

GWENDAL LE COGUIC

FORMATIONS

Chaque formation est axée sur des démonstrations pratiques, des exercices interactifs et des discussions sur des situations réelles afin de garantir l'acquisition de compétences clés.

Chaque session peut être suivie :

- sur site ou à distance
- en français ou en anglais
- individuellement ou en groupe

Devis sur demande

Tel: +33 7 69 02 25 10

Email: contact@glc.st

INTRODUCTION AU BUG BOUNTY



a. Description

*Cette formation d'une demi-journée offre une introduction complète au monde du bug bounty. **Adaptée aux directeurs, RSSI et chefs d'équipe**, cette session aborde tous les aspects, de l'historique et de la structure des programmes de bug bounty au signalement et au tri des vulnérabilités en situation réelle. Grâce à des **études de cas**, des **bonnes pratiques** et des **analyses sectorielles**, les participants repartiront avec des bases solides pour démarrer (ou améliorer) leur expérience du bug bounty, **tant du point de vue du hacker que de celui de l'entreprise**.*

b. Objectifs pédagogiques

- Comprendre ce qu'est un programme de *bug bounty*
- Apprendre comment le *bug bounty* s'intègre dans une stratégie de sécurité
- Identifier les rôles et responsabilités clés
- Savoir comment gérer les rapports de vulnérabilités
- Évaluer la préparation de votre organisation au *bug bounty*

c. Pré-requis

- Compréhension de base des principes de cybersécurité
- Familiarité avec la gestion des vulnérabilités et l'évaluation des risques

d. Public cible

- Responsables de la cybersécurité et équipes de sécurité
- RSSI et professionnels de la gestion des risques
- Organisations novices en matière de *bug bounty*

e. Programme

Présentation

- Présentation du formateur et des participants
- À quoi s'attendre lors de la formation
- Qu'est-ce que le *bug bounty* et pourquoi est-il important ?

Comprendre le *bug bounty* : l'écosystème

- Historique et évolution des programmes
- Rôles et motivations : entreprises, plateformes, hackers, tiers
- *Test d'intrusion* vs. *bug bounty* : principales différences

Anatomie d'un programme de *bug bounty*

- Structure des programmes
- Programmes publics vs. privés
- Attentes des entreprises vs. attentes des hackers

Rapports : tri et gestion des conflits

- Cycle de vie d'un rapport
- Gestion des doublons et des litiges

Gestion des politiques et des programmes

- Ce que les entreprises doivent préparer avant le lancement
- Evolution d'un programme : périmètre, récompenses, confidentialité
- Erreurs courantes à éviter

Règles, éthique et études de cas réels

- Règles non officielles du *bug bounty*
- Sphère de sécurité, politiques de divulgation
- Échecs et réussites : *Verizon*, *Shopify*, *Zomato*...

Synthèse et questions-réponses

- Résumé de la journée
- Questions-réponses ouvertes et conseils personnalisés