



Moteur de renseignement sur le darknet et le deep web, spécialisé dans les documents d'entreprise.

SPÉCIMEN
données fictives

Spécimen. ACME et toutes les organisations, personnes, adresses et valeurs citées dans ce document sont fictives. Il reproduit la forme et le niveau de détail d'un relevé remis à un client.

Relevé d'exposition darknet : ACME

Destinataire : ACME Aérostructures SAS et ACME Aero Belgium SRL

Domaines relevés : acme-aero.example, acme-aerostructures.example, acme-aero-be.example

Date de remise : 1er octobre 2026

Réalisé par : SitinCloud, éditeur d'OwlyScan

Nature du relevé : collecte passive. Aucun accès à vos systèmes, aucun scan de votre infrastructure, aucun essai des identifiants ni des clés retrouvés. Nous n'avons lu que ce qui est déjà exposé.

Résumé exécutif

ACME n'est elle-même la cible d'aucune revendication de rançongiciel. Aucun partage de fichiers d'ACME n'a été publié en bloc, et aucun groupe ne la cite comme victime.

Pourtant, des secrets d'ACME circulent en clair, et deux appellent une action aujourd'hui. Quatre publications concernent ACME directement : 119 documents, dont 12 de criticité élevée. Leurs origines n'ont rien de commun : des journaux d'infostealer (logiciel voleur d'identifiants) volés sur 14 postes de salariés, six collages sur un service public de partage de texte depuis le 21 septembre 2026, les fichiers de votre cabinet comptable publiés par un groupe de rançongiciel, des fils de forum qui décrivent votre réseau. Une recherche élargie à vos fournisseurs porte le total à sept sources, indexées entre le 12 mai 2023 et le 29 septembre 2026.

Rubrique demandée	Constat	Gravité
Secret des affaires	Relation avec votre usineur reconstituée (quantités, livraisons, temps machine, un défaut de qualité), 14 fournisseurs avec coordonnées bancaires et calendrier de règlement	Moyenne, élevée en cumul
Données techniques et industrielles	Aucun plan lu, mais le dossier de contrôle d'une pièce en titane et l'index des plans, avec leurs classes d'exportation, publiés chez un sous-traitant	Élevée
Informations sensibles défense	Aucun document classifié, aucun marquage, aucun programme de défense. Des plans classés à l'exportation (<code>9E991</code> , <code>EAR99</code>)	Faible, à surveiller
Données RH	14 salariés dont le poste est infecté, 6 personnes de la finance nommées avec leur ligne directe, le circuit de validation des paiements	Moyenne
Points d'entrée cyber	Un identifiant VPN de la comptabilité fournisseurs, une clé de facturation et un mot de passe de base collés le 27 septembre 2026	Élevée
Points d'entrée d'une approche physique	Calendrier, quai et contenu des expéditions vers votre ligne d'assemblage, gardiennage de nuit de Lavaur	Moyenne

Les quatre points qui appellent une décision.

- Deux secrets d'ACME ont été collés en clair le 27 septembre 2026.** La clé de l'API de facturation `acme_bill_[...]` et le mot de passe de la base `billing_prod`. C'est l'élément le plus direct du relevé : la rotation des deux secrets ferme ce scénario.

2. **Un identifiant VPN de la comptabilité fournisseurs est dans des journaux d'infostealer.** Le compte `slématique`, volé le 22 juillet 2026 à Laval. Il se combine avec la passerelle décrite par un forum et les noms de la finance publiés avec les fichiers de votre cabinet comptable : trois publications, aucune ne le montre seule. Il manque la liste d' enrôlement du second facteur, que nous ne voyons pas.
3. **La documentation des pièces d'ACME est dans le partage de Globex Machining.** Contrôle de premier article, bon de commande, non-conformité, index des plans, plan de charge : 312 Go publiés le 2 juin 2026, après une annonce de vente. Le nom d'ACME n'y figure pas, le code client `AC-0092` suffit.
4. **Les fichiers de votre cabinet comptable sont publiés.** Factures avec leurs vrais numéros, coordonnées bancaires de 14 fournisseurs, calendrier de règlement, noms et lignes directes de la finance : de quoi écrire un faux courrier de changement de coordonnées bancaires qui ressemble à un vrai.

La lecture d'ensemble. Ce que risque ACME n'est pas d'abord la divulgation de son savoir-faire : c'est qu'on entre chez elle avec ses propres clés et qu'on parle à ses équipes avec ses propres mots. Trois éléments issus de trois sources sans lien entre elles se complètent : la clé, la porte et la personne. Des cinq scénarios d'attaque que calcule OwlyScan pour ACME, deux sont de gravité élevée (se connecter au VPN, appeler l'API de facturation), deux moyens (hameçonner la finance, détourner un règlement) et un faible (cartographier le réseau). Le durcissement à conduire porte sur les secrets, sur l'authentification du VPN et sur la chaîne d'approvisionnement, où la documentation de vos pièces circule hors de vos murs, sous un code client.

1. Synthèse

ACME n'apparaît dans aucune revendication de rançongiciel. Pourtant, des documents et des secrets d'ACME circulent, issus de quatre endroits sans rapport entre eux : des postes de travail infectés, une habitude d'exploitation (déposer des fichiers de travail sur un service public), un cabinet comptable et, un cran plus loin, un usineur et son transitaire. **Sept sources distinctes** ont été identifiées, et 55 % des documents datés ont moins d'un an : l'exposition est récente, elle n'est pas historique.

Le mécanisme est celui des fuites de proximité : ce n'est pas votre système d'information qui cède, ce sont des maillons voisins qui livrent ce qu'ils savent de vous. Chacun détient un morceau d'ACME, aucun n'a l'ensemble, et c'est l'assemblage qui devient utilisable. Quatre points appellent une décision de votre part.

Deux secrets collés en clair. La clé de l'API de facturation et le mot de passe de la base `billing_prod` ont été déposés le 27 septembre 2026 sur un service public de partage de texte, avec l'adresse du serveur de base. Les six collages de la série sont nouveaux depuis le 21 septembre.

Un accès VPN en trois éléments. Le compte d'une comptable fournisseurs de Laval figure dans un lot de journaux d'infostealer (poste infecté le 22 juillet). La passerelle vient d'un forum, l'identité et la fonction de la titulaire des fichiers de votre cabinet comptable. Un élément manque, que seule votre équipe peut voir : le second facteur.

La documentation de vos pièces, dans le partage de votre usineur. Les fichiers de Globex Machining, 312 Go, ont été publiés le 2 juin 2026, quatre jours après une annonce de vente. Vos références y figurent sous un code client, avec les contrôles, la commande et l'index des plans. Les manifestes de son transitaire, Initech Freight, montrent les mêmes pièces en route vers votre ligne d'assemblage.

Les fichiers de votre cabinet comptable. Ceux de Contoso Expertise Comptable, publiés le 24 mars 2026, livrent pour ACME des factures, les coordonnées bancaires de 14 fournisseurs, le calendrier de règlement, la finance nommée et le circuit de validation.

Rien de classifié, aucun plan lu, aucun code source : ce que vous risquez, c'est l'entrée par la bonne porte, avec la bonne clé.

2. Périmètre, méthode et limites

Ce que nous avons interrogé. L'index OwlyScan couvre les sites de revendication de rançongiciel, les archives d'exfiltration accessibles par des adresses `.onion`, les lots de journaux d'infostealer, les services de collage de texte et des forums. Trente-quatre requêtes ont été passées sur vos noms de domaine, vos raisons sociales (ACME Aérostructures SAS, ACME Aero Belgium SRL), vos dirigeants, vos plages d'adresses IP et les références de pièces que vous nous avez confiées (préfixe `7Q-4410-`). Les sources sont repérées par une lettre, de A à G (section 4).

Volumétrie brute.

Requête	Occurrences	Observation
"acme-aero.example"	131	dont 36 doublons (même fichier dans plusieurs archives)
"acme-aerostructures.example"	9	
"acme-aero-be.example"	12	
"vpn.acme-aero.example"	19	dont 14 dans les fils du forum
"ACME AEROSTRUCTURES"	87	dont 29 homonymes sans rapport
"acme_bill_"	2	la clé, et le nom de la variable dans le fichier de configuration
"203.0.113.40"	17	passerelle VPN
"198.51.100."	11	serveurs de recette et base de facturation
"7Q-4410-114"	21	14 chez Globex Machining, 6 chez Initech Freight, 1 annonce de vente
"AC-0092"	11	5 chez Globex Machining, 6 chez Initech Freight

Ce que nous avons écarté. La chaîne `acme` seule remonte plus de 3 000 résultats, presque tous des configurations de serveurs web contenant un répertoire `acme-challenge` : aucun rapport. Sur les 87 occurrences de `ACME AEROSTRUCTURES`, 29 désignent des homonymes (une société de charpente métallique, un fabricant d'échelles). Dix-huit adresses `@acme-aero.example` figurent dans d'anciennes compilations d'identifiants issues de sites tiers : elles ne dénotent aucune compromission d'ACME. Les 36 doublons du premier domaine ont été fusionnés.

Ce que nous n'avons pas trouvé, et qui compte autant. Aucune revendication de rançongiciel au nom d'ACME. Aucune annonce de vente d'accès VPN, de bureau à distance ou de passerelle sur les places de marché indexées. Aucun code source. Aucun plan lu : l'index des plans de Globex Machining est publié, mais aucun fichier de plan ne figure dans la partie de l'archive que nous avons lue. Aucun document de l'intégrateur ni du client final. Aucune donnée de paie, aucun dossier de salarié. Aucune liste d' enrôlement du second facteur.

Comment le lien avec ACME est établi. Le nom d'ACME ne figure dans aucun fichier de Globex Machining ni d'Initech Freight : ils désignent leur client par un code, `AC-0092`. Le rattachement repose sur trois constats. Les références de pièces (`7Q-4410-114`, `-116`, `-120`) sont les vôtres, vous nous les avez confiées. Dans deux sources qui ne se connaissent pas, le partage de Globex et les manifestes d'Initech, elles sont toujours associées au même code client, et l'annonce de vente les cite sans lui. Enfin, la commande `P0-2026-0412` (240 supports, 120 ferrures, semaine 18) se retrouve à l'identique sur le manifeste `MAN-55810`, et le journal des achats 2025 du cabinet comptable (source C) cite Globex Machining parmi vos usineurs. C'est une inférence solide, pas une preuve : seul votre service achats peut confirmer que `AC-0092` est bien votre code.

Datation. La date d'indexation est celle de la première lecture par OwlyScan, pas celle de la fuite. Sur les 119 documents des sources A à D, 112 portent une date exploitable, et 62 d'entre eux ont moins d'un an, soit 55 % des documents datés.

Limite de l'exercice. Un relevé passif ne voit que ce qui a été publié et indexé : une exfiltration en cours de négociation reste invisible. L'archive de Globex Machining est lue partie par partie. Les 14 documents cités sont tous

dans la partie 07, et les autres parties, en cours de traitement, peuvent en contenir davantage, plans compris. Nous n'avons testé aucun identifiant ni aucune clé, qui ont pu être changés depuis leur publication. Ce relevé est arrêté au 30 septembre 2026.

3. Réponse rubrique par rubrique

3.1 Secret des affaires

Une relation d'approvisionnement est reconstituée, avec ses volumes et son calendrier.

Globex Machining (sources E et G). Son partage de fichiers, publié le 2 juin 2026, contient le bon de commande **P0-2026-0412** : 240 supports **7Q-4410-114** indice C et 120 ferrures **7Q-4410-116** indice B, livraison en semaine 18 au quai B de l'usine « Plant 2 », clause qualité **QC-7** (contrôle de premier article exigé). Le plan de charge **Plant2_load_wk14-26.xlsx** ajoute le temps machine : en semaine 18, 96 heures sur la machine **M4** pour les supports, soit 24 minutes par pièce. Les manifestes d'Initech Freight (source F) donnent la cadence : quatre expéditions en avril 2026 (40, 60, 80 et 100 pièces), puis, en mai, un lot d'échantillons et deux caisses (240 supports, 120 ferrures).

Un défaut de qualité, daté et expliqué. Le rapport de non-conformité **NCR-2026-031** consigne un alésage à 12,06 mm pour une cote de 12,00 mm +0,05, la reprise décidée, la demande de concession adressée à la qualité du client **AC-0092** et la cause : l'usure du montage d'usinage de la machine 4.

Ce que cela donne à un concurrent : le nom de votre usineur, la quantité et la semaine de livraison de chaque lot, le temps d'usinage unitaire, la montée en cadence et l'historique d'un défaut sur une pièce en titane. De quoi estimer votre coût de revient et préparer une offre concurrente.

Le cabinet comptable (source C). Ses 38 documents listent 14 fournisseurs récurrents (dont Globex Machining, Soylent Matériaux pour le titane, Wonka Traitements de Surface, Fabrikam Outillage, Umbrella Métrologie et Vandelay Sécurité), avec factures, montants et échéances. Les six dernières déclarations de TVA, d'août 2025 à janvier 2026, donnent le chiffre d'affaires mensuel.

Gravité : moyenne, élevée en cumul. Aucun contrat-cadre, aucune facture client, aucun prix de vente n'a été retrouvé. Mais l'ensemble dessine votre structure de coûts sur une pièce, votre calendrier de livraison, vos fournisseurs et votre rythme de trésorerie.

3.2 Données techniques et industrielles

Pas de plan lu, mais le dossier de contrôle d'une pièce de structure. Tout vient de la partie 07 de l'archive **globex_shares_part07.7z**, publiée sur le site de revendication d'un groupe de rançongiciel (hôte **mojzk4yj...onion**) le 2 juin 2026.

Le rapport de contrôle de premier article. Fichier **globex/Shares/Quality/FAI/FAI_7Q-4410-114_revC.xlsx**, contrôlé le 14 mars 2026 et approuvé le 16 mars. En tête :

```
Part number;7Q-4410-114;Rev;C
Part name;Bracket, wing-to-pylon fairing
Customer;AC-0092;Purchase order;P0-2026-0412
Material;Ti-6Al-4V AMS 4928;Heat lot;H-22871
Drawing;7Q-4410-114 sheet 1-3;Export class;9E991
```

Suivent huit caractéristiques avec leur cote, leur tolérance et la valeur mesurée. La caractéristique 4, l'alésage B, est notée **NOK**.

L'index des plans. Le fichier `globex/Shares/Engineering/Drawings/index.csv` recense 12 références pour `AC-0092`. Les trois premières :

```
drawing;rev;title;customer;export
7Q-4410-114;C;Bracket, wing-to-pylon fairing;AC-0092;9E991
7Q-4410-116;B;Fitting, fairing aft;AC-0092;9E991
7Q-4410-120;A;Shim set;AC-0092;EAR99
```

Les neuf autres, de `7Q-4410-130` à `7Q-4410-146`, sont les composants qui s'assemblent sur la `7Q-4410-114` : chacun a son rapport de contrôle dans le partage. La structure de l'assemblage se reconstitue sans plan. Le collage du 29 mai 2026 (source G, `/p/8fd2c1`) met le partage en vente et revendique les plans :

```
Globex Machining full share dump 312 GB, incl. engineering drawings for aerospace customers (7Q-4410-114, 7Q-4410-116...)
```

Nous ne pouvons affirmer ni que ces plans sont dans l'archive, ni qu'ils n'y sont pas : la partie lue n'en contient aucun.

Gravité : élevée. Ce n'est pas un plan, mais c'est le dossier de contrôle d'une pièce de structure d'un programme d'avion commercial : matière, coulée, tolérances, classe d'exportation. Il est sorti d'un sous-traitant de rang 1 où vos exigences de confidentialité ne s'appliquent plus que sur le papier. Le nom d'ACME n'est pas dans le fichier, mais la référence est la vôtre.

3.3 Informations sensibles défense

Aucun document classifié, aucun marquage de protection, aucune référence de programme de défense dans l'index pour ACME. Le périmètre relevé est celui d'un programme d'avion commercial.

Une information de conformité est cependant exposée. L'index des plans classe chaque référence à l'exportation (`9E991` pour les deux premières, `EAR99` pour la troisième), et le manifeste `MAN-55794` porte la mention « export-controlled, keep paperwork with the crate ». Ce ne sont pas des marquages de défense, ce sont des classements de contrôle à l'exportation : ils indiquent que vos pièces relèvent d'un régime d'exportation et que leur circulation est encadrée par un dossier de papiers (voir 3.6).

Gravité : faible aujourd'hui, à surveiller. Le risque n'est pas la divulgation d'un secret de défense, c'est qu'un document sous contrôle à l'exportation circule hors de la chaîne autorisée.

Recommandation spécifique : faire vérifier par votre responsable conformité export que ces classes sont celles que vous avez déclarées, et si cette circulation appelle une information de l'intégrateur.

3.4 Données RH

Deux sources nomment vos équipes : les journaux d'infostealer et le dossier du cabinet comptable. Aucun bulletin de paie ni dossier individuel n'a été retrouvé.

Les postes infectés (source A). Les journaux viennent de 14 postes de travail (8 à Laval, 3 à Castres, 3 à Ath), infectés entre le 2 février 2024 et le 9 août 2026, dix d'entre eux depuis octobre 2025. Chaque poste livre deux fichiers d'identifiants (un par navigateur) et une fiche système : nom du poste, de l'utilisateur, pays, logiciels installés. S'y ajoute une liste d'hôtes SSH, `ssh_hosts.txt`, retrouvée sur le poste d'administration `LAV-PC009`, soit 43 documents. Les postes suivent la convention `SITE-PCnnn` (`LAV-PC114`, `CAS-PC027`, `ATH-PC031`). Sur les 28 fichiers d'identifiants, 8 sont de criticité élevée : ils contiennent un identifiant d'un service d'ACME (VPN, messagerie web, ERP, portail d'achats). Les 20 autres mêlent usage privé et usage professionnel.

La finance, nommée (source C). La fiche de contacts du dossier ACME, datée du 20 novembre 2025 :

Nom	Fonction	Contact direct exposé
Marianne Chauvet	Directrice administrative et financière	+33 5 36 49 02 08
Nathalie Vasseur	Responsable comptabilité et trésorerie	+33 5 36 49 02 21
Sylvie Lemaitre	Comptable fournisseurs	+33 5 36 49 02 17, +33 6 39 98 41 52
Arnaud Barbier	Comptable clients	+33 5 36 49 02 19
Étienne Brossard	Contrôleur de gestion	+33 5 36 49 02 24
Charlotte Morel	Assistante comptable	+33 5 36 49 02 26

Y figurent aussi Quentin Wauters, directeur du site d'Ath, et Aurélie Hanot, gestionnaire administrative et financière. Côté cabinet, la lettre de mission nomme Mathieu Roche, expert-comptable associé, et Inès Navarro, qui tient le dossier.

Pourquoi ce croisement compte. Une équipe financière se devine sur les réseaux professionnels. Ce qui ne s'y devine pas, c'est qui détient quel droit : la comptable fournisseurs prépare les règlements, la responsable comptabilité et trésorerie les valide, la directrice administrative et financière contresigne au-delà de 20 000 € (point 3.5.d). Le compte VPN volé (point 3.5.a) est celui de la première, la personne la mieux placée pour déclencher un paiement.

Gravité : moyenne. Aucune donnée de santé ni de paie. Mais un nom, une fonction, une ligne directe et un droit de validation suffisent à rendre crédible un appel ou un courriel.

3.5 Points d'entrée d'une attaque informatique

a. Un accès VPN au nom de la comptabilité fournisseurs

Source : hôte `x4hq7p2d...onion`, archive `FR_FREEPACK_2026-08.zip`, lot de journaux d'infostealer mis en vitrine par un revendeur, indexé le **14 août 2026**. Poste `LAV-PC114`, infecté le **22 juillet 2026**. L'entrée enregistrée par le navigateur :

```
URL: https://acces.acme-aerostructures.example/  
Login: slemaitre  
Password: [...]
```

Analyse. L'adresse est un alias de la passerelle sur l'ancien domaine, et l'identifiant suit la convention initiale du prénom plus nom. Seule, l'entrée ne dit ni si l'alias répond encore, ni qui est `slemaitre`. Deux autres publications répondent. Le forum (source D) établit que cet alias et `vpn.acme-aero.example` pointent vers la même adresse, `203.0.113.40`, et que la page de connexion répondait encore le 3 juillet 2026. Le cabinet comptable (source C) donne le nom, la fonction et la ligne directe de Sylvie Lemaitre, comptable fournisseurs. Preuves réunies : **3 sur 4**. Nous n'avons pas trouvé la liste des comptes enrôlés au second facteur.

Aucune publication ne montre ce scénario seule : c'est leur assemblage qui le compose. Un mot de passe volé le 22 juillet 2026 a dix semaines à la date de ce relevé : si le compte n'exige pas de second facteur, il peut suffire. Il doit être considéré comme brûlé, les sessions de `LAV-PC114` révoquées et le poste réinstallé.

b. Une clé de facturation et un mot de passe de base de données, collés le 27 septembre 2026

Source : hôte `dmp5cnzx...onion`, service de collage de texte. Six collages d'un même auteur anonyme, indexés du **21 au 29 septembre 2026**, tous nouveaux depuis le 21 septembre.

Date	Contenu	Criticité
21 septembre	script de déploiement, clé d'API codée en dur libellée « recette »	moyenne

Date	Contenu	Criticité
23 septembre	sept serveurs de recette, de 198.51.100.11 à 198.51.100.17	moyenne
24 septembre	extrait de journal d'application : cinq adresses professionnelles	faible
27 septembre	fichier de configuration avec l'identifiant et le mot de passe de la base billing_prod	élevée
27 septembre	clé d'API de facturation acme_bill_[...]	élevée
29 septembre	description de la sauvegarde, sans secret	faible

Le fichier de configuration, secrets masqués :

```
db_host: 198.51.100.23
db_name: billing_prod
db_password: [...]
```

Analyse. La clé collée le 27 septembre n'a pas le marqueur _test de la clé de recette du script du 21 septembre : tout indique une clé de production. Nous ne sondons pas le réseau : nous ne savons pas si 198.51.100.23 est joignable depuis Internet. Si oui, le mot de passe ouvre directement la base de facturation ; sinon, il aide qui entre déjà par ailleurs, par le VPN du point a par exemple. Rien n'indique une intrusion chez vous : la série a le profil de fichiers de travail déposés depuis un poste de développement. Mais le service est public, lu par des collecteurs automatiques, et nous ne pouvons pas dire qui d'autre a lu ces collages. Les sept serveurs de recette figurent aussi dans la liste d'hôtes SSH de la source A, avec un bastion (198.51.100.5) en plus : les deux sources se confirment.

C'est l'élément le plus direct du relevé. La rotation de la clé et du mot de passe ferme ce scénario et justifie à elle seule une action aujourd'hui.

c. Le réseau d'ACME, décrit par un forum

Source : forum de langue russe, hôte f2tn5vby...onion, 32 messages du 11 mai 2023 au 3 juillet 2026, indexés à partir du 12 mai 2023. Trois membres, dans des fils d'échange de listes de cibles de l'aéronautique européenne. Aucun message n'offre d'accès à la vente.

Machine	IP	Première mention	Fonction
vpn.acme-aero.example (et acces.acme-aerostructures.example)	203.0.113.40	11 mai 2023	accès distant
webmail.acme-aero.example	203.0.113.41	11 mai 2023	messagerie web
erp.acme-aero.example	203.0.113.44	2 février 2024	gestion de production
portail.acme-aero.example	203.0.113.46	14 octobre 2024	dépôt de documents fournisseurs
vpn.acme-aero-be.example	192.0.2.18	9 avril 2025	accès distant, site belge

Les messages donnent aussi la convention de comptes (initiale du prénom plus nom) et celle des postes de travail (SITE-PCnnn).

Analyse. Rien d'exploitable seul : ni compte, ni vulnérabilité annoncée, ni mot de passe. Mais l'inventaire est établi : le bloc 203.0.113.0/24 n'a pas changé de 2023 à 2026, la passerelle est connue sous deux noms, la convention de comptes est publique. Quiconque prépare une opération contre ACME part de ces cinq noms de machines, sans avoir à chercher. Il convient de vérifier que chacun de ces services doit être joignable depuis Internet, et sous quelle authentification.

Gravité : faible en soi. Mais cette reconnaissance est faite et partagée depuis plus de trois ans, et elle fournit la porte du scénario du point a.

d. Le circuit de règlement des fournisseurs, avec ses documents types

Source : dossier ACME du cabinet Contoso Expertise Comptable, publié par un groupe de rançongiciel (hôte `h6wk3zr5...onion`) le **24 mars 2026**, indexé le **25 mars 2026**. Sur près de 6 400 fichiers, tous clients confondus, 38 concernent ACME :

Type de document	Nombre	Criticité
Registre des coordonnées bancaires fournisseurs (<code>RIB_fournisseurs_2026.xlsx</code>)	1	élevée
Calendrier de règlement 2026 (<code>calendrier_reglements_2026.xlsx</code>)	1	élevée
Courriers de changement de coordonnées bancaires (scans)	3	moyenne
Factures fournisseurs (scans)	17	moyenne
Journaux des achats 2023, 2024 et 2025	3	moyenne
Fiche de contacts de l'équipe financière	1	moyenne
Lettre de mission, avenant, déclarations de TVA, courriers divers	12	faible

Le circuit. L'avenant du 18 décembre 2025 à la lettre de mission décrit la procédure. Les règlements partent le 5 et le 20 de chaque mois. La comptable fournisseurs les prépare, la responsable comptabilité et trésorerie les valide, la directrice administrative et financière contresigne au-delà de 20 000 €. Un changement de coordonnées bancaires est pris en compte sur courrier signé du fournisseur, scanné et transmis au cabinet, qui met le registre à jour. Aucun rappel du fournisseur à un numéro connu n'est prévu avant cette mise à jour.

Analyse (scénarios 3 et 4, gravité moyenne). Les factures portent de vrais numéros, montants et échéances : `SM-2026-01877` (Soylent Matériaux, 14 janvier 2026), `F0-2026-03317` (Fabrikam Outillage), `WTS-26-0315` (Wonka Traitements de Surface). Une relance pour l'une d'elles, adressée à la comptable fournisseurs, est crédible (scénario 3). Les trois courriers de changement de coordonnées bancaires fournissent un modèle complet : papier à en-tête, formule, signataire. Avec le registre et le calendrier du 5 et du 20, un faux courrier arrive au bon moment et à la bonne personne (scénario 4). Ces scénarios restent de gravité moyenne : ils exigent un faux soigné et le bon moment, mais le circuit décrit n'a aucune étape qui les arrêterait.

Gravité : élevée. Deux accès sont à portée (points a et b) : la clé de facturation, qui ne dépend que de sa validité, et le VPN, qui dépend d'un second facteur que nous ne voyons pas. Les deux se ferment en moins de 24 heures.

3.6 Points d'entrée d'une approche physique

Source : manifestes d'Initech Freight (source F), dossier `initech/Ops/Manifests`, hôte `ynm3mex5...onion`, publiés le **21 mai 2026**, 6 documents ; factures et fiche de contacts du cabinet comptable (source C).

Manifeste	Dossier	Contenu
<code>MAN-55700</code> , <code>-55709</code> , <code>-55718</code> , <code>-55727</code>	2026-04	destinataire <code>AC-0092</code> , <code>7Q-4410-114</code> : 40, 60, 80 puis 100 pièces
<code>MAN-55794</code>	2026-05	5 pièces pour un nouveau contrôle de premier article, vraisemblablement après la reprise de la <code>NCR-2026-031</code> ; « export-controlled, keep paperwork with the crate »
<code>MAN-55810</code>	2026-05	expéditeur Globex Machining Plant 2, destinataire <code>AC-0092</code> (ligne d'assemblage final), 2 caisses, 240 supports et 120 ferrures, valeur déclarée 71 400 €

Analyse. Qui prépare une approche physique sait, avant d'avoir mis un pied sur le site : quand les caisses partent (semaine 18, quai B de « Plant 2 »), ce qu'elles contiennent et valent, que le papier d'accompagnement fait foi, et à quelle ligne elles arrivent. Le cabinet ajoute le standard de Lavour (`+33 5 36 49 02 00`), la réception des marchandises (`+33 5 36 49 02 31`) et le gardiennage : la facture `VS-2026-0311` de Vandelay Sécurité (28 février 2026) décrit deux agents de nuit, sept nuits sur sept, et un agent en journée le week-end. Aucun plan de site, code

d'accès, liste de badges ni consigne de visite n'est exposé. Castres et Ath n'exposent rien de physique : seulement leurs postes de travail et, pour Ath, une passerelle.

Point à noter : le manifeste est le papier qu'un faux transporteur chercherait à imiter pour enlever un lot, et six exemplaires réels sont publiés.

Gravité : moyenne, par la logistique. Rien ne donne l'accès au site : ce qui est exposé, c'est le moment, le lieu, le contenu et le papier d'un transfert de pièces sous contrôle à l'exportation.

3.7 Ce qu'un adversaire déduit en croisant avec l'information publique

Aucun des éléments ci-dessus n'est décisif isolément. Recoupés, et croisés avec ce qui est publiable sur ACME (site internet, offres d'emploi, profils professionnels), ils composent cinq scénarios, du plus grave au moins grave.

#	Scénario	Gravité	Ce qui est réuni
1	Se connecter au VPN d'ACME comme comptable fournisseurs	Élevée	3 preuves sur 4 : identifiants (A), passerelle (D), noms de la finance (C). Manque : l'enrôlement du second facteur
2	Appeler l'API de facturation avec la clé collée	Élevée	une seule publication (B) : la clé et le mot de passe de base, collés le 27 septembre 2026. La rotation des deux ferme le scénario
3	Hameçonner la finance avec de vrais numéros de factures	Moyenne	factures, contacts, calendrier (C)
4	Détourner un règlement par un faux courrier de changement de coordonnées bancaires	Moyenne	registre, courriers types, circuit de validation (C)
5	Cartographier le réseau d'ACME à partir d'un forum	Faible	inventaire et conventions de nommage (D)

Premier raisonnement : la clé, la porte et la personne viennent de trois endroits. Les journaux d'infostealer donnent la clé, le forum la porte (la passerelle, son adresse, ses deux noms), le cabinet comptable la personne (nom, fonction, ligne directe, place dans le circuit de validation). Trois origines sans lien entre elles, et aucune ne montre le scénario seule. L'information publique n'a presque rien à ajouter : une offre d'emploi suffit à confirmer qu'un poste de comptable fournisseurs existe à Lavaur.

Deuxième raisonnement : la valeur d'ACME est aussi chez ses fournisseurs. Le partage de Globex Machining prouve qu'un dossier de contrôle de votre pièce **7Q-4410-114** circule, sans que votre nom y figure. Le rattachement se fait sans effort pour qui connaît vos références : le cabinet comptable cite Globex parmi vos usineurs, et le site public de Globex vante ses moyens d'usinage du titane et ses clients de l'aéronautique. L'annonce du 29 mai montre que vos pièces servaient d'argument de vente. Le raisonnement est immédiat : lire le dossier d'un sous-traitant coûte moins cher que viser son donneur d'ordre, et il est moins bien gardé.

Troisième raisonnement : le vocabulaire est disponible. Factures, montants et échéances donnent le contenu d'un faux courriel, les courriers de changement de coordonnées le modèle, le calendrier le moment, le circuit de validation les noms et le seuil de 20 000 €. Côté qualité, **P0-2026-0412**, **NCR-2026-031**, la coulée **H-22871** et la clause **QC-7** rendent crédible un faux courriel de « concession accordée » adressé à vos achats ou à votre qualité.

Nuance importante. Rien ne dit que l'un de ces scénarios se joue : nous n'avons testé aucun accès et ne voyons pas l'intérieur d'ACME. Nous constatons que les pièces nécessaires à chacun sont en ligne, certaines depuis plus de trois ans (la passerelle), d'autres depuis quatre jours (les secrets). La parade porte d'abord sur ce qui se périme (secrets, mots de passe, sessions), puis sur les circuits (qui valide quoi, avec quel rappel), enfin sur ce que vos fournisseurs détiennent de vous.

4. Les sept sources, datées

#	Source	Date d'indexation	Documents	Ce qu'elle expose d'ACME
A	journaux d'infostealer, x4hq7p2d... onion	14 août 2026	43	14 postes de salariés, identifiants dont un VPN de la comptabilité, hôtes SSH
B	service de collage de texte, dmp5cnzx...onion	21 au 29 septembre 2026	6	clé de facturation, mot de passe de base , script de déploiement, serveurs de recette
C	Contoso Expertise Comptable, h6wk3zr5...onion	25 mars 2026	38	factures, coordonnées bancaires de 14 fournisseurs, calendrier de règlement, finance
D	forum de langue russe, f2tn5vby...onion	12 mai 2023	32	passerelle VPN, noms d'hôtes, conventions de nommage
E	Globex Machining, groupe de rançongiciel, mojk4y...onion	2 juin 2026	14	contrôle de premier article, commande, non-conformité, index des plans, plan de charge
F	Initech Freight, ynm3mex5...onion	21 mai 2026	6	expéditions vers AC-0092 : contenu, cadence, valeur
G	annonce de vente, dmp5cnzx... onion	29 mai 2026	1	7Q-4410-114 et 7Q-4410-116 cités dans l'offre du partage Globex

Les sources A à D sont celles du tableau de bord OwlyScan : 119 documents, dont 12 de criticité élevée (8 pour A, 2 pour B, 2 pour C). Les sources E à G viennent d'une recherche élargie à vos fournisseurs et ne sont pas comptées dans ces 119 ; leur décompte est celui des documents qui citent 7Q-4410-114. Un huitième corpus, la liste des inscrits à un salon professionnel, mentionne ACME comme exposant. Sans portée.

Point de méthode à retenir. Les sources A et B ne sont pas des attaques contre ACME : ce sont des fuites de proximité, un poste de salarié et un geste d'exploitation. Les sources C, E et F sont trois victimes de rançongiciel distinctes, publiées sur trois sites en dix semaines (24 mars, 21 mai, 2 juin 2026) : le cabinet comptable, le transitaire, l'usineur. Aucune n'a ACME pour cible, et chacune livre pourtant un morceau d'ACME.

5. Annexe : inventaire des adresses retrouvées

@acme-aero.example

adminsyst, anne-laure.pons, arnaud.barbier, charlotte.morel, claire.bessiere, david.rouquette, didier.salles, etienne.brossard, facturation.clients, gaetan.pinel, gilles.peyrac, helene.cazals, isabelle.delmas, karim.benaissa, laurent.roussel, lucie.arnal, marianne.chauvet, mathilde.sabatier, nathalie.vasseur, olivier.marty, pascal.fabre, qualite, romain.duplessis, sandrine.cros, service.achats, sylvie.lemaitre, thierry.lacombe, yann.combes

@acme-aerostructures.example

comptabilite, nathalie.vasseur, qualite, reception, secretariat, sylvie.lemaitre

@acme-aero-be.example

aurelie.hanot, bernard.lambotte, comptabilite, expéditions, maxime.pirotte, nathalie.collard, quentin.wauters, sabine.dewaele

Soit 42 adresses distinctes, dont 14 présentes dans les journaux d'infostealer (source A).

6. Suite à donner

Ce relevé vous est remis à vous seul. Il ne contient aucune valeur de mot de passe ni de clé : les secrets y sont masqués.

Aujourd'hui. Renouveler la clé `acme_bill_[...]` et le mot de passe de `billing_prod`, puis relire les journaux d'accès depuis le 27 septembre 2026. Réinitialiser le mot de passe de `slemaitre`, révoquer ses sessions, exiger un second facteur sur la passerelle VPN, traiter de même les comptes des 8 fichiers de criticité élevée, réinstaller les 14 postes infectés.

Cette semaine. Demander à Globex Machining, à Initech Freight et à Contoso Expertise Comptable la liste des documents d'ACME contenus dans leur fuite. Exiger un rappel du fournisseur à un numéro connu avant toute modification de coordonnées bancaires. Faire examiner les classes `9E991` et `EAR99` par votre responsable conformité export.

Trois questions restent ouvertes, et vous seul pouvez y répondre :

- Le compte `slemaitre` exige-t-il un second facteur, et `acces.acme-aerostructures.example` est-il toujours en service ?
- L'adresse `198.51.100.23` est-elle joignable depuis Internet ?
- `AC-0092` est-il bien votre code client chez Globex Machining ?