Ma Démarche de Veille Technologique : De l'Information à la Pratique

Dans le cadre de mon parcours en BTS SIO (option SISR) et de mon alternance chez Neoform Industries, maintenir mes connaissances à jour est une nécessité absolue. Face à l'évolution constante des cybermenaces, notamment dans le milieu industriel, j'ai mis en place une démarche de veille technologique structurée en quatre étapes clés, allant de la détection de l'information jusqu'à son application pratique.

Étape 1 : Identification du besoin (L'élément déclencheur) Ma veille n'est pas passive ; elle est orientée par les problématiques concrètes rencontrées en entreprise. Par exemple, la recrudescence des attaques par Ransomware ciblant les infrastructures industrielles a été un point de départ majeur. L'objectif est d'identifier une vulnérabilité ou un besoin d'infrastructure spécifique avant qu'il ne devienne critique.

Étape 2 : Recherche et Collecte d'informations Pour ne pas être noyé sous l'information, j'utilise une approche automatisée (flux Push). J'utilise des agrégateurs de flux RSS comme Feedly pour centraliser les articles. Je m'appuie exclusivement sur des sources de références reconnues et fiables dans le domaine de la cybersécurité et de l'administration système, telles que les bulletins de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) ou du CERT-FR.

Étape 3 : Analyse et Synthèse Une fois l'information collectée, je procède à un tri rigoureux pour extraire les informations clés. Il s'agit de filtrer ce qui est réellement applicable à mon environnement de travail. Par exemple, je m'intéresse aux concepts émergents comme le ZTNA (Zero Trust Network Access) et je vérifie leur compatibilité avec notre infrastructure actuel (notamment les environnements Microsoft).

Étape 4 : Expérimentation en Laboratoire (La mise en pratique) C'est l'étape la plus importante de ma démarche. Une veille technique n'a de valeur que si elle est éprouvée. Lorsqu'une technologie ou une méthode de sécurisation retient mon attention lors de l'étape d'analyse, je la déploie dans un environnement de test isolé (Lab). J'ai par exemple pu tester la mise en place de l'authentification multifacteur (MFA) sur un serveur de bureau à distance (guacamole), afin de comprendre ses impacts sur l'expérience utilisateur et sur la sécurité de l'infrastructure avant d'envisager toute recommandation en production.