



**IT COPS**  
Safe Computing



Séminaire : Cybersécurité : une guerre toujours gagnable ?

# LE GUICHET UNIQUE DE LA CYBERSECURITÉ



# QUI SOMMES NOUS ?

IT COPS est une startup filiale de 2 sociétés établies depuis plus de 30 ans dans le secteur des technologies de l'information. Les équipes fondatrices sont rompues depuis de nombreuses années d'une part aux solutions de cybersécurité avec les acteurs majeurs du secteur, et d'autre part à la création et au développement de réseaux de partenariat.

Les fondateurs ont choisi de mettre en commun l'expérience respective de leurs sociétés pour construire la première offre intégrée de solutions de cybersécurité en guichet unique à destination exclusive des canaux de distribution et services IT & Télécom.



**HERVE LAYER**

40 ans de passion dans les nouvelles technologies. Dirigeant de l'ESN LAYER. En charge de l'innovation, de l'amélioration et de la sécurisation du capital numérique des entreprises.

***Président***



**PHILIPPE TINTIGNAC**

Serial entrepreneur depuis 40 ans. Fondateur du réseau de distribution Euralliance's. En charge du développement et de l'animation du réseau et des partenariats.

***Directeur Général***



“Il n'existe que deux types d'entreprises :  
celles qui ont été piratées et celles qui le seront”

Robert Mueller – Directeur du FBI 2001-2013





# LES DANGERS



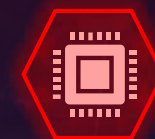
## **Violations de données :**

Accès non autorisé entraînant l'exposition d'informations confidentielles.



## **Intrusions de malware :**

logiciels détournés conçus pour perturber les systèmes informatiques.



## **Attaques par phishing:**

Tactiques trompeuses visant à inciter les utilisateurs à révéler des données sensibles.



## **Attaques DDoS :**

Submerger un système avec du trafic afin de perturber son fonctionnement normal.





# CONTEXTE DE LA CYBERSECURITÉ

## Nature des attaques en 2025

Selon les signalements des PME :

- **43 % phishing** (+19 points vs 2024)
- **18 % failles de sécurité exploitées**
- **11 % navigation sur sites vérolés**

## Tendances clés 2025

- Le nombre d'attaques **massives** (> 1 million de personnes touchées) a **doublé** entre 2023 et 2024... et continue en 2025.
- L'écosystème cybercriminel utilise massivement :
  - **Ransomware-as-a-service**
  - **Phishing automatisé**
  - **Deepfakes vocaux / vidéos**

## STATISTIQUES CYBERSÉCURITÉ FRANCE – 2023-2025

### 2023



**54%** des entreprises ont subi une cyberattaque

**49%** des attaques ont atteint leur objectif

### 2024



**67%** des entreprises ont été touchées

**1er** vecteur d'attaque : le phishing



**+15%** d'incidents de sécurité signalés par l'ANSSI

### 2025



**43%** des TPE/PME attaquées par hameçonnage

Les violations massives de données continuent d'augmenter



# ATTAQUES EXTERNALISÉES



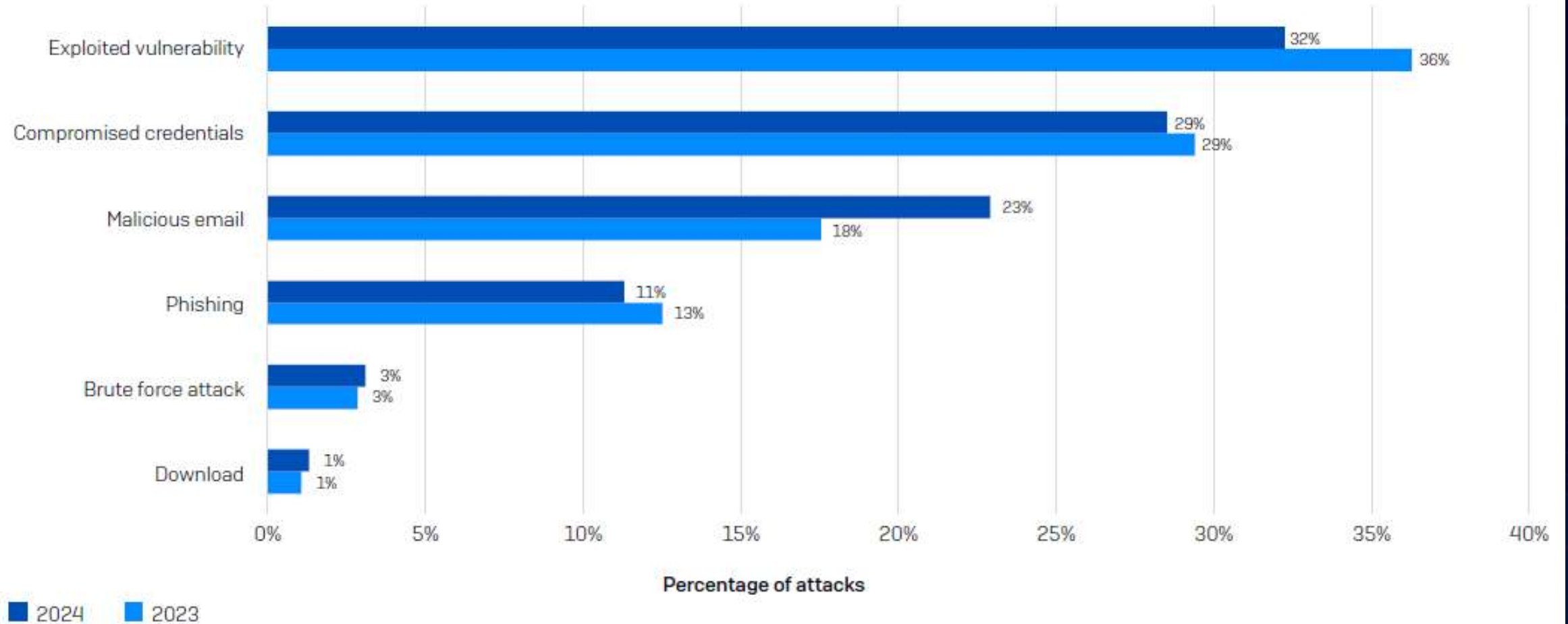
Aujourd'hui, les Pirates se comportent comme des Corsaires.

Ils reçoivent une lettre de mission de leurs gouvernements qui les autorisent à pirater les pays avec lesquels ils sont en conflit.

Ils vous attaquent sans quitter leurs domiciles.



# LES DIFFÉRENTS CANAUX D'ATTAQUES



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=2,974 organizations hit by ransomware.

Source SOPHOS



# Risque d'une Architecture simplifiée

**385 000**

entreprises paralysées  
par une cyberattaque

**30 000**

entreprises victimes  
d'incendie

**10x**

plus de risque d'être  
victime d'une cyberattaque  
que d'un incendie



- Le risque d'être attaqué par un Ransomware est 10 X supérieur à celui d'avoir un incendie



# NOTRE MISSION



Proposer aux prestataires IT & Télécom une offre pour leurs clients sans investissement de leur part en ressources humaines.



Disposer d'une offre complète et intégrée.



Garantir le meilleur niveau de protection disponible sur le marché.



Utilisation d'une IA Européenne et éthique



# AVANTAGES DU GUICHET UNIQUE

## SIMPLIFICATION DES PROCESSUS :

En regroupant toutes les solutions sur une plateforme unifiée IT COPS propose une facilité de déploiement inégalée pour ses partenaires

## INTEGRATION DES SOLUTIONS :

Les solutions des différents éditeurs sont intégrées à la plateforme sans qu'il soit nécessaire de se connecter sur différents outils

## REDUCTION DES DELAIS :

Chaque demande d'activation est traitée instantanément sans qu'il soit nécessaire de s'adresser aux éditeurs ou à leurs grossistes individuellement

## AMELIORATION DES MARGES :

Les accords éditeurs engagés par IT COPS permettent à ses partenaires de bénéficier des meilleurs tarifs sans engagement de volume





# L'OFFRE IT COPS

Une panoplie complète pour une protection maximale.

## Antivirus et Analyse comportementale

Disponible pour toutes plateformes  
en conformité NIS2

## Inventaire , Assets Management, Patches et Chiffrement

Pour inventorier, gérer,  
automatiser et préserver  
les actifs de l'Entreprise  
même en cas de vol



## Sauvegardes Immuables

Les sauvegardes sont  
externalisées, immuable et  
inaltérable dans le respect  
du standard HDS et 27001

## Assurance

Spécifique pour la cybersécurité  
incluant les risques humains et le  
ransomware





# Ce que comprend l'ASSURANCE CYBER

En partenariat avec DATTAK

L'assurance Dattak couvre beaucoup plus que les assurances cyber classiques et notamment :

- Hotline d'urgence 24/7
- Intervention de différents experts
- Responsabilité civile cyber
- Responsabilité civile média
- Frais de monitoring et surveillance
- Frais de reconstitution du SI et des données
- Frais d'enquêtes et sanctions administratives
- Pertes d'exploitation
- Paiement de la rançon





# LES OFFRES IT COPS

| Postes et serveurs                 | Essentiel | Premium |
|------------------------------------|-----------|---------|
| Antivirus et Anti-malware Nexgen   | ✓         | ✓       |
| Protection contre les ransomwares  | ✓         | ✓       |
| Protection Navigation Web          | ✓         | ✓       |
| Gestion automatisée des correctifs | ✓         | ✓       |
| Contrôle et suivi des mises à jour | ✓         | ✓       |
| Isolation réseau                   | ✓         | ✓       |
| Analyse comportementale            | ✓         | ✓       |
| Prise de contrôle à distance       | ✓         | ✓       |
| Déploiement automatisable          | ✓         | ✓       |
| Chiffrement                        | ✓         | ✓       |
| Sauvegarde Cloud HDS               |           | ✓       |
| Sauvegarde S3                      |           | ✓       |
| Immuabilité                        |           | ✓       |





# PROTEGEZ VOTRE TENANT OFFICE 365

- ▶ Office 365 est LA suite d'applications bureautique cloud, avec plus de **345 Millions d'utilisateurs**.
- ▶ Créé par Microsoft, il vous permet de bénéficier d'une messagerie professionnelle, d'un drive conséquent ainsi que d'une multitude d'applications collaboratives.
- ▶ Toutes vos données sont alors hébergées sur des datacenters géo-redondants.
- ▶ La géo-redondance est le fait de pouvoir accéder à vos données, peu importe votre localisation.
- ▶ Malheureusement, Microsoft ne se charge pas de la sécurité de vos données dans les offres basiques, ils vous fournissent seulement un accès à ces dernières.
- ▶ C'est l'une des premières sources d'attaques pour voler de la donnée et détruire le SI de l'extérieur





# FONCTIONNALITÉS ESSENTIELLES

- ▶ Blocage des Malwares contenus dans vos mails
- ▶ Analyse avancée des menaces via Machine Learning et Sandboxing
- ▶ Détection des comptes compromis en faisant une analyse continue des bases de données revendues.
- ▶ Analyse des URL de vos mails
- ▶ Détection et blocage des Ransomware et Malware pouvant être contenus dans votre OneDrive et votre Sharepoint.
- ▶ Analyse des règles de messagerie



# LES OFFRES IT COPS

| Microsoft O365   | Essentiel | Premium |
|--|-----------|---------|
| Antivirus et anti-malware NextGen (NGAV)                                       | ✓         | ✓       |
| Analyse des contenus malveillants non détectées par O365 (Threat Intelligence) | ✓         | ✓       |
| Protection avancée de vos emails, des données SharePoint et de votre OneDrive  | ✓         | ✓       |
| Gestion des comptes compromis  | ✓         | ✓       |
| Protection des URLs  | ✓         | ✓       |
| Protection contre le Phishing et les attaques ciblées                          | ✓         | ✓       |
| Protection anti ransomwares  | ✓         | ✓       |
| Sécurisation et Audit de votre tenant O365                                     | ✓         | ✓       |
| Sauvegarde immuable et inaltérable   |           | ✓       |
| Sauvegarde Cloud HDS 27001 S3  |           | ✓       |





# POURQUOI CHOISIR IT COPS



## **La disponibilité des meilleures pratiques**

Issues de nombreuses années d'expertise,



## **La disponibilité immédiate de toute commande**

Inutile d'attendre plusieurs jours pour recevoir des clés pour effectuer les installations clients,



## **La souplesse du modèle**

Notamment avec la possibilité d'ajout d'éléments pour un client en cours de contrat, même annuel ou tri-annuel,



## **Le support technique et la formation**

IT COPS apporte à ses partenaires tout le support nécessaire à la résolution d'incidents. Lors de la mise en œuvre du partenariat une formation est distillée à chaque partenaire pour lui donner une totale autonomie dans son déploiement. Les outils mis à disposition du partenaire sont disponibles en marque blanche,







**IT COPS**  
Safe Computing

## Démonstration plateforme IT COPS



# Accès Partenaire




 Tableau de bord

 Devis assurance


 Fiche de suivi assurance

 Parc Informatique

 Réservations

 Clients

 Factures


 Revendeurs

 Partenaires

 Utilisateurs

Admin

 Configuration

 Durées D'engagement

 Volumes De Données

 Eléments

 Logs

 Systèmes D'exploitation

 Niveaux De Protection

## Tableau de bord Portail IT Cops



Bonjour  
Hervé Layer

 Déconnexion

### Statistiques

Un rapide aperçu de vos statistiques

Partenaires

3

Revendeurs

3

Clients

54

Sites

65

Parc informatique

754

Equipements actifs Essentiel

658

Equipements actifs Premium

15

### Nombre d'équipements actifs par élément

| Eléments              | Essentiel | Premium |
|-----------------------|-----------|---------|
| PC / Laptop           | 496       | 9       |
| Serveur / VM / NAS    | 118       | 6       |
| Connecteur Office 365 | 161       | 0       |
| Mobile                | 35        | 0       |

# Créer un Client / Devis

[illegible]



# Transformer en devis en commande

Réservations > Liste

## Réservations

Créer

Rechercher

| Scope                              |           |          |                     |  |
|------------------------------------|-----------|----------|---------------------|--|
| Client                             | Référence | Nb sites | Mis à jour          |  |
| Mairie de Chablis                  |           | 1        | 03/02/2025 13:21:50 | <a href="#">Activer</a> <a href="#">Modifier</a> <a href="#">Supprimer</a> |
| Garage Jeannin                     | BC1215    | 1        | 04/02/2025 13:00:34 | <a href="#">Activer</a> <a href="#">Modifier</a> <a href="#">Supprimer</a> |
| Affichage de 1 à 2 sur 2 résultats |           |          |                     |  |
|                                    |           | par page | 10                  |  |

### Activation de service(s)

Veuillez sélectionner ci-dessous les services réservés à activer.

Activer

1 élément sélectionné

Désélectionner tout



Matériel - 1 an  
Siège social





# Installer un site : EPP/EDR (NGAV)



Parc Informatique > Modifier

## Installer

**Antivirus** Supervision Sauvegarde

### Information sur le statut

Veillez suivre les étapes ci-dessous pour effectuer la configuration.



Télécharger



Configuration

### Clé d'activation

Voici la clé d'activation pour cet équipement:

**XT9L-876Y-CRTM-B8FX-7JVT**

Après installation sur la machine du client, vous pourrez retrouver directement sur la [console WithSecure](#) en vous connectant avec vos identifiants reçus par mail.

Précédent



# Installer un site : Supervision & RMM



Parc Informatique > Modifier

## Installer

Antivirus

**Supervision**

Sauvegarde

### Information sur le statut

Veuillez suivre les étapes ci-dessous pour effectuer la configuration.

01

Télécharger

02

Configuration

### Connection à la plateforme N-able

Vous pouvez vous connecter sur la [plateforme N-able](#) avec les identifiants que vous avez reçus par mail.



# Installer un site : Sauvegarde immuable



Parc Informatique > Modifier

## Installer

Antivirus Supervision **Sauvegarde**

### Informations sur le statut

La configuration de sauvegarde n'a pas été configurée. Veuillez suivre les étapes ci-dessous pour effectuer la configuration.

01 Télécharger

02 Configuration

03 Installation

### Informations sur l'état de génération du fichier

La génération du fichier a été effectuée avec succès *(Le fichier sera conservé uniquement pendant 7 jours, puis supprimé automatiquement, mais vous pouvez toujours en générer un nouveau.)* . [Téléchargez-le ici](#)

### Informations sur la prochaine étape

Une fois le fichier téléchargé, passez à l'étape suivante en cliquant sur le bouton Suivant.

Vous avez des problèmes avec le fichier téléchargé ? **Important**

Suivant



# Installer un site : Sauvegarde immuable



[Antivirus](#) [Supervision](#) [Sauvegarde](#)

### Informations sur le statut

La configuration de sauvegarde n'a pas été configurée. Veuillez suivre les étapes ci-dessous pour effectuer la configuration.

✓ Télécharger

02 Configuration

03 Installation

Cette étape consiste à installer et configurer l'agent de gestion téléchargé lors de l'étape précédente. Trois onglets (Windows, Linux et macOS) sont disponibles ci-dessous. Veuillez sélectionner l'onglet correspondant au système d'exploitation de votre machine, puis suivre les étapes indiquées.

Windows

Linux

MacOs

Pour installer un agent de gestion sur un ordinateur fonctionnant sous le système d'exploitation Linux :

Déploiement des agents de gestion Linux

Pour configurer un agent de gestion :

Configuration de l'agent de gestion

Précédent

Suivant

# Installer un site : Sauvegarde immuable



Parc Informatique > Modifier

## Installer

Antivirus Supervision **Sauvegarde**

### Informations sur le statut

La configuration de sauvegarde n'a pas été configurée. Veuillez suivre les étapes ci-dessous pour effectuer la configuration.



Télécharger



Configuration



Installation

### Terminer l'installation

Avant de terminer l'installation, assurez-vous que la configuration de l'agent dans les étapes précédentes a été effectuée et que le statut de l'agent est bien *connected*.

Terminer

Précédent



# Management : Supervision & RMM



DEVICE DETAILS

N-ABLE N-CENTRAL

SYSTEM TIME  
1:10 PM

Pc Philippe

LAUNCH CHAT

REMOTE CONTROL

ADD TASK

AUDIT TRAIL

CPU: Intel(R) Core(TM) Ultra 7 165L

DISK: 476.94 GB

MEMORY: 16.00 GB

OS VERSION: Microsoft Windows 11 Professionnel

CUSTOMER NAME: Internet Point

LAST CHECK-IN: Tue, Feb 04, 2025 01:18 PM CET

SYSTEM UPTIME: 0 Days 0 Hours 42 Minutes

DEVICE CLASS: Laptop - Windows

NETWORKING: Pc Philippe (192.168.1.37)

LOGGED IN USER: LAPTOP\_PHILIPPE\ntine

FEATURES: PRO

CPU USAGE  
2.10 GHz

7%

MEMORY USAGE  
10.24 GB / 15.58 GB

65%

Overview

Tools

Monitoring

Asset

Notes

Settings

Remote Control Settings

Reports

ACTIVE ISSUES

| Service   | Transition Time   |
|-----------|-------------------|
| Disk - G: | 2025-Feb-04 11:01 |

REFRESH NOW

ON

Refresh in: 10 minutes

Total: 1

CPU UTILIZATION BY TOP 5 PROCESSES

SYSTEM INFORMATION

|                                 |                                |
|---------------------------------|--------------------------------|
| LAST DISCOVERY:                 | Mon, Feb 03, 2025 04:50 PM CET |
| LAST SYSTEM WARRANTY DISCOVERY: | Thu, Jan 23, 2025 04:54 PM CET |
| SYSTEM NAME:                    | Pc Philippe                    |

MEMORY UTILIZATION BY TOP 5 PROCESSES

# Management : Supervision & RMM

IT COPS



ACTIVE ISSUES



N-ABLE N-CENTRAL



SYSTEM TIME  
12:56 PM

Views

- Active Issues
- All Devices
- Job Status
- NetPath
- Topology Maps

Dashboards

- Device - ESX Hosts
- Device - Network Devices
- Device - Printers
- Device - Servers
- Device - Workstations
- Manage - Antivirus
- Manage - Patch Status
- Manage Dashboards

Actions

- Add/Import Devices
- Add Customer

ACKNOWLEDGE NOTIFICATIONS

EDIT DEVICES

DELETE SERVICES

SERVICE MONITORING

ADD NOTE

ADD TASK

EXPORT

Filter by No Filter in all Sites with all services

| <input type="checkbox"/> Customer                  | Site | Remote Control | Tools | Device/Probe      | Device Class     | Serial Number  |
|--|------|----------------|-------|-------------------|------------------|----------------|
| <input type="checkbox"/> Code moi un mouton        | --   |                |       | ludovic-executive | Servers - Linux  | --             |
| <input checked="" type="checkbox"/> Internet Point | --   |                |       | Pc Philippe       | Laptop - Windows | BK33M8G24303M4 |
| <input type="checkbox"/> Test 4                    | --   |                |       |                   | Laptop - Windows | --             |
| <input type="checkbox"/> Test 4                    | --   |                |       |                   | Laptop - Windows | --             |

- Services
- Processes
- Registry
- Applications
- Startup Applications
- Printers
- Command Prompt
- File System
- Task Execution

Quickstart

REFRESH NOW

ON

Refresh in: 5 minutes

Selected: 1 Total: 4



# Management : Antivirus EPP / EDR (NGAV)





Événements de sécurité

+

Générer la synthèse

...

i

Afficher

No HOSPITAL

+

Le symbole des étoiles représente le contenu généré par le programme LLM.

i

Vous pouvez exporter les événements de sécurité dans MS Excel. Consultez le guide dans la communauté

Sélectionner un champ

▼

Équivaut à

▼

Sélectionner une valeur

▼

Appliquer

Annuler

Supprimer tous les filtres

73577 événements

↺

|   | Heure                                       | Gravité       | Source  | Entreprise | Cible | Description   | Reconnu par | Menu           |
|---|---|---------------|---|------------|-------|---|-------------|----------------|
|   | 3 févr. 2025, 10:26:51                      | Falsification | falsification   |            |       | La protection contre la falsification a protégé "SYSTEM32\USER32.dll" de "taskmgr.exe".   | Aucun(e)    | <div>...</div> |
| ▼ | il y a 36 minutes<br>3 févr. 2025, 10:26:41 | Attention     | EDR   |            |       | L'incident BCD à risque modéré portant l'id 155963364-33791 a été mis à jour  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 36 minutes<br>3 févr. 2025, 10:26:11 | Attention     | EDR   |            |       | L'incident BCD à risque modéré portant l'id 178082710-274038 a été mis à jour   | Aucun(e)    | <div>...</div> |
| ▼ | il y a 57 minutes<br>3 févr. 2025, 10:05:53 | Attention     | EDR   |            |       | L'incident BCD à risque modéré portant l'id 137106609-87979 a été mis à jour  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 58 minutes<br>3 févr. 2025, 10:04:16 | Information   | DataGuard   |            |       | DataGuard a détecté un accès à "import_gls.txt".  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:59:55    | Information   | DataGuard   |            |       | DataGuard a détecté un accès à "SINED_20250203095949.pdf".  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:59:00    | Information   | DataGuard   |            |       | DataGuard a détecté un accès à "SINED_20250203095854.pdf".  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:53:50    | Information   | DataGuard   |            |       | DataGuard a détecté un accès à "SINED_20250203095344.pdf".  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:51:19    | Attention     | Contrôle des appareils  |            |       | Une tentative de modifier le fichier sur l'appareil suivant a été bloquée : JetFlash Transcend 4GB USB Device   | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:51:03    | Information   | Événements système  |            |       | An account failed to log on.. ID de l'événement : 4625, source de l'événement : Microsoft-Windows-Security-Auditing.  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:49:29    | Information   | Événements système  |            |       | An account failed to log on.. ID de l'événement : 4625, source de l'événement : Microsoft-Windows-Security-Auditing.  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:46:35    | Information   | Événements système  |            |       | An account failed to log on.. ID de l'événement : 4625, source de l'événement : Microsoft-Windows-Security-Auditing.  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:46:32    | Information   | Événements système  |            |       | An account failed to log on.. ID de l'événement : 4625, source de l'événement : Microsoft-Windows-Security-Auditing.  | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:41:13    | Attention     | Navigation basée sur la réputation<br>Protection de la navigation |            |       | La page Web « hxxps://app.notifizone.com » a été bloquée en raison d'une réputation jugée dangereuse.   | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:35:08    | Information   | Contrôle des applications   |            |       | Le contrôle des applications a signalé un événement de type démarrage de l'application associé à Microsoft® Windows® Operating System sur la base de la règle Surveillance commandes CMD. | Aucun(e)    | <div>...</div> |
| ▼ | il y a 1 heure<br>3 févr. 2025, 09:35:08    | Information   | Contrôle des applications   |            |       | Le contrôle des applications a signalé un événement de type démarrage de l'application associé à Microsoft® Windows® Operating System sur la base de la règle Surveillance commandes CMD. | Aucun(e)    | <div>...</div> |

Le portail IT COPS nous permet d'avoir une supervision 24/7 sur tous les événements de sécurité au sein des vos clients, et de gérer en conséquence les différentes alertes.



Broad Context Detections

Broad Context Detections Recherche d'événements

< Retour à la liste des détections

Broad Context Detection 4 de 7198 < >

Grave 100 ID: 178082710-220957, Catégorie: Mouvement latéral ⓘ

Créée: 17.05.2024 12:00:01 UTC+03  
Modifiée: 10.06.2024 13:00:12 UTC+03

État ⓘ  
Fermé: Confirmé

Récapitulatif Arborescence des processus Chronologie Analyse Commentaires Journal

Informations et supérieur (p... ⌵ ⌵ ⌵

Détails du processus Rechercher

30 processus ajoutés Tout désélectionner

Actions rapides

Status ⓘ  
New

Quick actions

Analyze with Luminen

Isolate affected device

Scan device

Collect forensics package

Enumerate tasks

Enumerate processes

More Response actions ⓘ available

Summary Process Tree Timeline Analysis Device Details

Key detection

PIEGPA-241121

Process details Search

piegpa-241121  
8 processes added Unselect all

net.exe ⓘ Unselect

SHA1 900f1d634bb698

Execution start 14.01.202

Execution end 14.01.202

Show file metadata

Show reports

Kill process

Retrieve files

Delete files

SHA1 aedf41adc7a2d1b9bec091ece86a6fcc1e63e1d2

Lorsqu'un évènement de sécurité présente un risque grave pour l'entreprise, notre moteur EDR isole automatiquement l'appareil afin de protéger le reste des appareils.

# UTILISER L'INTELLIGENCE ARTIFICIELLE DANS UN CADRE ÉTHIQUE



**WI Elements™** European Operations  
WithElements Inc. v

Events / Broad Context Detections

## Broad Context Detections

Back to Detections list

Broad Context Detection 9 of 16

Severe 100 ID: 183720731-1037, Category: Lateral movement

New

Quick actions

- Generate BCD Summary
- Isolate affected device
- Scan device
- Collect forensics package

More response actions

Elevate to WithSecure

Company

WithElements Inc.

Affected devices (2)

- Desktop01.withelements.co...
- ADServer.withelements.com

Show all

Identical detections (0)

Similar detections (0)

Summary Process Tree Analysis Comments Log

Info and above (default)

**Executive Summary:**

On 2024-05-20T07:05:22Z/2024-05-20T07:05:50Z, the user 'WITHELEMENTS\michael.smith' on the 'Desktop01.withelements.com' host was observed engaging in a series of suspicious activities. This included the execution of the Microsoft Word application (winword.exe) launching child processes, such as PowerShell (powershell.exe), which were used to download files from external URLs, decode and execute payloads, and create scheduled tasks for persistence (T1059.001 - Command and Scripting Interpreter: PowerShell, T1053 - Scheduled Task/Job, T1204 - User Execution). Additionally, the CertUtil utility was used to download and decode files, potentially containing malicious payloads (T1105 - Ingress Tool Transfer, T1140 - Deobfuscate/Decode Files or Information). On 2024-05-20T07:06:00Z, the PsExec tool was used to execute PowerShell commands remotely on the 'ADServer.withelements.com' host, further indicating lateral movement and potential compromise (T1569.002 - System Services: Service Execution, T1021.002 - Remote Services: SMB/Windows Admin Shares).

**Main Events:**

- 2024-05-20T07:05:22Z/2024-05-20T07:05:50Z: Microsoft Word (winword.exe) launched child processes, including PowerShell (powershell.exe), to download files, decode payloads, and create scheduled tasks for persistence
- 2024-05-20T07:05:40Z/2024-05-20T07:05:44Z: CertUtil utility used to download and decode potentially malicious files
- 2024-05-20T07:06:00Z: PsExec tool used to execute PowerShell commands remotely on 'ADServer.withelements.com'

Close



## Services cloud

Ajouter une connexion

Vue Liste

Vue Abonnement

| <input type="checkbox"/> | Nom | Exchange | SharePoint | OneDrive <span>?</span> | Teams | Stratégie |
|--------------------------|-----|----------|------------|-------------------------|-------|-----------|
| <input type="checkbox"/> |     | 4        | 1          | 4                       | 1     |           |

|                          |                             |                              |         |  |  |                    |                        |
|--------------------------|-----------------------------|------------------------------|---------|--|--|--------------------|------------------------|
| <input type="checkbox"/> | Contenu malveillant : 1 URL | ✉ Votre Don (déduit des i... | MODÉRÉE | il y a un mois<br>déc. 29, 2024 08:57:41 |  | Boîte de réception | En quarantaine         |
| <input type="checkbox"/> | Contenu malveillant : 1 URL | ✉ Votre Don (déduit des i... | MODÉRÉE | il y a un mois<br>déc. 29, 2024 08:14:51 |  | Boîte de réception | En quarantaine         |
| <input type="checkbox"/> | Compte compromis            | ✉ commercial@domaine-...     | FAIBLE  | il y a 2 mois<br>déc. 11, 2024 15:53:20  |  | –                  | Notifier l'utilisateur |
| <input type="checkbox"/> | Compte compromis            | ✉ info@domaine-du-char...    | FAIBLE  | il y a 2 mois<br>déc. 11, 2024 15:53:20  |  | –                  | Notifier l'utilisateur |

## Quarantaine

Taille totale : 1.9 MB

Saisissez une valeur, puis appuyez sur Entrée.

Actualiser

Effacer tout

Tout

9 élément(s) affiché(s)

| <input type="checkbox"/> | État | ID de quarantaine                    | Service cloud | Date et heure          | Motif          | Action                |
|--------------------------|------|--------------------------------------|---------------|------------------------|----------------|-----------------------|
| <input type="checkbox"/> | ✉    | 53c47a8a-60fa-41e8-b006-16ca1ef43da9 | Exchange      | 03.02.2025<br>09:16:43 | URL dangereuse | Afficher la détection |
| <input type="checkbox"/> | ✉    | 833e99d3-529b-4612-ac6b-0f8d05e04cd4 | Exchange      | 27.01.2025<br>17:58:50 | URL suspecte   | Afficher la détection |
| <input type="checkbox"/> | ✉    | 5cc4bd26-67c7-49cf-9c4a-775949c036ed | Exchange      | 06.01.2025<br>08:24:17 | URL dangereuse | Afficher la détection |

L'Elements Collaboration Protection (ECP) protège un domaine Microsoft 365, couvrant Exchange, SharePoint, OneDrive et Teams.

# Management :



- Monitoring
  - Overview
  - Active Alarms
  - RPO & SLA
  - Resources & Billing
- Analytics
  - Session States
  - TOPs
  - Trends
- Management
  - Backup Jobs
  - Protected Data
- Clients
  - Companies
  - Resellers
  - Discovery

Discovered Computers

Hostname

Backup Policy: Assign...

☒ Agent Sta...

Selected: All 1 item

☒ Healthy

## Discovered Computers Backup Agents

Hostname



Backup Policy

Backup Policy: Assign...

Backup Agent

Activation

ITCOPSAdministrateur   
Administrator



Configuration

☒ Agent Sta... Company

Selected: All 1 items

☒ Healthy LAYER Co

Set Location

Patch

Upgrade

Restart

Reboot Remote Computer

Install CBT Driver

Uninstall CBT Driver

Delete

Download Logs



Filter (None)

Export to...

| Guest OS      | Available ... | Patch Level |  |
|---------------|---------------|-------------|--|
| Microsoft ... | Up-to-...     | -           |  |



# Restauration : Sauvegarde immuable



Browse

Search

Restore List

Audit

Monitoring

Overview

Active Alarms

RPO & SLA

Resources & B

Analytics

Session States

TOPs

Trends

Management

Backup Jobs

Protected Dat

## Browse [Silent]

Job:

Global Immuable Po...

Restore Point:

03/02/2025 09:52

▼ Root

▼ C:

▶ \$GetCurrent

▶ \$Recycle.Bin

▶ Cache\_Backup

▶ Config.Msi

▶ Intel

▶ IT\_COPS\_BKP\_Cacl

▶ OneDriveTemp

File or Folder

Add to Restore List

Remove from



Name

Type

Path

Selected: 0 of 2



GfxCPLBatchFiles

Folder

C:\Intel



IntelOptaneData

Folder

C:\Intel

# QUESTIONS / REPONSES



[info@itcops.fr](mailto:info@itcops.fr)



**+33 1 89 16 33 77**



[www.itcops.fr](http://www.itcops.fr)



**Pour aller plus loin :**

Contactez-nous pour plus de précisions sur  
notre programme de partenariat.



[info@itcops.fr](mailto:info@itcops.fr)



**+33 1 89 16 33 77**



[www.itcops.fr](http://www.itcops.fr)

---

---

---