



**Solution DevSecOps pour automatiser les tests de sécurité
applicative dans la chaine CI/CD**

Réunion OSSIR

09/03/2021

continus.io SAS

34 Avenue des Champs-Élysées

75008 Paris

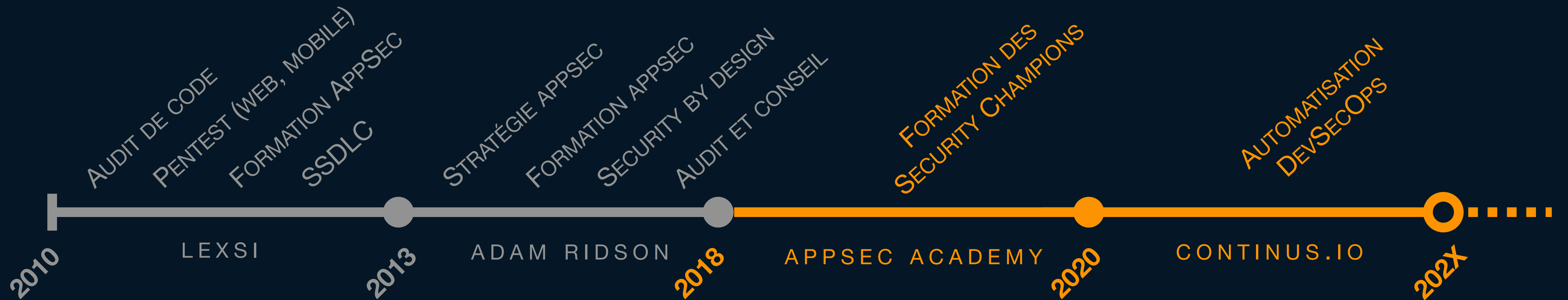
contact@continus.io

BIO

CTO & Co-Founder
Azziz ERRIME



CEO & Co-Founder
Tarik EL AOUADI



APPSEC ACADEMY

Assistance personnalisée

129 sur 28 Des tickets

ID	Statut	Sujet	Nom	Catégorie
73	Terminé	OCM, etc.	Fabian Webb	Suggestion d'amélioration
53	Terminé	Problème DiBuster	Benoit Stievenart	Problème technique lors de l'utilisation de notre plateforme
61	Terminé	aucune idée de comment appréhender / commencer les challenges S3-1/2/3	Yannick Lagarde	Aide à la compréhension du cours ou à la mise en oeuvre des exercices
71	Terminé	Accès à la session de coaching	Benoit Stievenart	Autre
70	Terminé	S4-4	Sébastien Lethellieux	Aide à la compréhension du cours ou à la mise en oeuvre des exercices
68	Terminé	lien de replay mardi semaine 4 KO	Stéphane Huette	Problème technique lors de l'utilisation de notre plateforme
69	Terminé	correction erronée sur un OCM S3-1	Didier Couderc	Suggestion d'amélioration

Prochains Événements > Téléprésentiel

2024/06/20

JUN 2020

- 2** Cours en Téléprésentiel #1 - Introduction aux risques et aux enjeux de la sécurité applicative
- 4** Coaching en Téléprésentiel - Nos experts AppSec répondent à toutes vos questions
- 9** Cours en Téléprésentiel #2 - Phase de découverte et sécurité des mécanismes d'authentification de sessions
- 11** Coaching en Téléprésentiel - Nos experts AppSec répondent à toutes vos questions

Suivez vos gains et vos pertes de Points et de SecCoins

Current Year

Synthèse des Points & SecCoins gagnés et perdus durant votre parcours de formation

Graph showing points and SecCoins over time (Jan to Dec).

★★★★★

"Au-delà de nos espérances : A la recherche d'une formation / d'actions nous avons décidés de faire confiance au concept novateur proposé par AppSec Academy. Le résultat a dépassé nos espérances, en effet nos développeurs, malgré la charge de travail projet, se sont pris au jeu en s'investissant pleinement pour réussir les challenges proposés. Le groupe dispose maintenant de plusieurs security champion qui sont force de proposition ... après avoir été de l'autre côté de la force pendant la session de formation"

Serge P.
RSSI

★★★★★

"Juste formidable cette formation."

Hichem L.
Développeur

★★★★★

"Bonne animation et des formateurs compétents. Le système de travaux pratiques est tip-top."

Ludovic B.
Développeur

Burp Suite Community Edition v2020.9.1 - Temporary Project

Issue activity [Pro version only]

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank...	/url-shorten
SMTP header injection	http://insecure-webs...	/contact-us
Serialized object in HTTP message	http://insecure-bank...	/blog
Cross-site scripting (DOM-based)	https://insecure-ban...	/
XML external entity injection	https://vulnerable-w...	/product/stock
External service interaction (HTTP)	https://insecure-web...	/product
Web cache poisoning	http://insecure-bank...	/contact-us
Server-side template injection	http://insecure-bank...	/user-homepage
SQL injection	https://vulnerable-w...	/
OS command injection	https://insecure-web...	/feedback/submit

log

9 20 Dec 2020 Info Proxy Proxy service

SQL Injection challenge

Difficulty level: ★★★

Detect, exploit & fix the SQL injection vulnerability - 1000pts

Detection | Exploitation | Remediation

Injection SQL Introduction

This article is focused on providing clear, simple, actionable guidance for preventing the entire category of Injection flaws in your applications. Injection attacks, especially **SQL Injection**, are unfortunately very common.

Application accessibility is a very important factor in protection and prevention of injection flaws. Only the minority of all applications within a company/enterprise are developed in house, where as most applications are from external sources. Open source applications give at least the opportunity to fix problems, but closed source applications need a different approach to injection flaws.

Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code, often found in SQL queries, LDAP queries, XPath queries, OS commands, program arguments, etc. Injection flaws are easy to discover when examining code, but more difficult via testing. Scanners and fuzzers can help attackers find them.

Depending on the accessibility different actions must be taken in order to fix them. It is always the best way to fix the problem in source code itself, or even redesign some parts of the applications. But if the source code is not available or it is simply uneconomical to fix legacy software only virtual patching makes sense.

Application Issues

[S1] Cours, Validation des acquis et Lab d'expérimentation

INTRODUCTION AUX RÉSULTATS ET ENJEUX DE LA SÉCURITÉ APPLICATIVE
RAPPEL SUR LES TECHNOLOGIES WEB
INTRODUCTION AUX TESTS D'INJECTION ET AUX MÉCANISMES DE DÉFENSE
PRÉSENTATION DE VOTRE LAB D'EXPÉRIMENTATION
Introduction #Rappels #OWASP

VOIR LE CRÉDIT DU MODULE

MODULE INCLUANT

- 9 Challenges
- 3 Démonstrations

Classement des meilleurs Hackers sur la plateforme

Afficher les meilleurs et prenez la première place de notre classement!

#	Avatar	Nom	Points	Niveau
1		Sébastien Lethellieux	42000	Wannabe hacker
2		Fabian Webb	43100	Adventuro
3		Didier Couderc	37700	Neubebe
4		Gilles Gosart	31000	Adventuro
5		Oth Tan	22400	Neubebe
6		Stéphane Huette	21800	Neubebe
7		Philippe Poggi	15600	Wannabe hacker
8		Yannick Lagarde	15200	Wannabe hacker
9		Louis Chessaix Bordes	13400	Adventuro

Membres inscrits

9 Inscrits

41 Sièges restants / 50 Sièges au total

Prénom	Nom	Email	Statut	Module
Adam	idson	tark.khous@admission.com	En cours	Exercice Progression
Krist	el	1stiaou@gmail.com	En cours	Démois Essais
Mawa	EL ADJADI	mawel@ctftrous.com	Pas commencé	T5:CH5P/C
Oth	Tan	othmane.tamagart@dam-dam.com	En cours	MUCC:BNK
Tarik	EL ADJADI	tark.khous@appsec.academy	Pas commencé	UP:5EUST

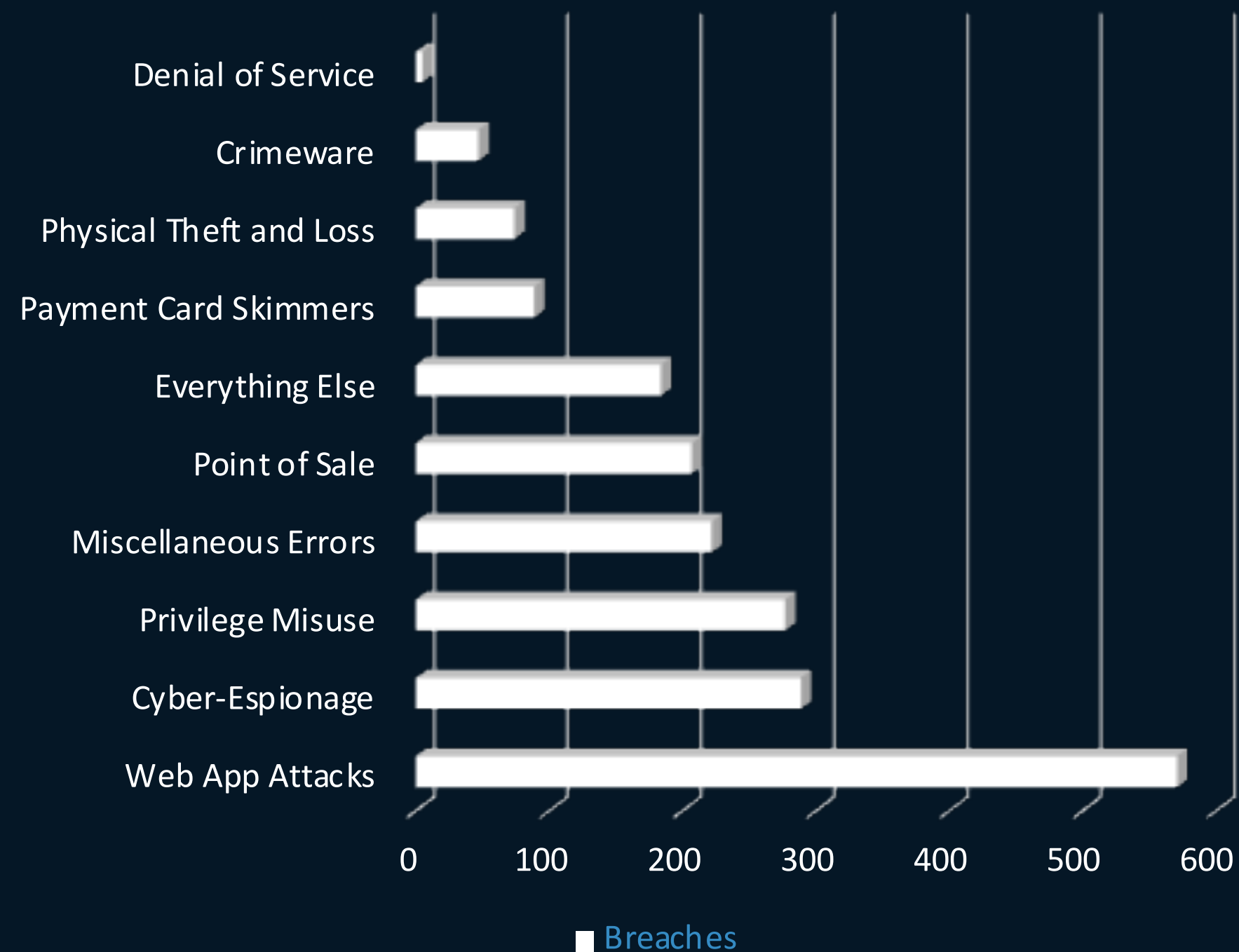
20 par Page

Chefs de projet

2 chef(s) de projet

Ajouter un chef de projet

Les applications sont la **Source #1** des fuites de données et la **Cible #1** des cyber-attaques



Source: 2017 Verizon Data Breach Report (DBIR)

Le respect de la vie privée, la conformité, la transformation numérique, le cloud, le DevOps, les API, le mobile et l'IdO contribuent à accroître de manière **exponentielle les risques liés à la sécurité des applications**

La sécurité des applications est **un sujet majeur pour le RSSI**



Top 5 Application Security **Risks**

- Manque de sensibilisation aux risques de sécurité des applications
- Développement de code source non sécurisé
- Méthodes de test médiocres/inadéquates
- Manque de budget pour soutenir les initiatives de sécurité applicative
- Staffing



Top 5 **Priorities**

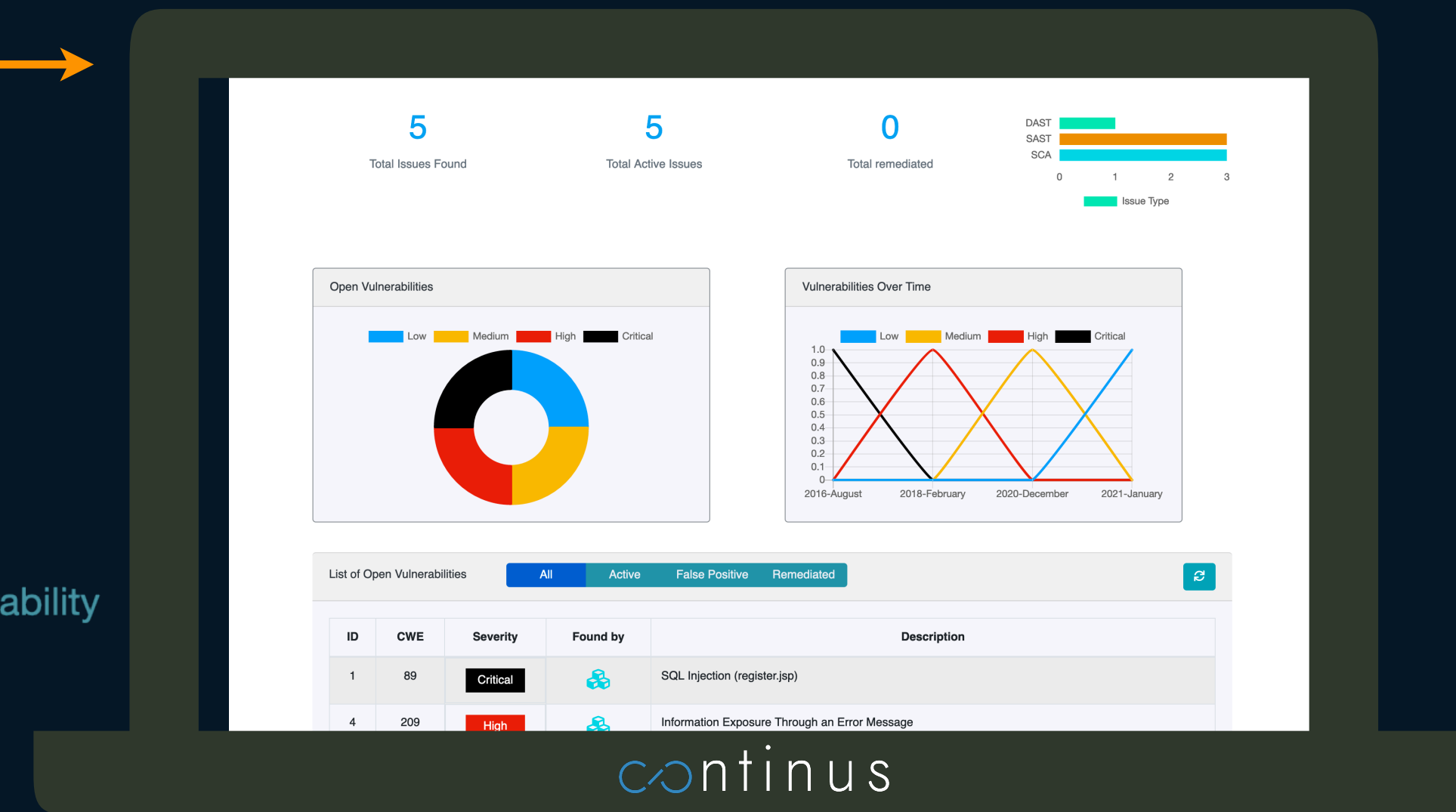
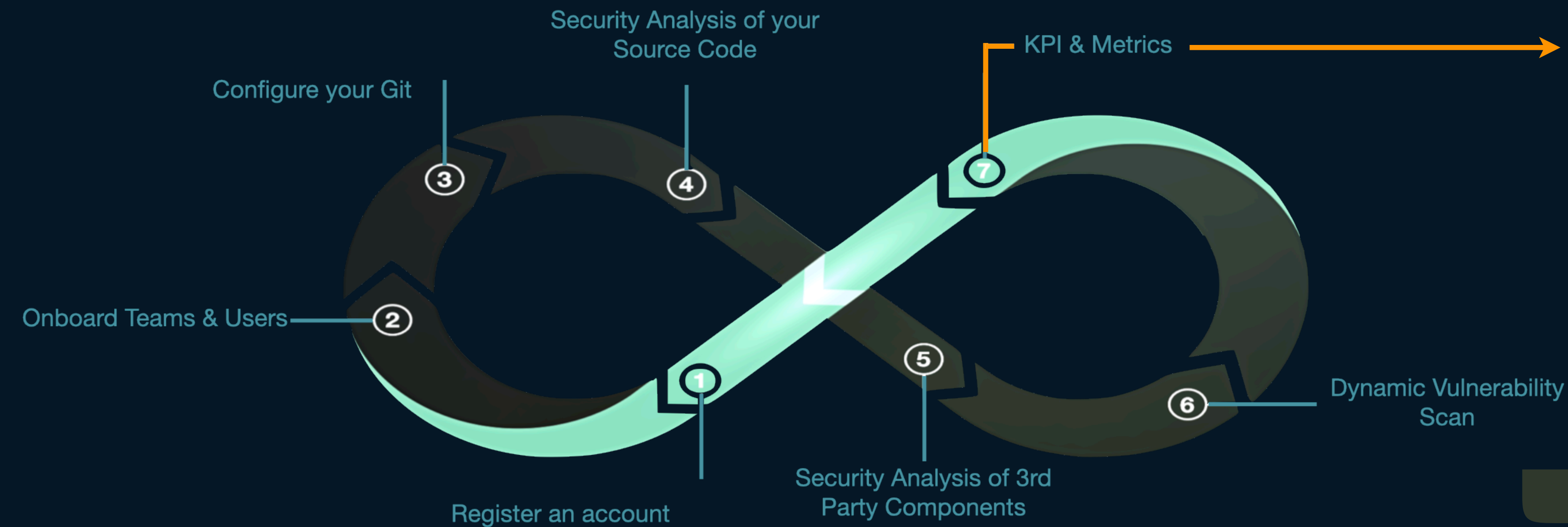
- Sensibilisation à la sécurité et formation des développeurs
- Sécuriser les processus du cycle de vie du développement
- Tests de sécurité pour les applications
- Gestion de la vulnérabilité des applications
- Analyse statique du code source pour trouver des failles de sécurité



Top 5 **Challenges**

- Disponibilité de ressources qualifiées
- Niveau de sensibilisation à la sécurité et sponsoring
- Méthodes de test médiocres/inadéquates
- Un budget adéquat
- Changement organisationnel

Approche continue de la sécurité applicative



CAPACITÉS

→ SAST - Static Application Security Testing

Secure your source code by building and scanning your repositories to identify sources of vulnerabilities to be fixed.

→ DAST - Dynamic Application Security Testing

Build and Deploy your code in a virtual environment to run sophisticated scans in order to detect vulnerabilities in your code changes with minimal user interactions

→ SDLC Coverage

Transparent and easy integration in the SDLC to secure build and deployment.

→ SCA - Software Composition Analysis

identifies risks in third-party and open source components that have been integrated into your applications and your containers.

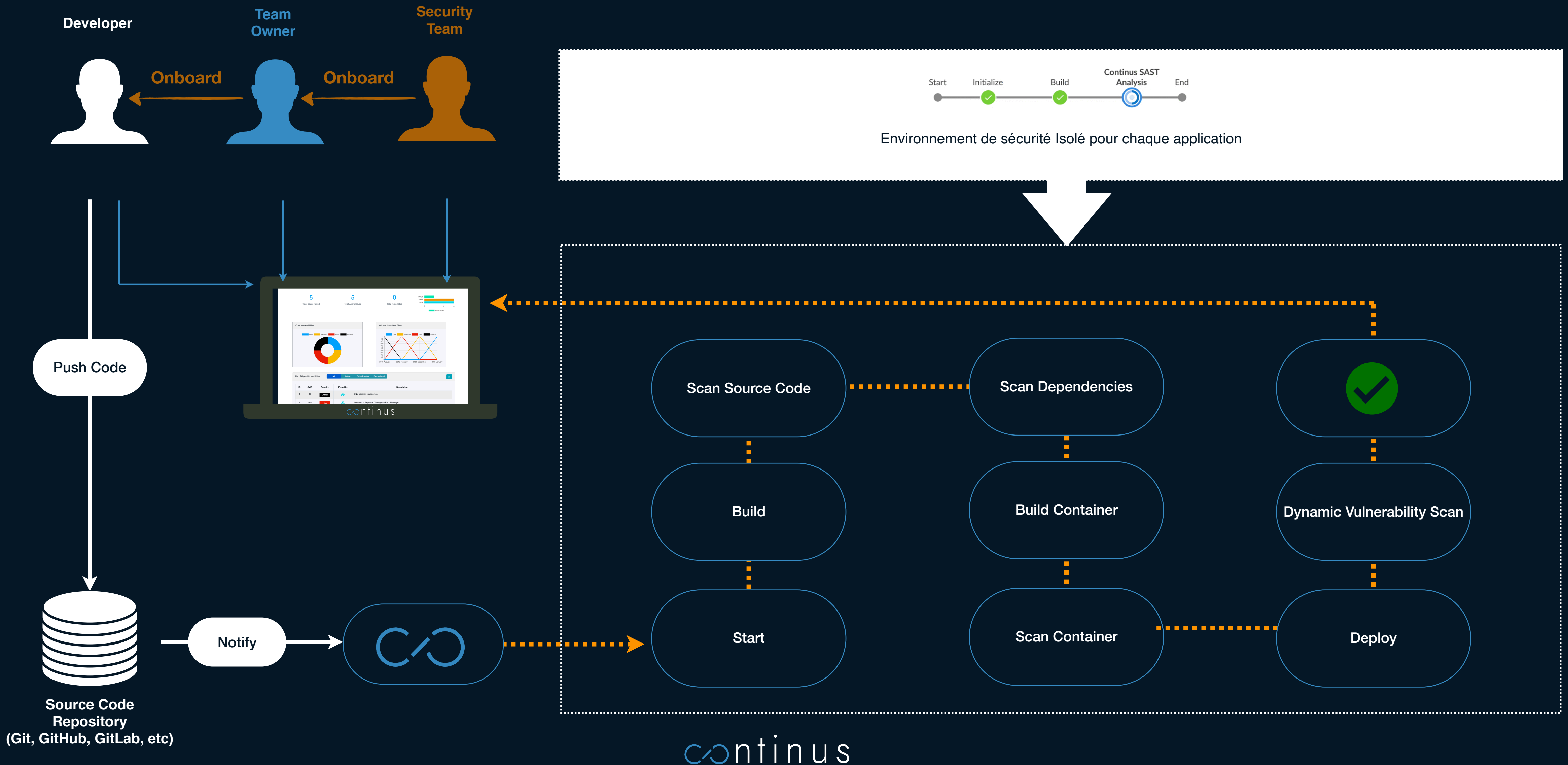
→ Automation and Speed

Just bring your own code, continus.io will take care of orchestrating the necessary application security tests in a dedicated environment without slowing your Time-To-Market

→ Security

Deploy a Dedicated and Isolated DevSecOps pipeline for each team to increase Security.

Comment ça marche ?



Dashboard

Executive Metrics

Technical Metrics

Operational Metrics

Governance

Team Management

Awareness

Security Testing

Source Code Analysis

Software Composition Analysis

Vulnerability Scanning

Dashboard

team excellence

team excellence

Team Details

Owned Teams

+ Add Team

Team Details

FR API Back

Connect to GitHub

Enter Repository Name

Select

#	Username	Email	Action
---	----------	-------	--------

Member has been saved successfully!

Member Email

azziz.errime@continus.io

Trained for security

+ Add Member

Close

Team Details ✕

team excellence

Activation Status: Activated

[Connect to GitHub](#)

Enter Repository Name Select

AppSec-Academy/dvwa	
AppSec-Academy/OfflineLab	
AppSec-Academy/bodgeit	
AppSec-Academy/juiceshop	
AppSec-Academy/webgoat	
AppSec-Academy/vulnapp	

	Action
	Edit remove

Trained for security

[+ Add Member](#)

[Close](#)