THALES
DIGITAL
FACTORY

Les challenges

1. Adapter la stratégie sécurité au contexte digital de Thales Digital Factory
2. Gagner la confiance des utilisateurs en montrant que l'innovation permet d'élever son niveau de sécurité
3. S'assurer que les risques cyber sont maintenus à un niveau acceptable
4. Être en conformité avec les lois et normes en vigueur (GDPR...) et à la politique du groupe Thales

Les bénéfices

Les programmes de Bug Bounty lancés par Yogosha ont permis à Thales Digital Factory de découvrir des failles critiques rapidement et de les corriger à moindre coût. Ils constatent aujourd'hui **80% de vulnérabilités en moins** sur leurs MVPs.

Les résultats

TYPE DE MISSION
Bug Bounty

NB. DE PROGRAMMES
+40 programmes

CHERCHEURS
5 à 20 par programme

PRIX / VULNÉRABILITÉ
50 à 2 000€

PAROLE DE REDTEAM MANAGER

Pour nos activités numériques, l'intérêt du Bug Bounty réside dans la souplesse de son utilisation et sa rapidité d'exécution. Les programmes de Bug Bounty sont lancés en 1 ou 2 jours, le gain de temps est considérable. Chez Thales Digital Factory, nous privilégions plutôt la qualité des hackers et leurs compétences à la quantité. Yogosha s'intègre parfaitement dans notre dispositif de Red Team et est un outil central pour assurer la sécurité de nos solutions.

TAOUFIK FARES

RedTeam Manager