

# ENHANCE API SECURITY for Kong 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 Kong Gateway offers a good set of capabilities for role based access control, traffic throttling and basic 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. 42Crunch integrates with Kong to enhance the API management offering, with a robust set of security testing and governance features, enabling full end-to-end API security.

### RUNTIME PROTECTION KONG

- Protect APIs against unauthenticated access
- Protect APIs against unauthorized access
- HTTP Header verification
- JSON Threat protection
- JSON Schema Validation
- Rate limiting
- OpenAPI specification Validation

### 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 Kong basic schema validation policies
- Automatically test APIs conformance to the specifications
- Test security resilience of the APIs as part of continuous integration
- Enhance Kong APIOps approach with API security compliance rules
- Deliver security certified OAS files into the enterprise OAS Validation plugin



## 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 OAS file into your API Management lifecycle, enabling your API Gateway to protect your API calls.

# AUTOMATING API SECURITY WITH 42CRUNCH

Leveraging 42Crunch, Kong 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, Kong 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 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 in Kong's dataplane configuration with the Kong OAS validation plugin or JSON Schema validator.
- 04** API Gateway or Mesh Ingress Controller is updated with the security approved configuration.
- 05** Automate all steps above using your preferred CI/CD tools to ensure continuously enhanced security.

