YES WE H/CK

Brittany Ferries

BRITTANY FERRIES

Étude de Cas

France Cyber Maritime est une association à but non lucratif qui a pour mission d'apporter des réponses concrètes et adaptées en matière de cybersécurité au monde maritime et portuaire. L'association vise à renforcer la résilience du secteur et à promouvoir l'excellence française en matière de cybersécurité maritime en Europe et dans le monde.

Dans un contexte où les cyberattaques se multiplient, notamment dans le secteur maritime et portuaire, France Cyber Maritime s'attache à développer des solutions innovantes pour protéger les systèmes informatiques et les infrastructures du secteur.

C'est dans ce cadre que France Cyber Maritime s'est associée à YesWeHack, membre de l'association, pour lancer Battleship, le premier Live Bug Bounty dédié au monde maritime et portuaire en Europe. Cette initiative permet de renforcer la sécurité des systèmes informatiques des entreprises maritimes et portuaires en identifiant les vulnérabilités avant qu'elles ne soient exploitées par des cybercriminels.

La première édition de Battleship s'est déroulée en mai 2022 avec la participation de la compagnie maritime Brittany Ferries.

Fondée en 1972, la compagnie maritime française BAI (Bretagne-Angleterre-Irlande) devient en 1974 Brittany Ferries, aujourd'hui premier transporteur maritime sur la Manche occidentale et centrale. Avec une flotte de 10 navires, Brittany Ferries opère des traversées entre la France, le Royaume-Uni, l'Irlande et l'Espagne et transporte environ 2 millions de passagers par an.

Pendant 48 heures, quelques dizaines de chercheurs en sécurité informatique de la communauté YesWeHack ont mis à l'épreuve la plateforme de réservation en ligne de l'entreprise pour détecter d'éventuelles failles de sécurité. Cette première édition a été un succès et a permis à Brittany Ferries de renforcer la sécurité de sa plateforme de réservation en ligne.

Ian Frens, RSSI de Brittany Ferries, a accepté de partager avec nous son expérience de participation à cet événement inédit. Il nous explique comment la compagnie s'est préparée à cet événement et quel a été l'impact de cette initiative sur la sécurité informatique de l'entreprise.

YES WE HACK

QUELLES ONT ÉTÉ LES RAISONS QUI ONT POUSSÉ BRITTANY FERRIES À PARTICIPER À BATTLESHIP ?

IAN FRENS, RSSI, BRITTANY FERRIES :

Avant la tenue de Battleship, Brittany Ferries venait de refondre son système de réservation en ligne, une application essentielle pour l'entreprise car la plupart des réservations de traversées se font désormais sur internet.

Malgré la réalisation d'un test d'intrusion avant sa mise en production, deux vulnérabilités assez importantes ont été découvertes. Nous avions donc quelques inquiétudes sur le niveau de sécurité de ce site.

Lorsque France Cyber Maritime nous a proposé de participer, nous nous sommes dit que ce Live Bug Bounty serait une opportunité intéressante pour évaluer la sécurité de notre application de réservation, et ce même si nous n'avions pas d'expérience dans le domaine.

Le choix du périmètre à tester s'est donc imposé assez naturellement même si nous avons hésité à inclure d'autres applications web dans le scope. En raison de notre manque d'expérience dans le domaine du Bug Bounty, nous avons finalement décidé de nous concentrer sur l'application principale de réservation en ligne. Rétrospectivement, je pense que cette décision était judicieuse, car cela a permis aux chercheurs de se concentrer sur un périmètre précis.

COMMENT AVEZ-VOUS PRÉPARÉ VOTRE PARTICIPATION À CE LIVE BUG BOUNTY ?

IAN FRENS, RSSI, BRITTANY FERRIES :

L'approche étant totalement nouvelle pour Brittany Ferries, la première étape a été de bien comprendre le déroulement et l'organisation de l'événement en participant à des réunions avec France Cyber Maritime et YesWeHack. Ces réunions nous ont permis de mieux nous préparer et de savoir à quoi nous attendre lors du Live Bug Bounty.

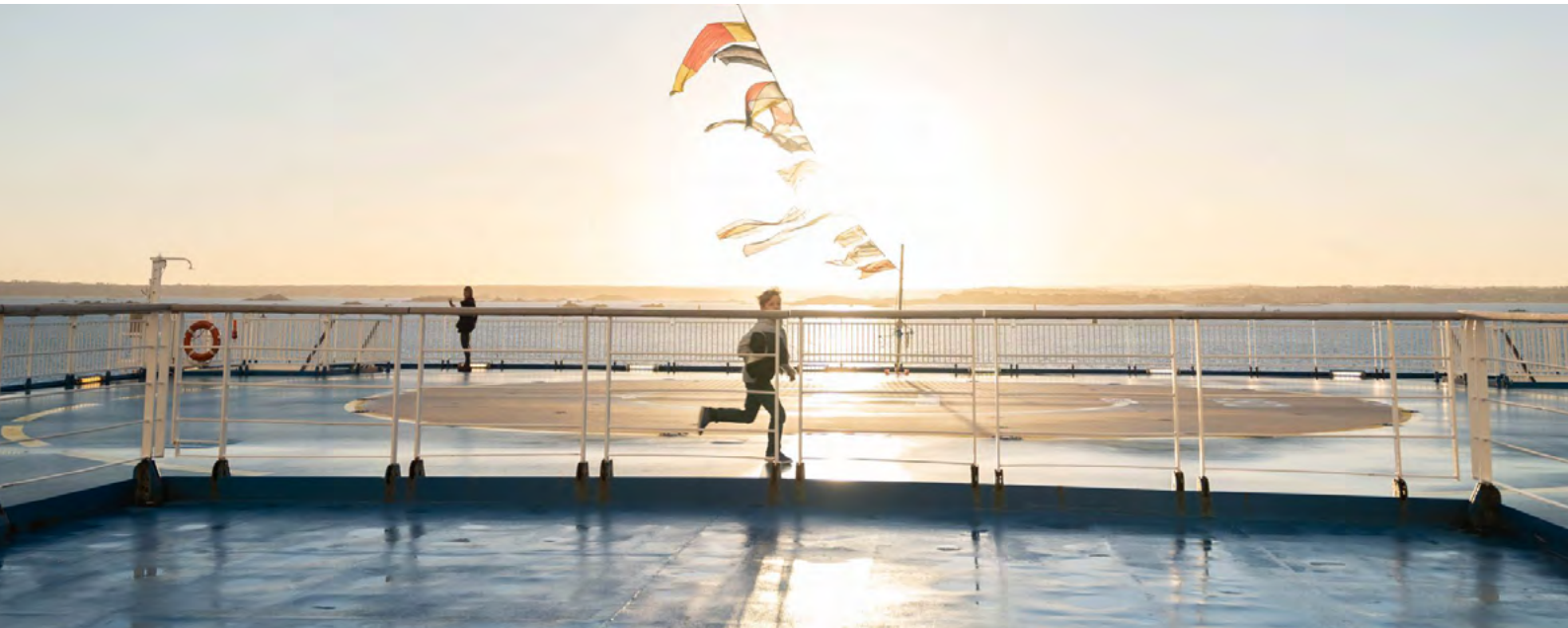
Ensuite, nous avons entamé la définition de notre programme. Même si nous avions déjà l'intention de tester l'application, il était crucial de bien définir :

- Les vulnérabilités à rechercher et à exclure
- Les primes à attribuer
- Les règles à suivre par les chercheurs pendant l'événement

Nous avons travaillé en étroite collaboration avec l'équipe YesWeHack et avons impliqué dès le départ les équipes responsables de l'application.

Une fois le programme défini, les équipes internes de Brittany Ferries, comprenant l'équipe applicative, le RSSI et l'équipe de production, ont été mobilisées pour les deux jours de l'événement. Participer à un événement de ce type nécessite des compétences internes réelles en sécurité, que ce soit dans le domaine applicatif ou web, en vue de rédiger le programme mais aussi de qualifier les vulnérabilités découvertes pendant l'événement.

Bien que l'équipe YesWeHack effectue une pré-qualification en live, il est impératif de bien comprendre les rapports pour prendre la décision d'accepter ou non les vulnérabilités et de valider les récompenses correspondantes.



EST-CE QUE BRITTANY FERRIES AVAIT DES PRÉOCCUPATIONS OU DES CRAINTES PARTICULIÈRES AVANT DE PARTICIPER À CE LIVE BUG BOUNTY ?

IAN FRENS, RSSI, BRITTANY FERRIES :

Dès le départ, nous avons perçu l'intérêt du Bug Bounty, malgré la nouveauté de cette approche. Ainsi, l'accueil a été plutôt positif. Bien sûr, nous avons dû obtenir l'approbation de la direction en expliquant et rassurant sur certains points tels que la sélection des chercheurs en sécurité, l'impact sur la production et la confidentialité des résultats. Les inquiétudes ont été rapidement levées et nous avons ainsi pu participer à Battleship.

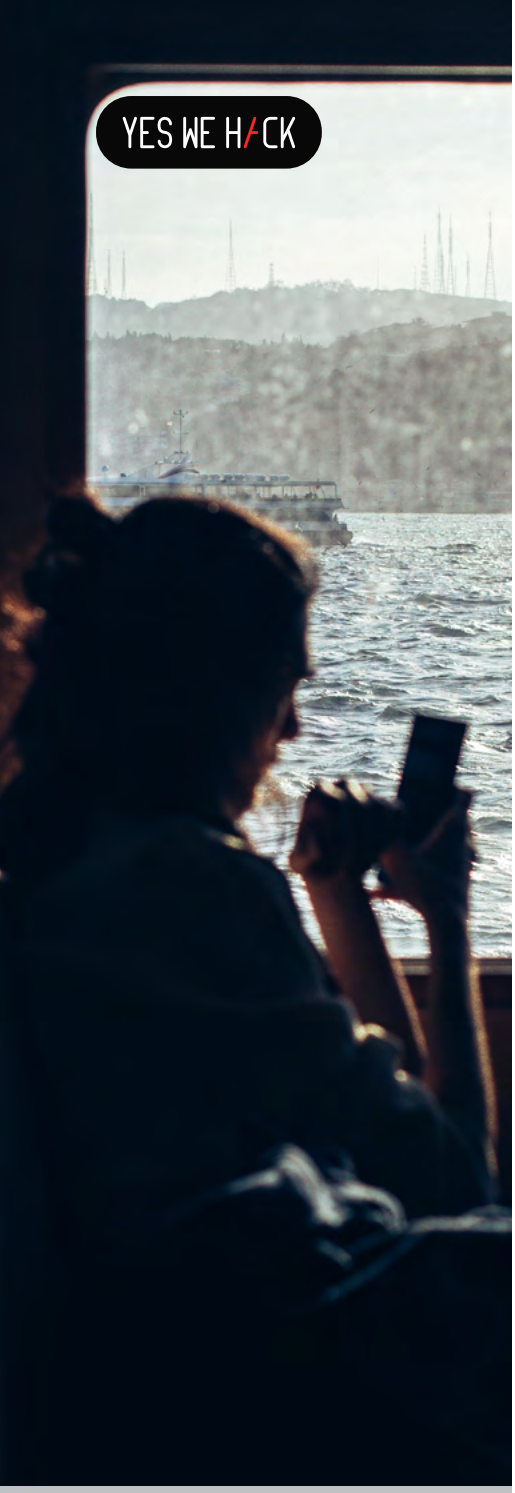
QUE PENSEZ-VOUS DES CRAINTES QUE LES ENTREPRISES PEUVENT AVOIR À L'IDÉE DE LANCER UN PROGRAMME DE BUG BOUNTY DANS UN ENVIRONNEMENT DE PRODUCTION ?

IAN FRENS, RSSI, BRITTANY FERRIES :

La définition du programme n'empêche pas quelques effets de bord, en effet. Pour faciliter l'identification des attaques provenant du Bug Bounty, nous avons demandé aux chercheurs d'ajouter un header spécifique à toutes leurs requêtes de test.

Au cours de l'événement, nous avons été confrontés à une situation où un chercheur a utilisé un outil de bruteforce pour tester l'une de nos API. L'équipe en charge de la production a été alertée rapidement grâce à nos outils de monitoring. Nous avons ensuite discuté avec le chercheur pour trouver une solution, et une fois l'incident résolu, il n'y a plus eu d'autres problèmes similaires.

Il convient de souligner qu'il est toujours possible d'interagir avec les chercheurs pendant l'événement pour recadrer leurs recherches si nécessaire. Pour ce faire, il est essentiel que les équipes internes de l'entité participante soient disponibles tout au long de l'événement.



Brittany Ferries

QUE VOUS A APPORTÉ VOTRE PARTICIPATION À BATTLESHIP ?

IAN FRENS, RSSI, BRITTANY FERRIES :

Tout d'abord, le Bug Bounty a permis de nous rassurer sur le niveau de sécurité de notre application. En effet, bien que des vulnérabilités aient été découvertes, aucune vulnérabilité critique n'a été signalée. De manière générale, les chercheurs ont jugé le niveau de sécurité de l'application plutôt satisfaisant.

En ce qui concerne les vulnérabilités découvertes, cela a été une occasion pour nous de les corriger. Nous avons constaté que le rapport coût-efficacité était très satisfaisant, surtout si l'on compare avec nos tests d'intrusion habituels.

Les équipes de développement internes ont grandement apprécié cet événement. La collaboration interactive offerte par le Bug Bounty leur a permis de mieux comprendre la mentalité des attaquants ainsi que les techniques qu'ils utilisent. Cette expérience leur a également permis de prendre conscience que des erreurs mineures de codage ou de configuration peuvent être exploitées à des fins malveillantes. Cette prise de conscience est un avantage majeur du Bug Bounty par rapport aux tests d'intrusion.

Pour finir, en ce qui concerne la communication, nous avons immédiatement réalisé que le fait de communiquer sur notre participation à cet événement pourrait inspirer confiance à nos clients et partenaires en montrant que la cybersécurité est une priorité majeure chez Brittany Ferries.

Dans l'ensemble, notre bilan de cet événement est très positif. C'est pourquoi nous avons décidé, à la fin de Battleship, de pérenniser ce type d'initiative en intégrant le Bug Bounty à notre plan d'audit annuel, en complément des méthodes plus traditionnelles.

> **“ Nous avons constaté que le rapport coût-efficacité était très satisfaisant, surtout si l'on compare avec nos tests d'intrusion habituels.**

À PROPOS DE

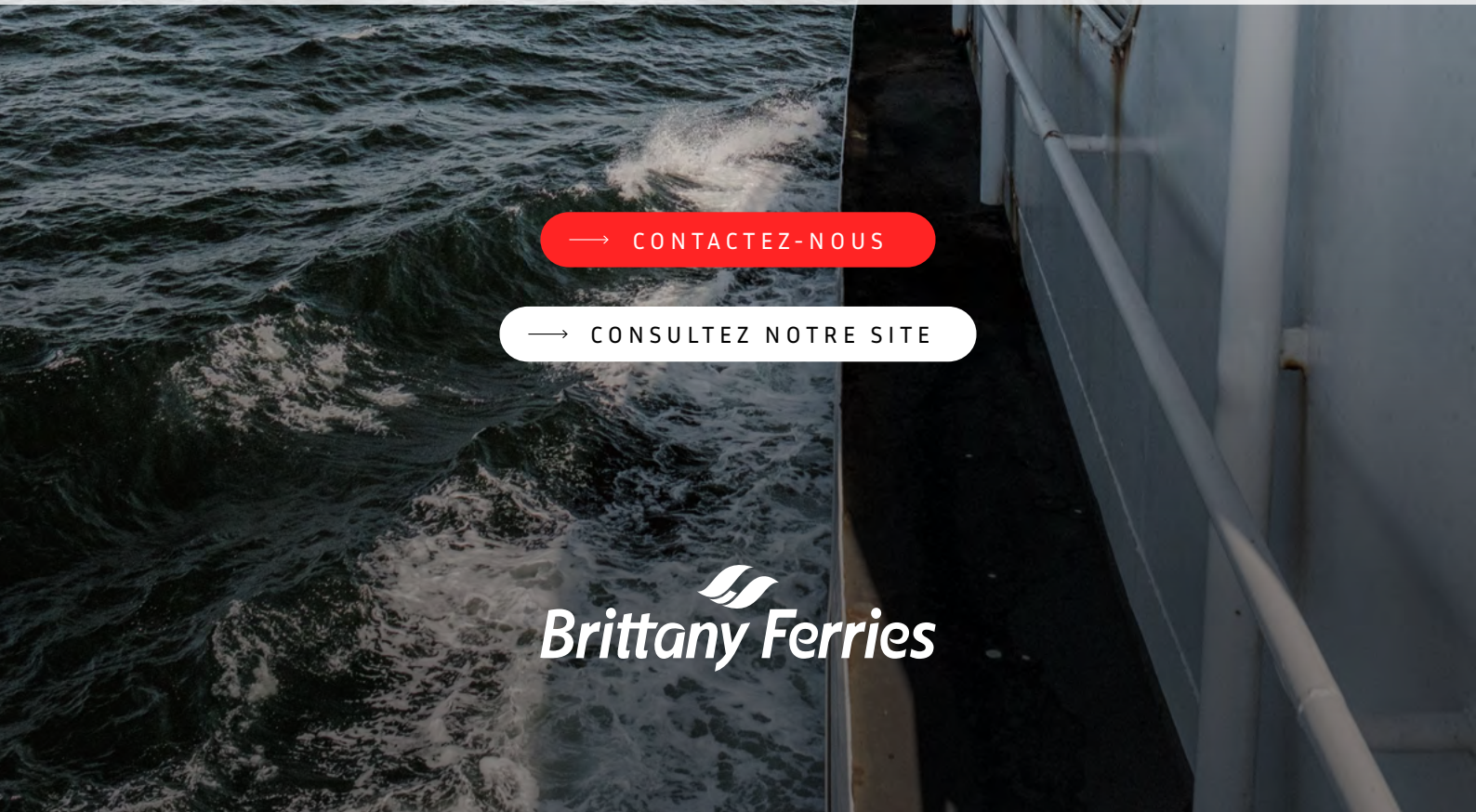
YES WE HACK

Créée en 2015, YesWeHack est une plateforme mondiale de Bug Bounty et de VDP.

Notre plateforme connecte des dizaines de milliers d'experts en cybersécurité (« hackers éthiques ») répartis dans 170 pays avec des organisations de toutes tailles et de tous secteurs pour sécuriser leurs périmètres exposés et rechercher les vulnérabilités (bugs) de leurs sites web, applications mobiles, infrastructures et objets connectés.

YesWeHack gère des programmes privés (seulement accessibles sur invitation) et des programmes publics pour des centaines d'organisations à travers le monde, en conformité avec les réglementations européennes les plus strictes.

En plus de sa plateforme de Bug Bounty, YesWeHack offre également : une solution de création et de gestion de politique de divulgation des vulnérabilités (VDP), une plateforme de pentest management, une plateforme d'apprentissage pour les hackers éthiques appelée Dojo et une plateforme de formation pour les institutions éducatives, YesWeHackEDU.



⟶ CONTACTEZ-NOUS

⟶ CONSULTEZ NOTRE SITE

Brittany Ferries