TECHNICAL SOLUTION BRIEF

UPGRADE API SECURITY
for WSO2 API Management

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 WSO2 API Gateway offers a good set of capabilities for role-based access control, traffic throttling and verification of content, but that is not enough in today's world. It requires an approach that starts at the beginning of the API lifecycle and automates it until it hits production. 42Crunch integrates with WSO2 to upgrade its API management offering, with a robust set of security testing and governance capabilities, enabling full end-to-end API security.

RUNTIME PROTECTION **WSO2**

- Integrate with Identity Management systems to protect against unauthenticated and unauthorized access
- Content validation
- JSON Threat protection
- Threat protection through pre-build REGEX
- Rate limiting

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 content validation policies inside the WSO2 API Gateway
- Automatically test the APIs' conformance to the specifications
- Test security resilience of the APIs as part of continuous integration
- Deliver security certified OAS files into the API Gateway

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.

API Runtime Protection

Feed your truly secure OpenAPI Specification into your API Management lifecycle, enabling your API Gateway to protect your API calls.

AUTOMATING API SECURITY WITH 42CRUNCH

Leveraging 42Crunch, WSO2 admins 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, WSO2 admins can focus on driving API utilization in the API Marketplace.

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

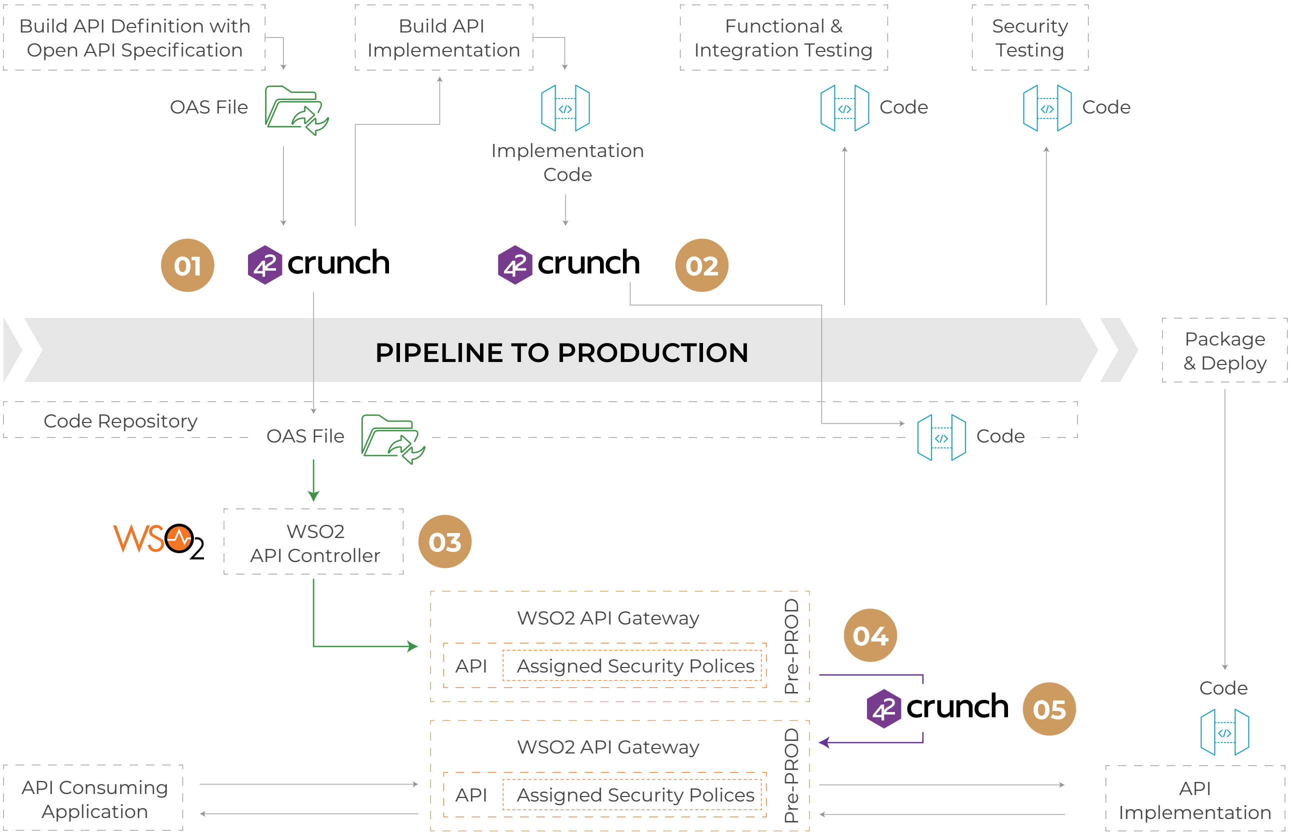
01 42Crunch audits your OAS files for known OWASP API Security Top 10 Vulnerabilities and provides remediation help inside the developer's IDEs.

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

03 Approved OAS file is used with the WSO2 API Controller(apictl) to create an API in an API Gateway in the development environment.

04 Utilizing the apictl export/import feature you can promote the API into higher environments following the lifecycle of the API implementation from development to production.

05 Make sure to use the 42Crunch scan in a Security Quality Gate (SQG) in your promotion pipeline to allow only the truly secure APIs get promoted to production.



© 42Crunch.com 2023