DATASHEET

API Inventory

Understanding Where Your APIs Are

The old adage of 'you can't protect what you can't see' applies perfectly to API security. As the number of APIs grows exponentially, fueled by business demand, it is increasingly difficult for the security teams to maintain visibility of what APIs exist and what risk they expose. Consequently, if an organization does not have up-to-date API inventory under version control, it could be at risk for things like shadow or zombie APIs, or unauthorized access to user data and Account Takeover (ATO) through the API. When older API versions are not properly retired or locked down, they may have security holes that malicious actors can exploit. By keeping an accurate inventory of APIs and using good version control, organizations can greatly reduce the risk of cyber attacks like these.

Key Elements of Secure API Inventory Include:

- How are new APIs introduced and tracked in the organization?
- Prioritize your APIs, starting with the most critical. We recommend assessing network access to the API, data sensitivity and access control to the API as essential steps to perform.
- Discovery of the API inventory by introspection of source code repositories to discover hidden API artifacts
- Runtime inventory management of APIs

How 42Crunch Helps

42Crunch automatically discovers API files that your developers have created by integrating to various developer repositories such as GitHub. From there we automatically audit and scan for vulnerabilities and provide remediation guidance steps to enable developers to immediately fix the APIs before they ever reach deployment. 42Crunch works seamlessly within the GitHub flow used by your developers to ensure that API security is baked into your standard process.

> Our automation of scanning of API files in GitHub repos accelerates the deployment of secure APIs
>
> **Isabelle Mauny, Field CTO 42Crunch, 2023**