

# Synthèse de veille technologique

## I. Description du thème choisi:

Thème choisie : Les vulnérabilités, menaces ET les technologies, outils de protection

## II. Outillage

### A. Collecte

Utilisation de Feedly pour agréger et suivre des flux d'informations fiables:

- Source principales: Blogs cybersécurité (Krebs on Security, Dark Reading, CNET, etc....)
- Sites Référencée (CERT, ZDNet Actualités), et chaînes youtube Techno\_Trash Rabbin des Bois.
- Mots-clés: cybersécurité, ransomware, phishing, IoT security, zero-day

### B. Traitement, Filtrage, Classement

**Méthodologie:**

- Séparer les actualités en deux catégories:
  1. Technologies et outils de protection (Logiciel Windows Quick Machine Recovery)
  2. Menaces émergentes (Fuites des données)
- Prioriser les sources selon leur crédibilité et pertinence
- Éliminer les informations redondantes ou non fiables.
- Outils complémentaire:
  - **Notion** pour classer et annoter les informations.
  - **Alertes Google** pour être informé rapidement des nouvelles publications.

### C. Diffusion/Publication

- Document PDF (Synthèse Veille Technologique)
- Site Veille Technologique

**Feedly** est une plateforme de curation de contenu et un lecteur de flux RSS (Really Simple Syndication). Elle permet de centraliser et d'organiser des informations provenant de diverses sources en ligne, comme des blogs, des sites d'actualités, des chaînes YouTube, des newsletters ou des forums, afin de suivre facilement les mises à jour et les nouvelles dans un format unifié.

## III. Difficultés rencontrées

**Problèmes de quantité d'informations:** Certaines actualités ne sont pas assez réactives ou disponibles, notamment sur les menaces émergentes spécifiques.

**Solution proposée:**

- Diversifier les sources en intégrant les forums spécialisés (Reddit: r/cybersecurity).
- Suivre des experts sur LinkedIn ou Twitter/X pour des analyses plus rapides.

**Gestion du flux important d'informations:** Trier manuellement les données peut être chronophage.

**Solution proposée:**

- Utiliser des filtres dans Feedly pour automatiser le tri des articles par mots-clés.

- Prioriser les publications des leaders du secteur (Cisco, Palo Alto Network)

#### IV. Bilan quantitatif

- **Nombre de sources suivies:** 2 Blogs, 18 sites officiels; 3 forums communautaires et 3 chaînes Youtube officielles et spécialisées ainsi que 4 magazines informatiques.
- Articles collectés et analysés: 15 au total.

#### V. Bilan qualitatif

##### Points positifs:

- Accès à une diversité de sujets couvrant les aspects techniques et stratégiques.
- Identification des principales menaces actuelles (phishing, ransomware, IoT).

##### Points à Améliorer:

- Approfondir l'analyse des outils de protection, notamment sur leur efficacité face aux nouvelles menaces
- Ajouter des cas concrets d'attaques récentes pour enrichir la partie "Vulnérabilités émergentes".

#### VI. Perspectives

##### 1. Amélioration des outils:

- Tester des plateformes alternatives à Feedly, comme Inoreader ou Pocket pour des flux plus variés.
- Intégrer des outils d'analyse comme Threat Intelligence Platforms (TIP).

##### 2. Collaboration:

- Échanger les résultats avec d'autres étudiants ou experts pour compléter la veille.
- Participer à des webinaires ou conférences sur la cybersécurité.

##### 3. Production Finale:

- Consolider les informations sous forme de rapport détaillé avec infographies et études de cas
- Organiser une présentation pour partager les résultats.