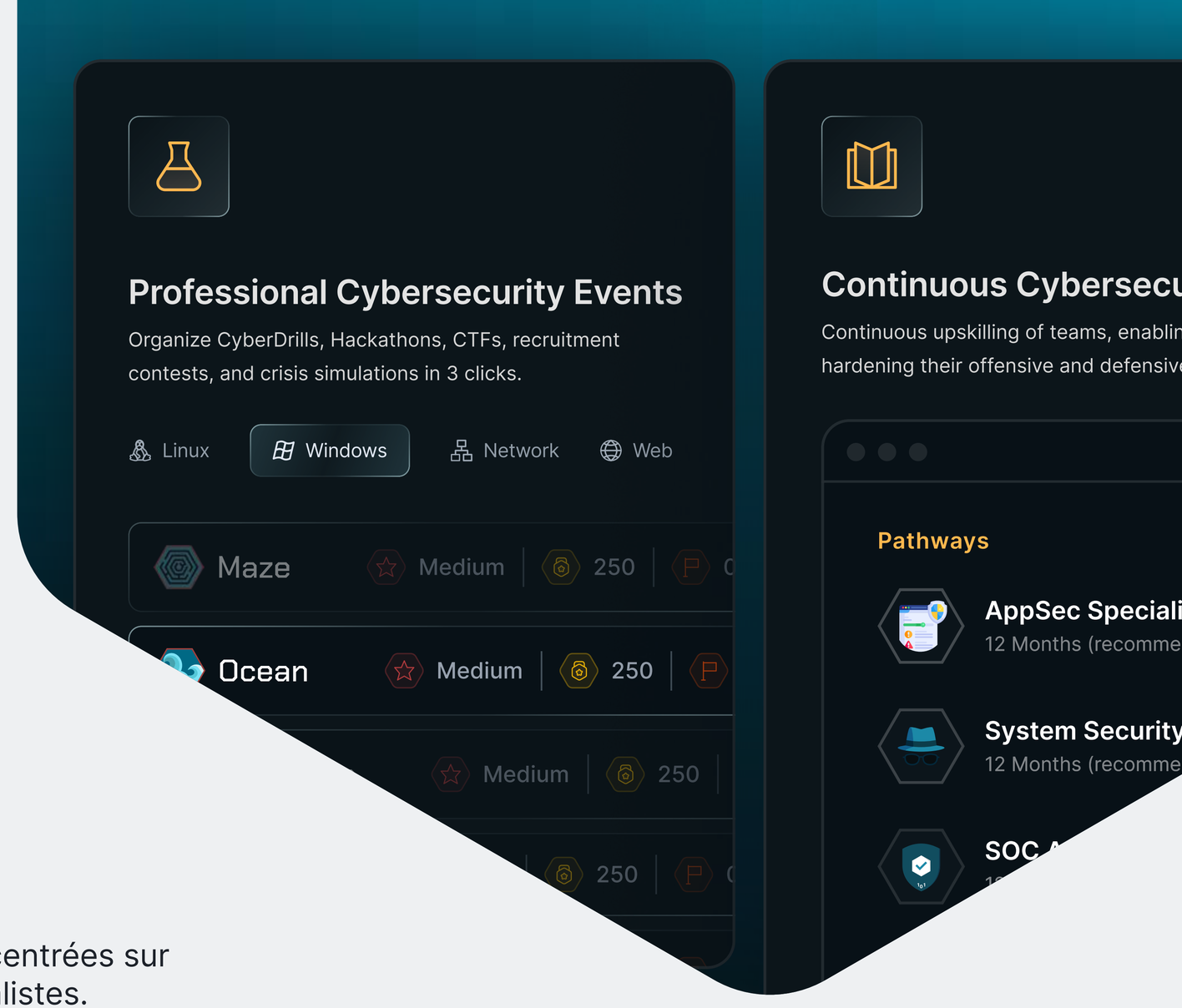
SecDojo



SecDojo

Accélérez la résilience cyber grâce à des entraînements centrées sur l'humain, des simulations et des exercices cyber hyperréalistes.

contact@sec-dojo.com

PÔLE D'EXCELLENCE CYBER

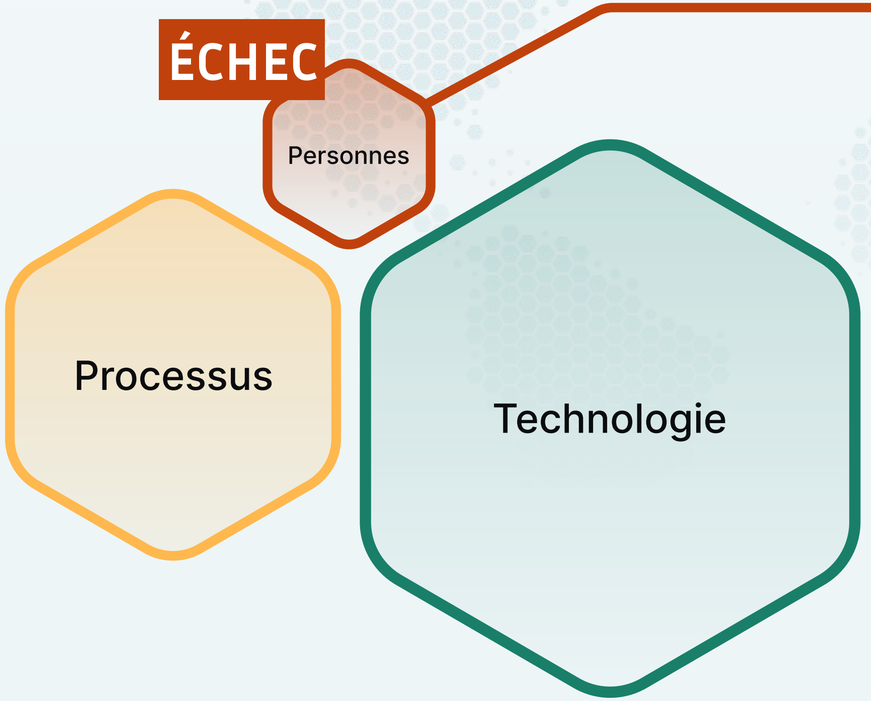
ECSO

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

SecDojo

LE CHALLENGE DE LA RÉSILIENCE CYBER

68% Des organisations associent leurs risques à un manque de compétences en cybersécurité.



Résilience cyber

=

Une bonne **stratégie** exécutée par des **équipes compétentes** en utilisant des bons **outils**.

SecDojo

PÉNURIE DE TALENTS EN CYBER EN AUGMENTATION AU FIL DES ANNÉES

Première ligne de défense

- Développeurs
- Administrateurs systèmes
- Chefs de projet IT
- ....

Manque de compétences en cybersécurité

Exemple : Absence de compétences en secure coding pour les développeurs

Seconde ligne de défense

- Analystes SOC
- Pentesteurs
- AppSec champion
- ....

Pénurie mondiale de talents en cybersécurité*

Manque de job readiness

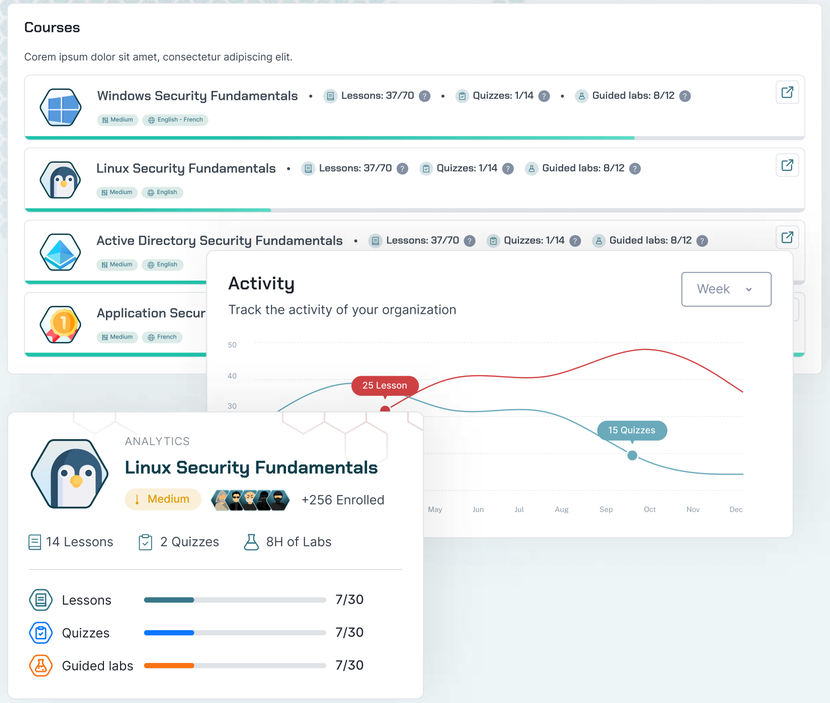
* Rapport ISC2 **2023** : **4 millions** de postes non pourvus en cybersécurité **(+15 %)**

SecDojo

CAS D'USAGES : SECDOJO

La Cyber Académie Par SecDojo :

- Upskiller les équipes **IT** pour intégrer la **sécurité by design.**
- **Booster la "cyber readiness"** grâce à des entraînements avancés représentant les **actualités** Cyber
- **Évaluer** les **compétences** Cyber pour un **recrutement efficace** et un meilleur suivi de **l'évolution de carrière.**
- Tests grandeur nature (**Cyber Drills**) pour les équipes IT et Cyber en mode hackathons, simulation crise, etc.



SecDojo

PLATEFORME DE “CYBER READINESS” BASÉ SUR LES FRAMEWORKS DE CYBER SKILLS

SecDojo

UNE EXPÉRIENCE D'APPRENTISSAGE EN CYBERSÉCURITÉ COMPLÈTE ET GAMIFIÉE

CyberLearn

Apprendre les **fondamentaux** et les **compétences** cyber de base.

CyberLab

Simulations Cyber **réalistes** et **gamifiées** en mode offensifs et défensifs.

CyberEvent

Organiser des **Cyber Drills** et des **simulations de crise** en quelques minutes.

CyberAwareness

Modules de sensibilisation, défis gamifiés et événements pour les profils techniques et non techniques.

Continuous Skills Validation

Certification, gestion de carrière et CyberHiring.

SecDojo

AVANTAGE COMPÉTITIF DE SECDOJO

- Un entraînement **engageant** et **gamifié** conçu pour stimuler la motivation et l'engagement
- Des **parcours d'upskilling complets** et une **validation des compétences** alignés sur les principaux **frameworks de cyber Skills.**
- Des **labs réalistes** simulant les **tâches IT** quotidiennes et abordant les **menaces cyber émergentes.**
- Un **modèle de pricing flexible** conçu pour favoriser l'**adoption de la technologie.**
- Une **marketplace** de solutions de sécurité pour créer des **labs personnalisés.**

FORRESTER®
WAVE LEADER 2023
Cybersecurity Skills And Training Platforms

Windows Server · Office · paloalto NETWORKS · f5 · FORTINET · CISCO · CHECK POINT
IBM Security · NGINX Plus · Symantec · GitLab · JUNIPER NETWORKS · Red Hat Enterprise Linux
CROWDSTRIKE · elasticsearch · TREND MICRO · tenable.sc · Qualys. · RAPID7

Annexes

SecDojo

LE PRINCIPAL FREIN À LA CYBER RÉSILIENCE DES ORGANISATIONS EST LA PÉNURIE DE COMPÉTENCES EN CYBER

Pénurie croissante de **talents** compétents en **cybersécurité**.

Cycles de recrutement, d'intégration et d'opérationnalisation des nouvelles recrues **longs et coûteux.**

Faible **maîtrise** des aspects de la **cybersécurité** par les équipes IT **(Dev, Sys Admin, DevOps, etc.).**

La **fidélisation** des collaborateurs nécessite des **plans optimaux d'évolution** de carrières.

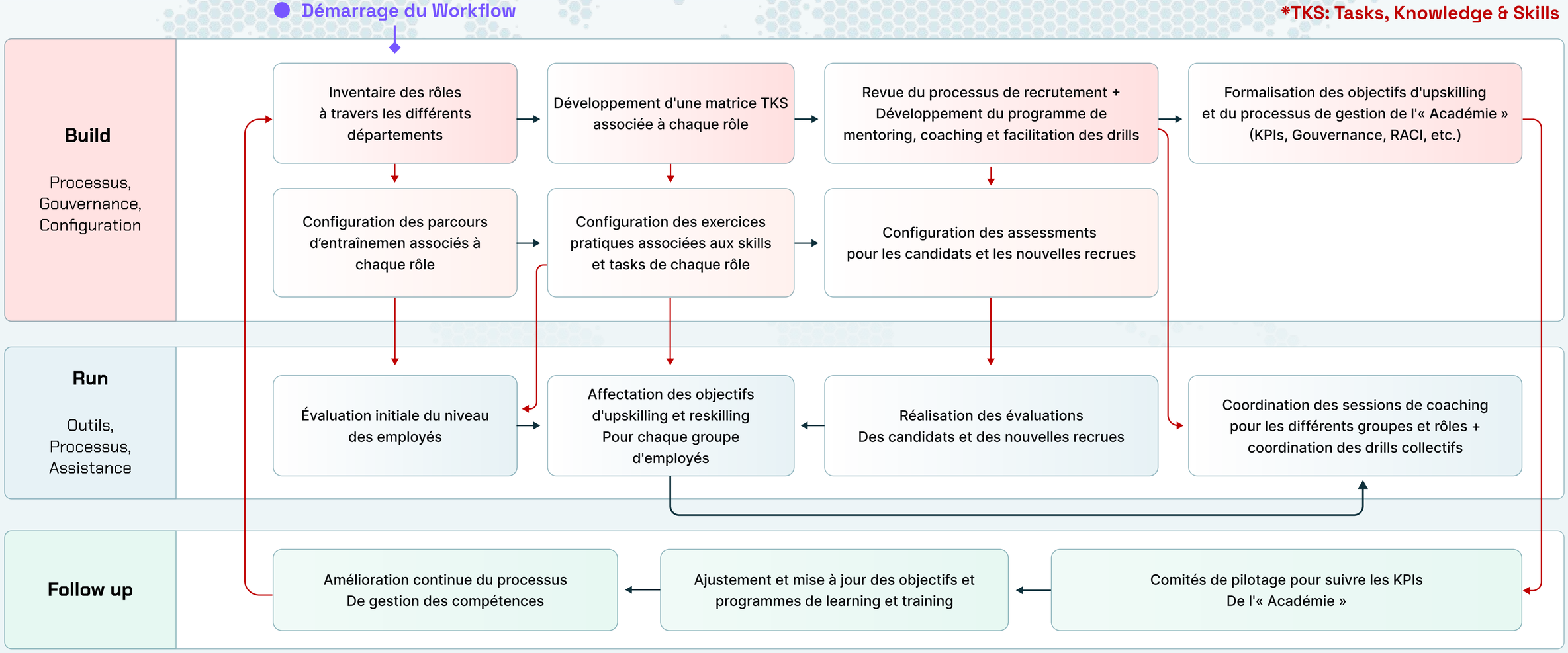
Taux de “**Turn Over**” élevés perturbant systématiquement les opérations et projets de cybersécurité.

SecDojo

CYBER ACADÉMIE : BUILD, OPERATE AND TRANSFER (BOT)

Démarrage du Workflow

*TKS: Tasks, Knowledge & Skills



Vulnérabilités du Top 10 OWASP

Le Projet Open Web Application Security (OWASP) est une communauté en ligne bien connue dans le monde de la sécurité des applications (AppSec), offrant une multitude de ressources pour vous aider à sécuriser vos applications web. Parmi ses ressources les plus reconnus figure le Top 10 OWASP, un document régulièrement mis à jour qui met en lumière les risques de sécurité d'application web les plus courant et les plus critiques.

OWASP Top 10

L'OWASP publie une version mise à jour de la liste du Top 10 tous les quelques années, généralement tous les trois à quatre ans.
Cette liste est compilée sur la base de l'analyse des vulnérabilités les plus prévalentes identifiées au cours des années précédentes (notamment au niveau des opérations de BugBounty).
Elle vise à guider les développeurs et les équipes de sécurité en mettant en évidence les problèmes récurrents et à haut risque et en encourageant une concentration sur ces domaines significatifs lors des modélisations de menaces, des évaluations de sécurité et de sécurisation des développements.

OWASP TOP 10 - 2010	OWASP TOP 10 - 2013	OWASP TOP 10 - 2017	OWASP TOP 10 - 2021
A1 - Injection	A1 - Injection	A1 - Injection	A1-Broken Access Control
A2-Cross Site Scripting (XSS)	A2- Broken Authentication and Session Management	A2- Broken Authentication and Session Management	A2-Cryptographic Failures
A3-Broken Authentication and Session Management	A3-Cross-Site Scripting (XSS)	A3-Sensitive Data Exposure	A3- Injection
A4 - Insecure Direct Object References	A4-Insecure Direct Object References	A4-XML External Entity (XXE)	A4-Insecure Design
A5-Cross Site Request Forgery (CSRF)	A5-Security Misconfiguration	A5-Broken Access Control	A5-Security Misconfiguration
A6-Security Misconfiguration	A6-Sensitive Data Exposure	A6-Security Misconfiguration	A6-Vulnerable and Outdated Components
A7-Insecure Cryptographic Storage	A7 - Missing Function Level Access Control	A7-Cross-Site Scripting (XSS)	A7-Identification and Authentication Components
A8 - Failure to Restrict URL Access	A8-Cross-Site Request Forgery (CSRF)	A8-Insecure Deserialization	A8-Software and Data Integrity Failures
A9-Insufficient Transport Layer Protection	A9-Using Components with Known Vulnerabilities	A9-Using Components with Known Vulnerabilities	A9-Security Logging and Monitoring Failures

SecDojo