



**Le live!**  
Un webinar by **koesio**

**WithSecure**

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

**W / T H**  
secure

**koesio**



# Intervenants

## Julien MACHIN

Channel Manager France  
Withsecure



## Jean-Philippe LASSERRE

Responsable Avant-Vente  
Koesio Corporate IT



# L'EDR - Rappels

```
autoReverted() { var m=a(), this=this, e=c(), f=g(), h=i(), j=k(), l=m(), n=o(), p=q(), r=s(), t=u(), v=w(), x=y(), z=aa(), ab=ac(), ac=ad(), ad=ae(), ae=af(), af=ag(), ag=ah(), ah=ai(), ai=aj(), aj=ak(), ak=al(), al=am(), am=an(), an=ao(), ao=ap(), ap=aq(), aq=ar(), ar=as(), as=at(), at=au(), au=av(), av=aw(), aw=ax(), ax=ay(), ay=az(), az=ba(), ba=bb(), bb=bc(), bc=bd(), bd=be(), be=bf(), bf=bg(), bg=bh(), bh=bi(), bi=bj(), bj=bk(), bk=bl(), bl=bm(), bm=bn(), bn=bo(), bo=bp(), bp=bq(), bq=br(), br=bs(), bs=bt(), bt=bu(), bu=bv(), bv=bw(), bw=bx(), bx=by(), by=bz(), bz=ca(), ca=cb(), cb=cc(), cc=cd(), cd=ce(), ce=cf(), cf=cg(), cg=ch(), ch=ci(), ci=cj(), cj=ck(), ck=cl(), cl=cm(), cm=cn(), cn=co(), co=cp(), cp=cq(), cq=cr(), cr=cs(), cs=ct(), ct=cu(), cu=cv(), cv=cw(), cw=cx(), cx=cy(), cy=cz(), cz=da(), da=db(), db=dc(), dc=dd(), dd=de(), de=df(), df=dg(), dg=dh(), dh=di(), di=dj(), dj=dk(), dk=dl(), dl=dm(), dm=dn(), dn=do(), do=dp(), dp=dq(), dq=dr(), dr=ds(), ds=dt(), dt=du(), du=dv(), dv=dw(), dw=dx(), dx=dy(), dy=dz(), dz=ea(), ea=eb(), eb=ec(), ec=ed(), ed=ee(), ee=ef(), ef=eg(), eg=eh(), eh=ei(), ei=ej(), ej=ek(), ek=el(), el=em(), em=en(), en=eo(), eo=ep(), ep=eq(), eq=er(), er=es(), es=et(), et=eu(), eu=ev(), ev=ew(), ew=ex(), ex=ey(), ey=ez(), ez=fa(), fa=fb(), fb=fc(), fc=fd(), fd=fe(), fe=ff(), ff=fg(), fg=fh(), fh=fi(), fi=fj(), fj=fk(), fk=fl(), fl=fm(), fm=fn(), fn=fo(), fo=fp(), fp=fq(), fq=fr(), fr=fs(), fs=ft(), ft=fu(), fu=fv(), fv=fw(), fw=fx(), fx=fy(), fy=fz(), fz=ga(), ga=gb(), gb=gc(), gc=gd(), gd=ge(), ge=gf(), gf=gg(), gg=gh(), gh=gi(), gi=gj(), gj=gk(), gk=gl(), gl=gm(), gm=gn(), gn=go(), go=gp(), gp=gq(), gq=gr(), gr=gs(), gs=gt(), gt=gu(), gu=gv(), gv=gw(), gw=gx(), gx=gy(), gy=gz(), gz=ha(), ha=hb(), hb=hc(), hc=hd(), hd=he(), he=hf(), hf=hg(), hg=hh(), hh=hi(), hi=hj(), hj=hk(), hk=hl(), hl=hm(), hm=hn(), hn=ho(), ho=hp(), hp=hq(), hq=hr(), hr=hs(), hs=ht(), ht=hu(), hu=hv(), hv=hw(), hw=hx(), hx=hy(), hy=hz(), hz=ia(), ia=ib(), ib=ic(), ic=id(), id=ie(), ie=if(), if=ig(), ig=ih(), ih=ii(), ii=ij(), ij=ik(), ik=il(), il=im(), im=in(), in=io(), io=ip(), ip=iq(), iq=ir(), ir=is(), is=it(), it=iu(), iu=iv(), iv=iw(), iw=ix(), ix=iy(), iy=iz(), iz=ja(), ja=jb(), jb=jc(), jc=jd(), jd=je(), je=jf(), jf=jg(), jg=jh(), jh=ji(), ji=jj(), jj=jk(), jk=jl(), jl=jm(), jm=jn(), jn=jo(), jo=jp(), jp=jq(), jq=jr(), jr=js(), js=jt(), jt=ju(), ju=jv(), jv=jw(), jw=jx(), jx= jy(), jy=jz(), jz=ka(), ka=kb(), kb=kc(), kc=kd(), kd=ke(), ke=kf(), kf=kg(), kg=kh(), kh=ki(), ki=kj(), kj=kk(), kk=kl(), kl=km(), km=kn(), kn=ko(), ko=kp(), kp=kq(), kq=kr(), kr=ks(), ks=kt(), kt=ku(), ku=kv(), kv=kw(), kw=kx(), kx=ky(), ky=kz(), kz=la(), la=lb(), lb=lc(), lc=ld(), ld=le(), le=lf(), lf=lg(), lg=lh(), lh=li(), li=lj(), lj=lk(), lk=ll(), ll=lm(), lm=ln(), ln=lo(), lo=lp(), lp=lq(), lq=lr(), lr=ls(), ls=lt(), lt=lu(), lu=lv(), lv=lw(), lw=lx(), lx=ly(), ly=lz(), lz=ma(), ma=mb(), mb=mc(), mc=md(), md=me(), me=mf(), mf=mg(), mg=mh(), mh=mi(), mi=mj(), mj=mk(), mk=ml(), ml=mm(), mm=mn(), mn=mo(), mo=mp(), mp=mq(), mq=mr(), mr=ms(), ms=mt(), mt=mu(), mu=mv(), mv=mw(), mw=mx(), mx=my(), my=mz(), mz=na(), na=nb(), nb=nc(), nc=nd(), nd=ne(), ne=nf(), nf=ng(), ng=nh(), nh=ni(), ni=nj(), nj=nk(), nk=nl(), nl=nm(), nm=nn(), nn=no(), no=np(), np=nq(), nq=nr(), nr=ns(), ns=nt(), nt=nu(), nu=nv(), nv=nw(), nw=nx(), nx=ny(), ny=nz(), nz=oa(), oa=ob(), ob=oc(), oc=od(), od=oe(), oe=of(), of=og(), og=oh(), oh=oi(), oi=oj(), oj=ok(), ok=ol(), ol=om(), om=on(), on=oo(), oo=op(), op=oq(), oq=or(), or=os(), os=ot(), ot=ou(), ou=ov(), ov=ow(), ow=ox(), ox=oy(), oy=oz(), oz=pa(), pa=pb(), pb=pc(), pc=pd(), pd=pe(), pe=pf(), pf=pg(), pg=ph(), ph=pi(), pi=pj(), pj=pk(), pk=pl(), pl=pm(), pm=pn(), pn=po(), po=pp(), pp=pq(), pq=pr(), pr=ps(), ps=pt(), pt=pu(), pu=pv(), pv=pw(), pw=px(), px=py(), py=pz(), pz=qa(), qa=qb(), qb=qc(), qc=qd(), qd=qe(), qe=qf(), qf=qg(), qg=qh(), qh=qi(), qi=qj(), qj=qk(), qk=ql(), ql=qm(), qm=qn(), qn=qo(), qo=qp(), qp=qr(), qr=qs(), qs=qt(), qt=qu(), qu=qv(), qv=qw(), qw=qx(), qx=qy(), qy=qz(), qz=ra(), ra=rb(), rb=rc(), rc=rd(), rd=re(), re=rf(), rf=rg(), rg=rh(), rh=ri(), ri=rj(), rj=rk(), rk=rl(), rl=rm(), rm=rn(), rn=ro(), ro=rp(), rp=rq(), rq=rr(), rr=rs(), rs=rt(), rt=ru(), ru=rv(), rv=rw(), rw=rx(), rx=ry(), ry=rz(), rz=sa(), sa=sb(), sb=sc(), sc=sd(), sd=se(), se=sf(), sf=sg(), sg=sh(), sh=si(), si=sj(), sj=sk(), sk=sl(), sl=sm(), sm=sn(), sn=so(), so=sp(), sp=sq(), sq=sr(), sr=ss(), ss=st(), st=su(), su=sv(), sv=sw(), sw=sx(), sx=sy(), sy=sz(), sz=ta(), ta=tb(), tb=tc(), tc=td(), td=te(), te=tf(), tf=tg(), tg=th(), th=ti(), ti=tj(), tj=tk(), tk=tl(), tl=tm(), tm=tn(), tn=to(), to=tp(), tp=tq(), tq=tr(), tr=ts(), ts=tt(), tt=tu(), tu=tv(), tv=tw(), tw=tx(), tx=ty(), ty=tz(), tz=ua(), ua=ub(), ub=uc(), uc=ud(), ud=ue(), ue=uf(), uf=ug(), ug=uh(), uh=ui(), ui=uj(), uj=uk(), uk=ul(), ul=um(), um=un(), un=uo(), uo=up(), up=uq(), uq=ur(), ur=us(), us=ut(), ut=uu(), uu=uv(), uv=uw(), uw=ux(), ux=uy(), uy=uz(), uz=va(), va=vb(), vb=vc(), vc=vd(), vd=ve(), ve=vf(), vf=vg(), vg=vh(), vh=vi(), vi=vj(), vj=vk(), vk=vl(), vl=vm(), vm=vn(), vn=vo(), vo=vp(), vp=vq(), vq=vr(), vr=vs(), vs=vt(), vt=vu(), vu=vv(), vv=vw(), vw=vx(), vx=vy(), vy=vz(), vz=wa(), wa=wb(), wb=wc(), wc=wd(), wd=we(), we=wf(), wf=wg(), wg=wh(), wh=wi(), wi=wj(), wj=wk(), wk=wl(), wl=wm(), wm=wn(), wn=wo(), wo=wp(), wp=wq(), wq=wr(), wr=ws(), ws=wt(), wt=wu(), wu=vw(), vw=wx(), wx=wy(), wy=wz(), wz=xa(), xa=xb(), xb=xc(), xc=xd(), xd=xe(), xe=xf(), xf=xg(), xg=xh(), xh=xi(), xi=xj(), xj=xk(), xk=xl(), xl=xm(), xm=xn(), xn=xo(), xo=xp(), xp=xq(), xq=xr(), xr=xs(), xs=xt(), xt=xu(), xu=xv(), xv=xw(), xw=xx(), xx=xy(), xy=xz(), xz=ya(), ya=yb(), yb=yc(), yc=yd(), yd=ye(), ye=yf(), yf=yg(), yg=yh(), yh=yi(), yi=yj(), yj=yk(), yk=yl(), yl=ym(), ym=yn(), yn=yo(), yo=yp(), yp=yq(), yq=yr(), yr=ys(), ys=yt(), yt=yu(), yu=yv(), yv=yw(), yw=xy(), xy=yz(), yz=za(), za=zb(), zb=zc(), zc=zd(), zd=ze(), ze=zf(), zf=zg(), zg=zh(), zh=zi(), zi=zj(), zj=zk(), zk=zl(), zl=zm(), zm=zn(), zn=zo(), zo=zp(), zp=zq(), zq=zs(), zs=zt(), zt=zu(), zu=zv(), zv=zw(), zw=zx(), zx=zy(), zy=zz(), zz=}
```

# EPP vs EDR – Définitions

## EPP – Définition

Un agent **EPP**, pour **EndPoint Protection Platform**, est une solution de sécurité des points terminaux issue du monde des **antivirus de nouvelle génération**.

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.

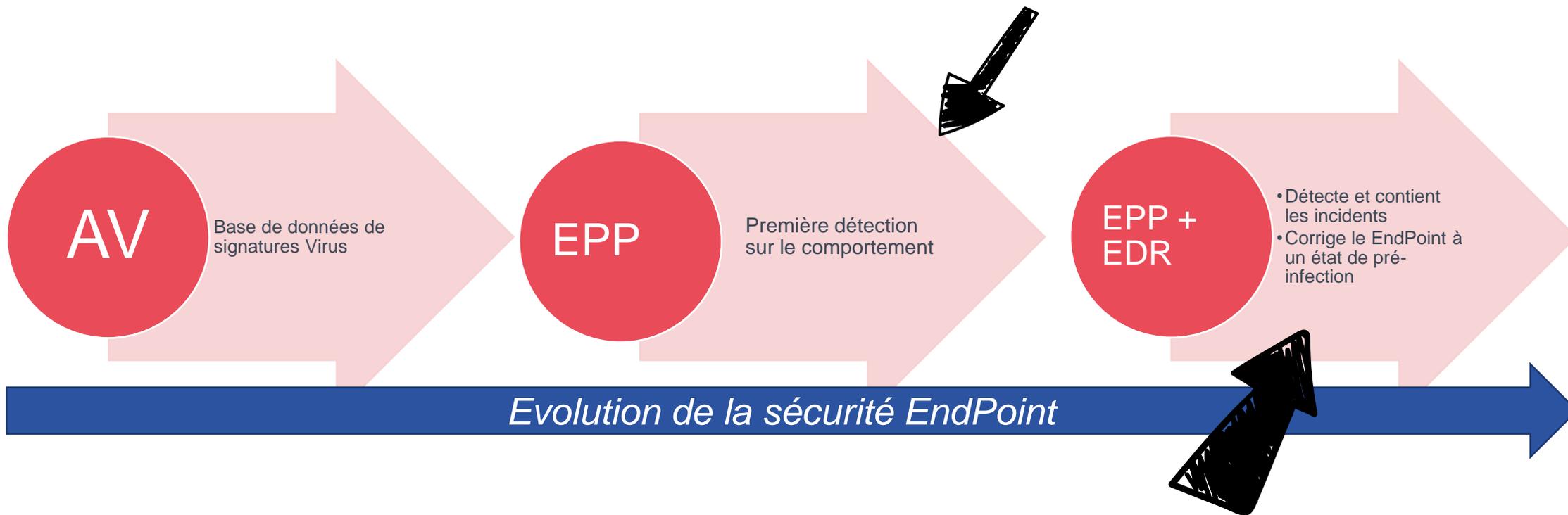
## EDR – Définition

Un agent **EDR**, pour **EndPoint Detection and Response**, identifie certains schémas de fonctionnement et détecte les anomalies.

Il collecte des **données télémétriques, comportementales issues des points terminaux**, pour les envoyer ensuite vers une base de données centralisée pour corrélation et analyse. Il s'appuie sur l'intelligence artificielle (IA).

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

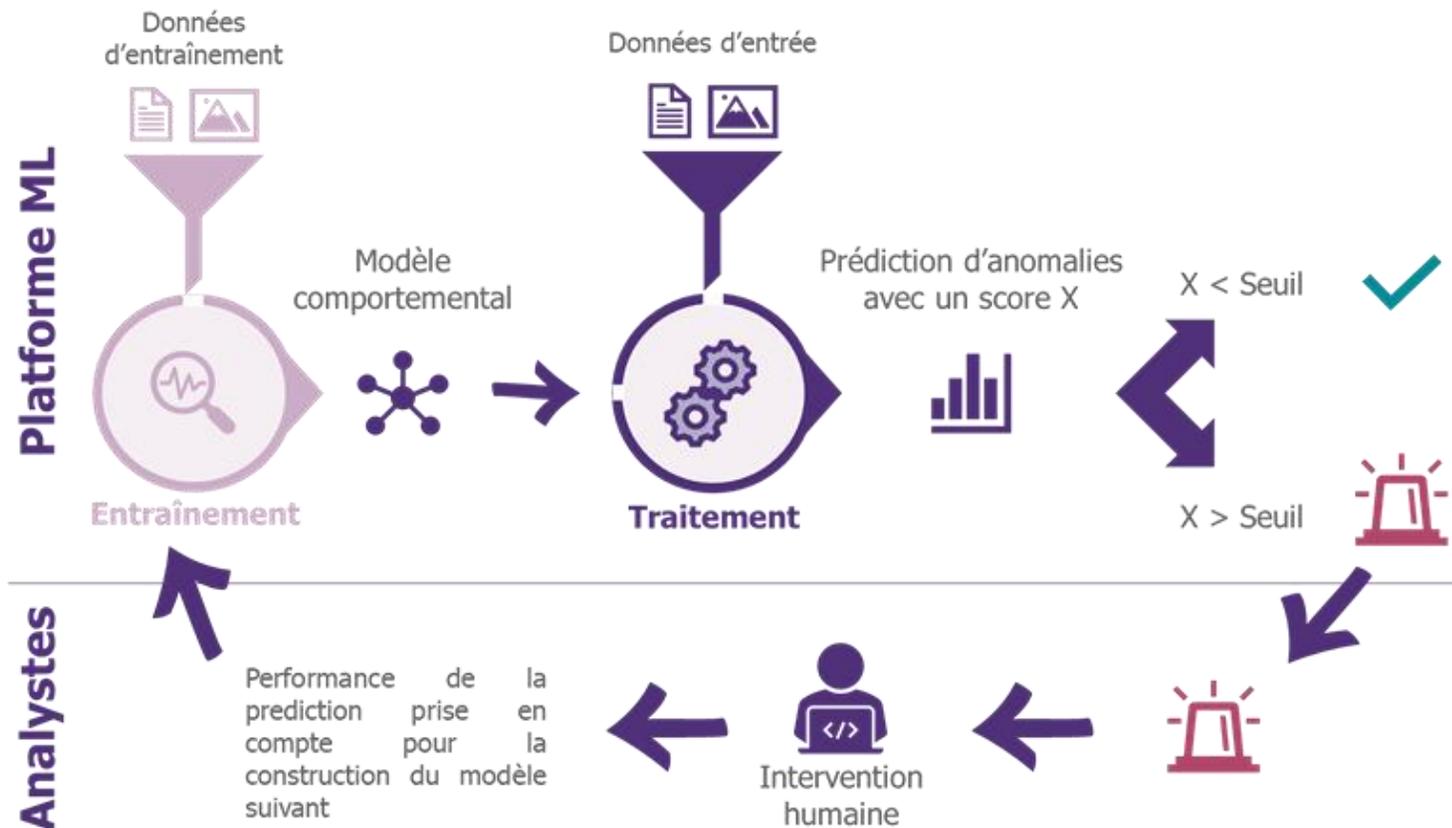


- **AV** : AntiVirus
- **EPP** : EndPoint Protection
- **EDR** : EndPoint detection and Response



# 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*



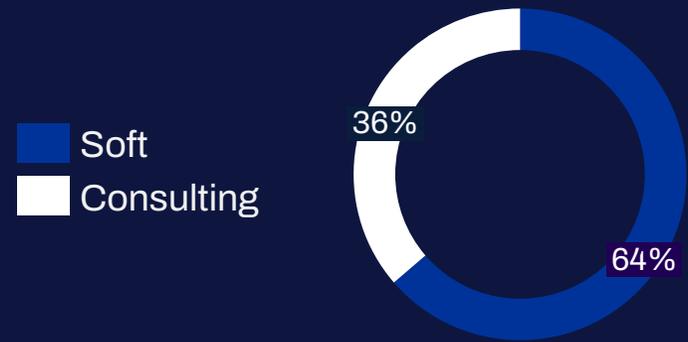
2

# La solution EDR de WithSecure

**W / T H**™  
secure

# WE ARE W / T H

secure



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

 **1 300 employés**

30  
Pays



Protection  
&  
confidentialité



**5 a 10 000 users**



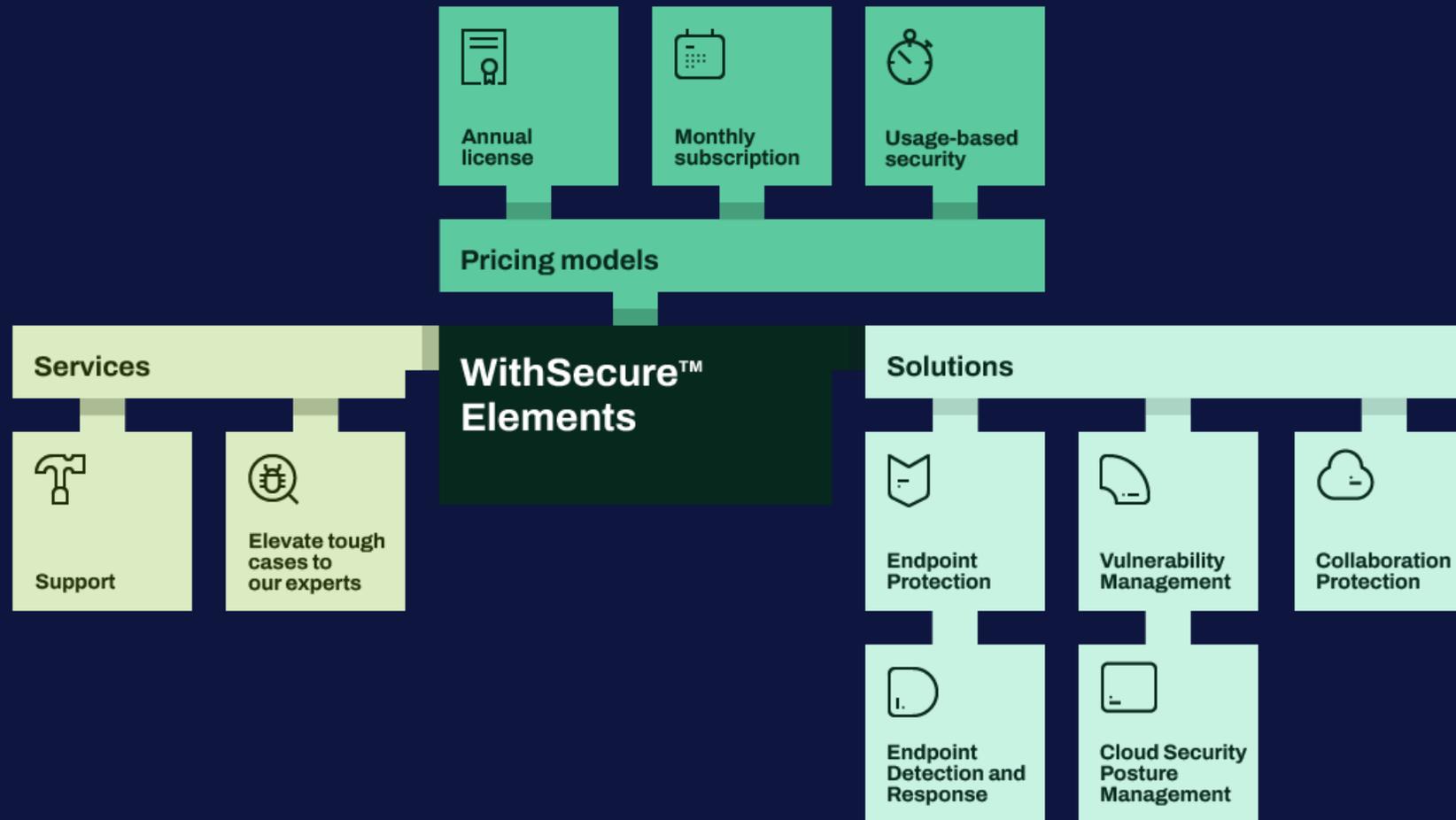
**Endpoint & cloud  
specialist**



**La co-sécurité**

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

# WithSecure™ Elements





### Computers

Windows, Mac, Linux



### Server

Windows, Linux



### Email

Microsoft Outlook



### Cloud collaboration apps

Microsoft Teams, SharePoint, OneDrive



### Networks

Vulnerability scans

## WI Elements™

Single agent

Unified data is analyzed  
with global threat  
intelligence

One Security Center

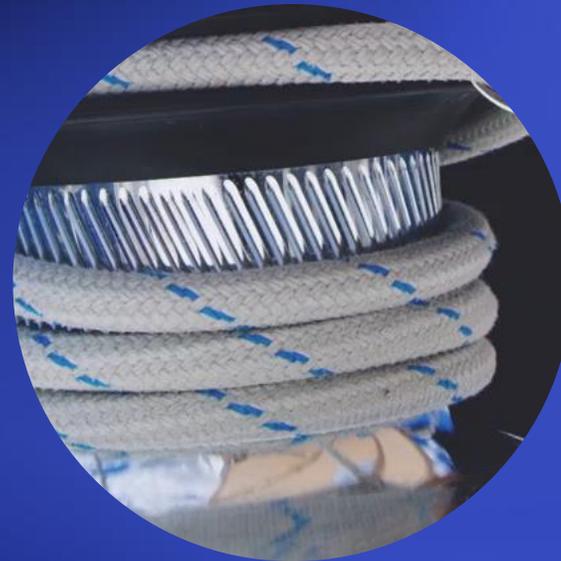


**koesio**

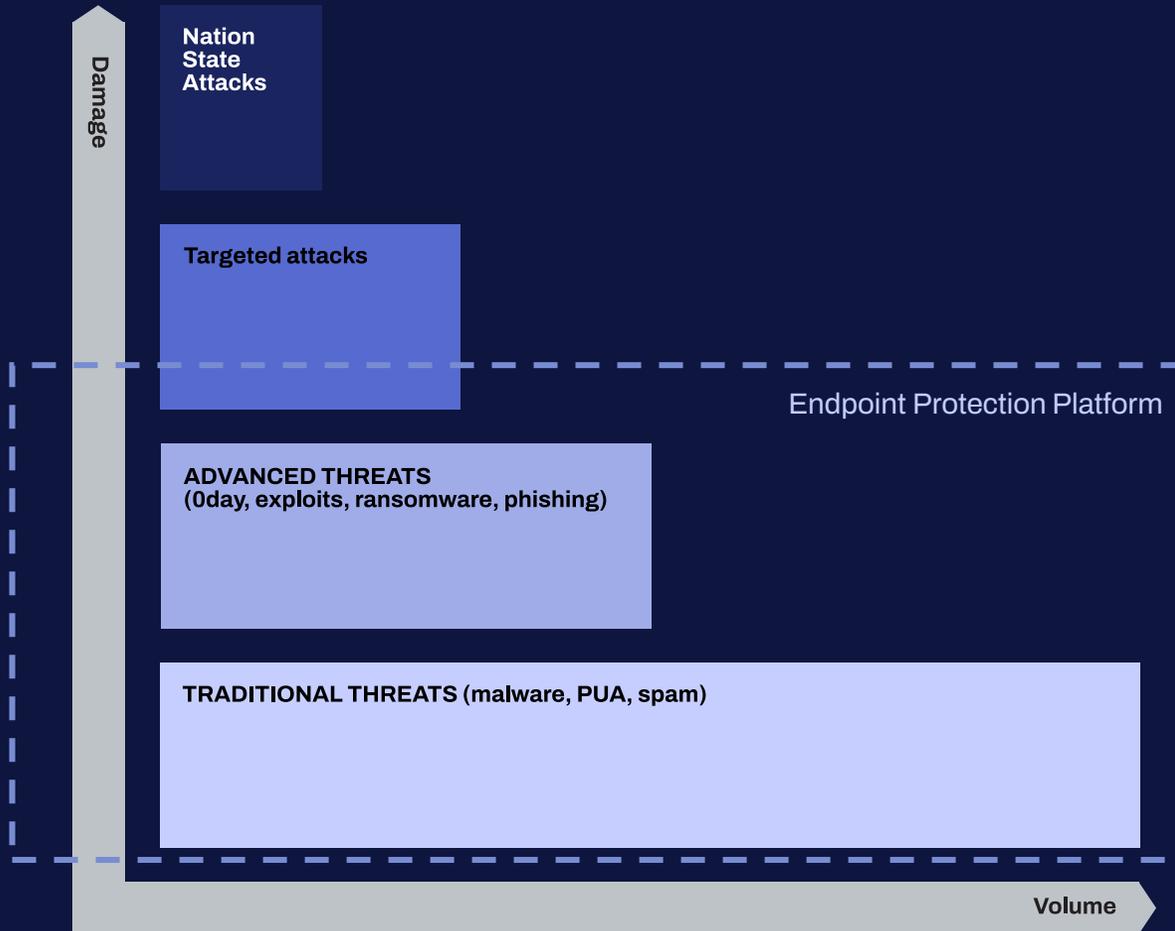
W / T H<sup>®</sup>  
secure

# Malwares

## Posture sécurité



# Faire face à la masse



Software and Operating system Hardening

Software Updater

Firewall

Application Control

Tamper Protection

Device Control

Network Level Protection

Web Traffic Protection

Browsing Protection

Reputaton Analysis

Web Content Control

Content Type Filtering

Connection Control

File Level Protection

Cloud Analysis

Heuristic Analysis

Behaviour Level Protection

AMSI Analysis

DataGuard Ransomware Protection

DeepGuard AI Based Behavioral Analysis

Process Monitoring

Exploit Interception

Ransomware Protection

## Tableau de bord

## Problèmes

	Type d'éléments	Gravité	Appareils concernés
^	<p>Analyse en temps réel désactivée</p> <p>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. <a href="#">Vérifiez 15 appareils</a></p> <p>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.</p>	❗ Critique	15
v	<p>Mises à jour logicielles critiques manquantes</p> <p>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. <a href="#">Vérifiez 8 appareils</a></p>	❗ Critique	8
v	<p>Problème lors de l'analyse en temps réel</p> <p>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. <a href="#">Vérifiez 3 appareils</a></p>	❗ Critique	3
v	<p>Exclusions dangereuses</p> <p>Vérifiez et gérez les exclusions dans le profil. Assurez-vous qu'il ne contient aucune exclusion dangereuse. <a href="#">Vérifiez 1 appareils</a></p>	❗ Critique	1
v	<p>Définitions de programme malveillant obsolètes</p> <p>Envoyer la mise à jour complète de l'état à l'appareil. Démarrer l'appareil. <a href="#">Vérifiez 1 appareils</a></p>	❗ Critique	1
v	<p>Appareils avec des incidents EDR graves ouverts</p> <p>Résoudre les incidents sur les appareils. <a href="#">Vérifiez 1 appareils</a></p>	❗ Critique	1
v	<p>Fin de vie des clients Windows</p> <p>Mettez à jour le logiciel client. Si des produits en fin de vie (EOL) sont utilisés, remplacez-les par des produits actuels (sidegrade). <a href="#">Vérifiez 22 appareils</a></p>	⚠ Important	22
v	<p>Il manque des mises à jour logicielles importantes</p> <p>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. <a href="#">Vérifiez 10 appareils</a></p>	⚠ Important	10
v	<p>Pare-feu désactivé par une stratégie de groupe</p> <p>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. <a href="#">Vérifiez 7 appareils</a></p>	⚠ Important	7
v	<p>Appareils avec des incidents EDR importants ouverts</p> <p>Résoudre les incidents sur les appareils. <a href="#">Vérifiez 6 appareils</a></p>	⚠ Important	6
v	<p>Appareil en attente de redémarrage</p> <p>Assurez-vous que les appareils sont redémarrés ou utilisez « Redémarrer l'appareil » sur la page Appareils. <a href="#">Vérifiez 4 appareils</a></p>	⚠ Important	4

**i** L'état de la sécurité est une nouvelle fonctionnalité qui prend en charge un no

## État de la sécurité (PILOTE) **i**

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

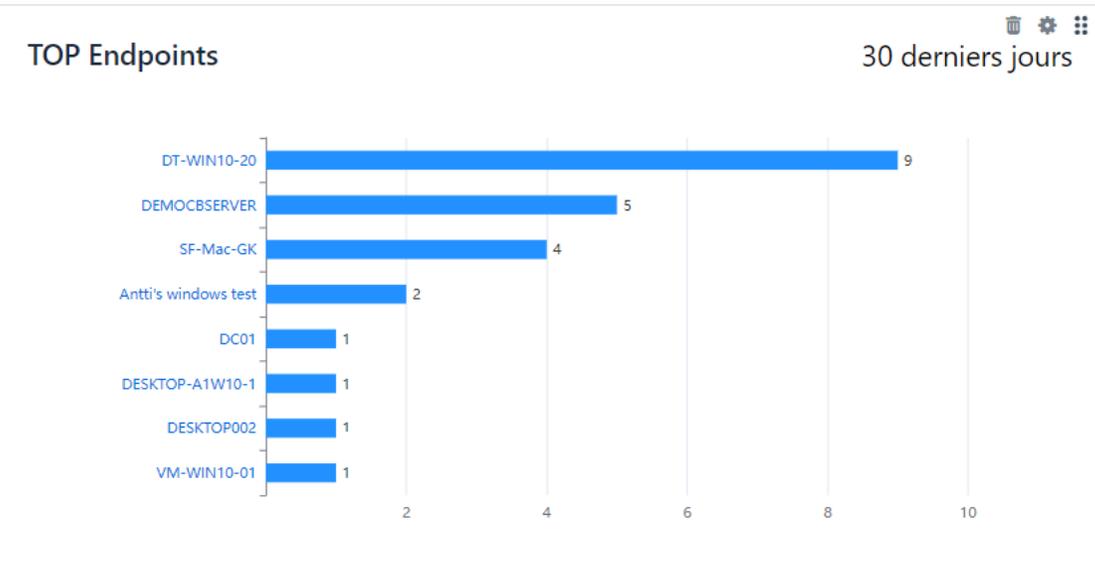
Endpoint Protection / Rapports

## Rapports

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

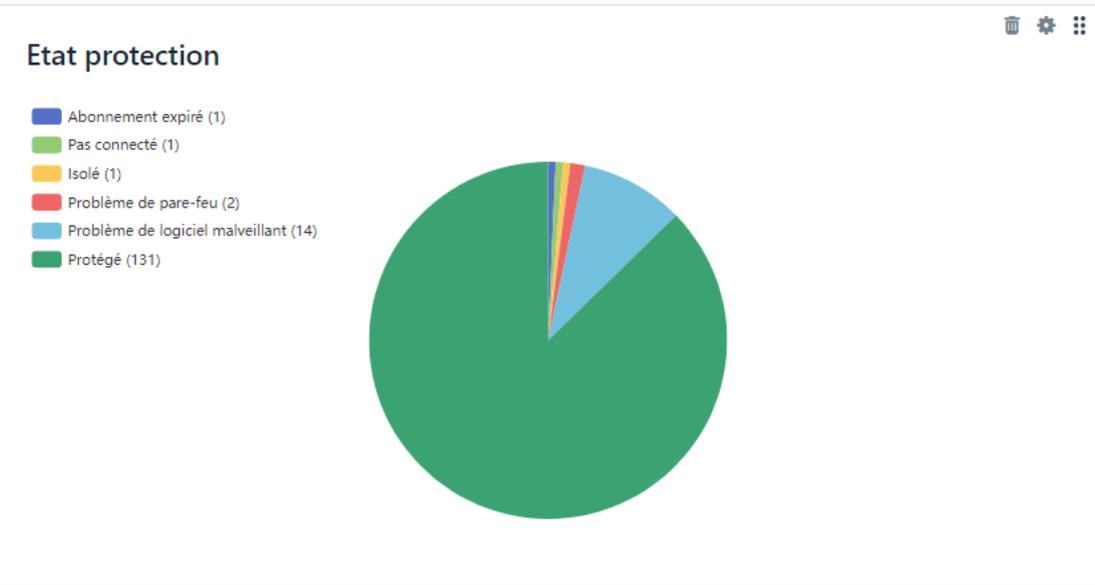
### TOP Endpoints

30 derniers jours



Endpoint	Nombre
DT-WIN10-20	9
DEMOCBSERVER	5
SF-Mac-GK	4
Antti's windows test	2
DC01	1
DESKTOP-A1W10-1	1
DESKTOP002	1
VM-WIN10-01	1

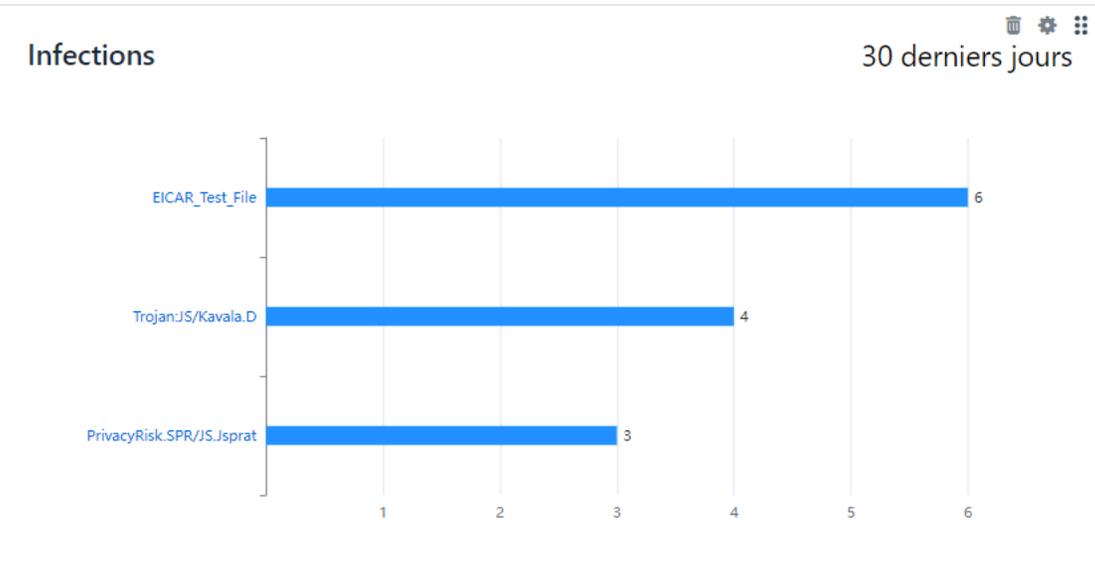
### Etat protection



Etat	Nombre
Abonnement expiré	1
Pas connecté	1
Isolé	1
Problème de pare-feu	2
Problème de logiciel malveillant	14
Protégé	131

### Infections

30 derniers jours



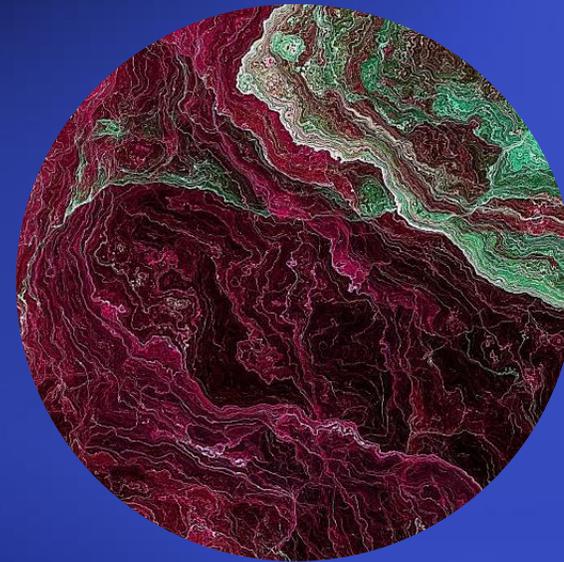
Infection	Nombre
EICAR_Test_File	6
TrojanJS/Kavala.D	4
PrivacyRisk.SPR/JS.Jsprat	3

### Seuil de verrouillage de compte



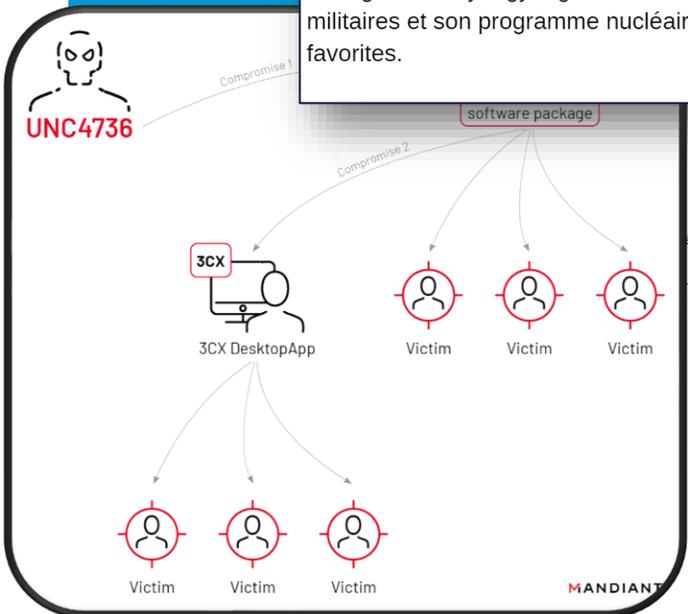
Configuration	Nombre
10	1
Non configuré	95

Des attaques de  
plus en plus  
avancées



Koesio WITH

# Attaques avancées



Établi en tant que leader mondial dans le domaine des communications d'entreprise. Grâce au standard ouvert SIP et PABX à une plateforme de communication complète, qui offre aux clients une solution simple, flexible et abordable pour augmenter leur productivité, optimiser l'expérience client, tout en diminuant fortement leurs coûts et le temps passé à

600k+  
INSTALLATIONS

12M+  
USERS

Attaque par la supply chain



# Attaques avancées

## Ransomware : les hackers ont frappé 58 victimes en France

Jean-Baptiste A.

Hive, un réseau de hackers qui a été démantelé, a ciblé plusieurs entreprises et collectivités, comme la justice judiciaire française.



3 France 3 Régions

## Cyberattaque à Lille : les pirates diffusent sur le web "une quantité phénoménale" de données volées

Près d'un mois après la cyberattaque visant la ville de Lille, les pirates informatiques ont revendiqué leur geste. Comme le révèle le blog...

Il y a 1 mois



La Voix du Nord

## La cyberattaque visant la mairie de Lille revendiquée par le groupe Royal

Ce lundi matin, selon le site Zataz et son expert en cybersécurité Damien Bancal, ce sont près de 300 gigaoctets de données qui auraient été...

Il y a 1 mois



## CIOP utilise un ODay et met à terre 130 entreprises en quelques minutes

Posted On 27 Mar 2023 By : Damien Bancal Comment: 0 Tag: oday, cl0p, faille, GoAnywhere MFT, zero day

## Attaque par la supply chain



## Hands on keyboard

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

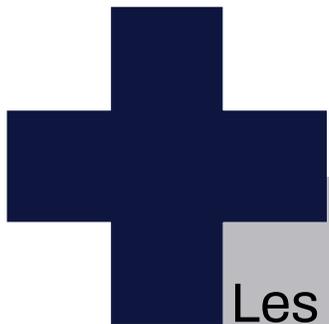
# Evaluer l'ampleur de l'attaque

- 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



# 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)
  - Étendre la collecte de logs
  - Attention aux logs rotatifs
  - Stocker les preuves
- Isoler rapidement même s'il s'agit d'un isolement total

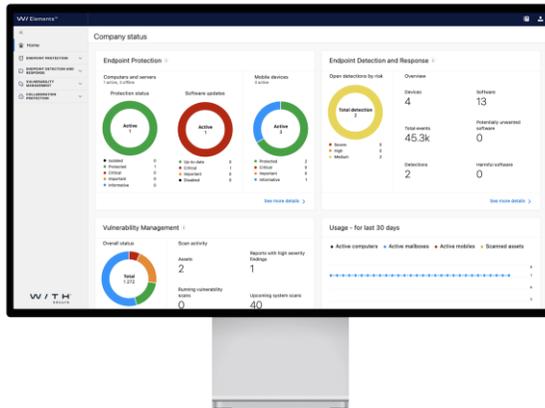
## A éviter !

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

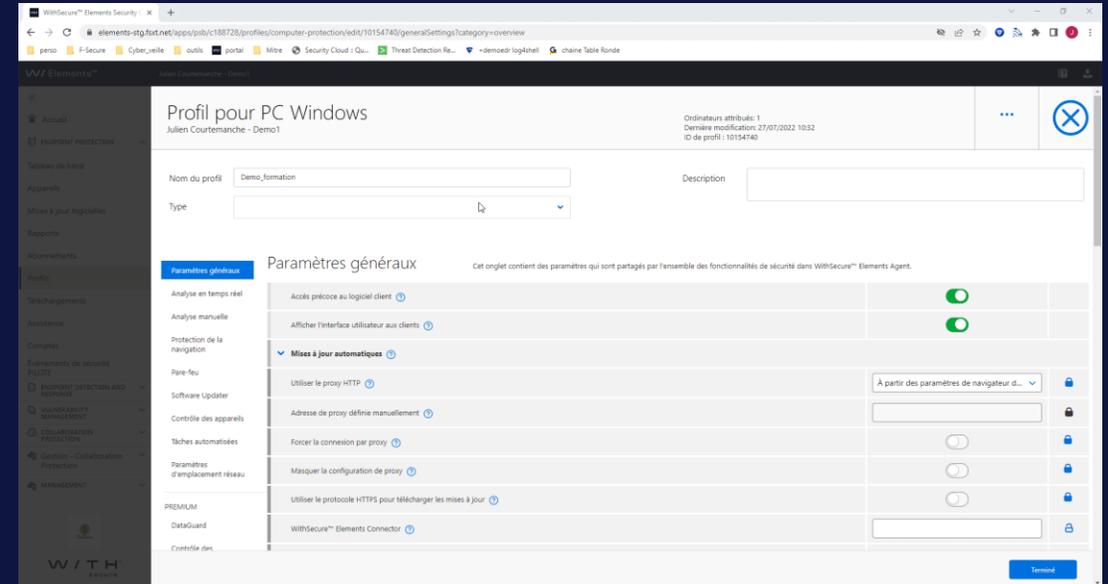


# Contenir

- Comment isoler des machines rapidement? Et si le contrôleur 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



# Les outils de réponse et remédiation

La suite WithSecure Elements

Delete Files

Delete  
Registry

Delete  
Scheduled

Delete  
Services

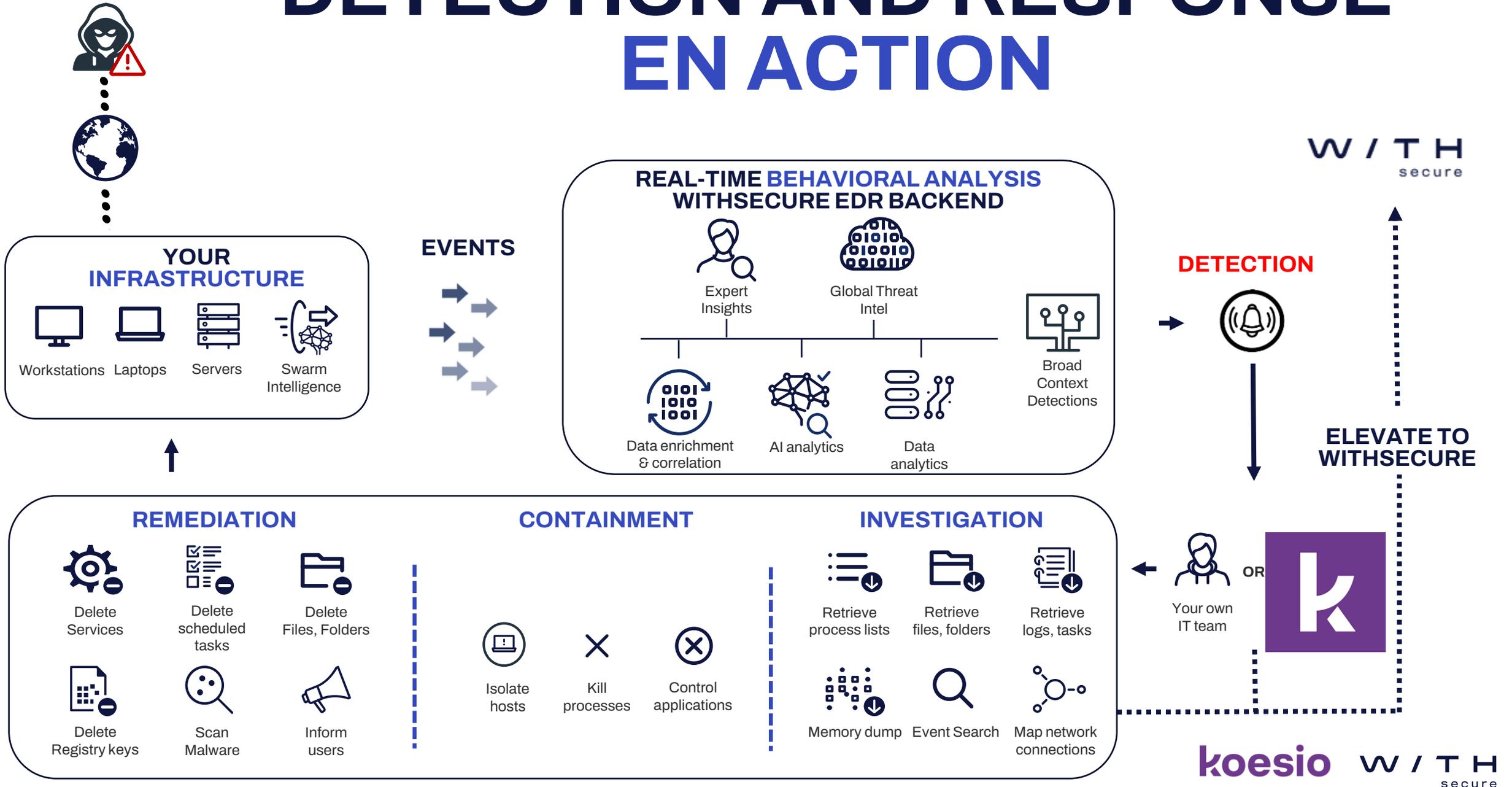
Install  
updates

Block  
network  
traffic

Block  
application  
behaviour

Block  
devices

# DETECTION AND RESPONSE EN ACTION



# 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**

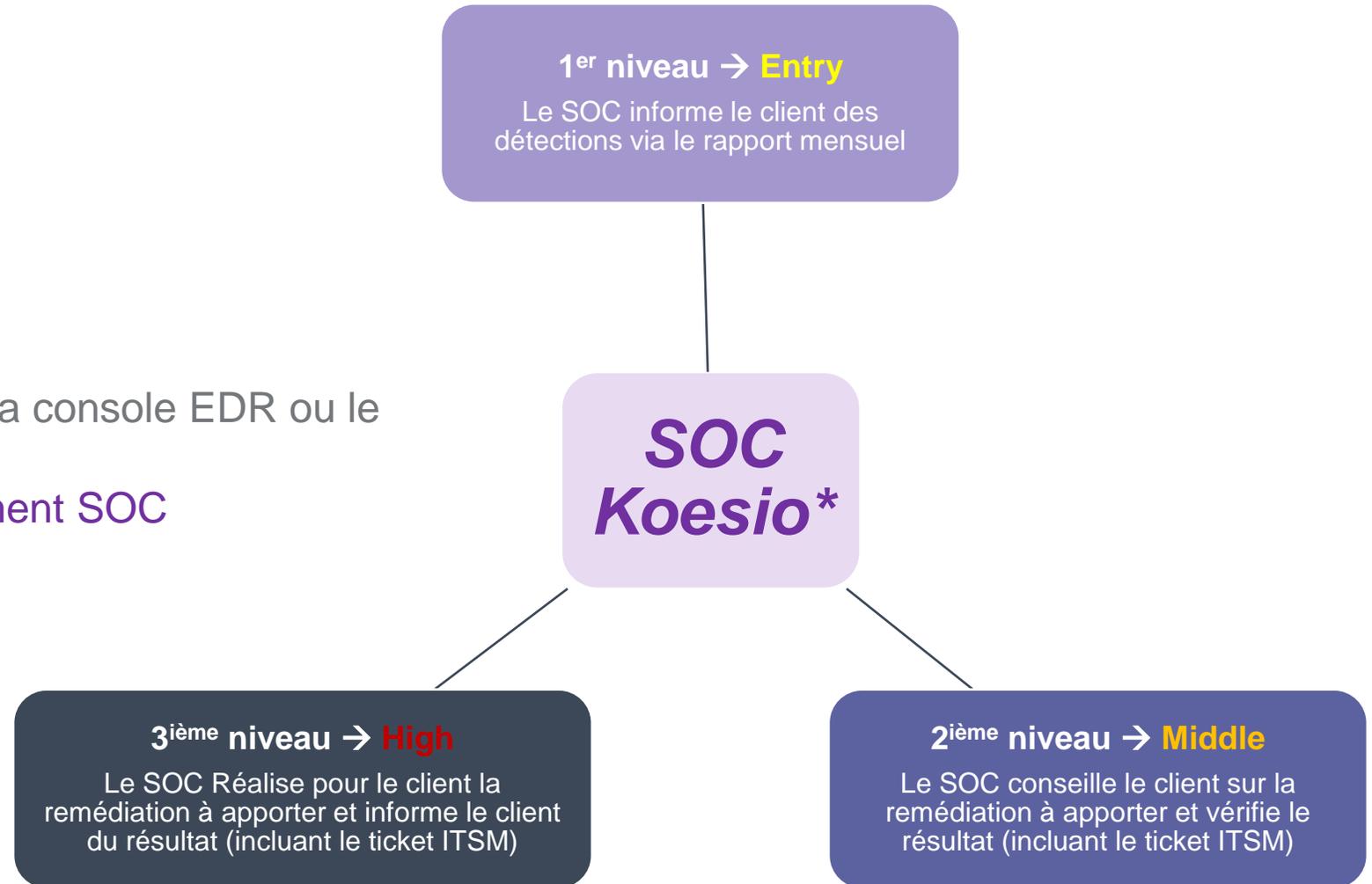
## Risque grave : Note de 91 à 100

- 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**

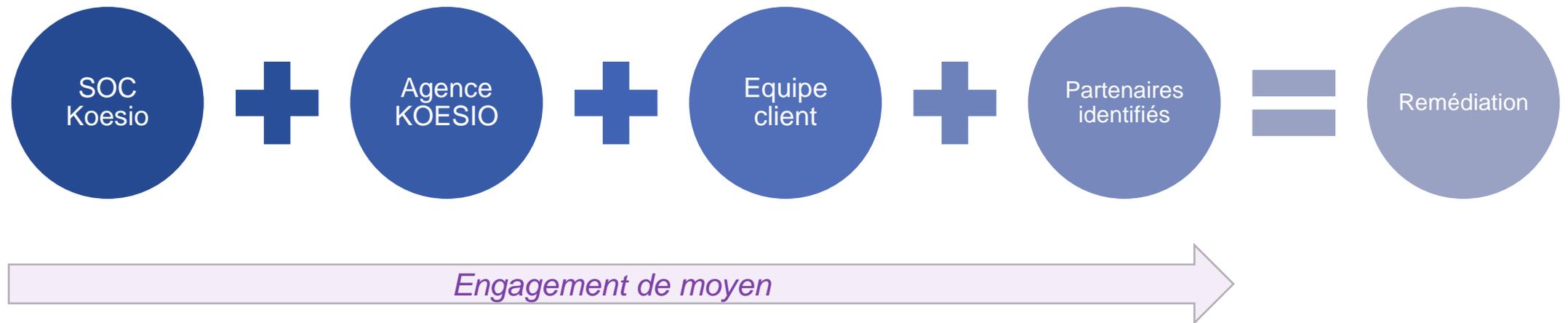


\* Le budget mensuel dépendra de l'accompagnement proposé – Option 24/7 possible

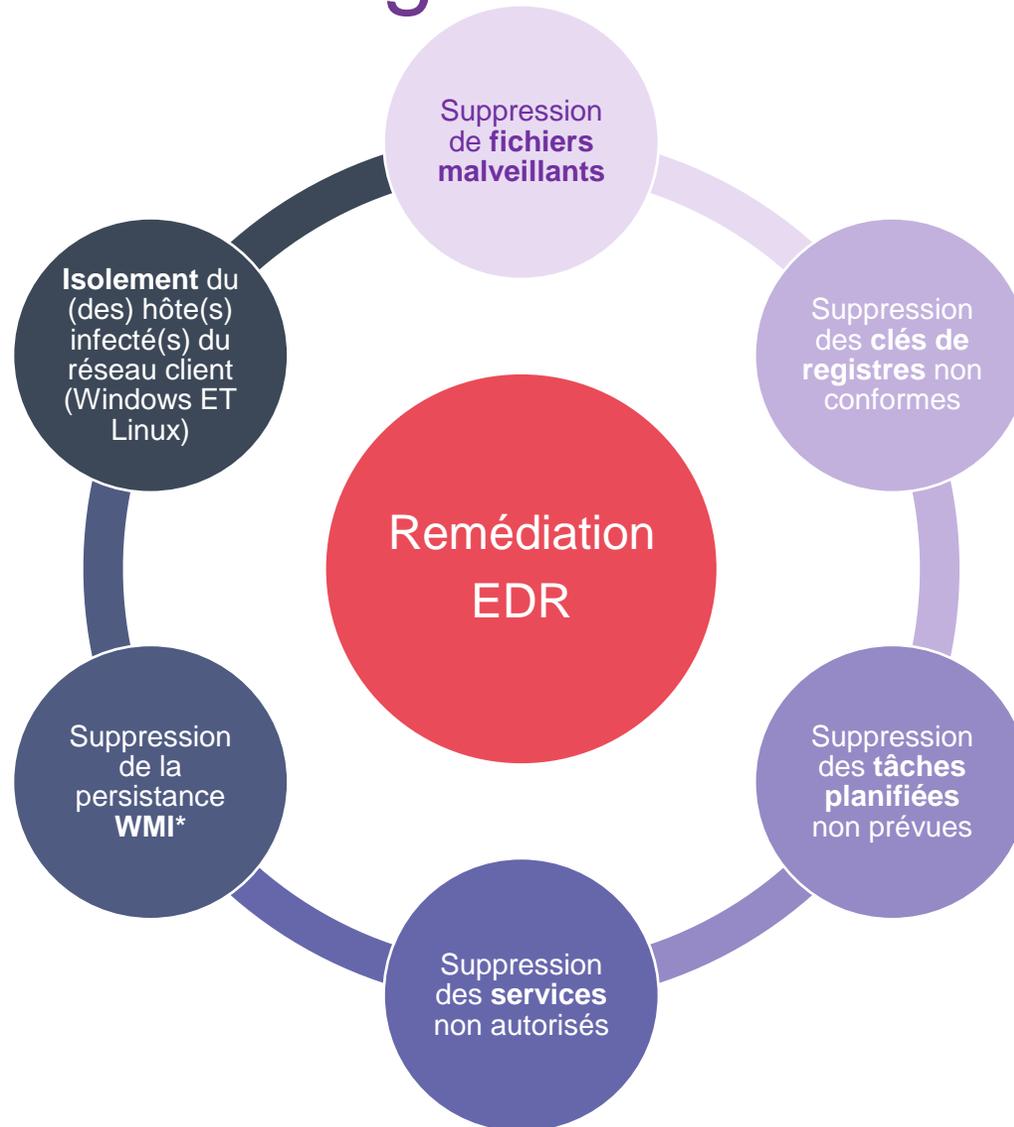
# Le SOC – La remédiation



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



# EDR – Les gestes de remédiation



\*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**