TECHNICAL SOLUTION BRIEF

IMPROVE API SECURITY for Apigee Edge Gateway

42CRUNCH HAS THE UNIQUE CAPABILITY TO FEED TRULY SECURITY TESTED APIs INTO THE API MANAGEMENT LIFECYCLE.

42Crunch implements a proactive approach to API security by certifying at design time the Swagger/ OAS files used to build the security policies for the API Gateway to protect APIs at runtime.

API Gateways have provided the platform for the explosion in the adoption of APIs over the past decade. The flipside of this success has been the rise of API attacks which now represent the most-frequent attack vector for data breaches of enterprise web applications. The Apigee Edge gateway offers a good set of capabilities for authorization & authentication, spike arrest and basic verification of content, but that is not enough in today's world. API Security requires an approach that starts at the beginning of the API lifecycle. 42Crunch integrates with Apigee to improve its API management offering, with a robust set of security testing and governance capabilities, enabling full end-to-end API security.

RUNTIME PROTECTION **APIGEE**

- Identity Management integration to protect against unauthenticated and unauthorized access
- JSON Threat protection
- XML Threat protection
- Threat protection through REGEX
- Spike Arrest

DESIGN TIME SECURITY GOVERNANCE **42CRUNCH**

- Detect potential security vulnerabilities from design time through analysis of OpenAPI/Swagger files
- Build secured JSON schemas which can be used effectively in the JSON threat protection policies
- Automatically test the API's conformance to the specifications
- Test security resilience of the APIs as part of continuous integration with gcloud CLI
- Convert security certified OAS files to API proxies using Apigee/DevRel tools in GitHub

AUTOMATE YOUR SECURE API LIFECYCLE

CI/CD PIPELINE

API Design

Test and harden your OpenAPI Specification(OAS) for known (OWASP API Top 10) vulnerabilities and best practices.

API Implementation

Verify your API Implementation for compliance with the OAS and your own security policies.

apigee

API Runtime Protection

Feed your truly secure OAS file into your API Management lifecycle, enabling your API Gateway to protect your API calls.

AUTOMATING API SECURITY WITH 42CRUNCH

Leveraging 42Crunch, Apigee users reduce manual tasks and automate security into the API workflow in order to get secure code quickly out the door and into production. Following the steps below, Apigee users can focus on enhancing API utilization and innovation.

HOW DOES 42CRUNCH **ENHANCE YOUR API MANAGEMENT SOLUTION**

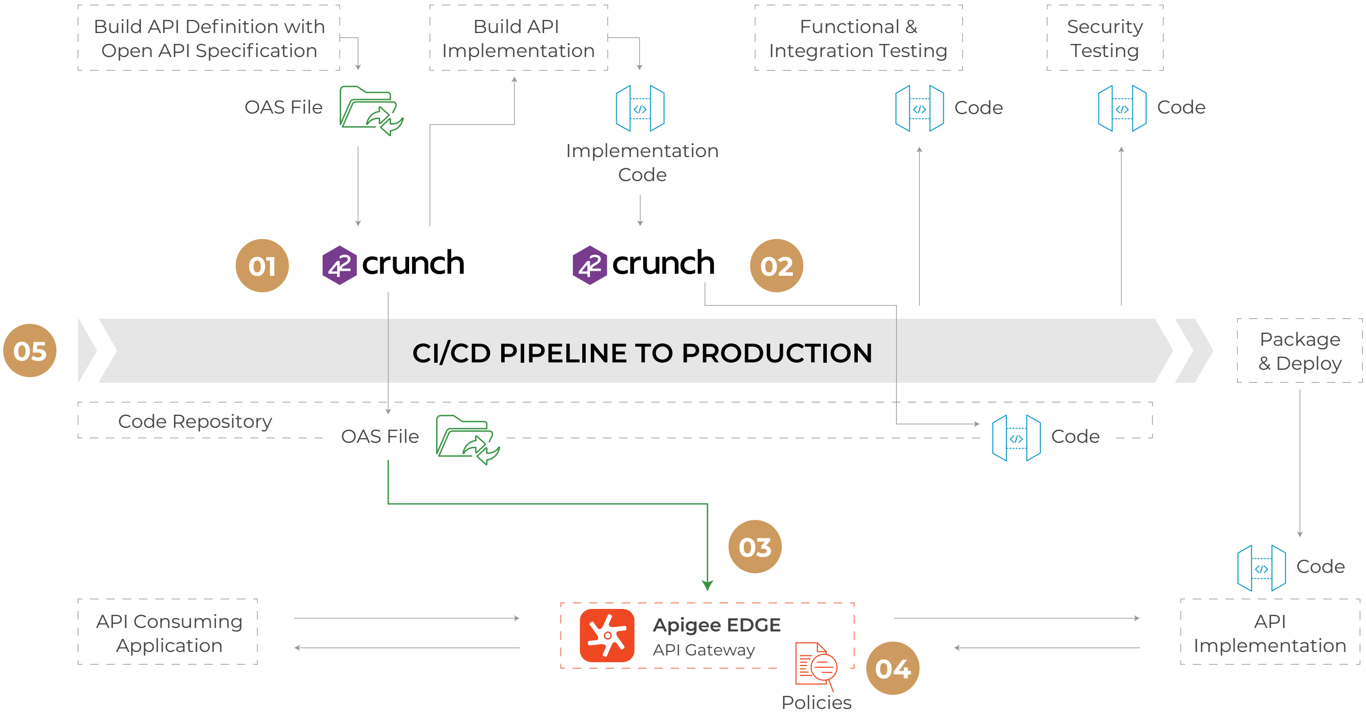
01 42Crunch audits your OAS files for known OWASP API Security Top 10 vulnerabilities and provides remediation help inside the developer's IDEs.

02 42Crunch scans the API implementation continuously against the contract, detecting drifts and implementation security issues.

03 Approved OAS file is used to create an API Proxy in the Edge gateway.

04 Add the OAS validation policy to the API proxy to enforce the tested security inside the OAS file.

05 All steps above can be automated using your preferred CI/CD tools and gcloud CLI to ensure continuous enhanced security.


Build API Definition with Open API Specification
Build API Implementation
Functional & Integration Testing
Security Testing
OAS File
Implementation Code
Code
Code
01
crunch
crunch
02
05
CI/CD PIPELINE TO PRODUCTION
Package & Deploy
Code Repository
OAS File
Code
03
Code
API Consuming Application
Apigee EDGE
API Gateway
Policies
04
API Implementation