

Veille technologique

Sujet : Cybersécurité en Entreprise (2025) -(2026)

Sommaire

<u>Introduction</u>	2
<u>Outils utiliser :</u>	2
<u>La recherche avancée sur Google</u>	2
<u>Paramétrage effectué</u> :.....	5
<u>Méthodologie et régularité de la veille</u>	5
<u>Tableau d'historisation</u> :	6
<u>Les Menaces émergentes en 2025</u>	6
<u>Analyse des risques pour les entreprises</u>	8
<u>Recommandations concrètes pour les entreprises</u>	9
<u>Conclusion</u>	11

Introduction

La transformation numérique des entreprises, l'essor du cloud, du télétravail et de l'IA générative ont multiplié les risques de cybersécurité.

Cette veille technologique a pour objectif :

- d'identifier les tendances et menaces émergentes,
- de présenter les technologies innovantes,
- et de proposer des recommandations pour améliorer la sécurité des entreprises.

Elle s'appuie sur des sources professionnelles : CERT-FR, ANSSI, CISA, OWASP, SANS Institute, ainsi que sur des outils de veille technique.

Outils utiliser :

Syft, Google, ANSSI – CERT-FR, Cybermalveillance.gouv.fr, CycloneDX CLI, Anchore Gype, Trivy (Aqua Security)

Trivy (Aqua Security) utilisé

Fréquence :

Collecte : quotidienne

Synthèse : hebdomadaire

Analyse : mensuelle

Paramétrage des outils de veille

Google Alerts

Objectif : recevoir automatiquement les actualités liées aux menaces de cybersécurité.

La recherche avancée sur Google

Qu'est-ce que la recherche avancée Google ?

La recherche avancée Google est une fonctionnalité qui permet d'affiner et de préciser les résultats de recherche. Contrairement à une recherche classique avec quelques mots-clés, elle utilise des opérateurs spécifiques et des filtres pour obtenir des informations plus pertinentes, fiables et ciblées.

Elle est très utilisée dans le cadre de la veille technologique, de la recherche académique ou professionnelle, car elle permet de gagner du temps et d'éviter les informations non pertinentes.

ALOUANI Fadi

Voici à quoi ressemble la page de recherche avancée

Google

Recherche avancée

Trouvez des pages avec...
tous les mots suivants : Saisissez les mots importants : *terrier tricolore*
ce mot ou cette expression exact(e) : Ajoutez des guillemets autour des mots exacts : "terrier"
l'un des mots suivants : Saisissez OR entre tous les mots à inclure : *miniature OR standard*
aucun des mots suivants : Placez un signe - (moins) devant les mots à exclure : -*rongeur*, -"Jack Russell"
nombres compris entre : et Placez deux points entre les nombres, et ajoutez une unité de mesure : *10..35 kilos, 300..500 USD, 2010..2011*

Affinez ensuite la recherche par...
langue : Rechercher des pages dans la langue sélectionnée
région : Rechercher des pages publiées dans une région précise
dernière mise à jour : Rechercher des pages mises à jour durant la période spécifiée
site ou domaine : Rechercher sur un site (tel que wikipedia.org) ou limitez vos résultats à un domaine tel que .edu, .org ou .gov
termes apparaissant : Rechercher des termes dans la page entière, dans le titre d'une page, dans une adresse Web ou dans des liens vers la page recherchée
type de fichier : Rechercher des pages dans le format que vous préférez
droits d'utilisation : Rechercher des pages que vous êtes libre d'utiliser

Comment utiliser la recherche avancée Google ?

Il existe deux manières principales d'utiliser la recherche avancée :

1 Via la page de recherche avancée

Google propose une interface dédiée accessible à l'adresse :
google.com/advanced_search

Cette page permet de :

- Rechercher une expression exacte
- Exclure certains mots
- Choisir la langue ou la région
- Limiter la recherche à un site web précis
- Filtrer par date de publication

C'est une méthode simple, idéale pour les débutants.

2 Avec les opérateurs de recherche (méthode avancée)

Les opérateurs sont des mots-clés spéciaux à taper directement dans la barre de recherche Google.

Voici les plus utilisés :

- "mot clé" → recherche une expression exacte
"intelligence artificielle"
- site: → recherche sur un site précis
site:lemonde.fr cybersécurité
- filetype: → recherche un type de fichier (PDF, PPT, DOC...)
filetype:pdf blockchain
- -mot → exclut un mot
cloud -météo
- OR → recherche l'un ou l'autre mot
IA OR intelligence artificielle

Intérêt pour la veille technologique

La recherche avancée Google permet de :

- Trouver des sources fiables et récentes
- Accéder à des documents techniques (livres blancs, rapports, études)
- Surveiller les évolutions d'une technologie
- Réduire le temps de recherche

Elle est donc un **outil essentiel pour une veille technologique efficace**.

Paramétrage effectué :

- Mots-clés surveillés :
 - *ransomware entreprise*
 - *cybersécurité PME*
 - *CVE critique*
 - *attaque supply chain*
 - *phishing IA*
- Langue : Français / Anglais
- Zone géographique : Monde
- Fréquence : Quotidienne
- Sources : Actualités, blogs, rapports
- Mode de réception : Email

Méthodologie et régularité de la veille

Étape	Description	Fréquence
Collecte	Alertes Google, sites officiels, blogs spécialisés	Quotidienne
Tri	Sélection des informations pertinentes	Hebdomadaire
Analyse	Évaluation de l'impact pour les entreprises	Mensuelle
Historisation	Ajout dans le tableau de veille	À chaque actualité
Synthèse	Mise à jour du dossier	Mensuelle

Tableau d'historisation :

Outils utiliser pour le Tableau d'historisation : SYFT(actualité cybersecurités dans les entreprise)

<i>Date de l'actualité</i>	<i>Informations</i>
03/12/25	Le rssi de rti partage des stratégies de cybersécurité pour les institution au ressource limitées
04/12/25	Microsoft defender : Enquête sur une interruption du portail due a un pic de trafic .
05/12/25	Campagne de phishing : usurpation d'identité de marques pour voler des identifiants google et facebook
09/12/25	Des extention de Vscode malveillantes infectent les machines avec des logiciel malveillants
10/12/25	L'ia de Picus security transforme les actualités sur les menaces en defenses validées
11/12/25	Un guide aide les entreprise a évaluer les fournisseur de surveillance des mots de passe
25/12/25	Le NIST investit 20 millions de dollars dans deux centres pour l'IA dans la fabrication et la cybersécurité
28/12/25	Microsoft IA renforce la cybersécurité gouvernementale avec détection des menaces

Les Menaces émergentes en 2025

ALOUANI Fadi

Ransomwares ultra-ciblés

- Attaques plus discrètes et rapides grâce à l'IA.
- Ciblage accru des PME et ETI, souvent moins protégées.
- Exfiltration systématique des données → double extorsion.

Attaques supply chain (chaîne logicielle)

- Exploitation des dépendances logicielles.
- Importance croissante du SBOM (Software Bill of Materials).
- Attaques dans les pipelines CI/CD.

Phishing + IA générative

- Emails impossibles à distinguer du vrai.
- Voix et vidéos deepfake utilisées pour escroquer le personnel.

Cybercriminalité cloud

- Mauvaises configurations (buckets S3 exposés).
- Accès non autorisés via des clés API compromises.

Exploitation des IoT et systèmes industriels

- Caméras, capteurs, machines industrielles vulnérables.
- Augmentation des attaques sur les hôpitaux, usines et collectivités.

Technologies et solutions de cybersécurité à surveiller

. SBOM & sécurité des dépendances

Les entreprises doivent inventorier leurs logiciels pour prévenir les attaques supply chain.

Outils clés :

- **Syft** (inventaire logiciel / SBOM)
- **Trivy** (SBOM + vulnérabilités, le plus simple et complet)
- **Grype** (analyse vulnérabilités basées sur un SBOM)
- **CycloneDX** (norme OWASP)

EDR / XDR nouvelle génération

Protection avancée contre ransomwares et activités suspectes.

Solutions reconnues :

- CrowdStrike
- Microsoft Defender XDR
- SentinelOne
- Sophos Intercept X

. Sécurité Zero Trust

Principe : “*Ne jamais faire confiance, toujours vérifier*”.

Technologies :

- Gestion avancée des identités et des accès (Okta, Azure AD)
- Segmentation réseau
- MFA obligatoire

IA pour la sécurité (AI Security Ops)

- Détection automatique d'anomalies.
- Analyse des journaux via des modèles d'IA.
- Automatisation de la réponse aux incidents.

Sécurité Cloud (CSPM / CWPP)

Protection des environnements cloud publics.

- As
- Nuage Prisma
- Dentelle

Analyse des risques pour les entreprises

Risque	Niveau	Impact	Description
Ransomware	Élevé	Perte activité	Attaques automatisées, chiffrage total

Risque	Niveau	Impact	Description
IA de phishing	Élevé	Vol identifiants	Emails parfaits et crédibles
Fuite de données cloud	Moyen/Élevé	RGPD, image	Mauvaise configuration, clés API
Dépendances vulnérables	Moyen	Entrée dans le SI	chaîne d'approvisionnement d'exploitation
IoT exposés	Moyen	Accès réseau	Matériel non mis à jour

Recommandations concrètes pour les entreprises

Renforcer la sécurité opérationnelle

- Activer MFA partout
- Mettre en place un EDR/XDR
- Sauvegardes chiffrées + tests mensuels
- Formations anti-phishing régulières

Maîtriser la chaîne logicielle

- Générer un SBOM pour chaque projet (Syft / Trivy)
- Scanner les dépendances dans la CI/CD (Trivy, Snyk)
- Surveiller les alertes de vulnérabilités (CERT-FR, CISA)

Sécuriser le cloud

- Utiliser un CSPM (Wiz, Prisma)
- Auditer les autorisations IAM
- Désactiver les clés API inutilisées

Déployer une approche Zero Trust

- Segmentation réseau
- Accès au moindre privilège
- Vérification continue des identités

Automatiser la veille

- Feedly : suivre CERT-FR / ANSSI / CISA
- Google Alerts : mots-clés (ransomware, CVE critiques, etc.)

ALOUANI Fadi

Date	Source / Auteur	Type de source	Informations clés / Résumé	Impact pour les entreprises	Fiabilité
05/2025	ANSSI (Agence nationale de la sécurité des systèmes d'information)	Article officiel / rapport	Publication des nouvelles recommandations sur la protection des systèmes d'information, avec accent sur la sécurisation du cloud et la gestion des identités.	Aide les entreprises à renforcer leur posture de sécurité et à adopter des standards conformes.	★★★★★
03/2025	IBM Threat Intelligence Report	Rapport annuel	Hausse de 20 % des cyberattaques par ransomware visant les PME ; augmentation des attaques via les chaînes d'approvisionnement.	Sensibilise à la nécessité d'investir dans la cybersécurité même pour les petites structures.	★★★★★
02/2025	Le Monde Informatique	Article de presse	Présentation des nouvelles solutions d'IA pour la détection automatisée des menaces (SIEM/SOAR basés sur l'IA).	Possibilité pour les entreprises d'améliorer la détection précoce des menaces.	★★★★☆
11/2024	Microsoft Security Blog	Blog technologique	Annonce des nouvelles fonctionnalités de sécurité dans Azure (Zero Trust, MFA renforcée, isolation des workloads).	Encourage l'adoption de modèles Zero Trust dans les organisations.	★★★★☆
09/2024	Kaspersky Security Bulletin	Rapport de sécurité	Forte hausse des attaques de phishing ciblées utilisant des IA génératives pour créer des messages plus crédibles.	Doit inciter les entreprises à renforcer la formation des employés et l'analyse comportementale.	★★★★☆
06/2024	CNIL	Article réglementaire	Mise à jour du RGPD sur la protection des données dans les environnements cloud.	Impact fort sur la conformité légale des entreprises.	★★★★★
01/2024	Cisco Cybersecurity Report	Rapport	Augmentation de l'utilisation de VPN non sécurisés dans les entreprises, créant de nouvelles vulnérabilités.	Nécessité de migration vers des solutions ZTNA (Zero Trust Network Access).	★★★★☆

Conclusion

La cybersécurité en entreprise devient un enjeu stratégique en 2025.

Les menaces évoluent rapidement, portées par l'automatisation, l'IA et la sophistication des cybercriminels.

Pour rester protégée, une entreprise doit :

- anticiper les risques,
- mettre à jour ses outils,
- améliorer la visibilité sur ses systèmes,
- et automatiser la détection des vulnérabilités.