Une brève histoire du Bug Bounty chez Dailymotion

Retour d'expérience d'une plateforme web

Quentin Berdugo

Chief Information Security Officer (Dailymotion)

Une naissance sous une mauvaise étoile

- Déclenchement d'un Bug Bounty privé en Décembre 2016 dans le contexte d'un dispositif de réponse à incident avec l'objectif d'identifier la vulnérabilité en cause.

- Des résultats satisfaisants mais:
  - Un outil mal adapté pour l'objectif ciblé
  - Capacité limitée en interne à traiter les soumissions dans un contexte où l'attention est accaparée par la réponse à incident
  - Un coût élevé pour un objectif principal non atteint (vulnérabilité identifiée par investigation inforensique)

- Programme mis en pause dans son état en sortie de crise

Reprise en main du programme initial

- Nouveau tri et réévaluation des soumissions
  - Confusions dans les tickets
  - Réévaluation de la sévérité
- Suivi systématique dans le système de gestion de tickets interne
  - Pertes d'information entre le système de gestion de tickets interne et celui de la plateforme de Bug Bounty
  - Mise en place de tableaux de bord, suivi du plan de remédiation entendu avec les équipes
- Vérification de la remédiation des vulnérabilités
  - Failles non corrigées
  - Mitigations « naïves »
  - Failles « disparues » dans la nouvelle version

Lancement d'un nouveau programme privé

- Suite à la refonte complète du site
  - Besoin d'augmenter la confiance rapidement entre la mise en ligne et le premier audit

- Dans le cadre d'un plan d'assurance sécurité formalisé
  - Analyse de risques – plan d'audit
  - Audits techniques (archi, configuration, test d'intrusion, revue de code source)
  - Scans de vulnérabilité
  - Bug Bounty
  - Évaluations internes
  - Questionnaires sécurité fournisseurs

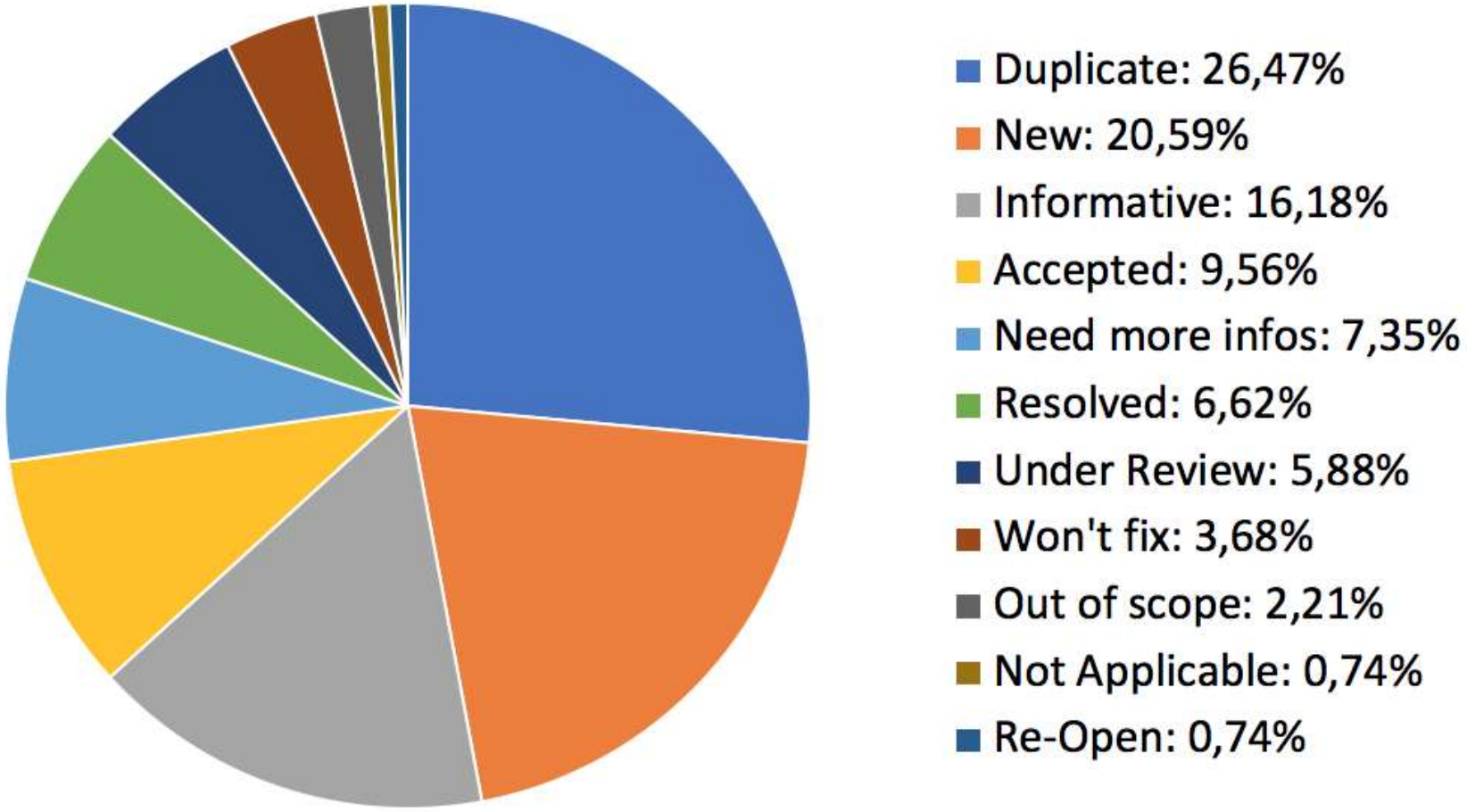
Lancement d'un nouveau programme privé

- Alignement des montants des primes au prix du marché
- Un règlement mieux défini
- Des objectifs atteints
  - En terme de couverture
  - En terme de résultats
  - En terme de coûts
- Complémenté par la suite d'un audit technique exhaustif

L’adolescence : passage du programme en public

- Un règlement à soigner
- Un plan de communication à maîtriser
- Un appel d’air au démarrage
  - Prévoir de la disponibilité pour le triage les premières semaines
  - Beaucoup de soumissions rejetées (doublons, hors périmètre, fantaisistes, incompréhensibles)
  - Faible sophistication des premières soumissions par effet d’opportunisme
  - Mais augmentation progressive de leur qualité au fur et à mesure de la raréfaction des gains faciles et de la familiarisation des chercheurs avec le périmètre

L’état des soumissions à 10 jours du lancement



La maturité à venir

- Établissement d'un « régime de croisière »
  - Process
  - Budget
  - Moyens humains
- Diversification des communautés de chercheurs
- Augmentation des primes
- Mise en place de programmes privés éphémères, ciblés sur un périmètre spécifique
  - Outil intermédiaire entre la revue interne et un audit de tierce partie

Les particularités du Bug Bounty dans le dispositif d'assurance sécurité

- Un outil supplémentaire à la disposition du RSSI qui complète mais ne remplace pas les approches existantes tels que les tests d'intrusion

Les particularités du Bug Bounty dans le dispositif d'assurance sécurité

- Nécessite une expertise technique forte en interne (ou en prestation)
  - Pas de confiance à priori dans la pertinence de la soumission
  - Enjeux économiques divergents
  - Capacité de « retests » limitée
  - Investissement à prévoir en temps ou en service

- Structure de coûts
  - Engagement de résultat
  - Difficilement prévisible et budgétisable
  - Un modèle inhabituel pour le service achats
  - Rentable (si le règlement et les primes sont adaptés)

Les particularités du Bug Bounty dans le dispositif d'assurance sécurité

- Inadapté à certains périmètres
  - Périmètre interne
  - Nécessité d'accès à des comptes sensibles
  - Nécessité de connaissances métier approfondies
- Orientabilité limitée
  - Possibilité de faire des programmes privés sur un périmètre ciblé
- Efficace
  - Multiplicité des talents et approches
  - Approche « boîte noire » très pragmatique

Remarques générales

- CVSS, la fausse bonne idée ?
- Baser l'évaluation de l'impact sur un scénario tangible et démontré
  - Gain de temps
  - Évite le « marchandage » du montant de la prime
- Droit à la correction des problèmes non récompensés

Remarques générales

- Correction des failles sévères moins sereines que dans le cadre d'un audit
  - Communication avec le chercheur
  - Extinction des services
  - Vérification des journaux
  - Rotation des secrets
  - Processus d'escalade

- Clauses d'exclusion à prévoir pour les prestataires d'audit et les employés

Devoir de transparence envers la communauté des chercheurs et respect du travail effectué

- Établir un règlement complet et intelligible qui explique les attentes et les interdits
  - Ex: https://bountyfactory.io/dailymotion/dailymotion-public-bug-bounty
- Corriger les failles au plus vite pour éviter les doublons
- Être honnête et équitable dans l'évaluation des risques

Devoir de transparence envers la communauté des chercheurs et respect du travail effectué

- Expliquer la logique de l'évaluation de la sévérité
  - Être ouvert à la discussion
  - Revenir aux risques métier
  - Rappels au règlement du programme
- Faire preuve de réactivité dans le traitement de la soumission
  - Y compris pour le versement de la prime

Le Bug Bounty du pauvre

- Avoir une politique de divulgation
- La publier dans un security.txt (https://securitytxt.org/)
- Avoir une adresse security@ (qui répond)