DAZZ.

Find and Remediate Secrets with Dazz

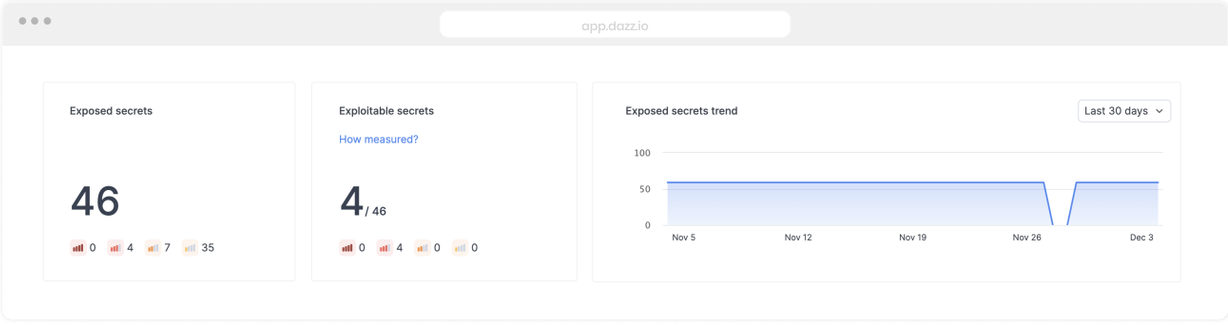
Given the fact that well-known data breaches in the last several years have originated from exposed secrets, it's no wonder that secret scanning has become imperative for DevSecOps teams. Secrets are used in data storage, cloud providers, dev tools, chatops tools and more, making it difficult to track which ones may have inadvertently been exposed to the public. It can be even harder to find exactly where the secret lives and who can fix it the fastest.

Our Approach to Secret Scanning

Dazz Secret Scanning is a core capability of our Pipeline Security offering. By simply connecting to your Source Code Management (SCM) platform, Dazz looks through repository HEAD and history to search for hard-coded secrets, including credentials, private keys, API secrets, and more.

Unlike other secret scanning solutions, Dazz can:

- Find old, potentially exploitable secrets from past commits to be fully removed from repo histories
- Verify that secrets are live and exploitable in order to prioritize which secrets to remediate first
- Map exposed secrets along the entire code to cloud pathway for full context over what is impacted when secrets are exposed



Benefits

Dazz continuously identifies hardcoded secrets and pipeline security gaps and to align your CI/CD process with security best practices. The Dazz Unified Remediation Platform connects the dots across your security and development tooling. Dazz correlates code, artifacts, deployments, infrastructure, and cloud environments with security findings and boils them down into actionable root cause to streamline remediation.

Secrets Prioritization

Identify secrets that are potentially exploitable, helping teams prioritize fixes across all repositories.

Remediation & Risk Mitigation

Reduce exposure and the likelihood of secrets being compromised by automatically generating tickets to the right developer when active secrets are detected.

DevSecOps Enablement

Monitor exposed secrets over time and align development with security best practices.