OWASP 2023 GLOBAL AppSec | DUBLIN IRELAND FEB 13-16

Do more

With less screen time

$ id

- OWASP Lifetime Member
- Open Source developer (opencre.org)
- Ocurity
- spyros@ocurity.com
- @0xfde.infosec.stackexchange
- https://www.linkedin.com/in/spyr/

Automated security testing has brought security teams an abundance of signal about codebases and infrastrucure without much manual effort. However, we now spend a lot of time triaging false positives and managing findings This doesn’t scale and results in us hiring more security experts as vulnerability pushers. Due to that, many teams struggle to achieve time-saving features like per-team configuration, conditional tool execution and automated reporting to different sinks based on code ownership. In this talk, we bring you a new free and open source Application Security Toolchain Framework with integrations for several scanners both under the OWASP umbrella and not. This allows security teams to schedule tool execution against both code and infrastructure, aggregate the results from many different tools, enrich them using several processors and finally consume them with a multitude of visualization platforms. All in a safe, performant and platform-agnostic way.

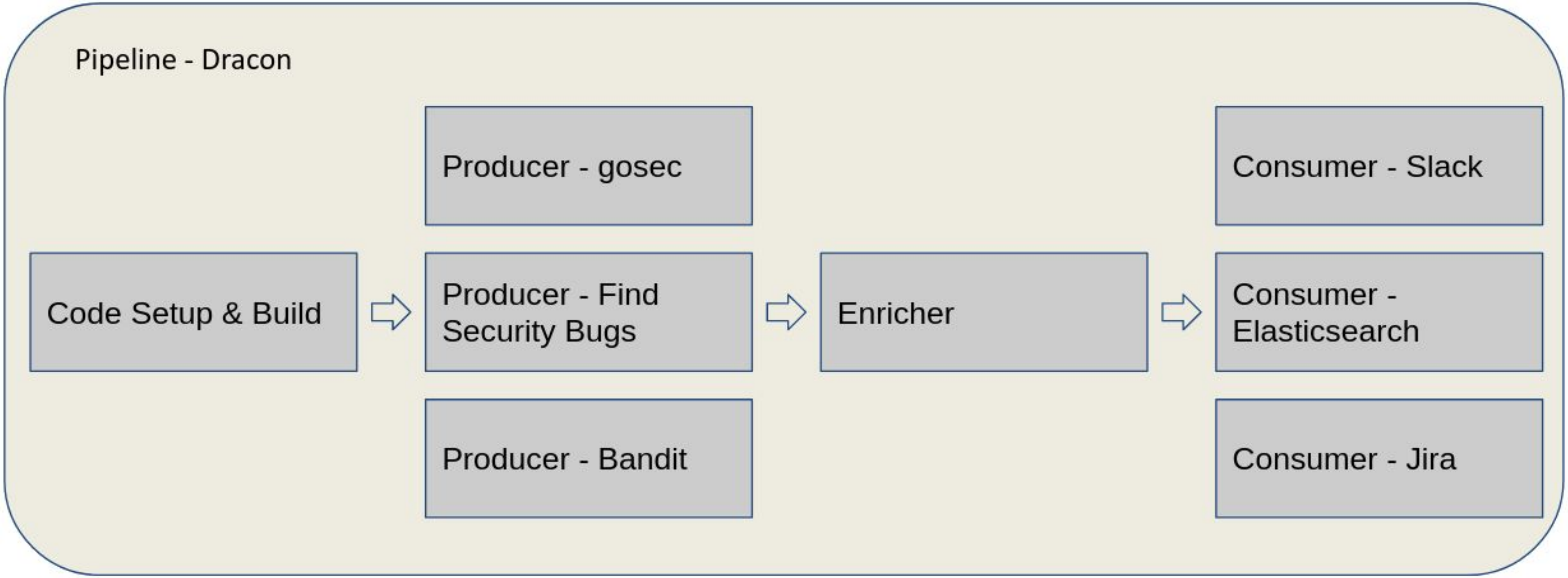
Detailed Outline

During the talk, we will introduce our use case, how it has helped us maintain a reasonable security baseline with less effort, how it allowed us to massively scale operations along with organizational growth without team expansion and how it allowed us to reuse tooling configuration among many different development teams. We then will introduce features that make it easy to create an automated security testing pipeline with most common security scanners, how we achieved this and how it can be done with little code. Furthermore we will showcase event-triggered pipelines, advanced supply chain security features, integration with several OWASP tools such as Dependency Track, ZAP, Defect Dojo and others as well as enriching beyond finding duplicates. Last we plan to deliver a demo of tooling execution and a short demonstration of how to integrate new tools. At the end of this talk, the audience will have a pretty good understanding of how to use this framework, what it can do for them and how to integrate their own tools/scanners.

Recap: ~~Problem~~ Challenge

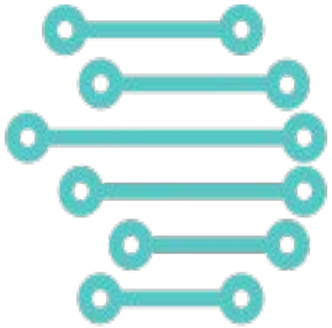
- Budget
- Fast pace
- Scale
- Many teams
- Not many Us

Recap: Tooling integration



Recap: v0

- SAST only
- Enrichment == duplicate tagging
- Jira as a vulnerability management platform



DRACON

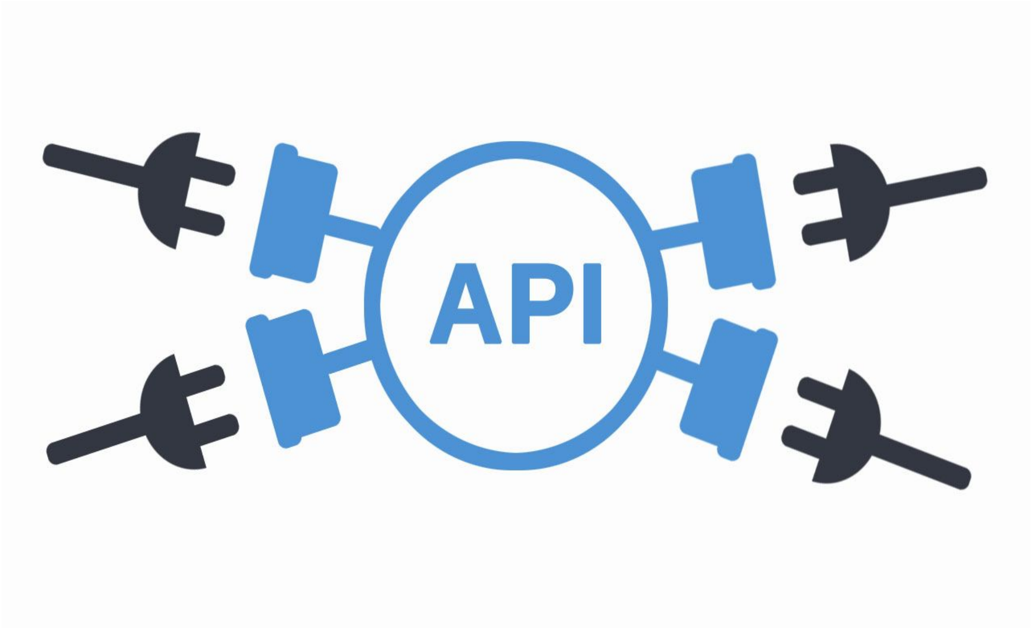
Overview: New Dracon

A **flexible** and **generic** security **workflow** and **orchestration** platform.

Unifies security tools, enriching information easily and efficiently.

New API

- More tooling categories (ANY scanning against a target).
- Arbitrary enrichment via annotations



New Producers

- Infrastructure As Code
- Composition Analysis
- SBOM generation
- ZAP (DAST)
- Writing producers trivial
- Generic SARIF and Cyclonedx

aqua tfsec

DEPENDENCY-CHECK

aqua trivy

CycloneDX

Enrichers

Open Policy Agent

More enrichers (policy via OPA)

Optionally signed enriched results

Consumers

- Dependency Track
- Generic Sarif consumer
- Generic webhook consumer
- Slack with templated messages

General UX

- Creating and maintaining pipelines –> almost no code.
- community-pipelines repository

Result useful to

- Developers
- Security champions
- Cloud/App Security engineers
- Security Directors
- Compliance Auditors
- Attack Surface Managers
- CISOs

DEMO

Recap

Dracon allows for **unification** of **security tooling** execution and r**esults management**.

It is

- Low code
- Core Dracon == Free, Open Source
- Community driven

Extensive component support with more on the way.

Future

- More Pipelines
- More Components
- Conditional Pipelines

Call to action

- Dracon == community
- Use it
- Use case blogs (ocurity.com/blog)
- Docs
- Integrate YOUR tools
- Talk to us (github.com/ocurity/dracon)
- Contribute pipelines! (github.com/ocurity/dracon-community-pipelines)

OWASP 2023
GLOBAL
AppSec

DUBLIN
IRELAND
FEB 13-16

THANK YOU!

OCURITY