Ignore APIs at Your Peril
Qualys and 42Crunch Partner to Deliver API Security

Jacques Declas
CEO, 42Crunch
Everyone loves containers

API Security Breaches are Mounting

“By 2022 API abuses will be the attack vector most responsible for data breaches within enterprise web applications”
Gartner Research - G342236
Why is securing APIs so difficult today?

<table>
<thead>
<tr>
<th>Enterprise Perimeter is Disappearing</th>
<th>Proliferation of end points, internet facing APIs, virtual network, micro-services architecture, distributed security enforcement points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of API Security Tools and Standards</td>
<td>No API Security standards, Complexity of API Security (Integrity, Confidentiality, AAA, non-repudiation..), no proven reusable API Security policies</td>
</tr>
<tr>
<td>Current Solutions Don’t Work for API’s</td>
<td>Web Application Security is not API Security, multiple solutions to cover part of API Security (CDN, WAF, API Gateway, Code...), API Developers often try to code Security into their APIs</td>
</tr>
</tbody>
</table>

Distributed, Unified, API Specific Security enforcement points
<table>
<thead>
<tr>
<th>Web App Security</th>
<th>API Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional White list/Black, hard to maintain, False positives</td>
<td><strong>Operational Model</strong></td>
</tr>
<tr>
<td>In-line WAF single layer north-south only, DMZ only</td>
<td><strong>Deployment</strong></td>
</tr>
<tr>
<td><strong>API Specific attacks</strong></td>
<td></td>
</tr>
<tr>
<td>API request validation (OAS 2.0)</td>
<td></td>
</tr>
<tr>
<td>XML &amp; JSON schema validation</td>
<td></td>
</tr>
<tr>
<td>XML Threat Protection.</td>
<td></td>
</tr>
<tr>
<td>JSON Threat Protection</td>
<td></td>
</tr>
<tr>
<td>JSON Path / JSON Pointer injections</td>
<td></td>
</tr>
<tr>
<td>SQL Injection Vulnerability detection in encrypted</td>
<td></td>
</tr>
<tr>
<td>OAuth Security ext. support PKCE, token binding</td>
<td></td>
</tr>
<tr>
<td>JOSE, draft-cavage-http-signatures</td>
<td></td>
</tr>
<tr>
<td>Cross-Site Scripting attack detection</td>
<td></td>
</tr>
</tbody>
</table>
Developers Must use the Standard
Changing the API Security Model

**API Security as a commodity**
- Controlled by Security
- Applied by Developers

**Pre-built, proven security policies**
- Standards Compliant Security Best Practices

**Bring Security into DevOps**
- Policies are applied as part of API lifecycle

**Microservices architecture compliant**
- Docker-based micro API Firewall

**EASY SECURITY**
**PROVEN SECURITY**
**SECURITY AS CODE**
**SECURITY AT SCALE**
API Security
DevSecOps approach

**Discover**
API and Open API Discovery Service

**Validate**
API Security Assessment and Scoring

**Verify**
Scan Compliance of Open API Spec Against API

**Protect**
Deploy API Firewall in Front of API

**Report**
Real Time Dashboard of All You APIs Security

- **DEV SEC OPS**
  - Discover all the APIs you expose & consume in the enterprise

- **DEV**
  - API developers upload their SWAGGER files => API Security Assessment report

- **DEV SEC**
  - API developers scan their APIs => Open API Compliance Report

- **SEC OPS**
  - Security team apply API Security Policies and Ops deploy the API Firewall

- **DEV SEC OPS**
  - Real time single pane view dashboard available to Developers, Security and Operations => API Security Dashboards
## Prebuilt Security Policies and Packages

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Transport Constraints</th>
<th>Request / Response Validation</th>
<th>Token Validation</th>
<th>Message Validation</th>
<th>Payload Crypto-Operations</th>
<th>Authentication</th>
<th>Authorization</th>
<th>Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWASP</td>
<td>TLS version and CipherSuites</td>
<td>Data Validation &amp; OWASP Attacks Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Banking</td>
<td></td>
<td>OAuth/OpenID Attacks Protection</td>
<td>OWASP Attacks Protection</td>
<td>Message Confidentiality &amp; Integrity</td>
<td>Identity Validation (Basic/OpenID)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI-DSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42C standard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
End to end API Security Process

- OpenAPI definition and code pushed to GitHub
- Automatic Security Assessment
- Automated Security Policies Generation
- Micro-firewall Image Generation
- Deploy API Firewall to protect your APIs

DEV  SEC  OPS
End-to-End API Security Platform
Thank You

Jacques Declas
CEO, 42Crunch