. This helps security and engineering teams fix compliance issues in a streamlined fashion, which greatly saves time and effort involved with meeting compliance requirements.

Effortlessly Generate Evidence for Attestation

In parallel to security controls being implemented, Appsec teams must generate evidence for attestation purposes. The evidence auditors request about software delivery pipelines is often housed in multiple tools and may even be split amongst repositories. For example, providing proof of separation of duties or a least privilege policy might require a list of privilege levels for every user, in every tool, and every repo. While not impossible, this is a daunting, often highly time-consuming request because of the types of information and number of locations in which this information lives. This is also true for many other common artifacts that may be required during an audit.

Cycode helps to automatically generate the evidence needed to satisfy auditors with regards software delivery pipelines and specific compliance mandates. Each compliance framework is mapped to policies built on top of our Knowledge Graph that are able to display or export the relevant evidence suitable for attestation. Automating the process of generating compliance evidence for software delivery pipelines is a powerful capability for AppSec teams because it saves time and effort which could be otherwise applied to tackling other mission critical security projects.

Bridge the Communication Gap

Security teams tend to be highly technical and the security controls they need to implement are often very specific, meanwhile, auditors usually hail from non-technical origins like accounting. The difference in technical skills can result in miscommunication around what is required to meet requirements and whether or not evidence supplied meets those requirements.

Cycode's compliance solution uses plain english to describe the security controls and policies that fulfill specific compliance requirements, but at the same time exposes the underlying query being used to generate that evidence. This enables security teams to understand how a security control is being technically implemented, but also to easily discuss it with auditors. Moreover, Cycode's knowledge graph can be used to create policies and queries that repeatably produce evidence for auditors based on specific organizational needs. Bridging the communication gap between security teams and auditors makes the audit process smoother, less painful, and less prone to delay.

Key Features include:

+ Pre-built, bi-directional integrations with popular SDLC tooling, including SCMs, build tools, container registries, cloud providers, and more.
+ Complete visibility across the entire SDLC, its tools, configurations, users, and activity.
+ Continuous compliance posture assessment that identifies gaps with framework requirements (e.g. SOC 2, ISO 270001, and more.).
+ Central policy and security control implementation to easily address compliance violations and gaps.
+ SDLC compliance evidence generation to effortlessly fulfill attestation requirements.

Complete Software Supply Chain Security

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, prevent code tampering, and enable organizations to efficiently tackle compliance for their software delivery pipelines.

More solution briefs at Cycode.com