How I reduced my AppSec workload (by 70%)

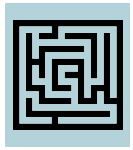
Nice to meet you

Spyros Gasteratos

- OWASP Volunteer
- OpenSource dev
- Founder – smithy.security

The Problem

Modern product security is slow, complex and expensive



Complicated
dev & ops stack

Different
third party systems

Manual effort
required for tickets

Lists of tests
(SAST, DAST, SCA), SBOM, audits

Many stakeholders
(i.e., Devs, DevOps, Compliance, CSO)

The realizations

1. Application Security is a **Business** and a **Human** set of problems
2. You need to combine the best solution for each category
3. You need to encode business practices and risk tolerance for each team into your AppSec programme

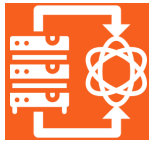
The Solution

Smithy makes security engineering faster, simpler and affordable at scale

No code
security orchestration

Easy to connect
any existing tools or own components

Automated workflows
for repetitive tasks



Security harmonization
and flexible result enrichment

One source of truth
for your entire team

Capabilities

A full suite of tools in one simple solution

- Reduce DevSecOps Noise via filtering
- Reduce MTTR via enrichment
- Suggest Secure Defaults via enrichment
- Report to multiple sinks
- Generate a queryable source of truth

Demo – Low Noise DevSecOps

- All your AppSec automation
- Setup in seconds
- Any vendor/tool
- Noise reduction
- Reporting wherever you want it

Plug and Play

Smithy can connect to anything

Seamlessly connect to all state of the art security tools, integrations or own custom components.

Security Tools

Configuration

checkov

Secrets

GitGuardian

DAST

test SSL

SCA

aqua trivy

Safety

DEPENDENCY-CHECK

yarn

snyk

mend.io

SAST

aqua tfsec

sonarqube

Semgrep

Bandit

KICS by Checkmarx

Checkmarx

VERACODE

Integrations

Vulnerability Mngmt

Alerting & Comms

Ticketing Systems

JIRA

Backstage

Datalakes

MongoDB.

elastic

Google Big Query

Add your own

Any new tool, integration or custom component can be added by request.

Results

- MTTR reduction
  - Low noise
  - High Signal
- Noise reduction
  - Reprioritization
  - Duplicate detection
  - Exploitability
  - Reachability
- Seamless audits
  - Scanning evidence
  - Remediation evidence
  - Triaging evidence

More automation ideas

- Threat modeling (semi-generated) STRIDE-GPT, Threat Dragon, or PyTM
- Run on events.

Thank you

Questions?

Smithy – give us a star?: https://github.com/smithy-security/smithy