Ayoub TOUIL

BTS SIO option SISR – Deuxième année

DOSSIER DE VEILLE TECHNOLOGIQUE

Du VPN au Zero Trust et ZTNA

Évolution de la sécurisation des accès distants

Année 2025-2026

Sommaire

1. Introduction

Présentation du thème

Sujet : Évolution de la sécurisation des accès distants, du VPN traditionnel au Zero Trust et ZTNA (Zero Trust Network Access).

Depuis vingt ans, les VPN constituent la solution de référence pour sécuriser les accès distants en entreprise. Mais en 2025-2026, avec le cloud généralisé, le télétravail massif et la sophistication des cybermenaces (ransomwares, attaques par mouvements latéraux), ce modèle montre ses limites structurelles.

Le Zero Trust, formalisé par le NIST (SP 800-207, 2020) et recommandé par l'ANSSI (guide juin 2025), propose une approche radicalement différente basée sur le principe « ne jamais faire confiance, toujours vérifier ». Le ZTNA en est la déclinaison technique pour l'accès applicatif : accès granulaire par application, vérification continue de l'identité et du contexte, applications masquées sur Internet.

Termes clés :

- **Zero Trust :** modèle de sécurité « ne jamais faire confiance, toujours vérifier » (NIST SP 800-207).
- **VPN :** tunnel chiffré réseau, confiance implicite après authentification.
- **ZTNA :** accès par application basé sur identité et contexte, sans accès réseau global.
- **Universal ZTNA :** extension Zero Trust au réseau interne (on-premise).
- **Microsegmentation :** cloisonnement réseau limitant mouvements latéraux.
- **SASE :** convergence SD-WAN et SSE (SWG, CASB, ZTNA, FWaaS) dans le cloud.

Justification du choix

J'ai choisi ce thème car il est au cœur de l'actualité cybersécurité 2025-2026. La directive NIS2 (transposée en France octobre 2024) impose aux entreprises des obligations renforcées en matière de gestion des accès et de segmentation réseau. Les chiffres confirment le basculement : 65% des entreprises subissent des incidents VPN annuels, 96% adoptent ou prévoient Zero Trust (Zscaler 2025), 65% prévoient remplacer VPN dans les 12 mois (Calmops mars 2026). Le marché SASE atteint 97 Mds USD 2025-2030 (Dell'Oro février 2026).

Ce thème est technique mais compréhensible, et directement lié à l'option SISR : gestion des accès, architecture réseau, IAM, surveillance continue. C'est une évolution majeure que je rencontrerai en tant que futur administrateur systèmes et réseaux.

Lien avec mon projet professionnel

Accepté en Licence Professionnelle ASR à l'UTEC Emerainville (septembre 2026), je recherche une alternance en administration systèmes et réseaux. Lors de mon stage chez Outscale (filiale Dassault Systèmes, cloud souverain SecNumCloud), j'ai travaillé sur l'infrastructure réseau d'un data center avec architecture spine-leaf.

Dès la première semaine (février 2026), j'ai configuré l'accès VPN avec double authentification via Authenticator. Mais j'ai rapidement observé les limites opérationnelles : une fois connecté au VPN, l'accès au réseau interne était global, sans segmentation applicative. Lors de mes échanges avec l'équipe infrastructure (semaine 7, mars 2026), nous avons discuté de l'application du Zero Trust dans notre architecture cloud spine-leaf pour limiter les mouvements latéraux.

Les compétences Zero Trust, ZTNA, microsegmentation, automatisation des règles réseau et architecture SASE seront attendues sur le marché : le ZTNA croît de 25,5% annuellement jusqu'en 2030 (MarketsandMarkets). Cette veille sur l'actualité 2025-2026 est essentielle pour ma future pratique professionnelle.

2. Comment j'organise ma veille

Mes sources d'informations

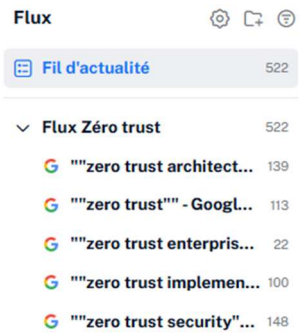
J'ai sélectionné des sources complémentaires couvrant actualité 2025-2026 : institutionnelles (ANSSI, NIST), analystes (Dell'Oro, MarketsandMarkets, Gartner), presse tech française et internationale (CyberExperts.tech, Tech Insider, SecurityWeek, IPAddressGuide, Calmops, Network Bachelor), et éditeurs (Zscaler, Netskope, Versa Networks).

Source / Média	Type	Lien
ANSSI (juin 2025)	Institutionnel	https://cyber.gouv.fr/publications/modele-zero-trust
Zscaler ThreatLabz (2025)	Éditeur/Rapport	https://www.zscaler.com/fr/learn/2025-vpn-risk-report
SecurityWeek (janv 2026)	Presse EN	https://www.securityweek.com/cyber-insights-2026-zero-trust
CyberExperts.tech (janv 2026)	Presse FR	https://www.cyberexperts.tech/le-reseau-interne-angle-mort-du-zero-trust
Dell'Oro Group (fév 2026)	Analyste	https://www.delloro.com/5-year-sase-forecast-97b
Versa Networks (fév 2026)	Éditeur/Webinaire	https://versa-networks.com/resources/webinars/from-vpn-to-zero-trust
Calmops (mars 2026)	Presse EN	https://calmops.com/technology/ztna-zero-trust-network-access-2026
Network Bachelor (avr 2026)	Presse EN	https://www.networkbachelor.com/ztna-vs-vpn-in-2026-buyer-guide

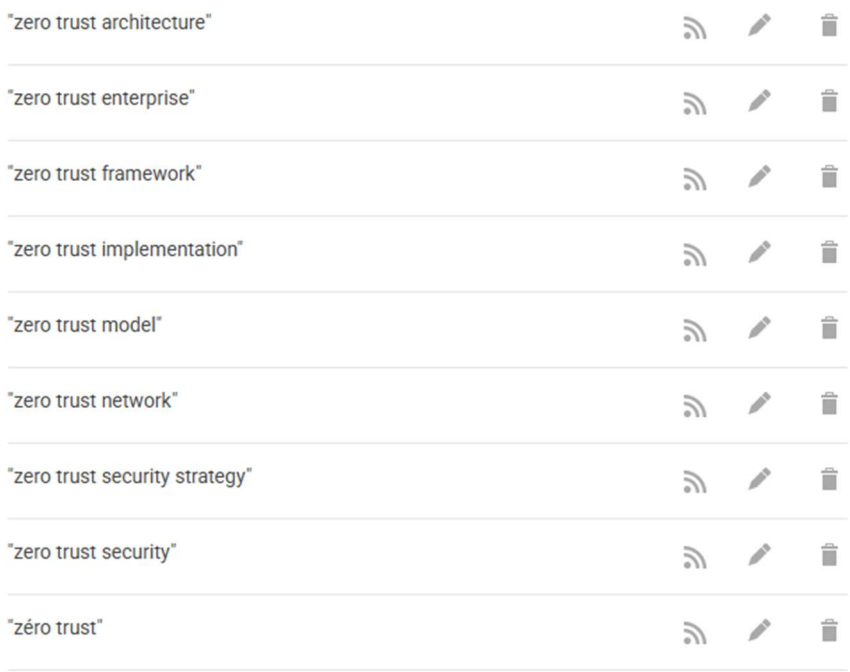
Les outils utilisés

J'utilise Inoreader comme agrégateur de flux RSS (Netvibes étant fermé). J'y ai ajouté 8 flux couvrant : actualités Zero Trust, SASE/SSE, VPN, ZTNA, NIS2, et cybersécurité générale. J'ai également configuré des alertes Google sur 'Zero Trust 2026', 'ZTNA actualités 2026', et 'VPN ransomware' pour automatiser la collecte.

Inoreader dashboard montrant flux Zero Trust



Google Alerts avec la configuration pour 'Zero Trust'



Exploitation des informations collectées

Je ne collecte pas passivement : j'exploite activement les informations. Exemple concret lors de mon stage Outscale (mars 2026) : après lecture de l'article CyberExperts.tech du 13 janvier 2026 sur l'angle mort du réseau interne dans les déploiements Zero Trust, j'ai engagé des discussions avec mes collègues de l'équipe infrastructure.

Contexte : chez Outscale, nous utilisions une architecture spine-leaf pour le data center. Les switches spine assurent l'interconnexion des leaf, qui eux-mêmes connectent les serveurs (châssis UCS, KVM). Après authentification VPN, l'accès au réseau était global, sans véritable segmentation applicative. L'article évoquait précisément ce point : le Zero Trust s'arrête souvent à l'accès distant, alors que le réseau interne reste en confiance implicite.

Discussion terrain : nous avons échangé sur l'application de la microsegmentation dans notre architecture. Les collègues ont confirmé que la segmentation actuelle reposait principalement sur des VLANs géographiques (par salle, par rack), et non sur une logique applicative. Les flux latéraux entre serveurs d'un même VLAN n'étaient pas contrôlés finement. Cette situation illustre exactement le propos de l'article. Veille → échange professionnel → prise de conscience terrain.

3. Détail de ma veille technologique

Les technologies

Cette partie présente l'évolution technologique avec un focus principal sur l'actualité 2025-2026.

Contexte historique rapide : VPN et émergence Zero Trust

Les VPN ont été développés années 1990 (PPTP, L2TP/IPSec, OpenVPN). Tunnel chiffré donnant accès réseau complet après authentification. John Kindervag (Forrester) formalise Zero Trust en 2010. NIST publie SP 800-207 en août 2020. ANSSI publie premier avis avril 2021. Le ZTNA émerge comme déclinaison opérationnelle 2020-2022 (Gartner).

Octobre 2024 : NIS2 transposée en France – catalyseur adoption

La directive NIS2 est transposée en droit français en octobre 2024. Elle élargit le périmètre à plus de 15000 entités (vs quelques centaines pour NIS1), couvrant énergie, transports, santé, alimentation, services numériques, gestion déchets. Exigences : gestion identités/accès (IAM), chiffrement, segmentation réseau, moindre privilège. Tech Insider (mars 2026) confirme : NIS2 accélère adoption Zero Trust/ZTNA en imposant obligations concrètes. Budgets ETI : 200-800K€ sur 2 ans pour conformité.

Lien : https://tech-insider.org/fr/architecture-zero-trust-pourquoi-chaque-entreprise-en-a-besoin-en-2026

Juin 2025 : ANSSI – Guide complet Zero Trust (ANSSI-PA-111)

L'ANSSI publie en juin 2025 le guide « Modèle Zero Trust – Les fondamentaux » (ANSSI-PA-111), destiné aux organisations françaises. Recommandations : analyse risque préalable, démarche incrémentale (commencer par applications Web/cloud puis étendre progressivement), ZT complète modèle périmétrique (ne le remplace pas totalement), exclure postes administration (doctrine admin sécurisée maintenue). Ce guide évite l'écueil de l'effet de mode marketing en proposant approche pragmatique et progressive.

Lien : https://cyber.gouv.fr/publications/modele-zero-trust

2025 : Zscaler ThreatLabz Report – 65% incidents VPN annuels

Zscaler publie en 2025 son ThreatLabz Report basé sur enquête auprès de 632 professionnels IT/cybersécurité mondiaux. Chiffres clés : 65% des entreprises subissent incidents sécurité VPN chaque année, 65% prévoient remplacer VPN dans 12 mois, 96% ont adopté ou prévoient adopter Zero Trust, 92% craignent ransomware via vulnérabilités VPN. Alerte importante : certains fournisseurs rebaptisent VPN 'Zero Trust' sans changer fondamentalement l'architecture (VPN hébergés cloud restent exposés avec IP publiques).

Lien : https://www.zscaler.com/fr/learn/2025-vpn-risk-report

Janvier 2026 : CyberExperts.tech – Angle mort réseau interne

CyberExperts.tech publie le 13 janvier 2026 un article crucial : le Zero Trust s'arrête souvent à l'accès distant. Une fois authentifiés via ZTNA, les utilisateurs

accèdent au réseau interne où persiste une confiance implicite. Mouvements latéraux possibles entre serveurs, applications, environnements. L'Universal ZTNA répond en étendant vérification continue au-delà de l'accès distant : sièges, agences, datacenters, clouds. Brique clé souvent négligée : microsegmentation. Elle rend flux explicites, assure visibilité complète, isole environnements critiques (OT, data centers, workloads cloud).

Lien : https://www.cyberexperts.tech/le-reseau-interne-angle-mort-du-zero-trust

Février 2026 : Dell'Oro Group – SASE 97 Mds USD 2025-2030

Dell'Oro Group publie le 3 février 2026 ses prévisions SASE : 97 milliards USD de dépenses cumulées 2025-2030, soit un triplement vs période 2020-2024. Changement structurel majeur : la sécurité dicte désormais l'architecture réseau (et non l'inverse). SSE (Security Service Edge) devient la couche politique autoritaire assurant contrôle, inspection, audit. SD-WAN devient couche exécution appliquant politique sécurité. Gartner confirme : 60% des achats SD-WAN intégrés SASE single-vendor en 2026 vs 15% en 2022.

Lien : https://www.delloro.com/5-year-sase-forecast-97b

Mars 2026 : IPAddressGuide – 48% ransomwares via VPN compromis

IPAddressGuide publie en mars 2026 : au cours de l'année écoulée, 48% des attaques ransomware ont utilisé identifiants VPN compromis comme vecteur d'accès initial. Problème fondamental VPN : confiance implicite après authentification. Une fois connecté, l'utilisateur accède au réseau entier, facilitant mouvements latéraux. Le ZTNA inverse le paradigme : l'identité devient le nouveau périmètre (nécessite IdP solide comme Okta, Microsoft Entra ID, Google Workspace). Même si un pirate vole une 'clé' (identifiants), il reste enfermé dans une pièce isolée sans accès au reste du bâtiment.

Lien : https://www.ipaddressguide.org/fr/comprendre-le-ztna-pourquoi-la-forteresse-du-vpn-seffondre-en-2026

Mars 2026 : Calmops – 65% entreprises remplacent VPN

Calmops publie le 3 mars 2026 son guide complet 'ZTNA 2026'. Facteurs accélération adoption : télétravail normalisé permanent (VPN conçus pour accès occasionnel), migration cloud (backhaul inefficace), posture sécurité (périmètre insuffisant), expérience utilisateur (latence VPN), conformité (audit trails granulaires requis). Chiffre clé : 65% des entreprises prévoient remplacer VPN par ZTNA, confirmant transformation massive sécurité réseau entreprise.

Lien : https://calmops.com/technology/ztna-zero-trust-network-access-2026

Avril 2026 : Network Bachelor – Architectures ZTNA (direct-routed vs proxy)

Network Bachelor publie le 2 avril 2026 (il y a 4 jours) un guide achat comparatif ZTNA. Évaluation 12 catégories capacités plateformes. Différenciateur critique : architecture. Direct-routed ZTNA : connexions directes user-apps sécurisées par politiques, sans passer par cloud vendor (faible latence, coûts réduits, pas exposition infrastructure partagée, comportement réseau déterministe requis environnements industriels). Proxy-based ZTNA : tout trafic routé via infrastructure cloud tierce (latence, coûts egress, contraintes architecturales).

Microsegmentation critique : plateformes avancées créent 'segment of one' par session/application, empêchent mouvements latéraux même si identifiants compromis. Conformité : alignement NIST SP 800-171, CMMC 2.0. Conclusion : ZTNA n'est plus optionnel en 2026, contrôle fondamental workforces hybrides.

Lien : https://www.networkbachelor.com/ztna-vs-vpn-in-2026-buyer-guide

Aspects commerciaux

Principaux acteurs du marché

- **Zscaler :** leader SSE Gartner Magic Quadrant, pionnier ZTNA (ZPA lancé 2016), ThreatLabz Report 2025 référence marché.
- **Palo Alto Networks :** Prisma SASE (lancé 2019), approche globale intégrant NGFW + ZTNA + threat detection, leader Gartner SASE.
- **Netskope :** Universal ZTNA (màj janvier 2026), leader SSE, étend ZT au réseau interne.
- **Cloudflare :** Cloudflare Access (lancé 2018), facile déploiement, version gratuite PME, accès via navigateur sans client.
- **Versa Networks :** migration PME VPN→ZTNA (webinaire février 2026), stratégie progressive.
- **Illumio :** Gartner Peer Insights 2026 Customer's Choice pour microsegmentation.

Chiffres économiques et graphiques

- **Marché ZTNA :** 1,34 Mds USD (2025) → 4,18 Mds USD (2030), CAGR 25,5% (MarketsandMarkets oct 2025)
- **Marché SASE :** 97 Mds USD dépenses cumulées 2025-2030, ×3 vs 2020-2024 (Dell'Oro fév 2026)
- **Taux adoption :** 96% entreprises adoptent/prévoient ZT, 65% remplacent VPN 12 mois (Zscaler/Calmops 2025-2026)
- **Budgets ETI (500-2000 sal.) :** 200-800K€ sur 2 ans incluant licences, intégrateur, formation (Tech Insider mars 2026)

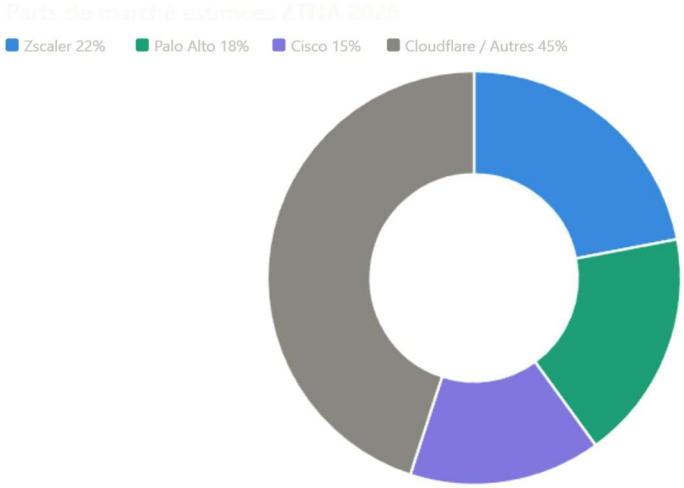
Les Parts de marché ZTNA estimées à courant 2026

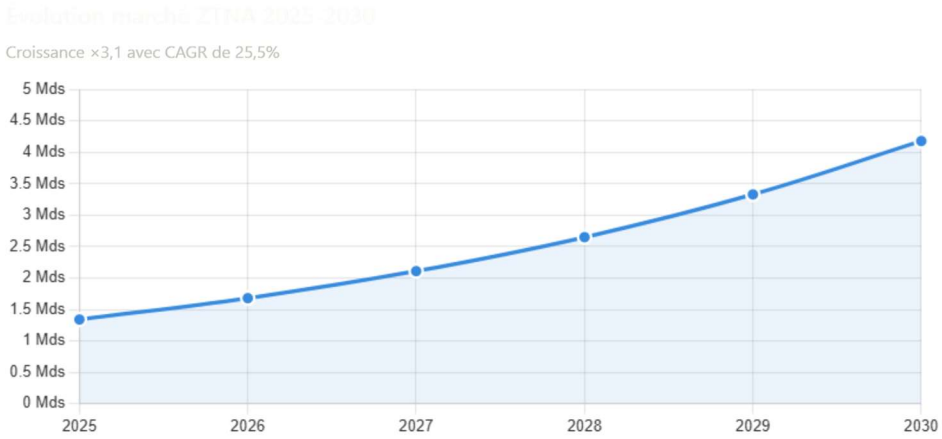
- Zscaler : 22%
- Palo Alto Networks : 18%
- Cisco : 15%
- Cloudflare / Autres : 45%

L'évolution marché ZTNA 2025-2030

2025 : 1,34 Mds USD → 2030 : 4,18 Mds USD (×3,1, CAGR 25,5%)

Graphique représentant les données énoncés :





Cycle d'authentification ZTNA — Architecture "Inside-Out"

L'application n'est jamais exposée directement sur Internet — le connecteur initie une connexion sortante vers le broker

Source : NIST SP 800-207 · Architecture ZTNA Gartner 2024

4. Revue de presse

Bloc 1 : Zscaler ThreatLabz – VPN Risk Report (2025)

Source : Zscaler ThreatLabz Report 2025, enquête 632 professionnels IT

Lien : https://www.zscaler.com/fr/learn/2025-vpn-risk-report

Résumé : 65% incidents VPN annuels, 65% remplacent VPN 12 mois, 96% adoptent ZT, 92% craignent ransomware VPN. Alerte faux ZT : VPN rebaptisés sans changement architecture.

Ce qui m'a marqué dans cet article :

Au début de ma veille, je pensais que les VPN étaient encore une solution fiable. Mais ces chiffres Zscaler m'ont vraiment ouvert les yeux : 65% d'incidents par an, c'est énorme. Ça montre que le VPN n'est plus adapté à la réalité 2026.

Ce qui m'a aussi frappé, c'est l'alerte sur les 'faux Zero Trust'. Certains éditeurs rebaptisent leurs VPN 'Zero Trust' sans rien changer. C'est du marketing, pas de la vraie sécurité. Pour un futur admin réseau, ça m'apprend à ne pas me fier aux buzzwords et à vérifier l'architecture réelle des solutions.

En lisant ce rapport, j'ai réalisé que la transition VPN→ZTNA n'est pas une tendance émergente mais une transformation déjà en cours. Pour un profil SISR comme moi, maîtriser le ZTNA deviendra aussi important que maîtriser TCP/IP.

Bloc 2 : CyberExperts.tech – L'angle mort du réseau interne (janvier 2026)

Source : CyberExperts.tech, 13 janvier 2026

Lien : https://www.cyberexperts.tech/le-reseau-interne-angle-mort-du-zero-trust

Résumé : ZT souvent limité accès distant. Réseau interne = confiance implicite. Universal ZTNA + microsegmentation répondent.

Mon analyse personnelle :

Cet article a changé ma compréhension du Zero Trust. Avant de le lire, je croyais que mettre du ZTNA pour l'accès distant suffisait. Mais en fait, c'est exactement ce que j'ai observé chez Outscale pendant mon stage (février-mars 2026) : une fois authentifiés via VPN avec double authentification, nous avions accès au réseau interne global. Les flux latéraux entre serveurs d'un même VLAN n'étaient pas contrôlés finement.

Après avoir lu cet article le 13 janvier 2026, j'en ai discuté avec mes collègues de l'équipe infrastructure lors de la semaine 7 (20 mars). Nous avons échangé sur l'application de la microsegmentation dans notre architecture spine-leaf. Ils ont confirmé que la segmentation actuelle reposait sur des VLANs géographiques (par salle, par rack), et non sur une logique applicative. Les mouvements latéraux entre serveurs d'un même VLAN restaient possibles sans contrôle granulaire.

C'est la preuve que cette veille ne sert pas qu'à lire passivement. Elle m'a permis d'engager une discussion professionnelle concrète sur notre infrastructure. Pour moi, c'est ça l'intérêt d'une vraie veille : transformer l'information en échange terrain.

Bloc 3 : Dell'Oro Group – Prévisions SASE 97 Mds USD (février 2026)

Source : Dell'Oro Group, 3 février 2026

Lien : https://www.delloro.com/5-year-sase-forecast-97b

Résumé : 97 Mds USD 2025-2030 (×3). SSE = couche politique, SD-WAN = exécution. Sécurité dicte réseau.

Ce que je retiens :

Ce triplement du marché SASE en 5 ans n'est pas un hasard. Ça confirme un changement de fond dans la manière de concevoir les réseaux. Avant, on construisait le réseau, puis on ajoutait la sécurité par-dessus. Maintenant, c'est l'inverse : la sécurité dicte l'architecture réseau.

Pour mon futur métier d'admin systèmes et réseaux, ça change tout. Les compétences traditionnelles (VLANs, routage statique, STP, port-channel) que j'ai pratiquées chez Outscale ne suffiront plus. Il faudra maîtriser IAM, politiques contextuelles, microsegmentation, intégration SIEM/SOAR. C'est pour ça que je vise la Licence Pro ASR : je sais que ces compétences seront attendues.

Ce chiffre de 97 milliards montre aussi que le marché valide cette évolution. Pour un futur alternant, c'est rassurant : les entreprises investissent massivement, donc elles auront besoin de profils formés à ces technologies.

5. Conclusion

Au départ, je voyais cette veille comme un exercice obligatoire pour le BTS. Mais en creusant le sujet, je me suis rendu compte que c'était bien plus que ça.

Cette veille m'a permis de suivre en temps réel l'actualité janvier-avril 2026 de la transition VPN→Zero Trust→ZTNA. Les chiffres sont clairs : 48% des ransomwares passent par des VPN compromis (mars 2026), 65% des entreprises prévoient de remplacer leurs VPN dans les 12 mois (mars 2026), le marché SASE va tripler pour atteindre 97 milliards USD d'ici 2030 (février 2026). Ces chiffres montrent que ce n'est pas une mode, mais une vraie transformation.

Ce qui m'a le plus marqué, c'est le changement de mentalité apporté par le Zero Trust. Le principe 'ne jamais faire confiance, toujours vérifier' inverse complètement la logique traditionnelle. Avant, on protégeait un périmètre et on faisait confiance à ce qui était dedans. Maintenant, on ne fait plus confiance à personne, même en interne. Face aux menaces actuelles (ransomwares, mouvements latéraux, attaques sophistiquées), c'est la seule approche qui tient la route.

Cette veille m'a aussi appris à m'organiser. Utiliser Inoreader, configurer des alertes Google, trier les sources, croiser les informations… Ce sont des compétences que je réutiliserai tout au long de ma carrière. Dans un domaine qui évolue aussi vite que la cybersécurité, savoir faire de la veille efficace est indispensable.

L'exemple le plus concret, c'est ce qui s'est passé chez Outscale. Grâce à l'article CyberExperts.tech sur l'angle mort du réseau interne, j'ai pu engager des discussions avec mes collègues de l'équipe infrastructure (semaine 7, mars 2026) sur l'application de la microsegmentation dans notre architecture spine-leaf. Ces échanges m'ont montré que la veille ne sert pas qu'à accumuler des connaissances, mais à les transformer en réflexions terrain.

Pour mon projet professionnel, je vise une alternance en administration systèmes et réseaux lors de ma Licence Pro ASR (UTEC, septembre 2026). Cette veille m'a convaincu que les compétences Zero Trust, ZTNA, microsegmentation, automatisation des règles réseau et architecture SASE seront attendues sur le marché. Le fait d'avoir suivi l'actualité 2025-2026 de près me donne un vrai avantage : je ne parle pas de concepts théoriques mais d'évolutions récentes que je peux expliquer et défendre.

Si je devais résumer en une phrase : le Zero Trust et le ZTNA ne sont pas l'avenir de la sécurité réseau, ils sont déjà le présent. Et en tant que futur admin réseau, je dois maîtriser ces technologies maintenant, pas dans 5 ans.