OWASP Bordeaux Meet Up

Comment Mirakl gère et capitalise sur son programme Bug Bounty

Hello :)

Alexis Cadoret

Security Operations Lead @Mirakl (depuis 2020)

Operations, Offensive Security, Incidents, Compliance

https://www.linkedin.com/in/alexiscadoret/

https://www.linkedin.com/company/mirakl/

$6B
GMV through Mirakl Platform in 2022

400+
active clients around the world

750+
employees worldwide

99.99%
Uptime

Grocery: Carrefour, Pour de Bon, Auchan

Generalist: MediaMarkt, Galeries Lafayette, El Corte Inglés

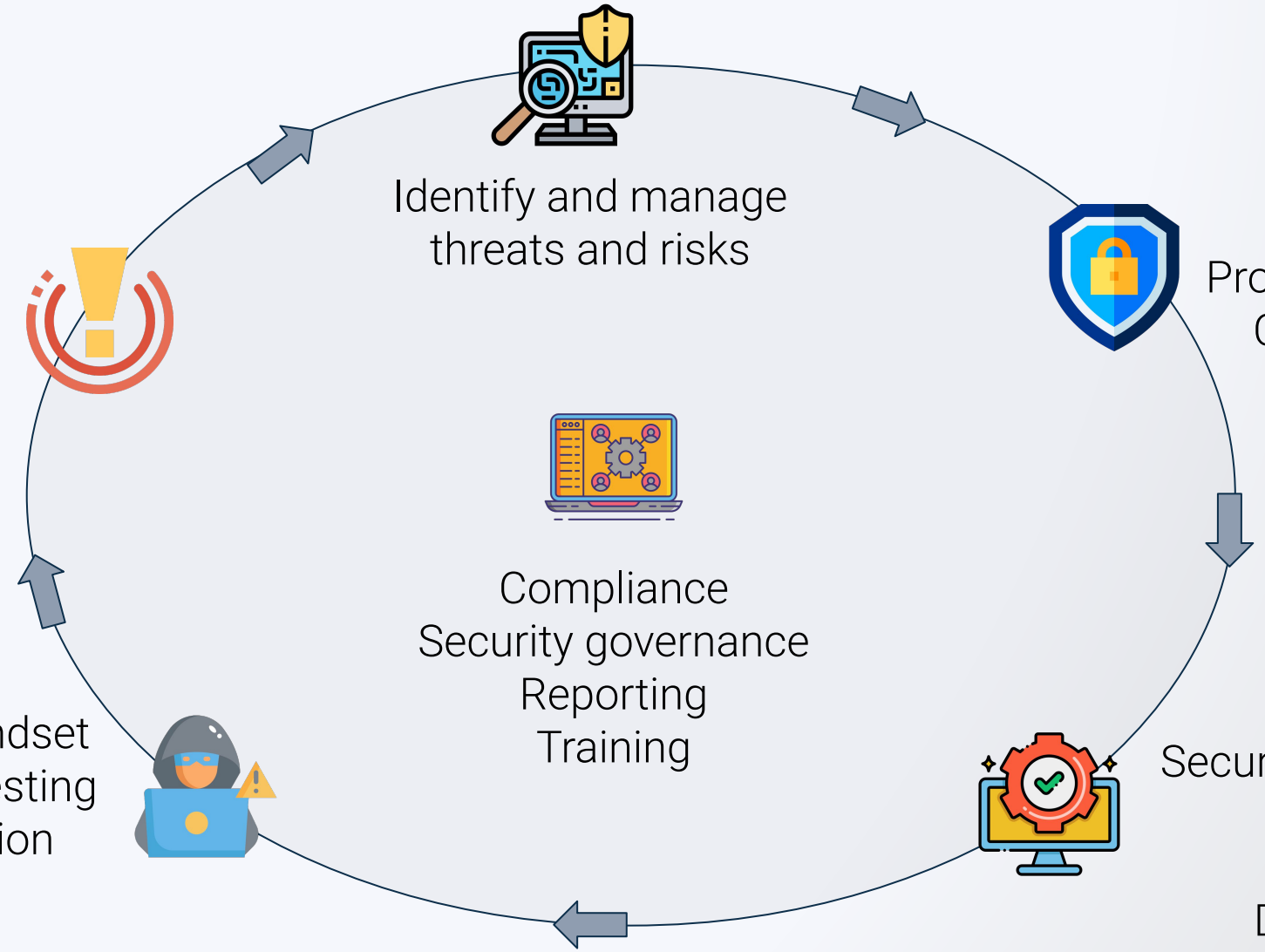
Apparel: H&M, Decathlon, ASOS

Specialist: Douglas, Leroy Merlin, Maisons du Monde

B2B: Airbus Helicopters, Conrad, Astore An Accor Brand

Mirakl powers scalable, profitable eCommerce growth

Security at Mirakl

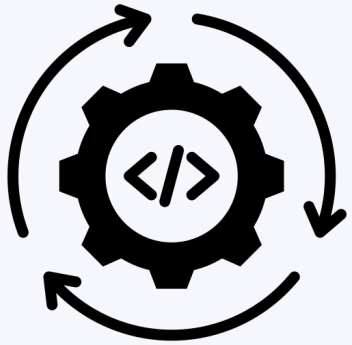


Le contexte

Solution SaaS

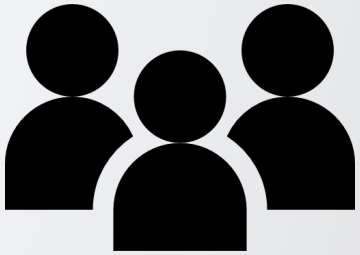
Multi Tenants

Multi Produits



Cycle de développement rapide

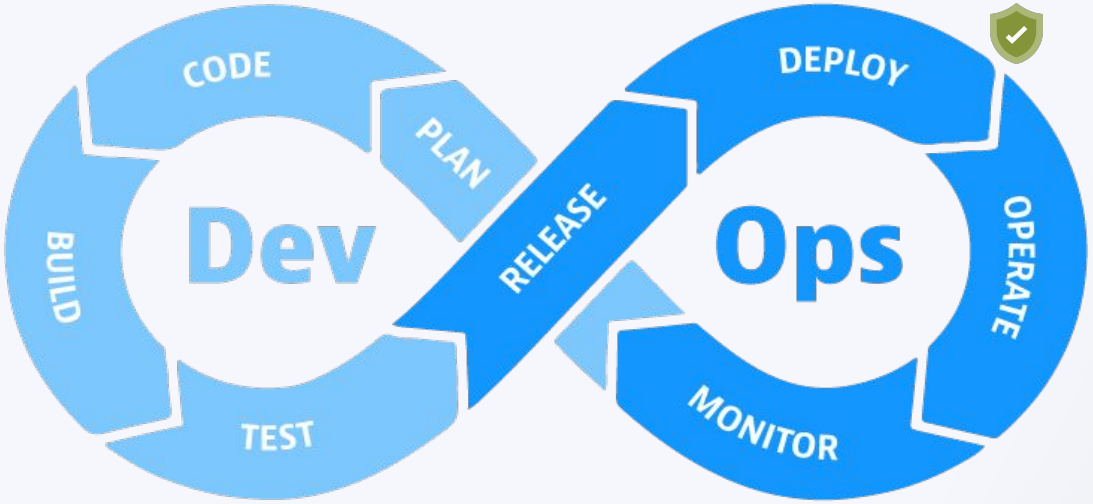
Livraisons régulières



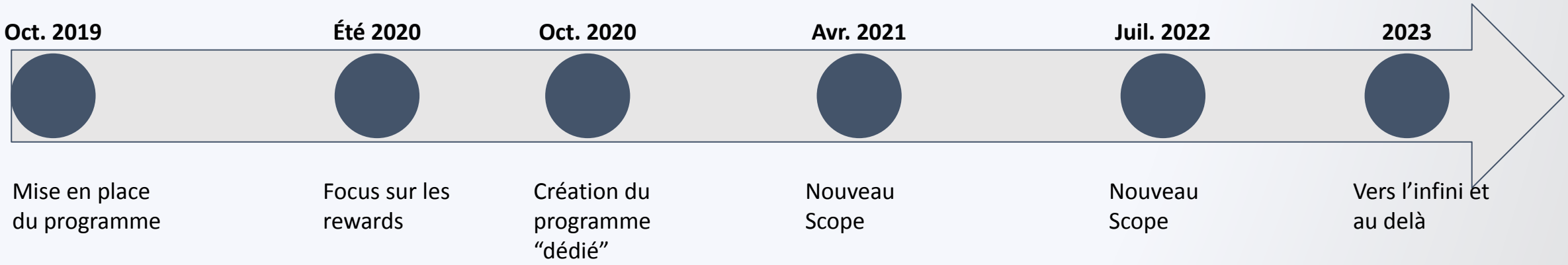
7 personnes

2 dédiés à la sécurité des opérations

Pourquoi le bug bounty?



Timeline


Oct. 2019
Été 2020
Oct. 2020
Avr. 2021
Juil. 2022
2023
Mise en place du programme
Focus sur les rewards
Création du programme “dédié”
Nouveau Scope
Nouveau Scope
Vers l’infini et au delà

Les grands jalons - Programme Mutualisé

Périmètre	Application “core” Mirakl uniquement Programme mutualisé entre les chercheurs (un seul tenant)
Positif	Bon moyen de couvrir le périmètre Plus intéressant que des pentests
Contraintes	Difficulté de rétention des chercheurs Manque de connaissance sur le produit
Résultats	Revues de sécurité plutôt alignées sur nos cycles de livraisons

Les grands jalons - Programme “Privé”

Périmètre	Application “core” Mirakl uniquement Programme dédié pour les “top” chercheurs de la plateforme (1 instance par chercheur)
Positif	Possibilité de tests plus approfondis Meilleure compréhension du contexte par les chercheurs impliqués Plus de communication avec les chercheurs
Contraintes	Coût supplémentaire (infrastructure et gestion)
Résultats	Rapports beaucoup plus pertinents Meilleure rétention des chercheurs sur le programme

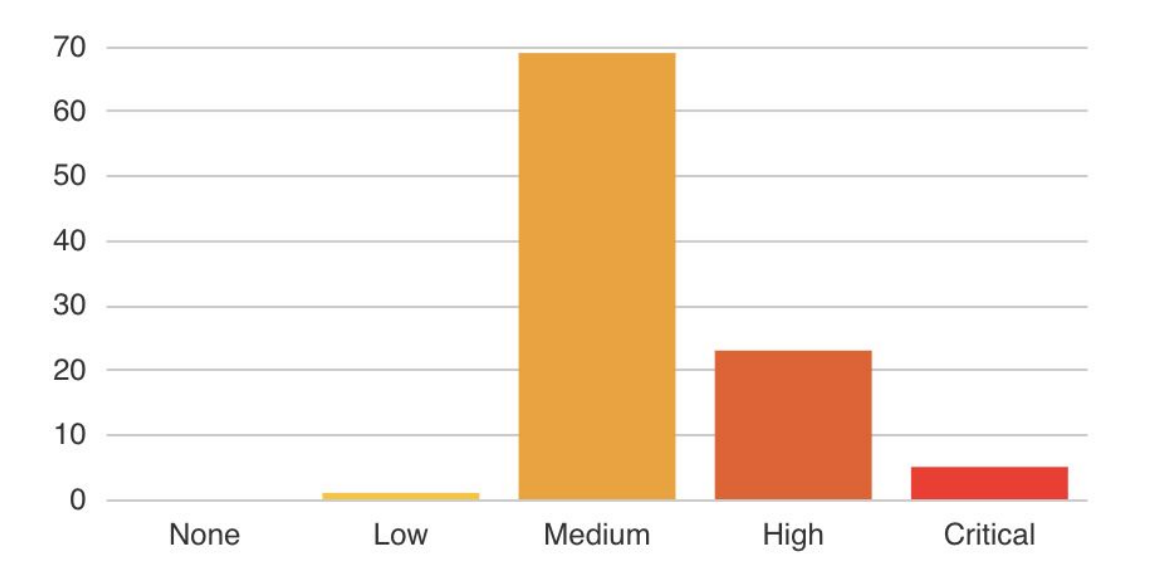
Le multi produit

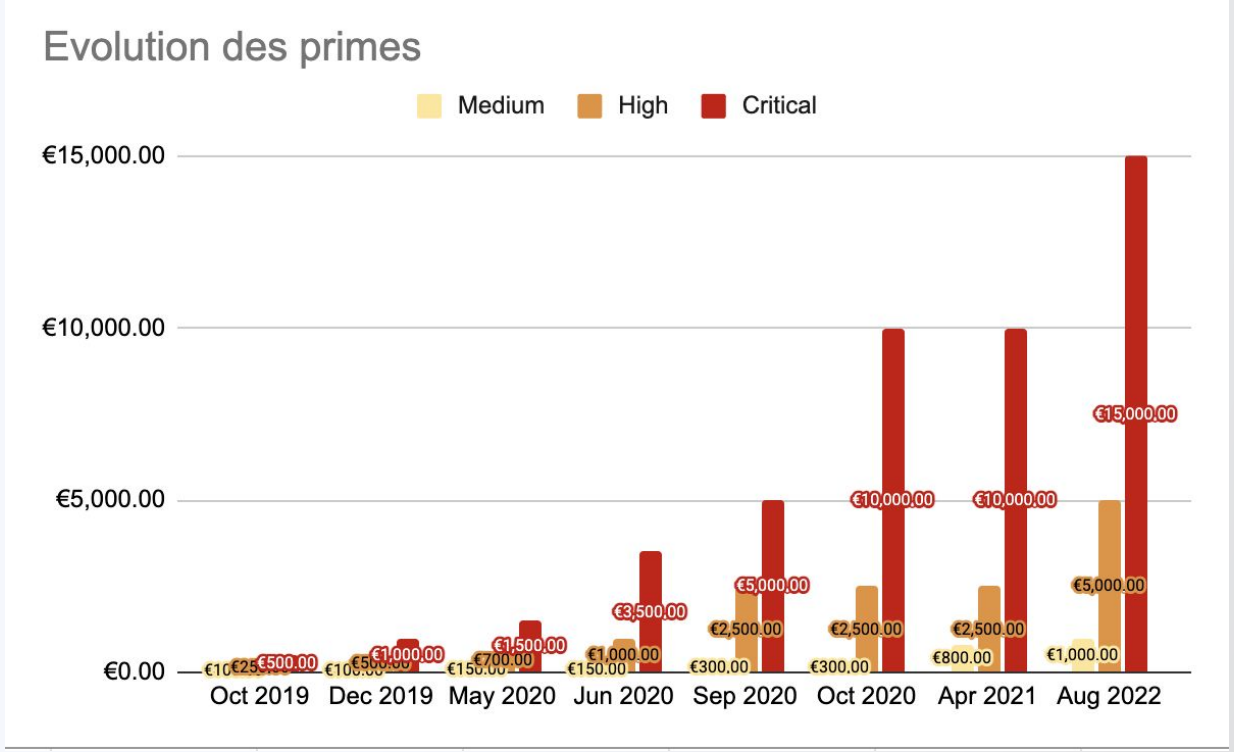
Comment maintenir l’engagement des chercheurs tout en élargissant le périmètre pour inclure différents produits ?

Mise en place de thématique mensuelles avec augmentation des primes et plus de contexte apporté (présentation de la fonctionnalité en détail)

Et en 2023 ?

Indicateurs





Merci :)