Revue d'actualité de l'OSSIR

13 janvier 2026

Jérémy De Cock
Melchior Courtois

<< La veille vous est fournie par cyberzen *>>*

L’équipe OSSIR vous souhaite

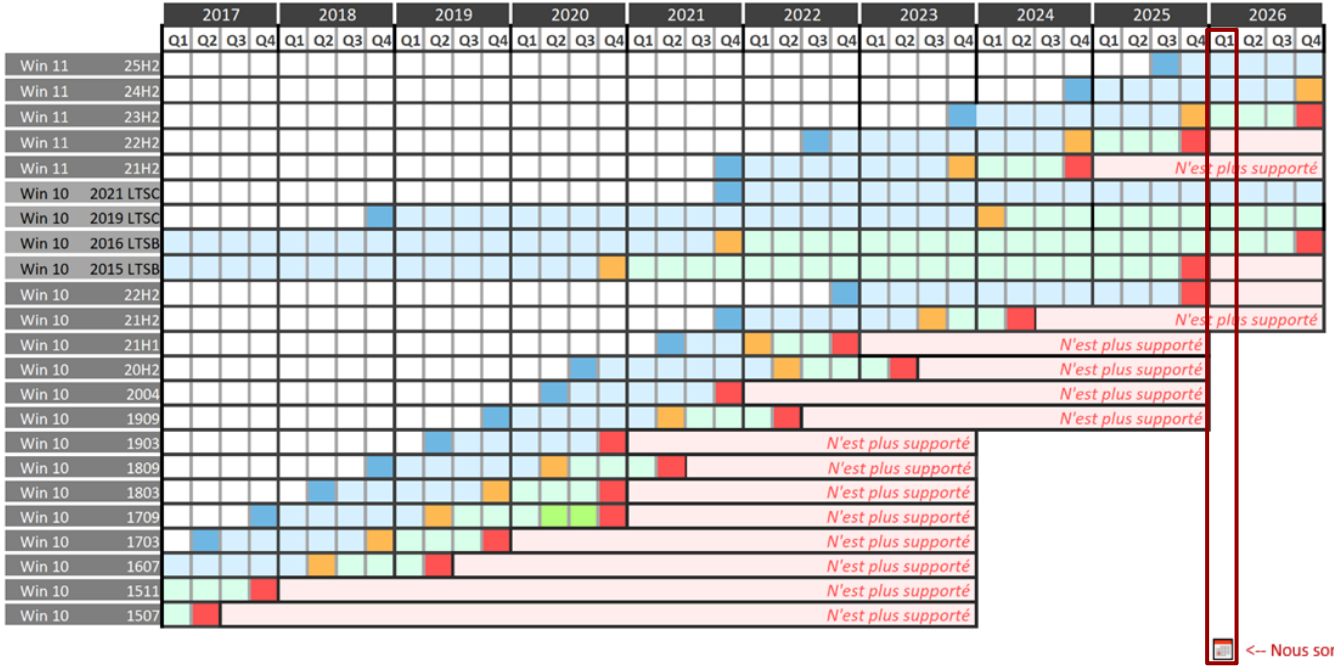
~~Nos~~ meilleurs vœux pour Ses 2026

La France est le pays européen le plus touché par les fuites de données en 2025 → Cela ne peut qu’être mieux en 2026 !

Rappel du support Windows en couleurs

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Windows ***Workstation***



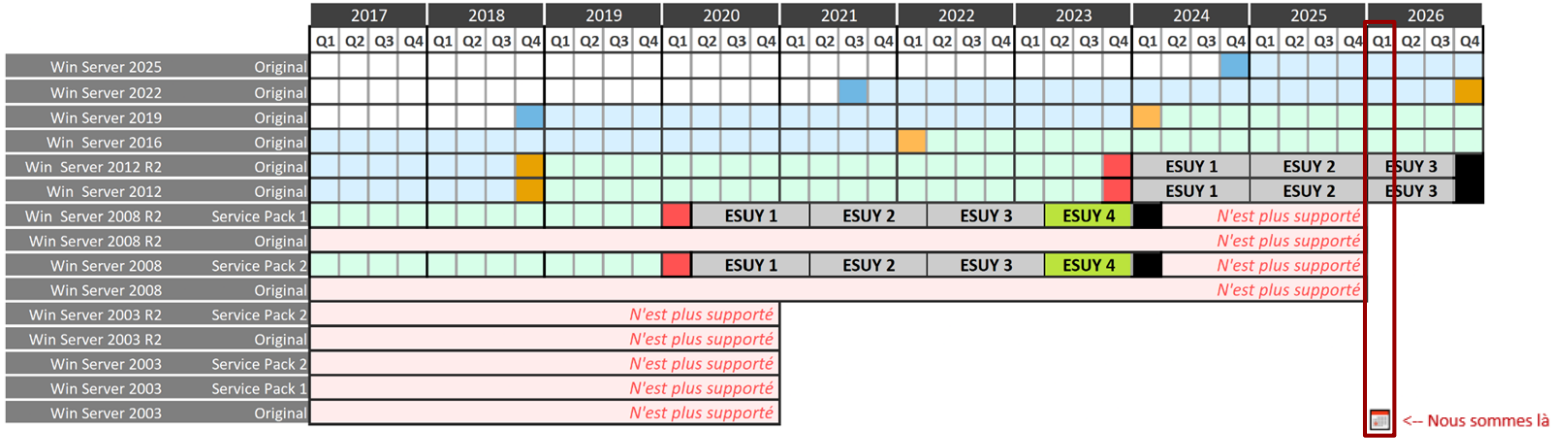
Sortie	Home, Pro	Entreprise
mardi 30 septembre 2025	mardi 12 octobre 2027	mardi 10 octobre 2028
mardi 1 octobre 2024	mardi 13 octobre 2026	mardi 12 octobre 2027
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 18 octobre 2022	mardi 14 octobre 2025	mardi 14 octobre 2025
mardi 16 novembre 2021	jeudi 13 juillet 2023	mardi 11 juin 2024
mardi 18 mai 2021	mardi 13 décembre 2022	mardi 13 décembre 2022
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 11 mai 2021
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
mercredi 5 avril 2017	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	mardi 9 mai 2017	mardi 9 mai 2017

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

LTSB : **L**ong-**T**erm **S**ervicing **B**ranch
LTSC : **L**ong-**T**erm **S**ervicing **C**hannel

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Server***



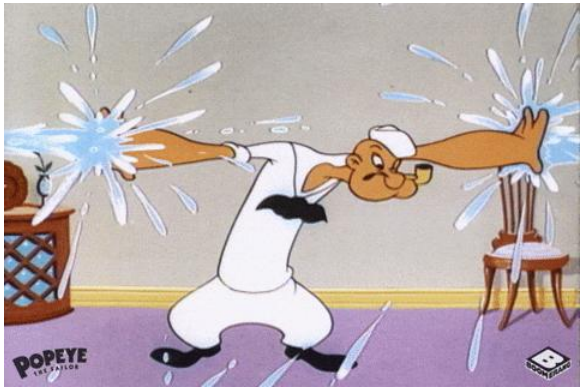
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 30 octobre 2012	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 22 février 2011	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
jeudi 22 octobre 2009	mardi 9 avril 2013		
mercredi 29 avril 2009	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
mardi 6 mai 2008	mardi 12 juillet 2011		
mardi 13 mars 2007	mardi 14 juillet 2015		
dimanche 5 mars 2006	mardi 14 avril 2009		
mardi 13 mars 2007	mardi 14 juillet 2015		
mercredi 30 mars 2005	mardi 14 avril 2009		
mercredi 28 mai 2003	mardi 10 avril 2007		

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour la version standard
- Support étendu pour LTSB/LTSC
- Fin de support étendu pour LTSB/LTSC
- X Extension d'une ou plusieurs années (ESUY)
- X Extension disponible uniquement avec Azure (Microsoft Entra ID)
- Fin de support pour la ou les extensions supplémentaires

ESYC : **E**xtended **S**ecurity **U**pdate **Y**ear

Failles / Bulletins / Advisories



Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de décembre, 57 vulnérabilités patchées dont

- 3 vulnérabilités de type 0-day :
  - [**CVE-2025-62221**] Elévation de privilèges, Pilote Cloud Files Mini Filter
    - Type « Use-After-Free »
    - Exploitée par les attaquants
    - Affecte Windows 10 et 11 & Windows Server 2022 et 2025
  - [**CVE-2025-64671**] Execution de code (en local), GitHub Copilot
    - Uniquement l'extension pour l'IDE JetBrains
    - Scénarios : commandes venant du serveur MCP ou de fichiers untrusted
  - [**CVE-2025-54100**] RCE, PowerShell
    - Cmdlet `Invoke-WebRequest`
    - Scénario : récupération du contenu d'une page Web comportant du script PS malveillant
    - Ajout d'un nouveau paramètre : `-UseBasicParsing` pour ne pas exécuter le code récupéré (+ avertissement)
- Hors vulnérabilités liées à Microsoft Edge

https://www.it-connect.fr/patch-tuesday-decembre-2025-microsoft-recapitulatif/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

Faille importante (sans CVE attribuée) dans Notepad++

- Auparavant, quelques signalements ont été faits liés au comportement de WinGUp
  - Il ne récupérait pas de MAJ de Notepad++ mais téléchargait à la place *%Temp%\AutoUpdater.exe*
  - Il effectuait une reconnaissance du système :
    - `cmd /c netstat -ano` : analyse des connexions réseau
    - `cmd /c systeminfo` : obtenir des informations système
    - `cmd /c tasklist` : lister les processus en cours
    - `cmd /c whoami` : identifier l'utilisateur actuel
  - Le fichier *a.txt* généré était envoyé vers temp.sh (= ça pue)
- Malvertising ? Enquête en cours
  - À savoir : le logiciel (légitime) interroge une URL pour vérifier la présence d'une nouvelle version
    - XML retourné en réponse
- La version 8.8.9 est sortie !
  - Le mécanisme de mise à jour vérifie maintenant la signature numérique (c'est pas trop tôt)

https://www.it-connect.fr/notepad-8-8-9-corrige-une-faille-importante-permettant-dinjecter-une-mise-a-jour-malveillante/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

NPM et sa bibliothèque jsPDF

CVE-2025-68428

- Possible de manipuler la fonction de génération du PDF
  - Peut entraîner une fuite de données
- Faiblesse si attaquant peut contrôler le premier argument transmis aux méthodes concernées (loadFile, addImage, html, addFont)
  - Si les chemins d'accès aux fichiers sont codés en dur ou depuis des sources fiables
    - → risque très réduit
- Patcher dans la version v4.0.0

https://www.it-connect.fr/faille-critique-jspdf-cve-2025-68428/

Example attack vector:

```
import { jsPDF } from "./dist/jspdf.node.js";

const doc = new jsPDF();

doc.addImage("./secret.txt", "JPEG", 0, 0, 10, 10);
doc.save("test.pdf"); // the generated PDF will contain the "secret.txt" file
```

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

Extraction de données sur MongoDB

CVE-2025-14847

- Problème avec la gestion de la bibliothèque zlib
  - Peut exposer des données : tokens, info personnelles, config internes, clés d'API…
- En plus :
  - Décompression réalisée **avant** l'authentification.. donc réalisable sans authentification
- + 85.000 instances vulnérables sur Internet
- Patch disponible pour les branches :
  - 8.2.3
  - 8.0.17
  - 7.0.28
  - 6.0.27
  - 5.0.32
  - 4.4.30

https://www.it-connect.fr/mongobleed-faille-cve-2025-14847-mongodb/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

4 failles corrigées sur Veeam

CVE-2025-55125
CVE-2025-59468
CVE-2025-59469
CVE-2025-59470

- Concernent la solution Veeam Backup & Replication
- 3 RCE et une écriture de fichiers en root
  - Besoin d'avoir au moins le rôle d'opérateur sur le système
- Concernent les versions de Veeam v13.X (12.X non concernées)
  - Patch sur la version v13.0.1.1071 disponible

https://www.it-connect.fr/veeam-backup-replication-4-failles-de-securite-janvier-2026/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

0-day sur RasMan

- Permet de faire crasher le service de Windows
  - Pas d'authentification requise
- Peut s'avérer critique en collaboration avec la CVE-2025-59230 (PrivEsc si service HS)
  - Patcher en octobre 2025
- Mini patch disponible par l'équipe d'ACROS Security
  - En attente du correctif de Microsoft

https://www.it-connect.fr/windows-une-nouvelle-faille-zero-day-dans-le-service-rasman-quels-sont-les-risques/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Piratage du ministère de l'Intérieur

- 13/12/2025 - Revendication sur BF d'une intrusion sur les systèmes du ministère de l'Intérieur
  - Intrusion détectée quelques jours auparavant, limitée aux services de messagerie
  - Conséquences ? Accès à des informations sensibles de plus de 16 millions de personnes
    - Notamment les antécédents judiciaires et des informations sur des personnes recherchées
  - Accès également revendiqués aux systèmes de la DGFIP et de la CNAV
- 17/12/2025 - Prises de paroles publiques par Laurent Nuñez
  - Accès identifié à des fichiers en utilisant des mots de passe échangés en clair via des mails
  - On ne parle pas d'un accès à plusieurs millions de données mais plutôt à plusieurs dizaines
- // - Interpellation d'un suspect en France
  - Melvin L. 22 ans, arrêté à Limoges, connu pour des faits similaires
  - Mis en examen pour « accès frauduleux [...] dans un STAD à caractère personnel [...] par l'Etat »

https://www.tribunal-de-paris.justice.fr/sites/default/files/2025-12/20251217CPCYBERMININT.pdf

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Les hôtels dans le viseur

- Campagne de phishing ciblant les hôtels
  - Usurpation de l'identité de Booking.com en prétextant une annulation de réservation
- Mail contient un lien vers un captcha faisant apparaître un faux BSoD
  - Contient des instructions : commandes PowerShell à exécuter
  - Télécharge un projet MSbuild qui sera exécuté par l'outil de Microsoft
    - Met en place des exclusions sur Defender, active une persistance et télécharge le DCRat
- Malware permettant d'exécuter des commandes, déployer des modules (mineurs de crypto) et un keylogger
- Si les permissions de l'utilisateur sont insuffisantes pour la compromission :
  - Passage en mode attaque psychologique avec du SPAM !

https://www.it-connect.fr/clickfix-avec-un-ecran-bleu-de-la-mort-et-phishing-booking-com-ces-pirates-ciblent-les-hotels/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

KMSAuto, le pirate arrêté

- Logiciel pirate pour Windows et Office
  - Version modifiée mise à disposition avec malware
- Modification de l'adresse crypto lors d'une transaction
  - 1.2 M€ ont été détourné, +3.000 victimes
- Opération réalisée par Interpol et extradition du pirate vers la Corée du Sud avec saisie des équipements

https://www.it-connect.fr/kmsauto-fin-de-partie-pour-le-pirate-qui-a-piege-28-millions-dutilisateurs-avec-un-malware/

Piratages, Malwares, spam, fraudes et DDoS
Panne

Teams ne répond plus

- Panne de Teams le 19 décembre à 14h30
- Impact sur l'ensemble des solutions Windows et mobiles, sur le territoire EU et en Europe
- Rétablissement à 15h30
- Pas d'information sur l'origine de la panne

https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-teams-is-down-and-messages-are-delayed/

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

Fuite de données chez NordVPN ?

- Mise en ligne d'un extrait d'un base de données de NordVPN
  - Contient des références de table API et des fichiers de config
  - Récupérer sur un serveur de développement Salesforce mal configuré
- Fuite de données réelle mais sur des données de PoC datant de 6 mois
  - Données fictives
- Aucun contrat n'a été signé avec le prestataire indique NordVPN

https://www.it-connect.fr/nordvpn-conteste-la-fuite-de-donnees-revendiquee-sur-breachforums-janvier-2026/

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

Contenu Musical de Spotify en libre accès

- Récupération de +300 To de données
  - Objectif : créer la plus grande bibliothèque ouverte de l'histoire de l'humanité
- Données accessibles via torrent

https://www.it-connect.fr/annas-archive-a-aspire-tout-le-catalogue-de-spotify-86-millions-de-fichiers-audio-voles/

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

Base de données, 340Go dans la nature

- Piratage du prestataire Axyon avec vol de données
  - Contient des données sensibles, d'architecture, de projets, de bases clients, administratives…
  - Concerne des clients importants : EDF, Eiffage, Bouygues, Engie, Renault, l'Armée de l'Air, la FFT et plusieurs entités publiques

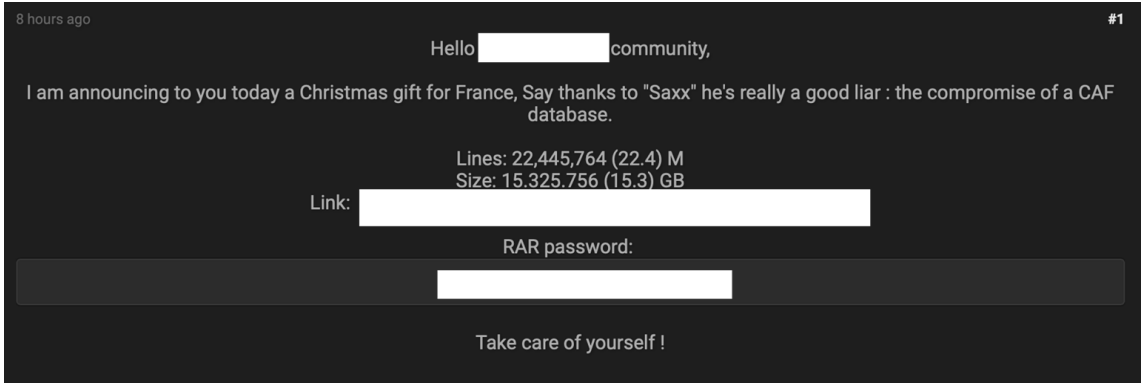
https://x.com/seblatombe/status/2007973233555829077

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

Fuite de données majeure liée au ministère des Sports

- Et non pas à la CAF !
  - Doute dû à échanges avec la CAF concernant le dispositif Pass'Sport
- Concerne 3.5 millions de foyers
  - Données remontant jusqu'à septembre 2024
  - Contient des informations sur les allocataires : identités, adresses postales / électroniques et n° de tél

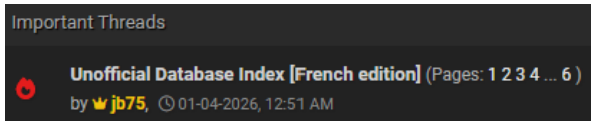
https://www.lesnumeriques.com/societe-numerique/exclusif-cyberattaque-massive-sur-la-caf-22-millions-de-victimes-dans-une-offensive-qui-frappe-l-etat-n248336.html



Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

Beaucoup, beaucoup.. de fuites de données concernant la France

- Un petit point sur toutes les fuites identifiées en décembre
  - Casino de Paris
  - Philarmonie de Paris
  - La quasi-totalité de toutes les Fédérations Françaises de Sport existantes
  - Easycash
  - Ecole de Management de Grenoble
  - L'université de Lille
  - PayTrip
  - HelloWork
  - Chronopost
  - PornHub
  - Fitness Park
  - Autosur
  - ANTS
  - UNSS
  - Et j'en passe..
- Lien utile pour s'y retrouver : https://bonjourlafuite.eu.org/
  - Même les cybercriminels s'aident entre-eux :



« Well, since France is currently a very leaky country, I decided to create a separate unofficial database index for this country. »

Piratages, Malwares, spam, fraudes et DDoS
Publication

Quand les smartphones « dévoilent » des personnels sensibles de l'État #LeMonde

- Un dataset commercial provenant d'un data broker a été utilisé pour l'enquête
  - > 16M d'identifiants publicitaires et 1Md de points GPS
  - Les données datent d'octobre 2024
- Ce que révèle l'enquête :
  - Des données publicitaires géolocalisées permettent de retrouver l'identité, le domicile et les habitudes de personnels très sensibles
    - Renseignement, protection de hautes personnalités, unités d'élite, bases nucléaires, défense, etc.
- « ID publicitaire » (propre à un téléphone) + OSINT = anonymat ❌
  - Facilite donc grandement l'espionnage
- Publication de l'ANSSI datant de novembre 2025 sur ce sujet :
  - https://cyber.gouv.fr/actualites/etat-de-la-menace-informatique-sur-les-equipements-mobiles/

https://www.lemonde.fr/pixels/article/2025/12/10/espions-policiers-ou-militaires-d-elite-francais-trahis-par-les-donnees-publicitaires-de-leurs-smartphones_6656694_4408996.html

Conférences

Conférences

N’oubliez pas :

- **JSSI**, 10 mars à Paris
  - Sujet : << **La Supply Chain, maillon faible de la Cyber** >>

https://www.ossir.org/conference/jssi-2026/

Encore 2 journée pour soumettre :

Sujets recherchés :

Cartographie et gouvernance de la chaîne de sous-traitance. Méthodes d'inventaire et d'évaluation des risques chez les fournisseurs et sous-traitants, modèles de compliance, suivi continu des tiers, agences de notation en cybersécurité.
Sécurisation du cycle de vie logiciel. Intégration de la sécurité dans les pipelines CI/CD, adoption et exploitation des SBOM (Software Bill of Materials), audits de dépendances et de composants open source.
Intégrité et fiabilité des composants matériels. Vérification des firmwares, détection de matériels compromis, bonnes pratiques d'audit et de contrôle qualité pour l'IoT industriel et l'OT.
Menaces émergentes et techniques d'attaque. Notamment compromission de la chaîne d'approvisionnement logicielle.
Stratégies de détection, réponse et résilience. Déploiement de solutions de threat intelligence, exercices de red teaming orientés chaîne d'approvisionnement, approches Zero Trust pour l'accès aux ressources tierces.
Études de cas et retours d'expérience. Présentations détaillées d'incidents récents, bilan des mesures correctives déployées, enseignements et recommandations pour renforcer la résilience.
Normes, référentiels et cadre réglementaire.

Et si le FIC 2026 vous intéresse, pensez à acheter vos billets (early bird = 60€) 🤑

Divers / Trolls velus

Divers / Trolls velus

Fin de l’activation de Windows par téléphone

- Mise hors ligne du serveur vocal Redmond
- Pas de mise à jour sur la page de support de Windows, indiquant que l’activation est toujours possible 😅
  - L’appel vocal renvoie vers un lien en ligne
- Obligation d’avoir un compte Microsoft aussi maintenant
  - Licences rattachées au compte
- Potentiel incident sur certains équipements Old Gen

https://www.01net.com/actualites/microsoft-supprime-lactivation-des-licences-de-windows-et-doffice-par-telephone.html

Divers / Trolls velus

Fake développeur chez Amazon

- Détection d'une fausse personne chez Amazon
  - Détecté par un délai de frappe de +100 ms (contre 10 ms normalement)
- Supposément basé au US, en réalité en Corée du Nord 😱
- Découverte d'une ferme d'ordinateurs pour l'espionnage simulant une présence local 😱😱
  - Femme complice pour gérait le lieu
- Pas la première tentative
  - +1.800 tentatives d'infiltration par des agents nord-coréens déjouait depuis avril 2024
  - Hausse de 27% de ces tentatives d'un trimestre à l'autre

https://www.it-connect.fr/comment-amazon-a-repere-un-faux-developpeur-grace-a-un-lag-de-110-ms/

Divers / Trolls velus

La fin de MDT #Windows

- Microsoft Deployment Toolkit - Solution On-Premise développée par Microsoft
  - Permettait de masteriser et de déployer Windows à travers le réseau local
- Sa version 8456 (dernière version) a été supprimée du site de Microsoft
  - Sa version 8450 (version antérieure) est toujours disponible sur le site
  - Ou sinon il faut passer sur des backups de la 8456 disponible un peu partout
    - Ex. : https://github.com/mdtkit/Microsoft-Deployment-Toolkit/releases/tag/8456
- Sans grande surprise…
  - L'outil ne recevait plus de mises à jour de fonctionnalités
  - Le support devenait quasi inexistant
- Une disparition progressive de « l'Imaging » pour laisser place au « Modern Management »
  - En d'autres mots : passer sur le Cloud (Microsoft Intune, Windows Autopilot, etc.)
- Il reste tout de même des alternatives :
  - Ex. : WAPT (Tranquil IT), DeployR de chez (2Pint), XOAP (RIS AG)

https://www.it-connect.fr/mdt-plus-disponible-au-telechargement-rip-janvier-2026/

FIN

Prochaine réunion ?

- RDV le **mardi 10 février 2026**

Accéder aux différents supports ?

Replays

Slides

https://www.youtube.com/@OSSIR

https://www.ossir.org/support-des-presentations/