tv

Le live !

Un webinar by koesio

WithSecure

# Un EDR européen opéré par Koesio Corporate IT en mode service managé


WITH secure

koesio

# Intervenants

## Julien MACHIN

Channel Manager France
Withsecure

## Jean-Philippe LASSERRE

Responsable Avant-Vente
Koesio Corporate IT

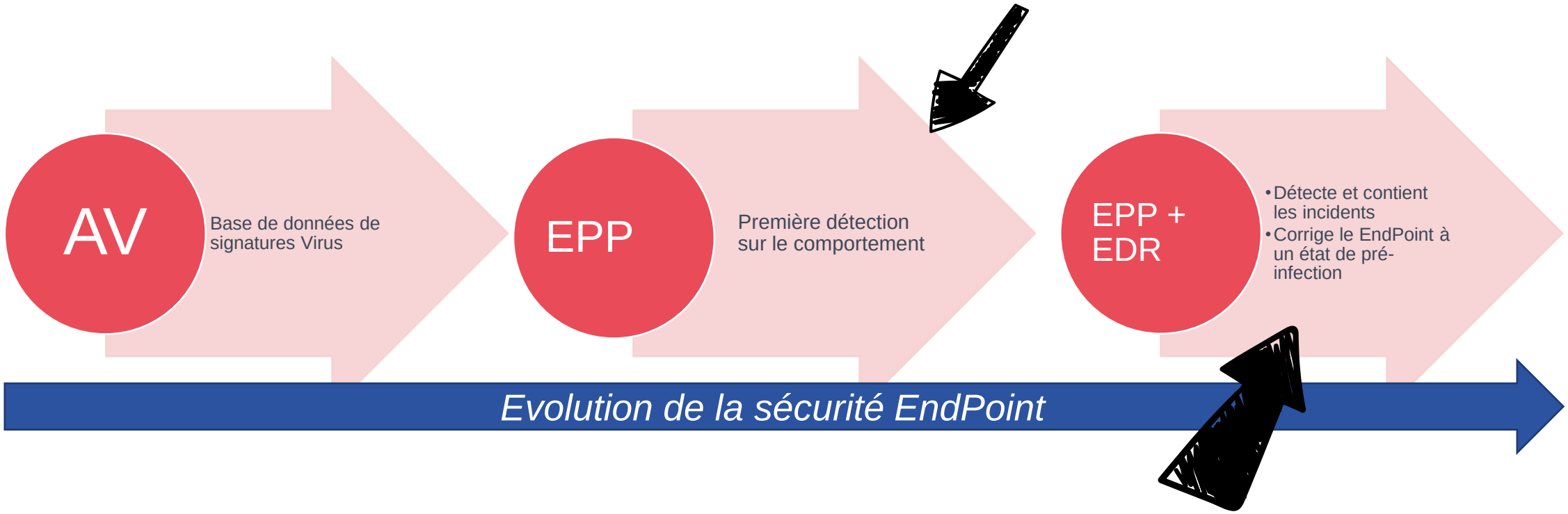
1

# L’EDR - Rappels

# EPP vs EDR – Définitions

| EPP – Définition | EDR – Définition |
| --- | --- |
| Un agent **EPP**, pour **E**ndPoint **P**rotection **P**latform, est une solution de sécurité des points terminaux issue du monde des **antivirus de nouvelle génération**.<br><br>Un tel agent est capable de prévenir de nombreuses attaques (comme par exemple les attaques par logiciels basés sur des fichiers ou via des activités malveillantes) et possède des fonctionnalités spécifiques contre de nombreux problèmes de sécurité tels que le phishing, l'exploitation 0-day, les attaques de réseau. | Un agent **EDR**, pour **E**ndPoint **D**etection and **R**esponse, identifie certains schémas de fonctionnement et détecte les anomalies.<br><br>Il collecte des données télémétriques, comportementales issues des points terminaux, pour les envoyer ensuite vers une base de données centralisée pour corrélation et analyse.<br>Il s'appuie sur l'intelligence artificielle (IA).<br><br>Grâce à son apprentissage automatique intégrée et une intelligence artificielle avancée, il peut identifier les comportements anormaux et les traiter. |

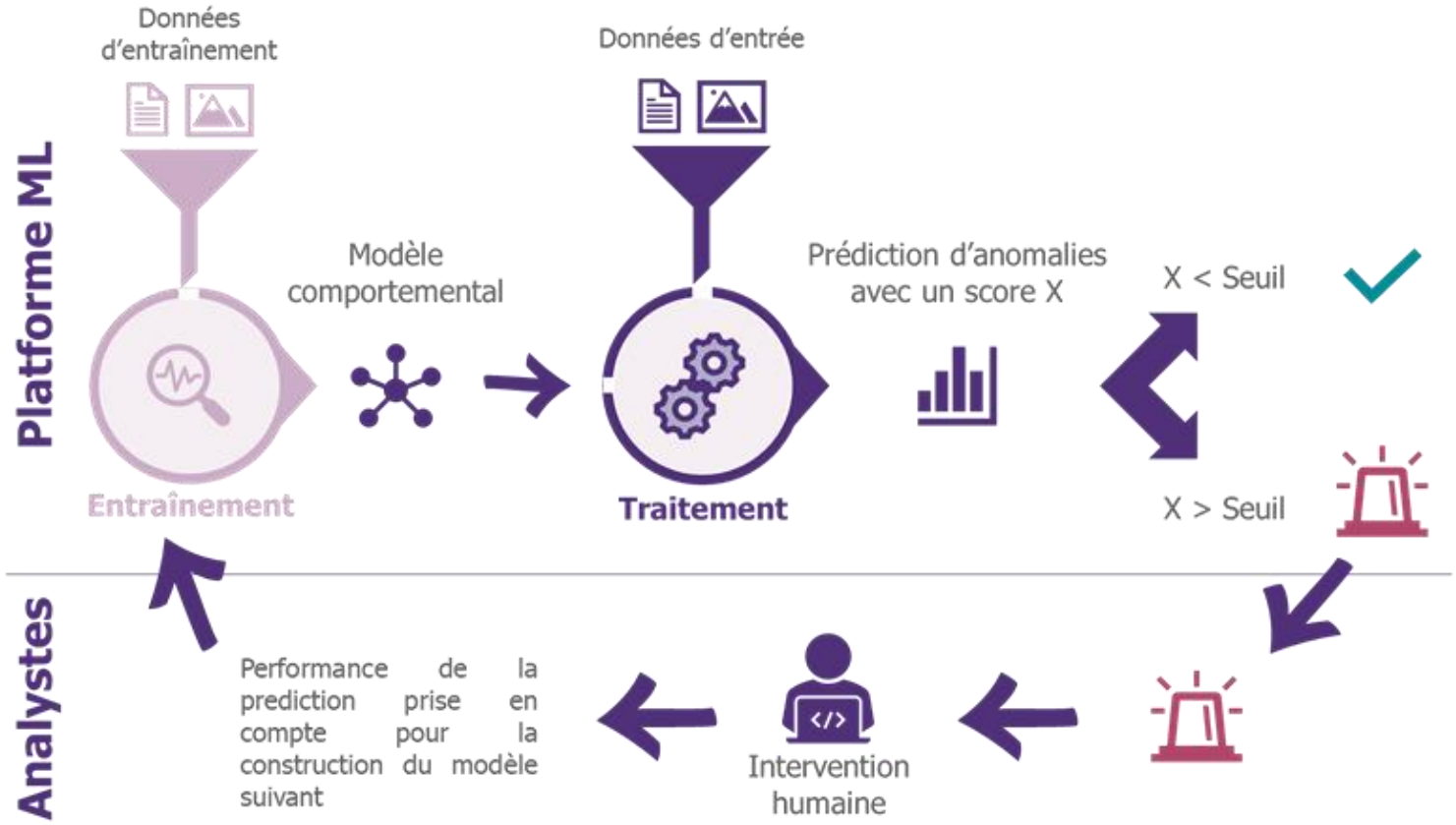
# **EPP vs EDR –** Evolution de la sécurité EndPoint



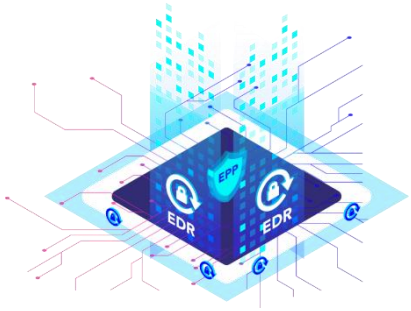

- ***AV*** *: AntiVirus*
- ***EPP*** *: EndPoint Protection*
- ***EDR*** *: EndPoint detection and Response*

# L’EDR en détail

***KOESIO Endpoint Detection and Response (EDR)*** *offre une visibilité complète sur tous les terminaux de l’entreprise et fournit des défenses supérieures, en automatisant les tâches de routine et en permettant à l'analyste de rechercher, de hiérarchiser, d'examiner et de neutraliser rapidement les menaces complexes ainsi que les attaques.*



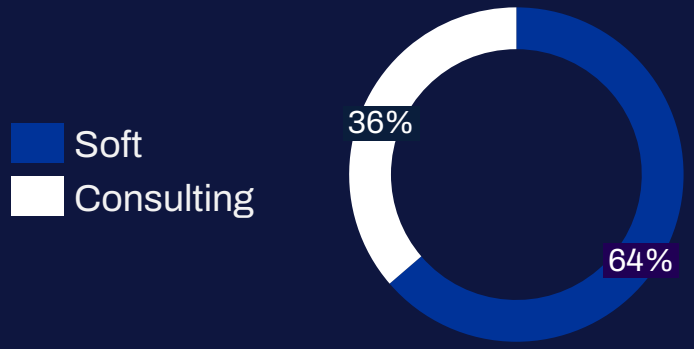

*KOESIO EDR utilise un **agent unique** qui peut être géré à partir d'une plateforme de gestion basée dans le cloud (SaaS) et à partir d'une console hors ligne dans les environnements isolés*



2

# La solution EDR de WithSecure

# WE ARE W / T H
secure




**1988**
**+ de 30 ans**
d'expertise

**1 300 employés**

koesio W / T H secure

**30**
**Pays**

**Protection**
**&**
**confidentialité**

koesio WITH secure

## 5 a 10 000 users

## Endpoint & cloud specialist

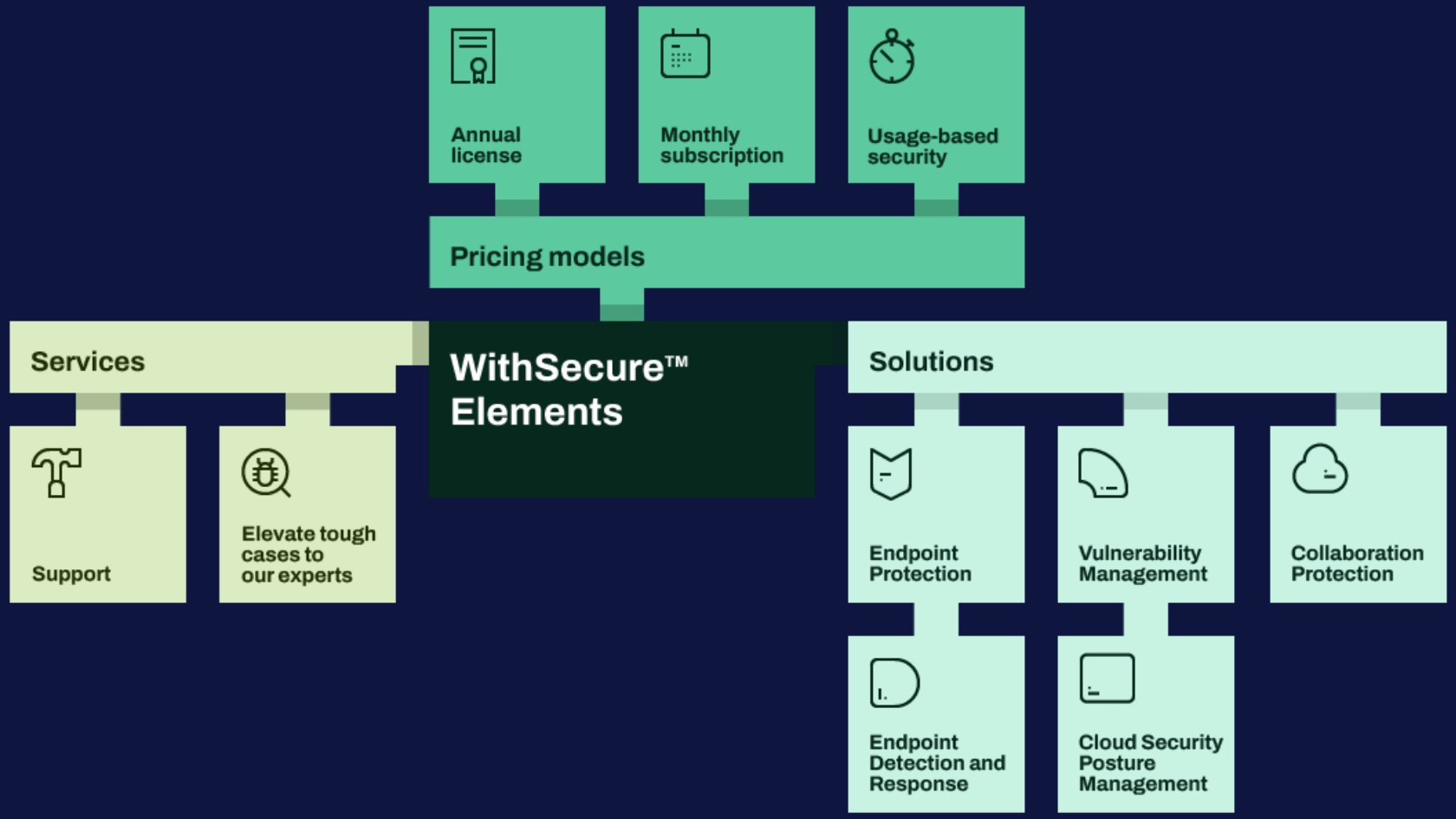
## La co-sécurité

Face aux défis de la cybersécurité, agir seul est sans effet.

WITH secure

koesio WITH secure

# WithSecure™ Elements




koesio WITH secure

Computers

Windows, Mac, Linux

Server

Windows, Linux

Email

Microsoft Outlook

Cloud collaboration apps

Microsoft Teams, SharePoint, OneDrive

Networks

Vulnerability scans

## WithSecure™ Elements™

Single agent

Unified data is analyzed with global threat intelligence

One Security Center

koesio

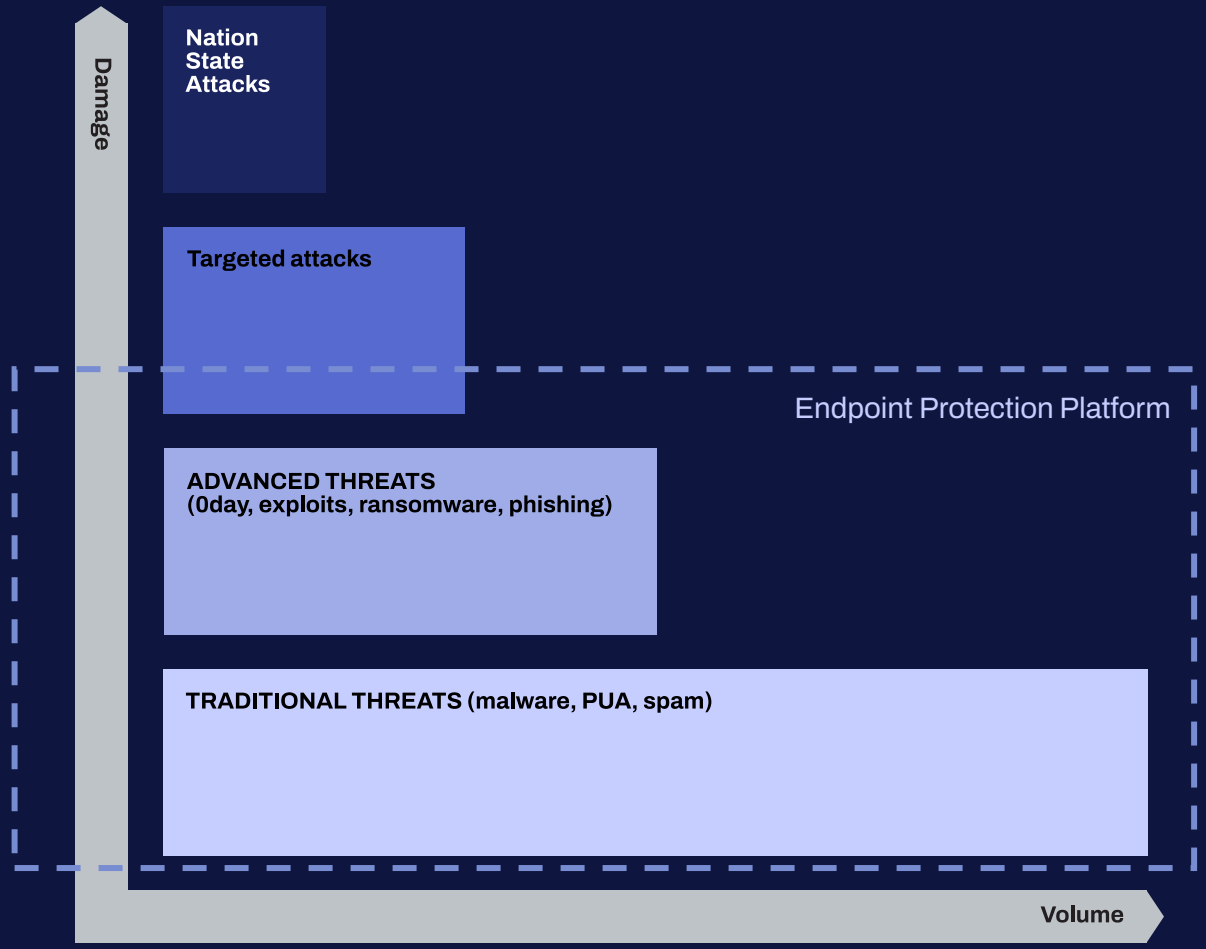
WITH secure

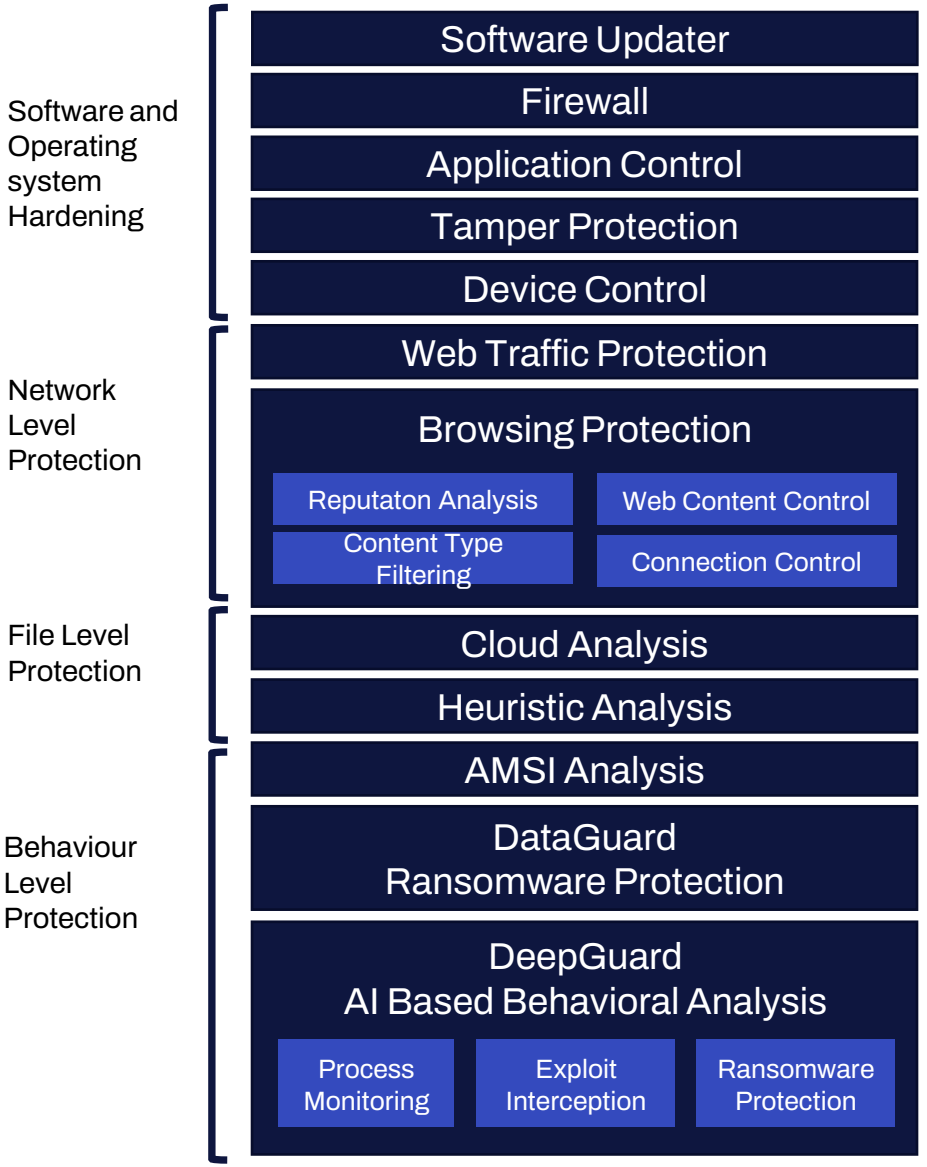
# Malwares

## Posture sécurité

koesio WITH secure

# Faire face à la masse




koesio

- Accueil
- ENDPOINT PROTECTION
  - Tableau de bord
  - Appareils
  - Mises à jour logicielles
  - Rapports
  - Abonnements
  - Profils
  - État de la sécurité (PILOTE)
  - Téléchargements
  - Assistance
  - Comptes
  - Événements de sécurité
- ENDPOINT DETECTION AND RESPONSE
- VULNERABILITY MANAGEMENT
- COLLABORATION PROTECTION
- Gestion - Collaboration Protection
- CLOUD SECURITY POSTURE MANAGEMENT
- MANAGEMENT


# Tableau de bord

## Problèmes

| Type d'éléments | Gravité | Appareils concernés |
|---|---|---|
| **Analyse en temps réel désactivée**<br>Vérifiez que l'analyse en temps réel est activée sur le profil. Si ce n'est pas le cas, activez le paramètre. Verrouillez-le afin que les utilisateurs ne puissent pas le désactiver. Vérifiez 15 appareils<br>L'analyse en temps réel a été désactivée sur l'appareil. Cela signifie qu'elle peut avoir été désactivée sur le profil, par un utilisateur ou que le logiciel a rencontré un bogue. Assurez-vous que l'analyse en temps réel est activée sur le profil et que les fonctions sont verrouillées afin que les utilisateurs ne puissent pas les désactiver. Redémarrez l'ordinateur si le portail indique que cela est nécessaire. | Critique | 15 |
| **Mises à jour logicielles critiques manquantes**<br>Utilisez Software Updater pour appliquer les mises à jour critiques. Utilisez « Tâches automatisées » dans le profil pour automatiser l'installation des mises à jour logicielles. Vérifiez 8 appareils | Critique | 8 |
| **Problème lors de l'analyse en temps réel**<br>Vérifiez la version du client. Assurez-vous que le lecteur système de l'appareil contient suffisamment d'espace disque disponible (plus de 5 Go). Redémarrez l'appareil. Vérifiez 3 appareils | Critique | 3 |
| **Exclusions dangereuses**<br>Vérifiez et gérez les exclusions dans le profil. Assurez-vous qu'il ne contient aucune exclusion dangereuse. Vérifiez 1 appareils | Critique | 1 |
| **Définitions de programme malveillant obsolètes**<br>Envoyer la mise à jour complète de l'état à l'appareil. Démarrer l'appareil. Vérifiez 1 appareils | Critique | 1 |
| **Appareils avec des incidents EDR graves ouverts**<br>Résoudre les incidents sur les appareils. Vérifiez 1 appareils | Critique | 1 |
| **Fin de vie des clients Windows**<br>Mettez à jour le logiciel client. Si des produits en fin de vie (EOL) sont utilisés, remplacez-les par des produits actuels (sidegrade). Vérifiez 22 appareils | Important | 22 |
| **Il manque des mises à jour logicielles importantes**<br>Utilisez Software Updater pour appliquer les mises à jour importantes. Utilisez « Tâches automatisées » dans le profil pour automatiser l'installation des mises à jour logicielles. Vérifiez 10 appareils | Important | 10 |
| **Pare-feu désactivé par une stratégie de groupe**<br>Assurez-vous que la stratégie de groupe est bien destinée à contrôler le pare-feu. Si c'est le cas, il n'est pas nécessaire de faire quoi que ce soit. Vérifiez 7 appareils | Important | 7 |
| **Appareils avec des incidents EDR importants ouverts**<br>Résoudre les incidents sur les appareils. Vérifiez 6 appareils | Important | 6 |
| **Appareil en attente de redémarrage**<br>Assurez-vous que les appareils sont redémarrés ou utilisez « Redémarrer l'appareil » sur la page Appareils. Vérifiez 4 appareils | Important | 4 |

Endpoint Protection / État de la sécurité (PILOTE)

Accueil
ENDPOINT PROTECTION
Tableau de bord
Appareils
Mises à jour logicielles
Rapports
Abonnements
Profils
État de la sécurité (PILOTE)
Téléchargements
Assistance
Comptes
Événements de sécurité
ENDPOINT DETECTION AND RESPONSE
VULNERABILITY MANAGEMENT
COLLABORATION PROTECTION
Gestion - Collaboration Protection
CLOUD SECURITY POSTURE MANAGEMENT
MANAGEMENT

L'état de la sécurité est une nouvelle fonctionnalité qui prend en charge un nor

# État de la sécurité (PILOTE)

Sélectionner un champ | Équivaut à | Sélectionner une valeur | Appliquer

Recommandations de sécurité

Conforme : 1  Non conforme : 6

| Recommandation de sécurité |
|---|
| La longueur minimale du mot de passe n'est pas définie ou est inférieure à 8 caractères. |
| Le chiffrement du lecteur système est désactivé. |
| Le seuil de verrouillage du compte n'est pas configuré. |
| Le protocole RDP est activé et le seuil de verrouillage du compte n'est pas configuré. |
| Plus de 10 % des stations de travail ont été dernièrement connectées par un utilisateur administrateur. |
| Système d'exploitation en fin de cycle de vie |
| La protection de l'intégrité du système est désactivée. |

## La longueur minimale du mot de passe n'est pas définie ou est inférieure à 8 caractères.

### Description

Ce paramètre détermine la longueur minimale du mot de passe qu'un utilisateur peut définir pour lui-même. Les valeurs recommandées par Microsoft sont de 8 à 14 caractères et le paramètre est défini via la stratégie de groupe à l'emplacement suivant : Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

. La longueur minimale du mot de passe est souvent définie en même temps que les exigences de complexité. Si les exigences de complexité sont activées, une longueur minimale de mot de passe plus courte peut être suffisante.
Les exigences de complexité des mots de passe sont configurées via la stratégie de groupe à l'emplacement suivant : Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

. Pour plus d'informations, reportez-vous à la documentation Microsoft pour :

Longueur minimale du mot de passe | Le mot de passe doit respecter des exigences de complexité | Stratégie de mot de passe

### Risque potentiel

Si cette valeur est indéfinie ou égale à 0, l'utilisateur n'a pas besoin de définir de mot de passe.
Une valeur trop courte peut être facile à deviner ou à forcer, surtout si l'exigence de complexité du mot de passe n'est pas activée.

Fermer

Endpoint Protection / Rapports

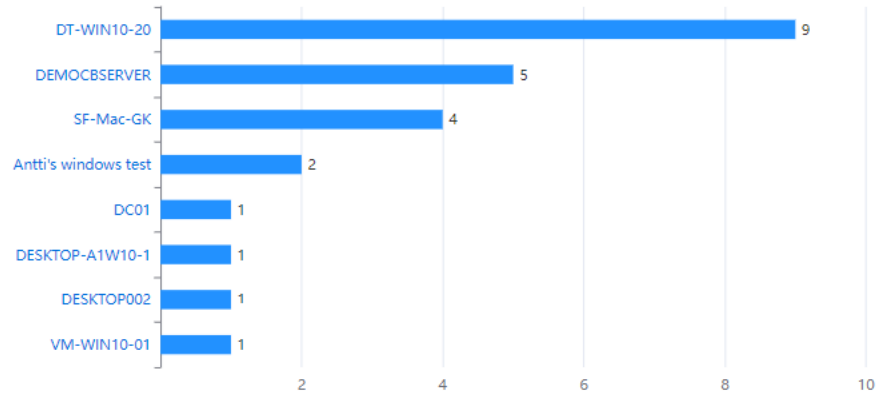
Accueil
ENDPOINT PROTECTION
Tableau de bord
Appareils
Mises à jour logicielles
Rapports
Abonnements
Profils
État de la sécurité (PILOTE)
Téléchargements
Assistance
Comptes
Événements de sécurité
ENDPOINT DETECTION AND RESPONSE
VULNERABILITY MANAGEMENT
COLLABORATION PROTECTION
Gestion - Collaboration Protection
CLOUD SECURITY POSTURE MANAGEMENT
MANAGEMENT

# Rapports

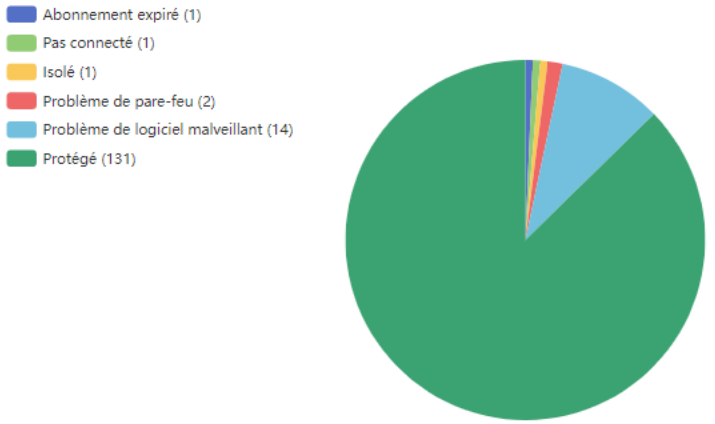
Mon rapport | Appareils | Événements de sécurité | Mises à jour logicielles | Journal d'audit

## TOP Endpoints

30 derniers jours

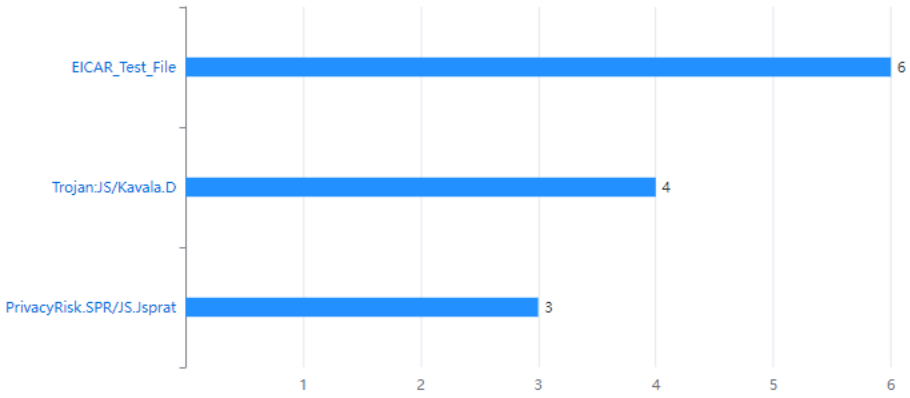



## Etat protection

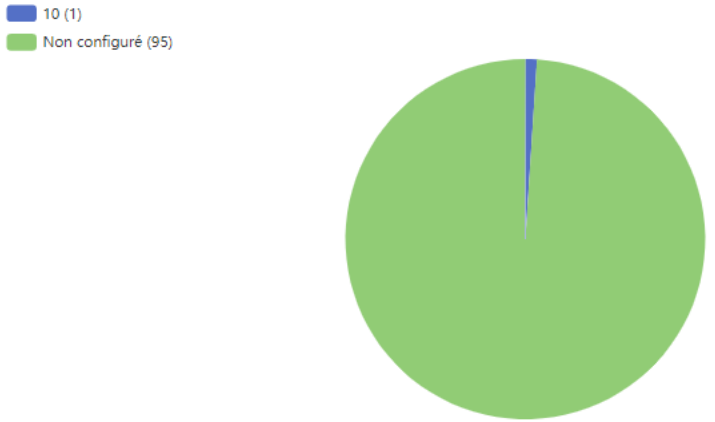



## Infections

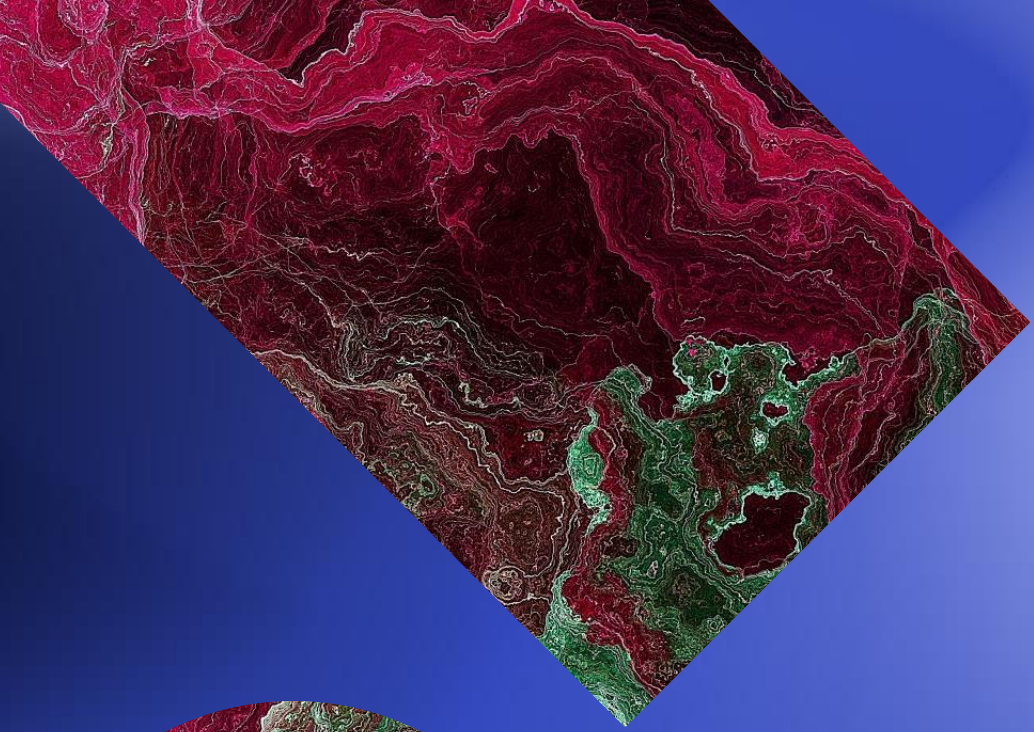
30 derniers jours

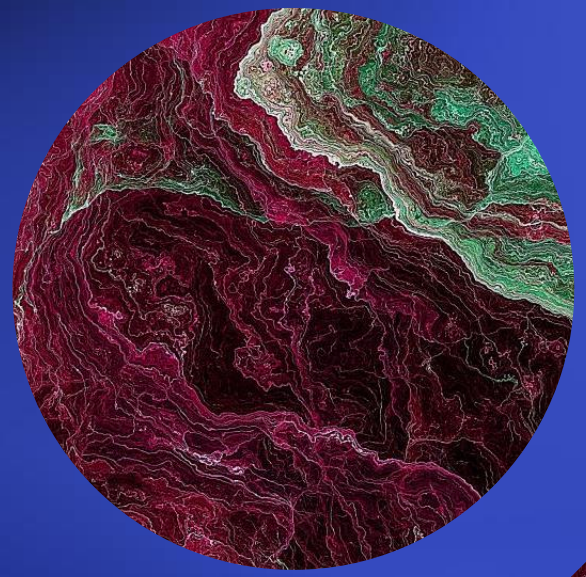


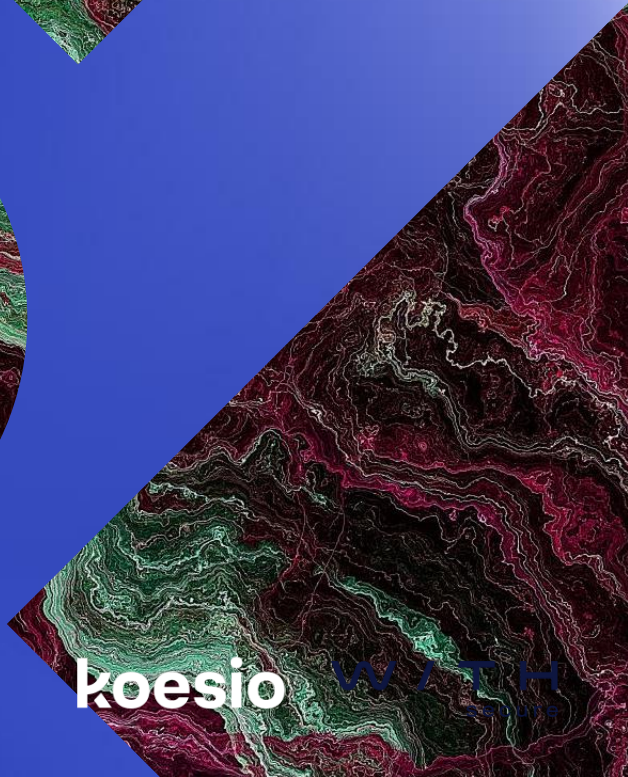

## Seuil de verrouillage de compte



# Des attaques de plus en plus avancées







# Attaques avancées


Attaque par la supply chain

3CX

solarwinds

CCLEANER

Kaseya

koesio

WITH secure

# Attaques avancées


## Attaque par la supply chain

3CX

solarwinds

CCLEANER

Kaseya

## Hands on keyboard

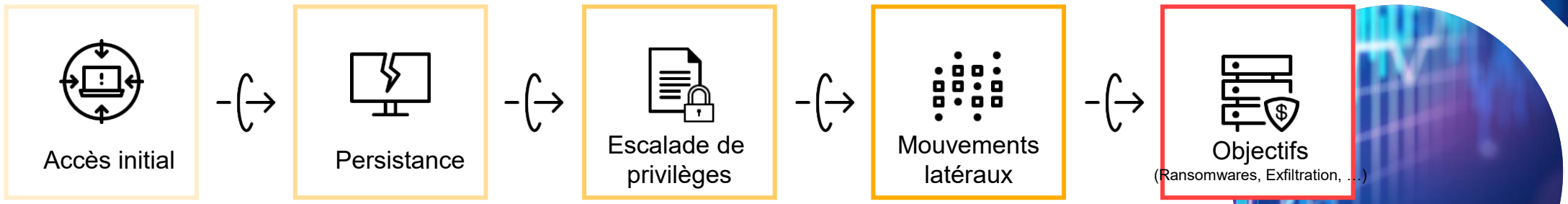
- BlackCat
- Black Basta
- Royal
- Hive
- Lockbit 3.0
- Phobos
- BianLian
- Play Ransomware

koesio WITH secure

# Evaluer l'ampleur de l'attaque

- Qualifier le niveau de l'incident
  - Concerne une machine, un utilisateurs, plusieurs, la totalité ?
  - Est ce que ça touche une activité de l'organisation, plusieurs, toutes ?
  - Est ce que ça touche le coeur de l'activité?
  - Est ce que des données sensibles / personnelles sont concernées ?
  - Quel est l'avancement de l'attaque ?

- Cette analyse déclenchera l'activation d'une cellule de crise




koesio WITH secure

# Endiguer

## Contenir et gagner du temps

### Les bons réflexes

- Priorité au backup !
- Consigner toutes les activités
- Préserver les preuves
  - Ne pas éteindre les machines
  - Déconnecter du réseau (logiciellement si possible)
  - Etendre la collecte de logs
  - Attention aux logs rotatifs
  - Stocker les preuves
- Isoler rapidement même s'il s'agit d'un isolement total

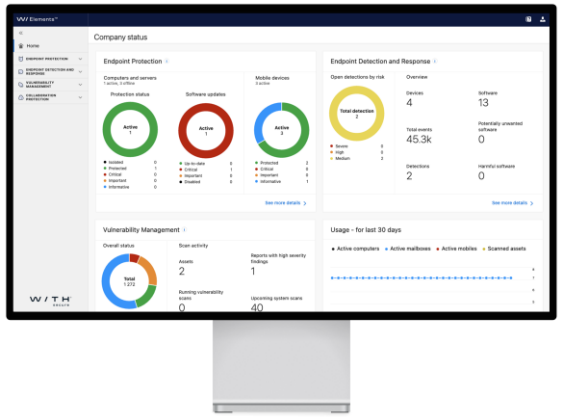
### A éviter !

- La précipitation :
  - Restaurer les sauvegardes
  - Faire des actions de réponse
- Lancer des outils tierces (AV concurrents, nettoyeurs, ...)
- S'ouvrir à des services externes (Gmail, WhatsApp, ...)

koesio WITH secure

# Contenir

- Comment isoler des machines rapidement? Et si le controleur de domaine est compromis ?
  - Trop d'organisations ont encore une approche purement périmétrique des flux réseaux
  - Une fois dans l'environnement, l'attaquant n'aura aucune difficulté à se déplacer dans le réseau
- **Elements EPP** dispose de nombreuses briques préventives dont la gestion du pare feu




**Centrally Managed Firewall***

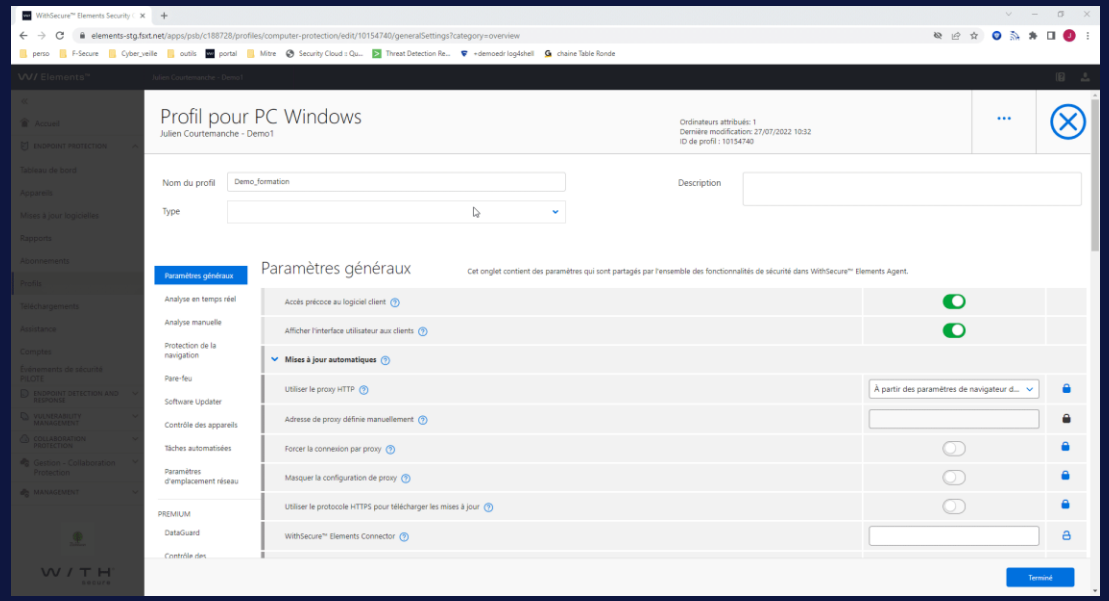
**Patch Management**

**Application Control***

**Device Control***

**Dataguard***

**Advanced Web Protection**




koesio W/TH secure

# Les outils de réponse et remédiation

## La suite WithSecure Elements

- Delete Files
- Delete Registry
- Delete Scheduled
- Delete Services
- Install updates
- Block network traffic
- Block application behaviour
- Block devices

# DETECTION AND RESPONSE EN ACTION

## YOUR INFRASTRUCTURE

Workstations Laptops Servers Swarm Intelligence

## EVENTS

## REAL-TIME BEHAVIORAL ANALYSIS WITHSECURE EDR BACKEND

Expert Insights

Global Threat Intel

Data enrichment & correlation

AI analytics

Data analytics

Broad Context Detections

WITH secure

## DETECTION

## ELEVATE TO WITHSECURE

## REMEDIATION

Delete Services

Delete scheduled tasks

Delete Files, Folders

Delete Registry keys

Scan Malware

Inform users

## CONTAINMENT

Isolate hosts

Kill processes

Control applications

## INVESTIGATION

Retrieve process lists

Retrieve files, folders

Retrieve logs, tasks

Memory dump

Event Search

Map network connections

Your own IT team

OR

koesio

WITH secure

3

# Les services managés de Koesio CIT sur EDR

# **Le SOC Koesio** – Sa raison d'être

Le **S**ecurity **O**peration **C**enter de Koesio a pour but de concentrer les compétences techniques autour de la sécurité du Système d'Information des clients sous contrats de services

- Protections **périmétriques** (FW, anti-spam)
- Configuration des **réseaux** (Selon les bonnes pratiques de séparation vLAN)
- Protection des **périphériques** (Serveurs, postes de travail)
  - EDR EPP
  - Sauvegardes

# EDR – Identification des criticités

## Aucun risque : Note de 1 à 35

- Pas d'action nécessaire
- Informations communiquées au client via l'accès aux consoles EDR et au reporting mensuel

## Risque faible : Note de 36 à 65 sur 100

- Code couleur : **Gris**
- Aucune activité inhabituelle notable
- Informations communiquées au client via l'accès aux consoles EDR et au reporting mensuel

## Risque modéré : Note de 66 à 75 sur 100

- Code couleur : **Jaune**
- Risque accru de cyberactivités malveillantes sans répercussions significatives notables
- Informations communiquées au client via l'accès aux consoles EDR et au reporting mensuel

## Risque élevé : Note de 76 à 90

- Code couleur : **Orange**
- Risque important de cyberactivités malveillantes ou l'incident potentiel peut occasionner des dégâts considérables dans l'environnement client
- Ouverture d'un ticket dans l'outil ITSM et, en option, **conseil à la remédiation ou assistance à la remédiation**

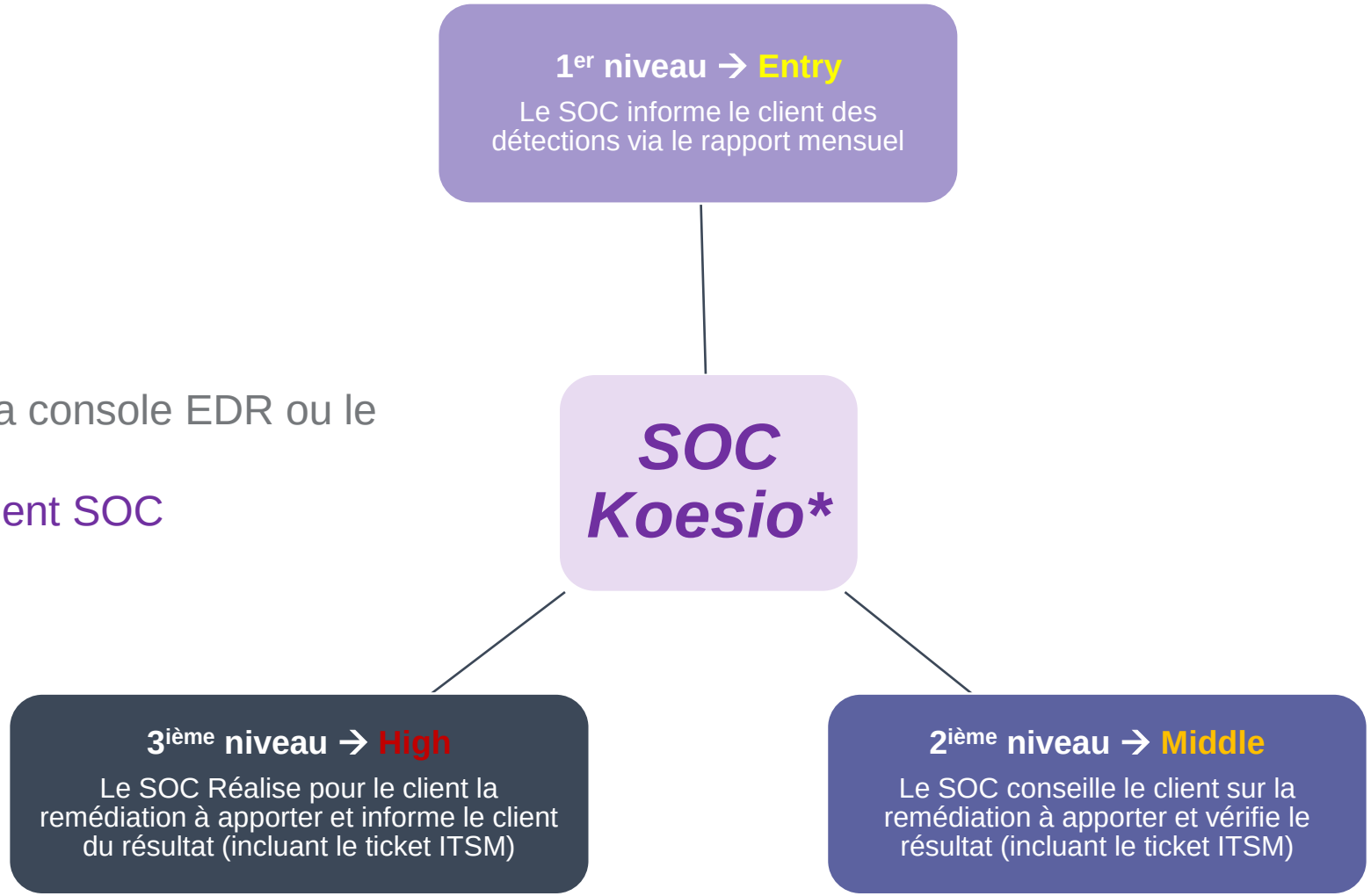
## Risque grave : Note de 91 à 100

- Code couleur : **Rouge**
- Risque grave de cyberactivités malveillantes ou l'incident potentiel peut compromettre des hôtes stratégiques dans l'environnement client
- Ouverture d'un ticket dans l'outil ITSM et, en option, **conseil à la remédiation ou assistance à la remédiation**

# EDR – Les niveaux d'interventions du SOC

**A partir de quelle criticité ?**

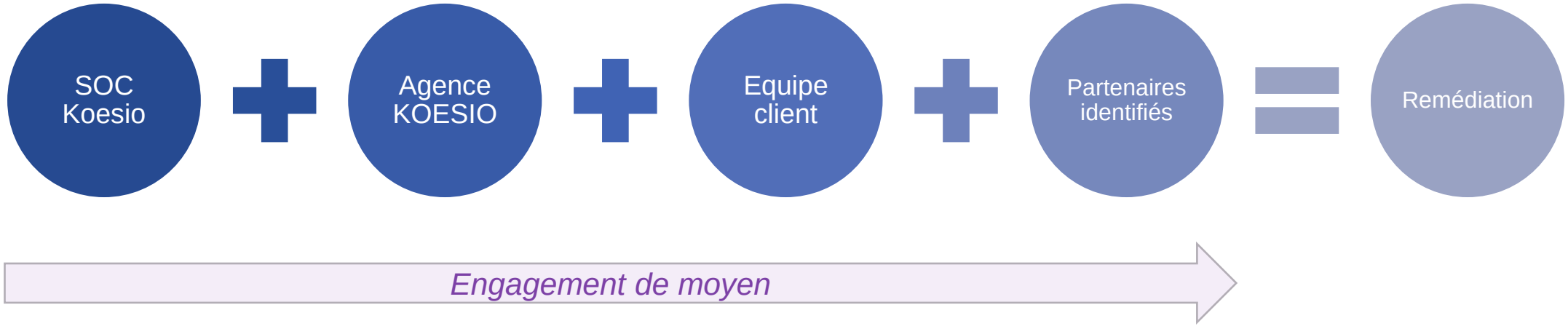
- **De 1 à 75** : **Information** via la console EDR ou le rapport mensuel
- **De 76 à 100** : Accompagnement SOC



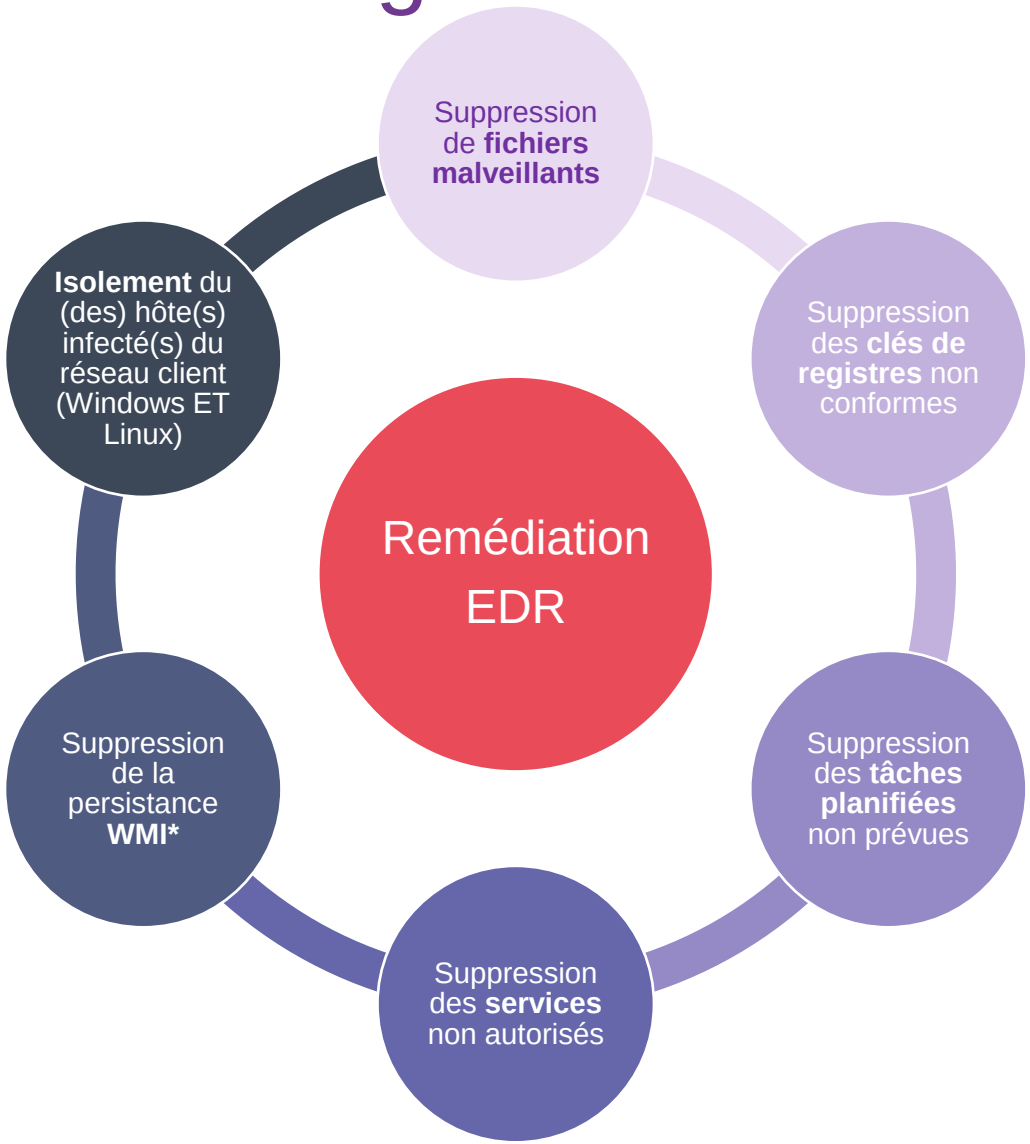

** Le budget mensuel dépendra de l'accompagnement proposé – Option 24/7 possible*

# **Le SOC –** La remédiation

Post incident, le SOC Koesio se positionnera en **engagements de moyens** pour accompagner le client vers une remédiation maitrisée



# **EDR** – Les gestes de remédiations




**Windows Management Instrumentation → Permet de surveiller les ressources Windows par l'OS. De la couche matérielle à la couche application (Exemple : Inventaire SCCM)*

# THANK YOU

## MERCI.

# Questions / Réponses

**Julien MACHIN**

Channel Manager France

WithSecure

**Jean-Philippe LASSERRE**

Responsable Avant-Vente

Koesio Corporate IT

Posez vos **questions via le chat**

Le **support de la présentation** vous sera envoyé par email avec un lien d'accès au **replay**