

Using Jenkins Pipeline and DevSecOps for API Security

Dmitry Sotnikov

Chief Product Officer, 42Crunch
Curator, <https://APIsecurity.io>

**DEVOPS
WORLD**
by CloudBees

“83% of all web traffic is now API call traffic.”

Akamai, State of the Internet 2018

“By 2022, APIs will become the #1 attack vector.”

Gartner, How to Build an Effective API Security Strategy

Source: API vulnerability reports at [APIsecurity.io](https://apisecurity.io)



Many APIs, Many Deployments

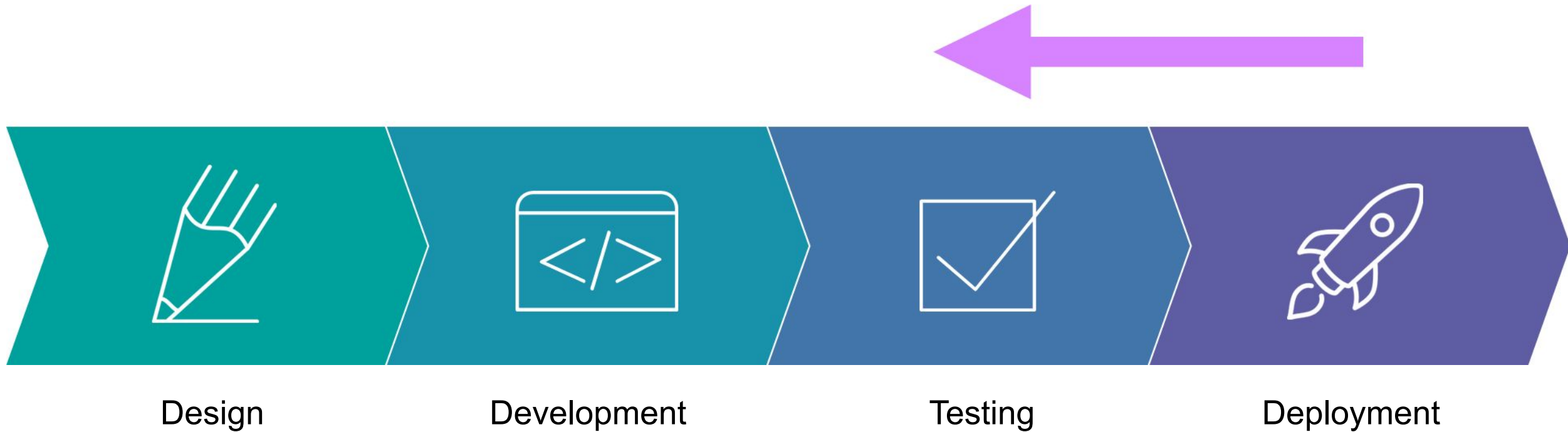


**APPLICATION
DEVELOPMENT**

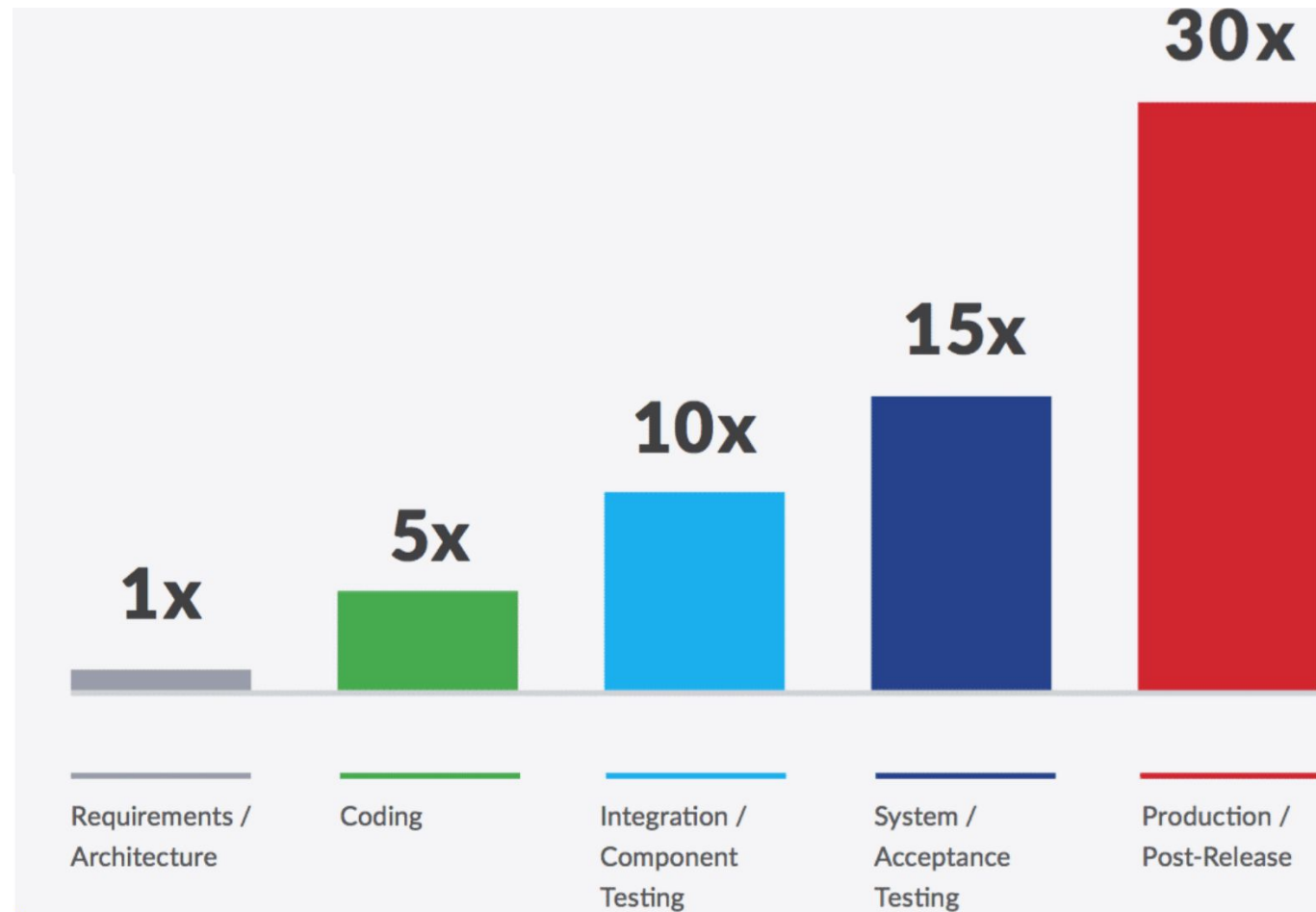


**APPLICATION
SECURITY**

Shift Left!



The Relative Cost of Fixing a Flaw per SDLC Stage



Source: NIST

DevSecOps for REST APIs in Jenkins

1. Sign up for <https://platform.42crunch.com/register>
2. Install Jenkins plugin: 42Crunch API Contract Security Audit
3. Configure it with the API key from 42Crunch
4. Add the build step to your pipeline
5. Enjoy the security enforced at each build!

Using Jenkins Pipeline and DevSecOps for API Security

Dmitry Sotnikov

Chief Product Officer, 42Crunch
Curator, <https://APIsecurity.io>

**DEVOPS
WORLD**
by CloudBees