HARO
Antoine
2 SIO SLAM

INSTITUT LIMAYRAC

Note de synthèse correspondant aux thèmes de veille.

Définition de ses thèmes de veille
Définition de la stratégie de collecte
Exploitation des données, dans le respect des bonnes pratiques
Synthèse
Diffusion

Définition de son (ses) thème(s) de veille:

1. CVE

Une CVE (Common Vulnerabilities and Exposures) est un identifiant unique attribué à une vulnérabilité de sécurité informatique rendue publique. Elle sert à référencer de manière standardisée les failles présentes dans des logiciels, systèmes ou matériels afin que les chercheurs, entreprises et équipes de sécurité puissent les identifier et en parler sans ambiguïté. Chaque vulnérabilité reçoit un identifiant au format *CVE-année-numéro* (ex : CVE-2026-XXXX). Le système est maintenu par MITRE Corporation et les CVE sont souvent associées à une évaluation de gravité grâce au standard Common Vulnerability Scoring System (CVSS). Elles facilitent ainsi le suivi, l'analyse et la correction des failles de sécurité.

Dans le cadre de mon BTS SIO se renseigner sur les CVE est indispensable car cela permet de ce tenir au courant de quand une faille est trouvée ou résolue.

2. Cyber-sécurité

Le thème de la cybersécurité permet de surveiller et analyser les menaces générales, vulnérabilités et évolutions technologiques liées à la sécurité des systèmes informatiques. Cette veille permet d'identifier rapidement les nouvelles failles, attaques, outils de protection et bonnes pratiques afin d'anticiper les risques et d'adapter les mesures de sécurité d'une organisation.

Elle renforce de manière plus générale les autres thèmes de veilles notamment sur le suivi des vulnérabilités publiées (comme les Common Vulnerabilities and Exposures) ou encore sur la mise en place de nouvelle méthode de Phishing tel que des méthodes d'attaque émergentes et des solutions de protection recommandées par des organismes spécialisés comme L'ANSSI.

3. Phishing

Le phishing (ou hameçonnage) est une technique de cyberattaque qui consiste à tromper un utilisateur pour lui faire divulguer des informations sensibles, comme des mots de passe, des coordonnées bancaires ou des données personnelles. L'attaquant se fait généralement passer pour une entité de confiance (banque, service en ligne, entreprise) en envoyant des e-mails, SMS ou messages frauduleux contenant un lien vers un faux site. L'objectif est d'inciter la victime à saisir ses informations confidentielles, qui seront ensuite utilisées de manière malveillante. Le phishing est considéré comme une forme d'Ingénierie sociale, car il exploite la confiance et la manipulation psychologique des utilisateurs.

Je l'ai choisi comme thème de veille car je trouve ça très interessant les stratégies mises en place par les attaquant pour faire preuve de Social Engineering et surtout pour sensibiliser les personnes les plus vulnérables (à mon échelle) qui sont très enclin à ce faire avoir par ce type de pratique.

4. Ransomware

Un ransomware (ou logiciel de rançon) est un type de malware qui bloque l'accès aux fichiers ou systèmes d'un utilisateur ou d'une organisation, généralement en les chiffrant, jusqu'au paiement d'une rançon à l'attaquant. Il se propage souvent via des e-mails piégés, des téléchargements infectés ou des vulnérabilités non corrigées. L'objectif est d'extorquer de l'argent ou d'obtenir d'autres avantages en menaçant de supprimer ou de divulguer les données. Les ransomwares sont l'une des menaces majeures de la cybersécurité moderne et nécessitent des mesures préventives comme les sauvegardes régulières, les mises à jour de sécurité et la sensibilisation des utilisateurs.

C'est intéressant de de tenir informé sur ce type d'attaque car généralement sur le logiciel concerné il s'n suit une CVE corrigée. C'est toujours intriguant de voir l'ingéniosité dont certains peuvent faire preuve pour percer un système médicale ou encore celui d'une entreprise du GAFAM.

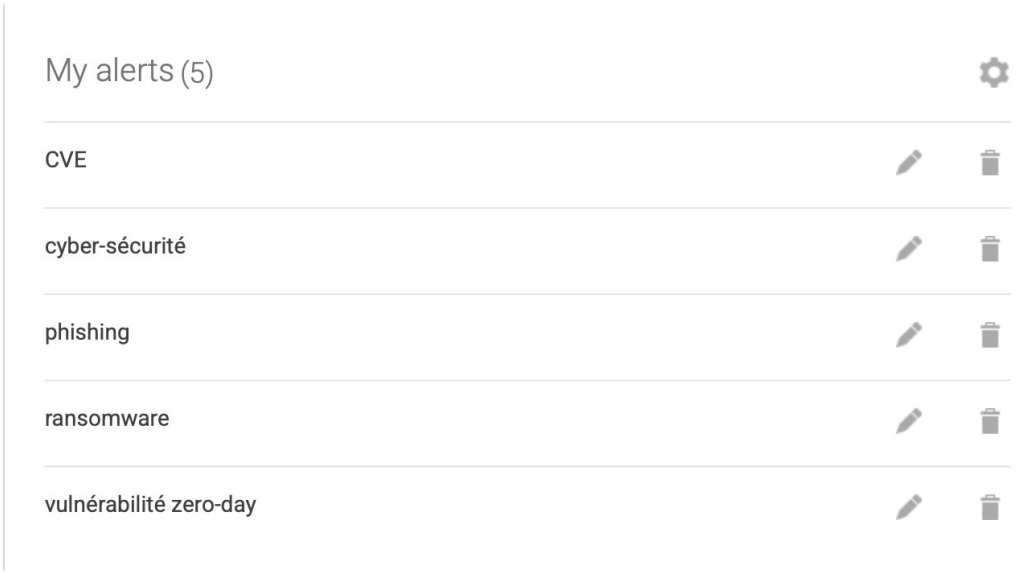
5. Vulnérabilité zero-day

Une vulnérabilité zero-day est une faille de sécurité inconnue du fabricant ou de l'éditeur du logiciel au moment de sa découverte. Elle est dite « zero-day » car aucun correctif n'existe encore, laissant les systèmes exposés dès le premier jour. Les attaquants peuvent exploiter cette vulnérabilité pour pénétrer un système, voler des données ou installer des malwares avant que des mesures de protection soient disponibles.

La détection et la gestion rapide de ces failles sont cruciales dans une stratégie de cybersécurité, et elles sont souvent suivies via des bases comme les Common Vulnerabilities and Exposures. Une vulnérabilité type zero-day peut donc suite à sa correction faire l'objet d'une CVE.

Définition de la stratégie de collecte :

Pour me tenir informé et mettre en place une stratégie de veille efficace j'ai choisi de mettre en place des alertes google : c'est un système qui permet d'envoyer les résultats d'une recherche par mail en la schedulant. Dans mon cas chaque matin à 07h00 je reçois un mail comprenant les résultats les plus récents sur les sujets définit au dessus.



Exploitation des données, dans le respect des bonnes pratiques :

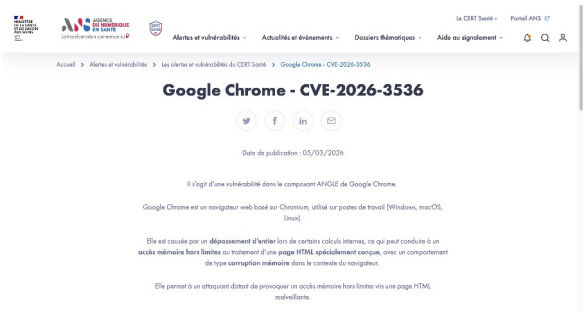
La mise en place d'une stratégie de veille et de la collecte des informations nécessite un esprit critique : on ne peut faire confiance qu'à des sources vérifiées et surtout où le sujet de l'article apparait sur plusieurs sources. Dans mon cas, lorsque je reçois ce récapitulatif quotidien je fais en sorte de vérifier la source, si elle est légitime et surtout si je retrouve le même sujet plusieurs fois.

Synthèse :

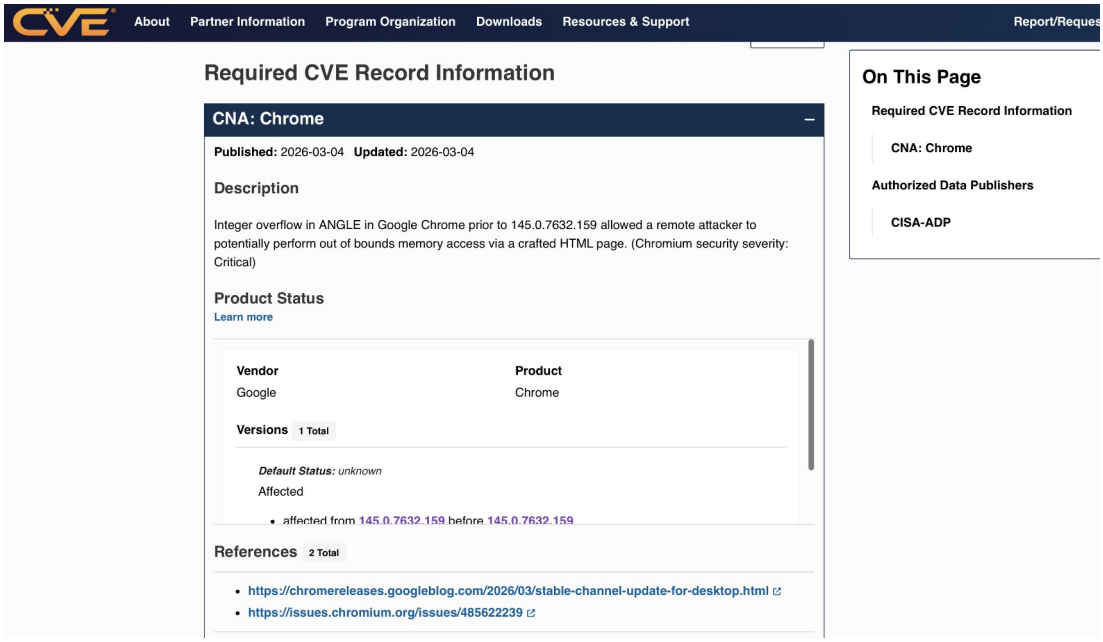
Typiquement un article interessant est ce celui qui le 5 mars sur Mix Vale*: L'article s'intitule « La mise à jour de Chrome corrige dix failles de sécurité et protège les données de millions d'utilisateurs ». Il traite de la dernière mise à jour de sécurité pour le navigateur Google Chrome, qui corrige dix vulnérabilités (dont plusieurs jugées critiques, comme CVE-2026-3536) afin de renforcer la protection des données de millions d'utilisateurs contre les attaques potentielles. L'article met l'accent sur l'importance d'installer sans délai cette mise à jour, car certaines des failles pourraient permettre l'exécution de code malveillant ou d'autres actions dangereuses si elles étaient exploitées avant d'être corrigées par Google.

*Mix Vale est un portail de presse brésilien qui publie des actualités générales couvrant divers sujets comme le *monde*, la *politique*, technologique et cybersécurité, l'économie. C'est le même système que Yahoo Actualités en France.

Pour vérifier la correction de cette CVE et confirmer les dires j'ai donc comparer les sources. J'ai donc trouver un site français en .gouv qui répertoriait et expliquer la CVE :



Puis j’ai regardé sur des sites vérifiés qui répertorient les CVE. Je suis donc allé vérifier sur CVE.org qui est le site officiel du programme CVE (Common Vulnerabilities and Exposures), utilisé comme base de référence pour cataloguer et décrire les vulnérabilités de cybersécurité publiquement connues. Il est exploité par MITRE Corporation, l’organisation à but non lucratif qui gère le système CVE, et sert à fournir une liste centralisée de vulnérabilités avec des identifiants uniques (CVE-Ids).



Diffusion :