ALOUANI Fadi

BTS SIO 1

Veille technologique

Sujet : Cybersécurité en Entreprise (2025)

Sommaire

ALOUANI Fadi

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.

Sujet : **Cybersécurité en Entreprise (2025)**

Outils utiliser :

syft,google,ANSSI – CERT-FR ,Cybermalveillance.gouv.fr , CycloneDX CLI ,
Anchore Grype ,. Trivy (Aqua Security)

Trivy (Aqua Security) utiliser

Fréquence :

- Collecte : quotidienne
- Synthèse : hebdomadaire
- Analyse : mensuelle

Les Menaces émergentes en 2025

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 S3 / buckets exposés.
- Accès non autorisés via 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.

SASE / SSE

Sécurisation du réseau pour entreprises multi-sites & télétravail.
Intègre : VPN cloud, filtrage web, CASB, DLP…

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
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 vulnérabilités (CERT-FR, CISA)

Sécuriser le cloud

- Utiliser un CSPM (Wiz, Prisma)
- Audit des 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.)
- Outils OSINT : Shodan, LeakIX, HIBP

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**,
- **décupler la visibilité sur ses systèmes**,
- et **automatiser la détection des vulnérabilités**.