END-TO-END API SECURITY
Throughout the API Lifecycle

42Crunch and Microsoft deliver a seamless DevSecOps environment for API security from design, through to production and runtime

API SECURITY COMPLIANCE AND GOVERNANCE ACROSS THE API ESTATE

Cloud applications are increasingly API-centric, with APIs at the core of data exchange. Inherently, APIs are easy to expose, but difficult to defend and traditional application security solutions are not optimized to protect APIs. 42Crunch and Microsoft have partnered to enable developers find and fix API vulnerabilities while giving security teams centralized governance across their APIs.

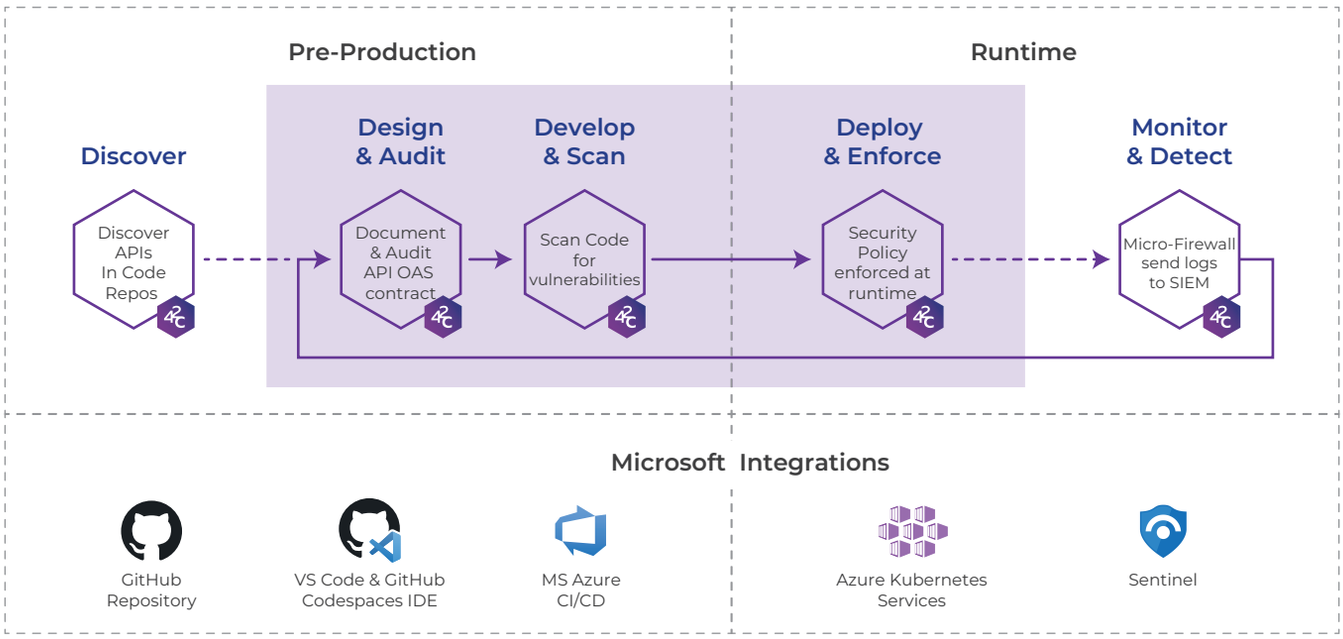
API SECURITY FIRST FOR EFFICIENCY & INNOVATION

An effective API security strategy starts early in the software development lifecycle. 42Crunch and Microsoft are collaborating to enable a DevSecOps approach that helps developers build more secure and resilient APIs without compromising on productivity or innovation. The 42Crunch Developer-First API Security platform is purpose-built to enable a combined shift-left and shield-right approach to securing APIs. The out-of the-box Integrations with many of Microsoft's key enterprise platforms enable a seamless DevSecOps experience for API security throughout the API lifecycle.

> Together with 42Crunch, we bridge the gap of API security from development to runtime and empower security teams to exercise governance over their API ecosystem throughout the development lifecycle.

VLAD KORSUNSKY

VP Cloud and Enterprise Security, Microsoft



API **INVENTORY**

WIth 42Crunch we meet developers where they are by integrating with leading IDEs like **VSCode** and **GitHub Codespaces** which allows them to get instant feedback on security issues without having to change environments. Through a GitHub action, during a pull request, 42Crunch automatically scans enterprise GitHub repositories for all OAS files and imports them to the API security platform.

API **TESTING**

42Crunch API Scan runs as an automated task within the CI/CD pipeline through **GitHub** or **Azure DevOps**. Alternatively, scans can be run incrementally by developers directly from **VSCode** or **Codespaces** to ensure that issues are caught earlier in the development process and don't result in a failed test.

Scan results are also shared with central security teams through an integration with Microsoft Defender for Cloud where they can be combined with runtime security insights found by Microsoft Defender for APIs.

API **MONITORING**

The 42Crunch API firewall sends logs to **Azure Sentinel** for analysis of real time attack data. Sentinel provides actionable insights and visualizations that highlight anomalous activity and attack patterns including account takeovers and malicious bots.

API **DESIGN**

42Crunch API Audit (downloaded by over half a million developers) runs as a plug-in in **VSCode** and **GitHub Codespaces** to automate testing as part of the CI/CD pipeline. Vulnerabilities found during the audit are presented to the developers directly in the IDE as well as both **GitHub Advanced Security** and **Azure DevOps** along with detailed remediation steps.

Audit results are also shared with central security teams through an integration with Microsoft Defender for Cloud where they can be combined with runtime security insights found by Microsoft Defender for APIs.

API **PROTECTION**

42Crunch API firewall runs in front of your API and uses a positive security model to ensure that API requests and responses conform to the audited OAS contract. The firewall runs as a VM or in **Azure Container** or **Azure Kubernetes Services** as a sidecar container alongside your API or **Azure API Management** gateway.

Member of
Microsoft Intelligent Security Association

Microsoft

42Crunch is now available for purchase on the Azure Marketplace

Get it from Microsoft Azure Marketplace