POLITECNICO
MILANO 1863

Scaling a DevSecOps Program: Lessons from Arduino Cloud Service

Alessandro Braccio - Alberto Pelenc

OWASP Italy Day 2023

Politecnico of Milan - 11th September 2023

Speakers

Alberto Pelenc

Engineering Manager @ Arduino

Alessandro Braccio

Senior Security Engineer @ Arduino
Italy Chapter Leader @ DevSecCon

Agenda

- What is Arduino
  - Core Values
  - Software Teams
  - The Arduino Cloud
  - Security Posture
  - Product Development Life-Cycle

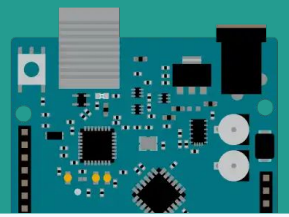
- Secure SDLC
  - AppSec vs. ProdSec
  - Objectives
  - Common Pitfalls
  - OWASP Methodologies
  - Tailored Model
- DevSecOps
  - Tailored CI/CD
  - Converter Extension
  - Validator Extension

What is Arduino

Hardware

From prototyping to production

- Boards
- Kits
- Turnkey solutions
- Third-party accessories
- Shields



Software & tools

Get the most out of your boards

- Editors & IDEs
- Code generators
- Compilers
- Debuggers
- Firmware update tools
- CLI

Focus of this presentation

Cloud services

Remotely monitor and manage your devices

- Dashboards
- Device management
- MQTT
- OTA
- Web & Mobile UI
- APIs

Knowledge

Unprecedented productivity

- Community
- Content
- Support
- Open source

ARDUINO
OPEN-SOURCE
COMMUNITY

Core Values

Mission / vision

Arduino's mission is to enable anyone to enhance their lives through accessible electronics and digital technologies.

Democratization and simplification of technology

Broaden the developers basis beyond specialized engineers, reducing friction.

Open source

Leverage a large developer community and knowledge, foster adoption and reduce lock-in risks for customers.

Provide creative solutions to everyday challenges

Empower students to learn by doing

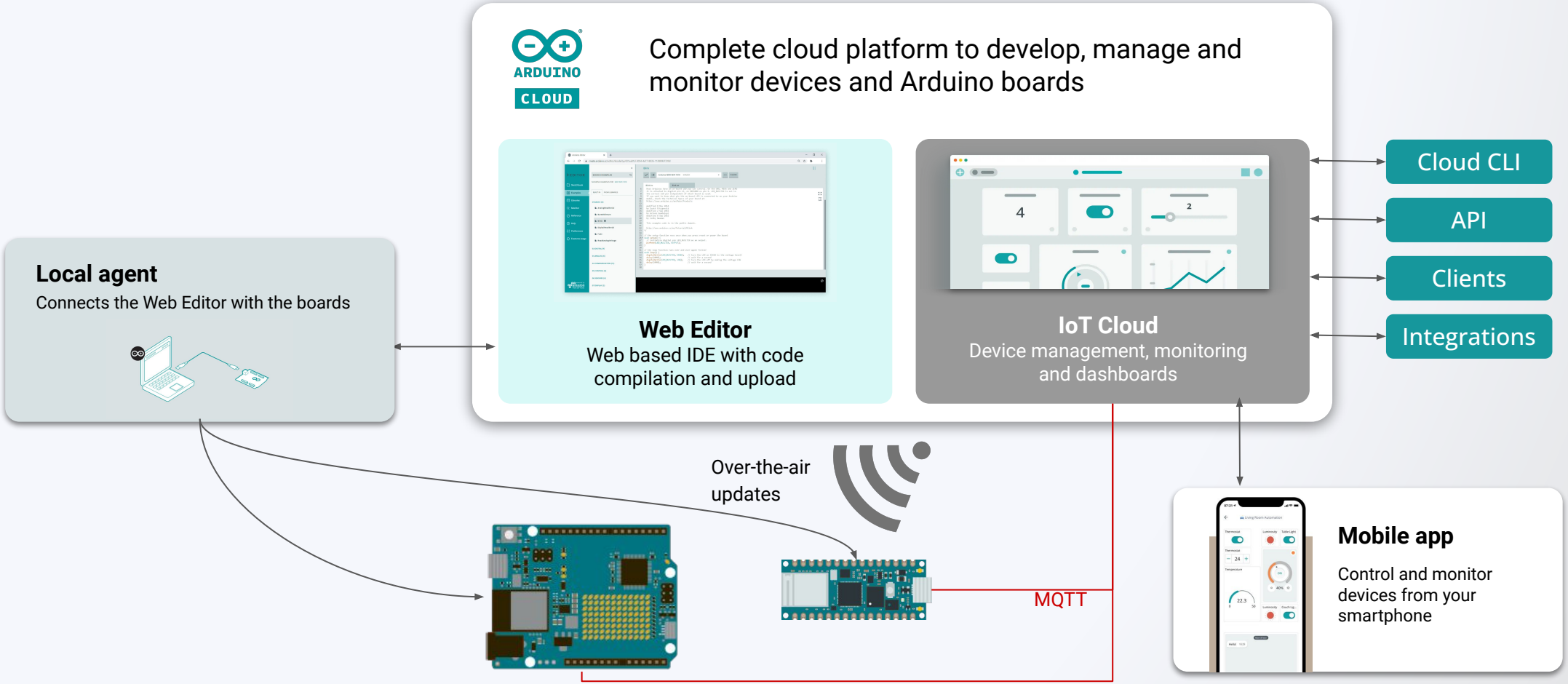
Enable business transformation

Software Teams

- 10 separate teams in the Software & Cloud division
- Different needs and tech stacks (Golang, C++, TypeScript, Python)

- Different kinds of teams:
  - Stream-aligned teams
  - Platform teams
  - Enabling teams


The Arduino Cloud



Arduino Cloud in Numbers

- Hundred thousands active users every month
- **10M** monthly page views, **30M** estimated active IDE users

Arduino Cloud:

- Active users: around **50K** monthly
- Messages processed: about **900M** each week
- Variables processed: about **1.8B** each week

Arduino Security Posture

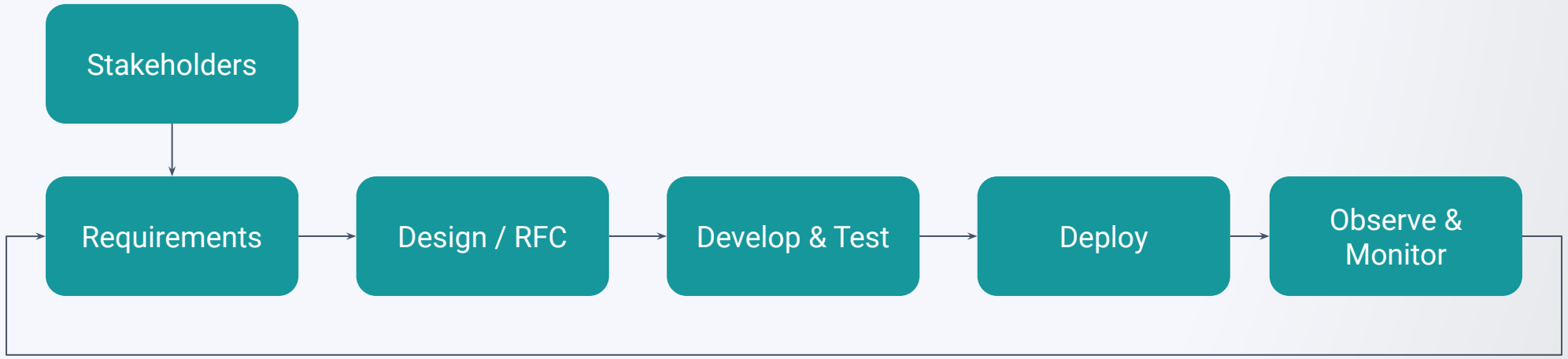
Arduino has a public page explaining the security lifecycle and software considerations

https://www.arduino.cc/en/security

Arduino Cloud Services are ISO 27001 certified

- Secure software development
- Access control
- System monitoring
- System testing
- Breach notification
- Data retention and disposal
- Vulnerability disclosure policy
- Security of Arduino services
- Security of Arduino tools and IDEs
- Status page
- Data protection (rest, in transit)
- Third party dependencies security

Product Development Life-Cycle



Reality:

- Stakeholders unexpected requests
- Change of business priorities
- Vulnerabilities and bugs

Secure Software Development Life Cycle

PLAN: security requirements are identified and analyzed. security risks and threats assessment.

DESIGN: security requirements are considered while defining the product architecture. Any workflow needing special security attention is designed and reviewed in detail before implementation.

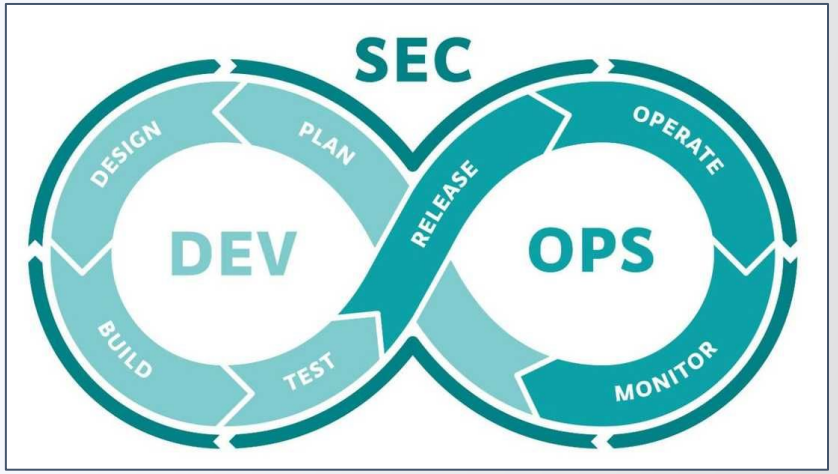
BUILD: secure coding principles and best practices are followed to minimize vulnerabilities and improve the overall “code hygiene”.

TEST: automated security activities, CI/CD pipelines are configured to perform these security tests as part of the build and test processes.

RELEASE: secure cloud configurations, access controls, and secure network architectures.

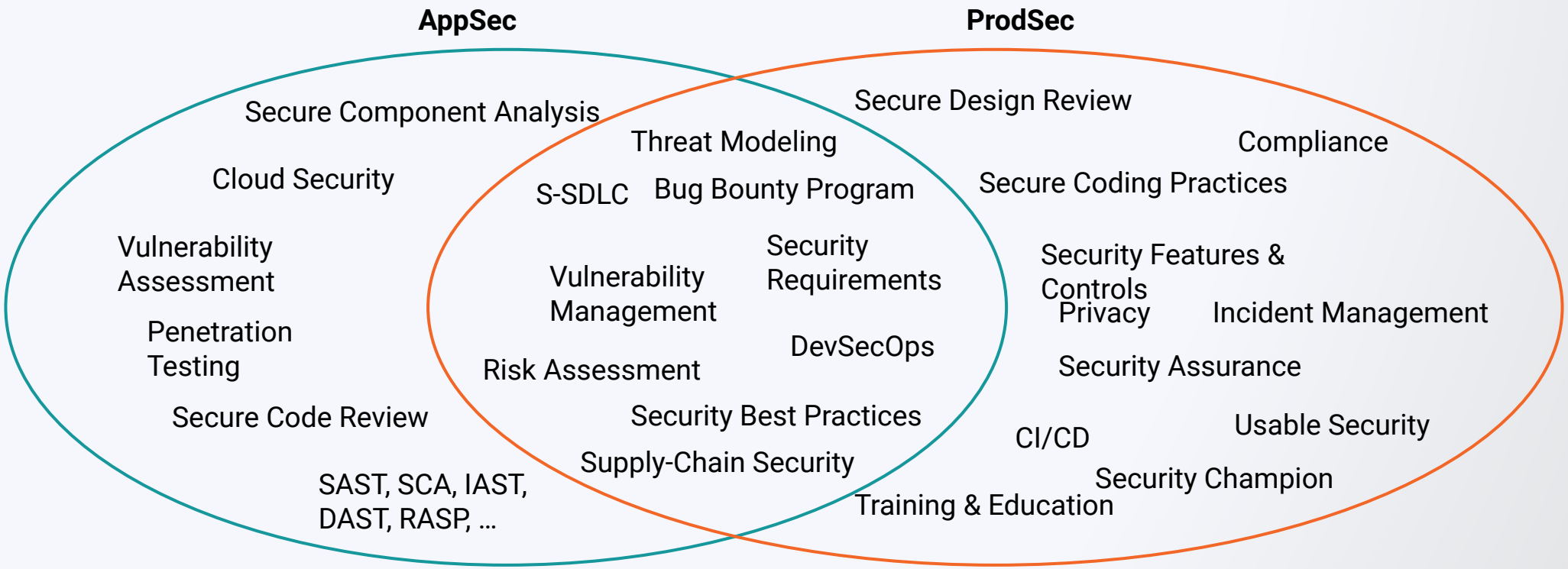
OPERATE: regular security audits and penetration tests are conducted to assess the system's resilience to attacks and ensure compliance

MONITOR: monitor the Cloud services status, detect anomalous behaviors and potential threats.



https://www.arduino.cc/en/security

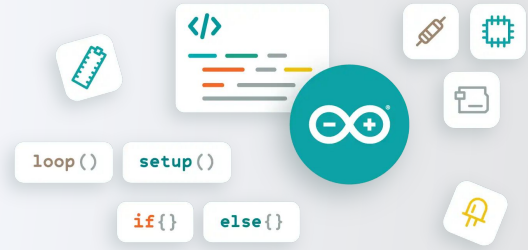
Application Security vs Product Security



"**Information Security** is the practice of protecting information by mitigating information **risks**"

"**Product Engineering** refer to the process of designing and developing a device, assembly, or system such that it be produced as an item for sale through some product manufacturing **process**"

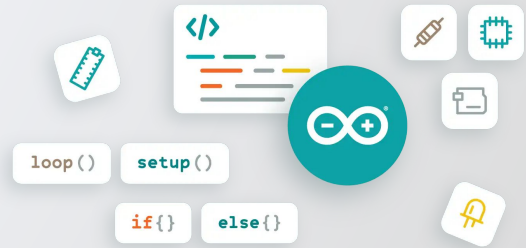
Objectives



- Embrace the Security-by-Design principle
  - from shift-left to shift-smart approach
- Spread and democratize security culture and practices between teams
  - Different teams means differents technologies, needs, context, behaviour, etc..
- Increase CI/CD automation maturity
- Security must intercept the products's time to market requirements
- Consider developers and devops as Security team's customers

Common Pitfalls

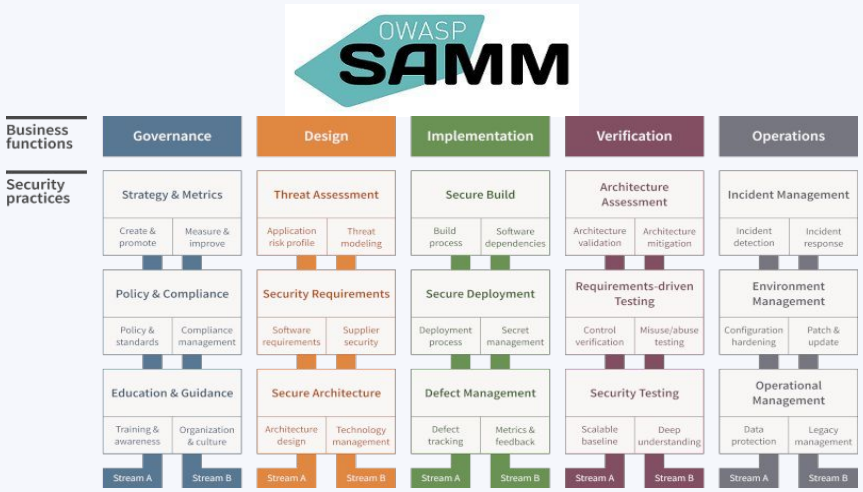
- Consider speed a reason to not implement, avoid, bypass, security controls
  - Initial Velocity vs Sustained Velocity
- Unfettered access to assets due to "agile approach"
  - Lack of Least of privilege, Defense in Depth, Security by Default
- Development team focused on self-risk-assessment without verification
- Siloed and inaccurate security tooling
- Lack of open communication between developers, devops, security team



OWASP Methodologies

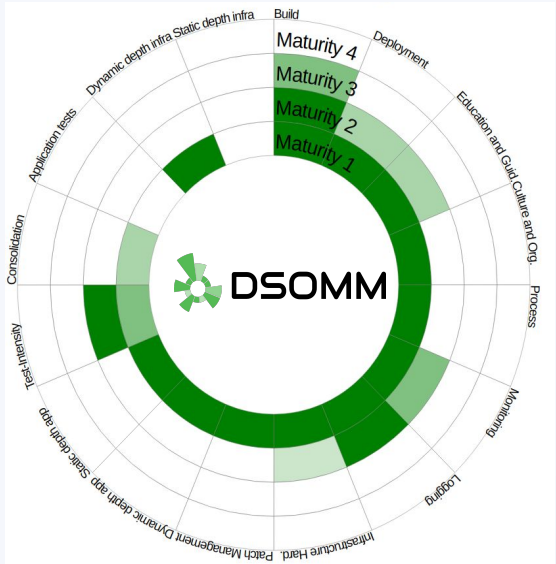
Software **A**ssurance **M**aturity **M**odel.
"SAMM provides an effective and measurable way for all types of organizations to analyze and improve their software security posture"

https://owaspsamm.org/



Dev**S**ec**O**ps **M**aturity **M**odel.
"Shows security measures which are applied when using DevOps strategies and how these can be prioritized."

https://dsomm.owasp.org/



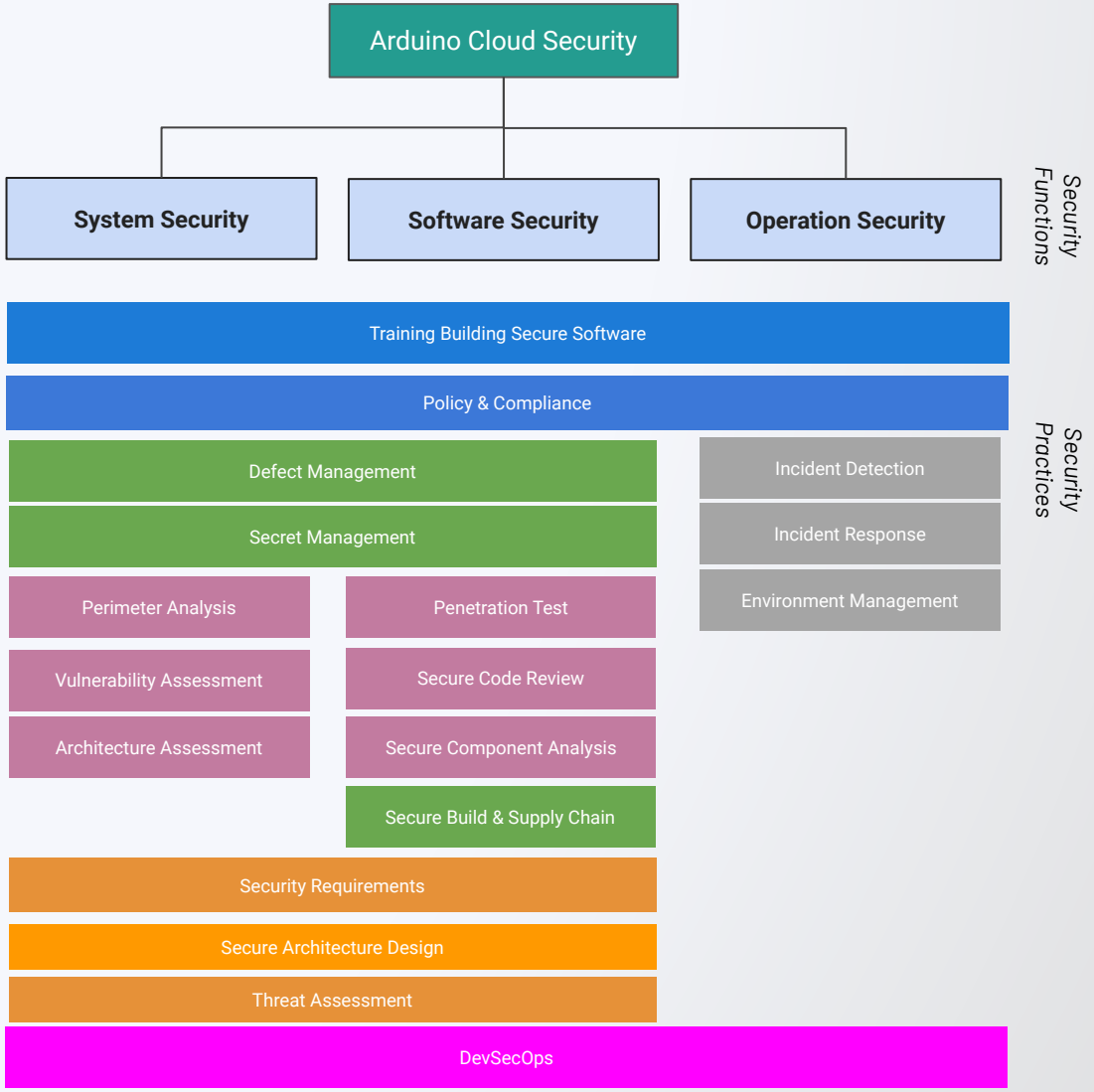
Testing Guide
"is a comprehensive guide to testing the security of web applications and web services"

Top 10
"is a standard awareness document for developers and web application security."

Tailored Model

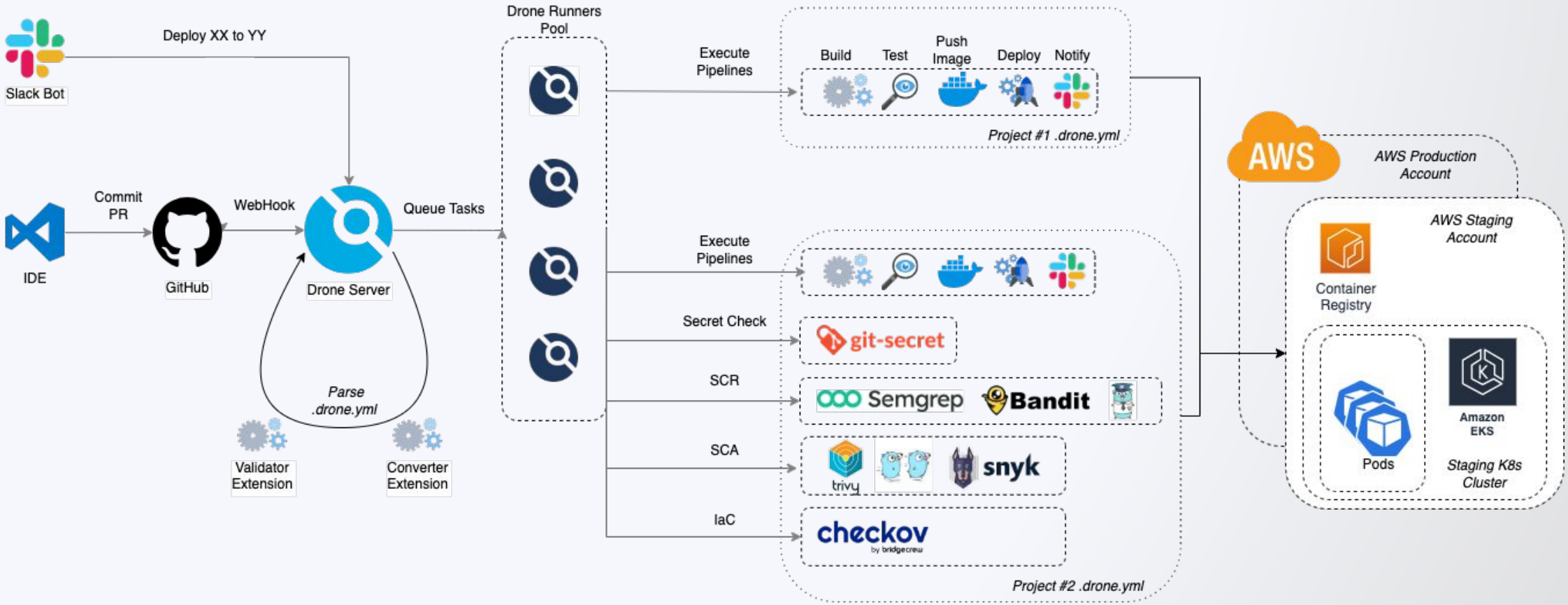
Benefits

- High level overview
- Strategic approach Top-to-Bottom
- Prioritize the roadmaps between years
- Team Independent
- Mapping practices to ISO 27001 policies and procedures
- Measurable maturity



DevSecOps in Practice

Tailored CI/CD

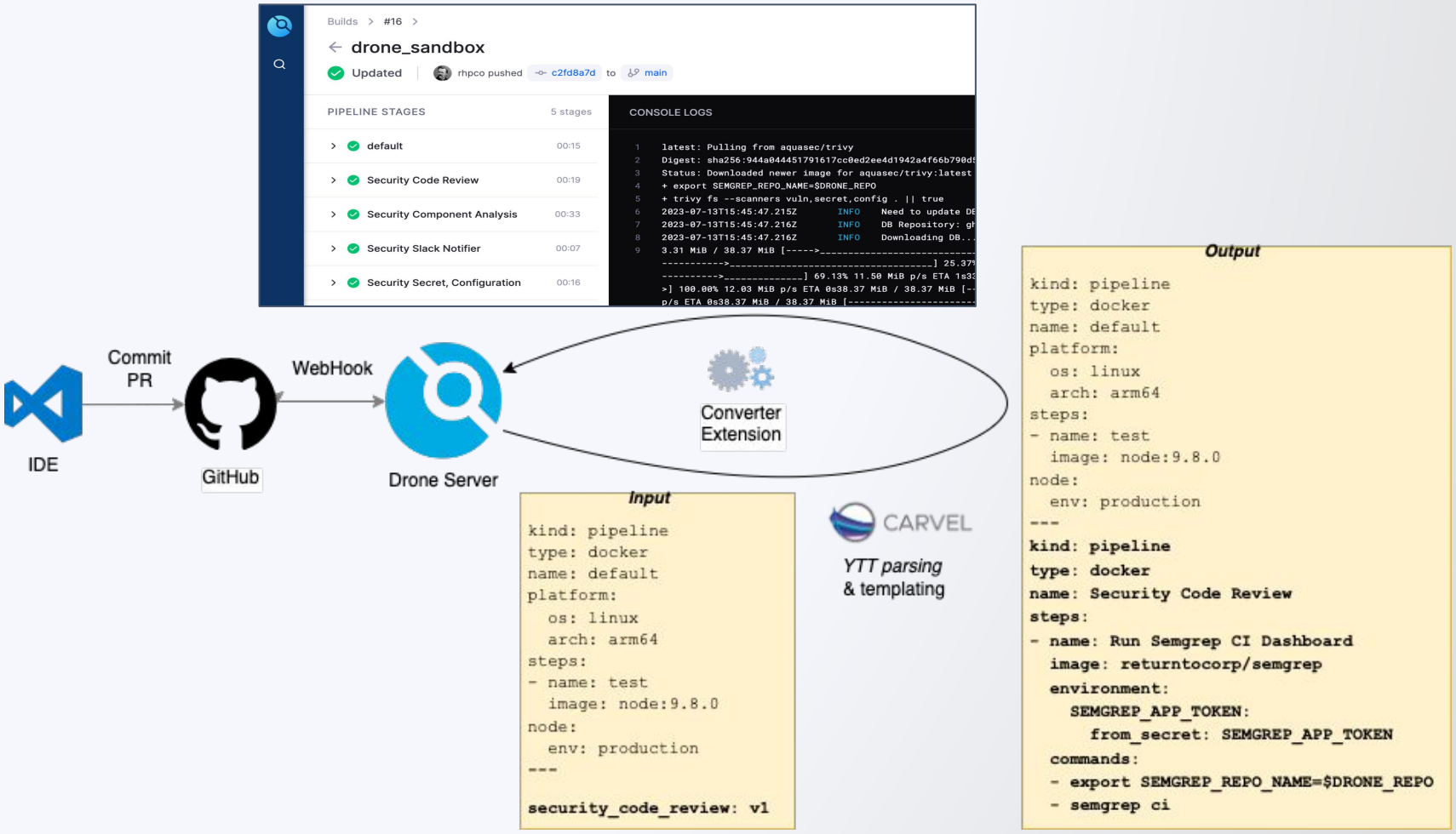


Converter Extension

Guarantee the *Defense in Depth* and *Security by Default* principles inside the CI/CD pipelines implementing security pipelines and templating mechanisms.

- Based on Carvel YTT tool (https://carvel.dev/)

- Solution implemented over YTT Overlays
- Custom template for:
  - Semgrep
  - Snyk
  - Trivy
  - Slack Notifier
  - etc..



Validator Extension

It adopts the ABAC (attribute based access control) strategy in order to verify if a particular attribute is accepted associated with specific object with the aim of guarantee the *Least of Privilege* strategy.

- Based on Casbin library (https://casbin.org/)
- Extremely customizable implementing tailored *Model*, *Policy*, *Matchers*
- Created to filter repositories that can use kubernetes specific service accounts associated with privileged IAM AWS roles.

1. **Model**:

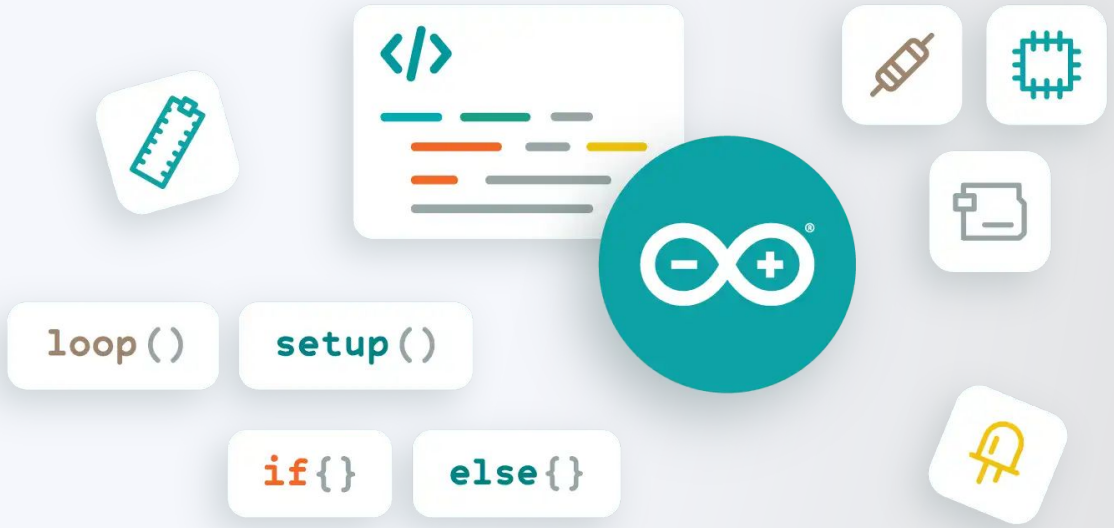
```
[request_definition]
r = sub, act

[policy_definition]
p = sub_rule, act

[policy_effect]
e = some(where (p.eft == allow))

[matchers]
m = eval(p.sub_rule) &&
r.act == p.act
```

2. **Policy**:

```
p, r.sub.Pipeline.ServiceAccountName == 'privileged-drone-runner-1' && r.sub.Request.Repo.Name == 'drone-test-repo', execute
p, r.sub.Pipeline.ServiceAccountName == 'privileged-drone-runner-2' && r.sub.Request.Repo.Name == 'users-api', execute
```

3. **Example**:

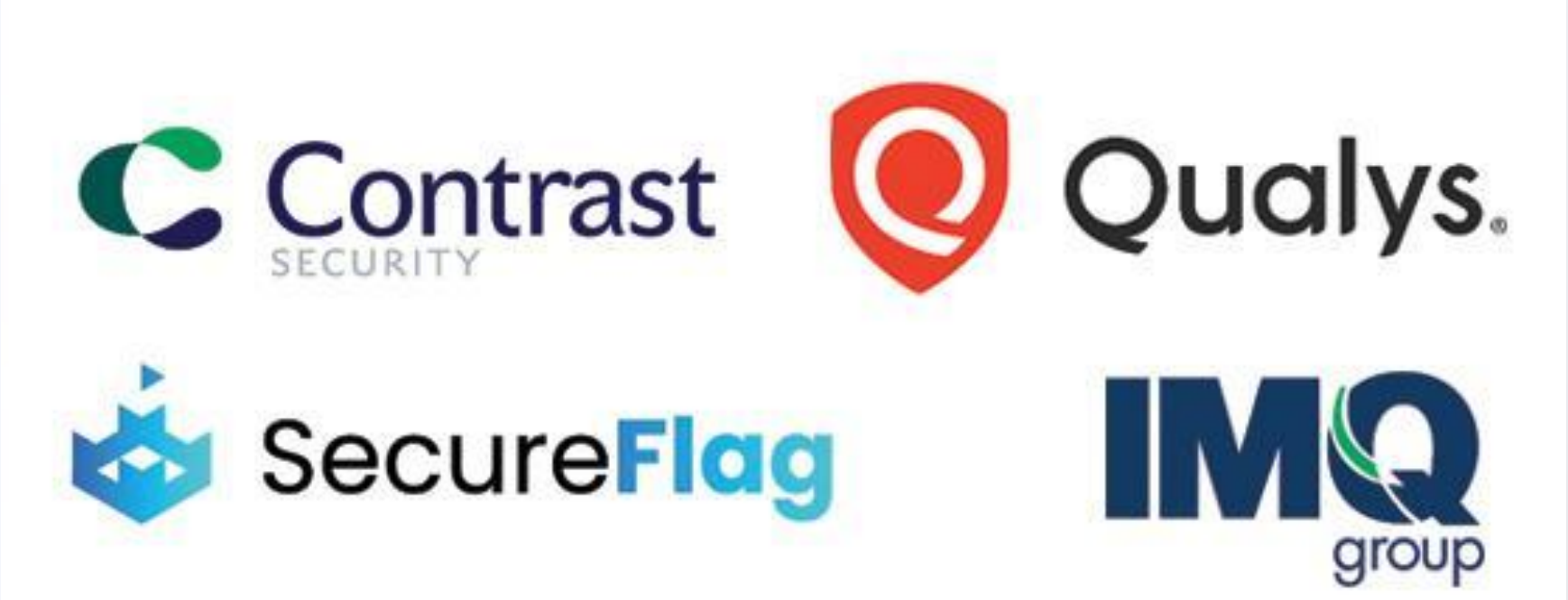
Questions



&

Answers

Thank you to our sponsors



OWASP 2023

ITALY DAY