WITH
secure

Attaques ciblées, Ransomware as a Service. Comment se déroule une attaque ?

Julien MACHIN
Channel Manager France

WITH secure

2 Marques distinctes pour le B2B et le B2C

WITH secure

« Société de sécurité as-a-service pour les Pro »

WithSecure Elements™

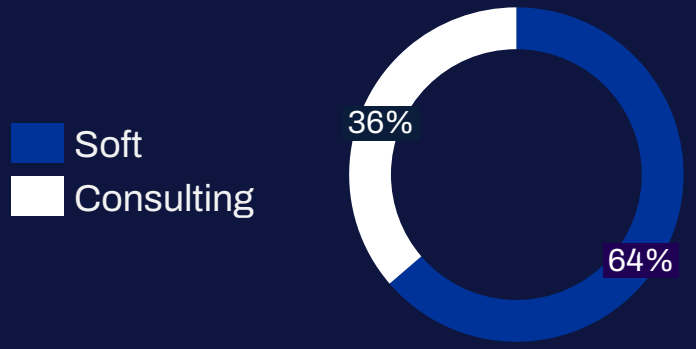
F-Secure

« Entreprise dédiée à la cybersécurité des particuliers. »

WITH secure

We are 

WE ARE W / T H secure



1988

+ de 30 ans
d’expertise

1 300 employés

W / T H secure

30
Pays

Protection
&
confidentialité

WITH secure

5 a 10 000 users

Endpoint & cloud specialist

La co-sécurité

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

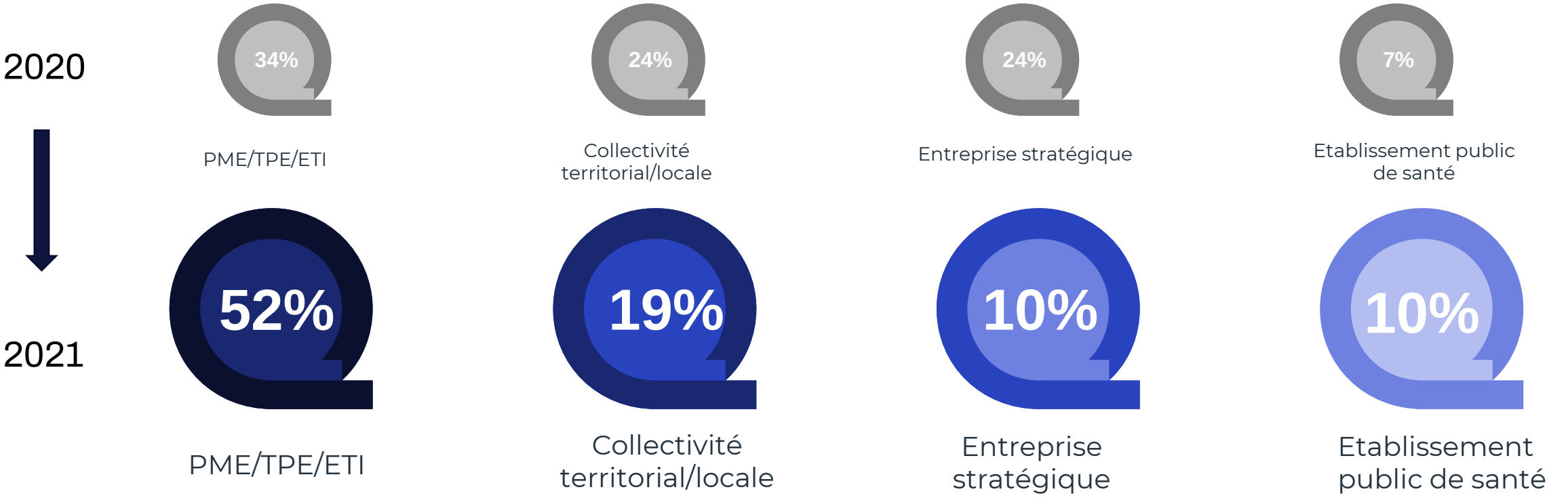
W / T H
secure

W / T H
secure

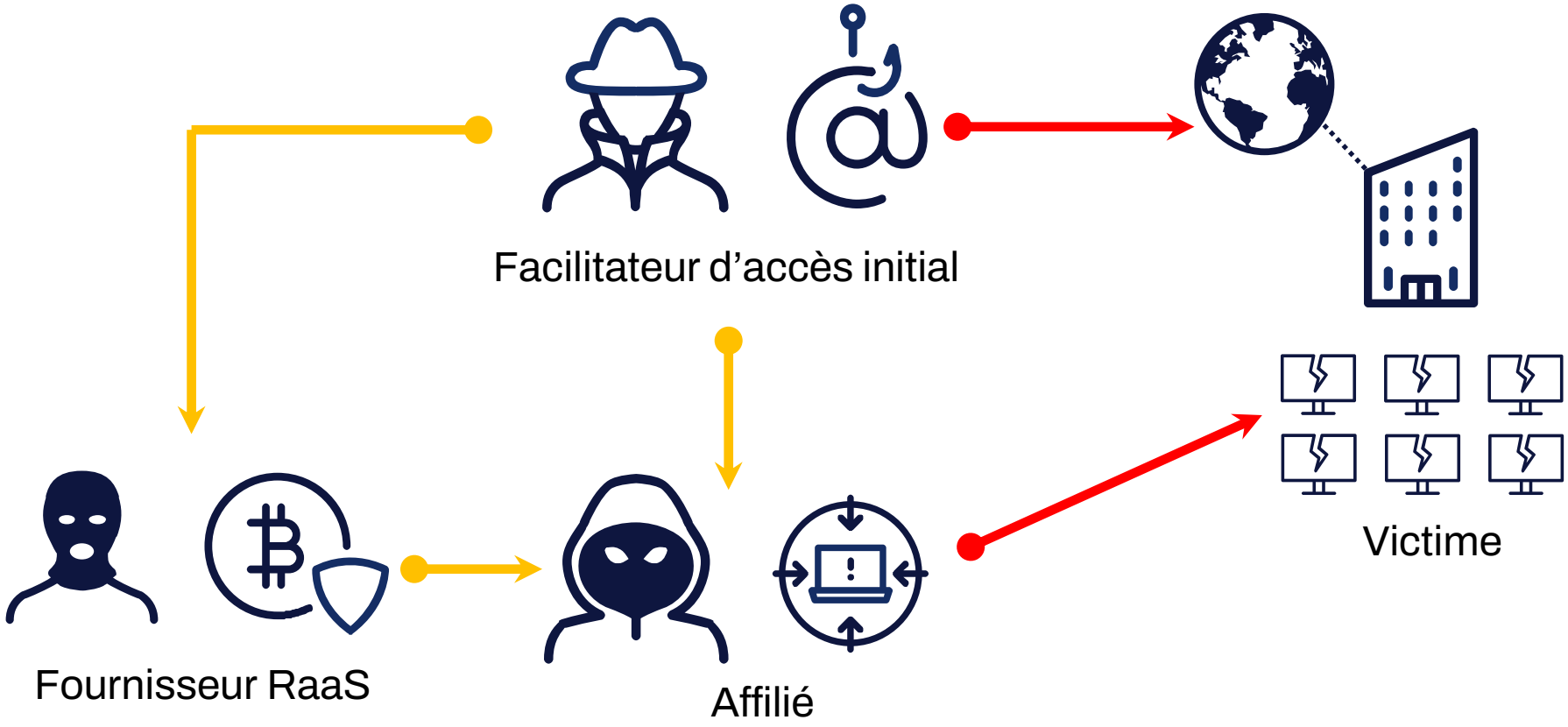
ETAT de la MENACE

WITH secure

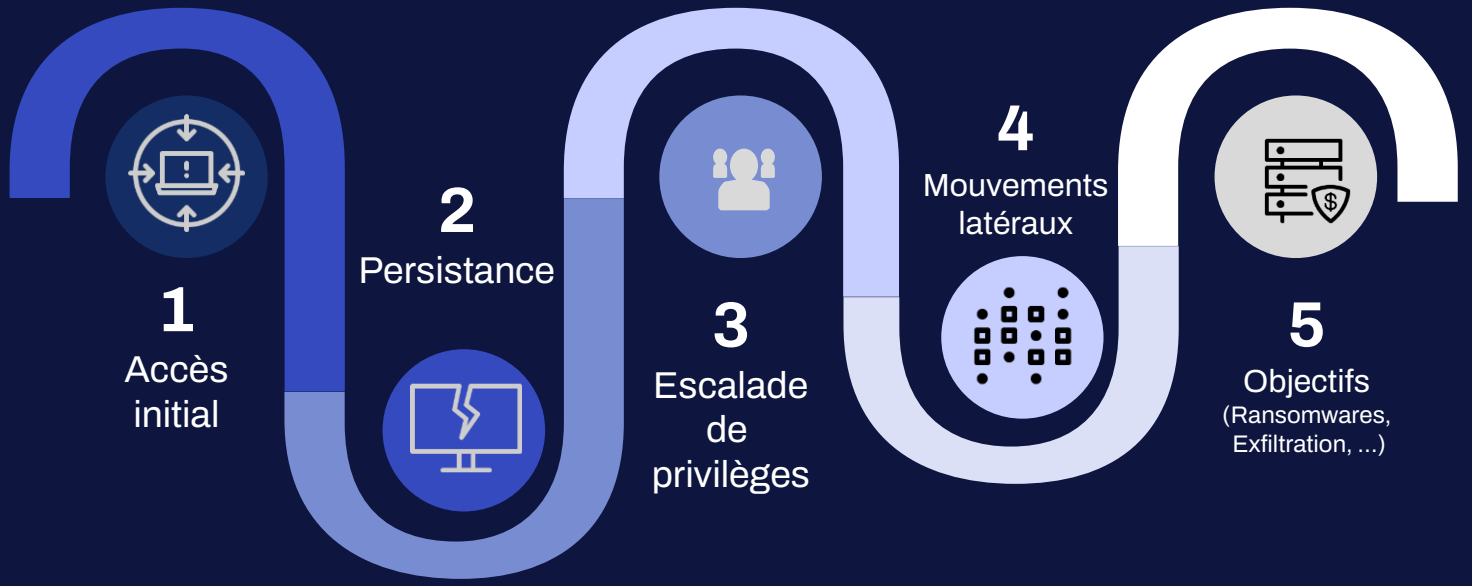
Quelles sont les cibles ?



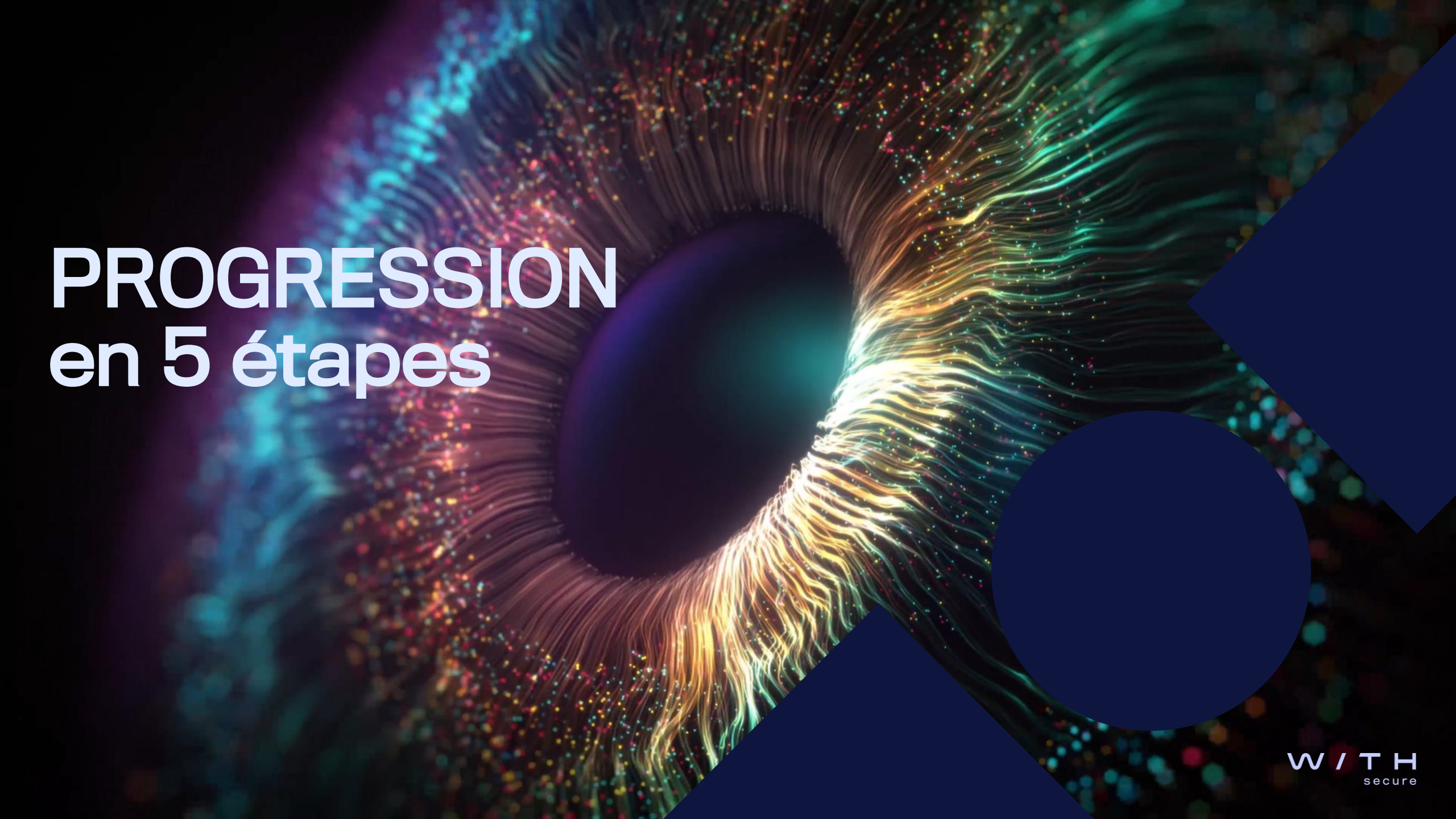
L'ECOSYSTEME de la CYBERCRIMINALITE



Progression de l'attaquant en 5 étapes



WITH secure


PROGRESSION
en 5 étapes

Etape 1- Accès initial
Le vecteur d’attaque

WITH secure

Accès initial : Rentrer avec les clés...

Le vol d'identifiant via un « phishing » est une solution simple et efficace

Office 365

- M365 est un magnifique outils, l'identité unique (AD, VPN, M365, ...) un confort pour l'utilisateur MAIS engendre un risque

WITH secure

PREVENT

WithSecure™ Elements Collaboration Protection

- Collaboration Protection
  Exchange
  SharePoint
  OneDrive
  Teams
  ...

- Threat intelligence
  & Multi-engine antivirus

- Sandbox

- Détection de comptes compromis

Breach details

Breach title:	Raccoon Stealer
Breach type:	Private
Password type:	PLAINTEXT
Password change (at the time of the detection):	03.06.2021, 09:09:12
Last password change:	11.02.2022, 09:38:00
Description:	Raccoon is a type of malware (or stealer) affecting Windows users. The Stealer has risen in popularity among cyber criminals as a means to procure credit card information, passwords, and cryptocurrency. The tool was first detected in April 2019. The payload is generally to victims via exploit kits, phishing and compromised software downloads.

WITH secure

Accès initial : Rentrer par une porte qui ferme mal…

- Voici le Top 10 des vulnérabilités exploitées en 2021 d'après l'ANSSI
  - CVE-2021-26855 – « ProxyLogon » => Exchange
  - CVE-2021-31207 – « ProxyShell » => Exchange
  - CVE-2021-26084 – Confluence => Extranet
  - CVE-2021-22205 – Gitlab => Versionning Dev
  - CVE-2021-22893 – Pulse Secure => VPN
  - CVE-2021-20016 – SonicWall => VPN
  - CVE-2021-22986 – F5 => WAF / loadbalancer
  - CVE-2021-21985 – VMware
  - CVE-2021-34527 – « PrintNightmare »
  - CVE-2021-44228 – « Log4Shell » => Serveur Application Java
- 8 sur 10 sont quasi systématiquement exposées à internet

WITH secure

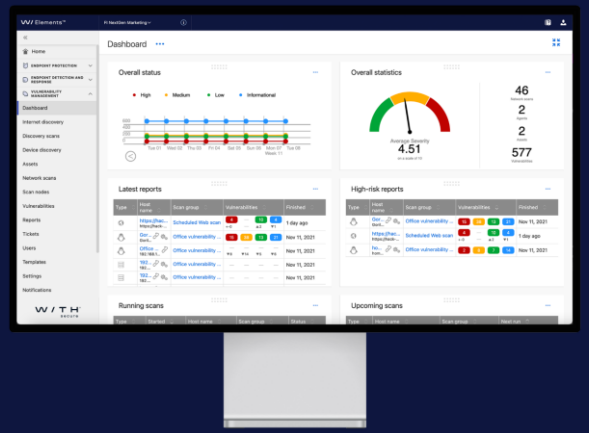
PREDICTION

WithSecure™
Software Updater

Inclus nativement
dans EPP

WithSecure™
Vulnerability Management

IP



WITH secure

PREVENT

Elements Endpoint protection ™

AI- Powered Endpoint
Détecte et bloque les attaques sophistiquées avec l'appui de l'IA Withsecure BlackFin

Analyse Comportementale
V6 DeepGuard

Protection et détection d'exploits, scripts malveillants, analyse comportementale, sandboxing local et Cloud

Analyse Statique
AV Engines

Analyse mémoire, analyse fichiers, analyse réseau, analyse de réputation Cloud

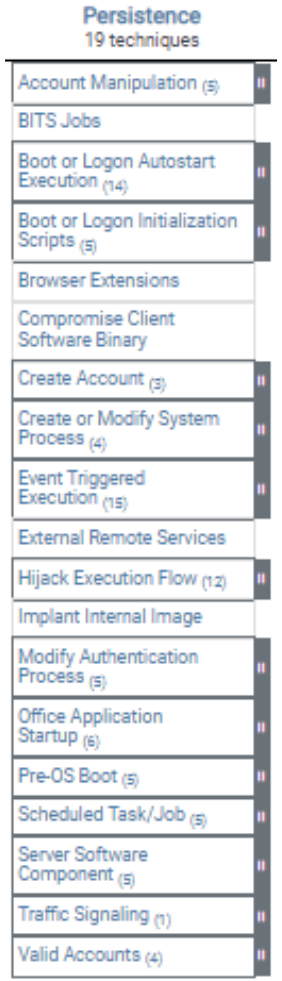
iOS Android

Etape 2- Persistance

La persistance

- Elle implique de déposer une charge sur une machine ou à minima un script
- Elle implique d'ajouter une entrée dans l'OS :
  - Une tache planifiée
  - Une extension de navigateur
  - Une clé de registre
  - Un service
  - Un « logon » script, ...

- L'EDR va identifier la mise en place d'une persistance et apporter de la visibilité sur une action qui était auparavant silencieuse



La persistance

Détection 3/14: Possible persistence by detected process Élevé Oct 25, 2021 12:30:46

Description Possible persistence operation, a detected process has performed a write registry that looks like a launchpoint.
Analyse
ID d'événement b7fc26c2-3594-11ec-8781-0242ac11000d

Écriture dans le registre
Clé de registre \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\bae8100
Nom de la valeur objectname
Valeur LocalSystem

Détection 4/14: Possible persistence by detected process Élevé Oct 25, 2021 12:30:46

Détection 5/14: Susp service reg persistence Élevé Oct 25, 2021 12:30:46

Description Detected a suspicious service image path containing cmd or powershell.
Analyse
ID MITRE ATT&CK T1543.003
ID d'événement b7fc0764-3594-11ec-8781-0242ac11000d

Écriture dans le registre
Clé de registre \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\bae8100
Nom de la valeur imagepath
Valeur %COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0A
dAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQB

schtasks.exe

Appareil JC-WIN10-3.JC-LAB.local
Nom d'utilisateur JC-LAB\Administrator
Ligne de commande "C:\WINDOWS\system32\schtasks.exe" /Create /F /RU System /SC WEEKLY /TN Avira_Security_Update /TR "\"C:\WINDOWS\system32\net.exe\" start AviraSecurityUpdater" /RL HIGHEST
Chemin d'accès %systemroot%\syswow64
PID 5928
SHA1 af506b15498f0db1a4e350cc26f2a60d6c12146c
Début de l'exécution Jan 25, 2022 13:53:16
Fin de l'exécution Jan 25, 2022 13:53:16

Détections

Détection 1/2: Created scheduled task Faible Jan 25, 2022 13:53:16

Description A scheduled task was created. This could be leveraged for persistence.
Analyse System or tool misuse
ID MITRE ATT&CK TA0003 , T1053
ID d'événement 0ddff11c-7ee3-11ec-ba4c-0242ac110007

Détection 2/2: Schtasks add run del Modéré Jan 25, 2022 13:53:16

Description A scheduled task was created, forcibly ran and deleted in a short timeframe. This is typically used by attackers to accomplish indirect execution.
Analyse
ID MITRE ATT&CK T1053.005
ID d'événement 0ddff11c-7ee3-11ec-ba4c-0242ac110007 , 0de12988-7ee3-11ec-ba4c-0242ac110007 , 49840dfa-7eea-11ec-a646-0242ac110007

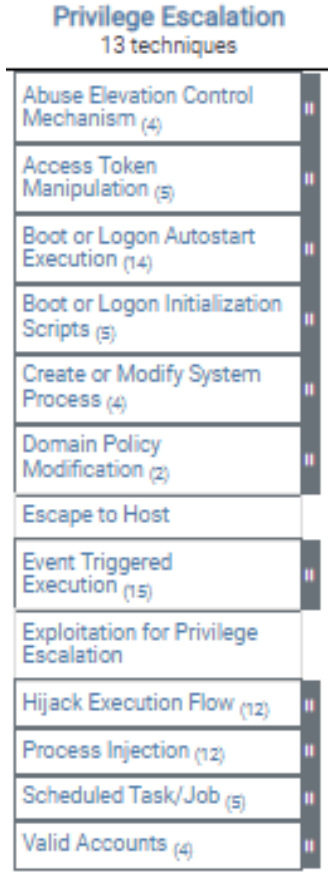
WITH secure

Etape 3- Escalade de Privilèges

L’escalade de Privilège

- Elle implique le plus souvent une faille déjà en place :
  - Compte à privilège
  - Logiciel avec une vulnérabilité (Office, Chrome, IE, …)
  - Droit d’écriture « trop généreux » permettant de manipuler des scripts exécutés avec privilège
  - Faiblesse de mot de passe ou manque de rotation

- L’EDR va identifier le gain en privilège et apporter de la visibilité sur une action qui était auparavant silencieuse

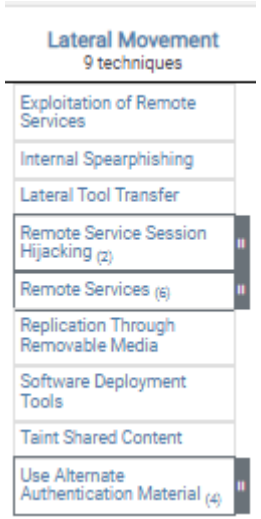


WITH secure

Etape 4- Mouvement Latéraux

Mouvement Latéraux

- L’idée ici est de reconnaitre la topologie du SI et se déplacer
- Le plus souvent, il s’agit pour l’attaquant de passer du monde « PC » vers les serveurs pour :
  - Identifier et altérer la solution de backup
  - Mettre la main sur l’Active Directory
  - Désactiver les solutions de sécurités
  - Préparer une exfiltration



- Encore une fois ici, l’EDR va identifier les mouvements latéraux et apporter de la visibilité sur une action qui était auparavant silencieuse

WITH secure

DETECTION & RESPONSE

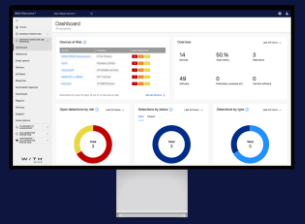
WithSecure™
Elements
Endpoint Detection
and Response

Detection

Containment

Investigation

Remediation



W / T H
secure

Etape 5- Objectif

Objectif atteint ...

- Ransomware
- Minage
- Exfiltration de données
- ...

Raisonner CO-SECURITE

ELEVATE TO WITHSECURE
Nos experts vous soutiennent à tout moment en étant disponibles dans les situations difficiles et en fournissant des conseils exploitables sur le confinement et la correction des attaques:

VALIDATION

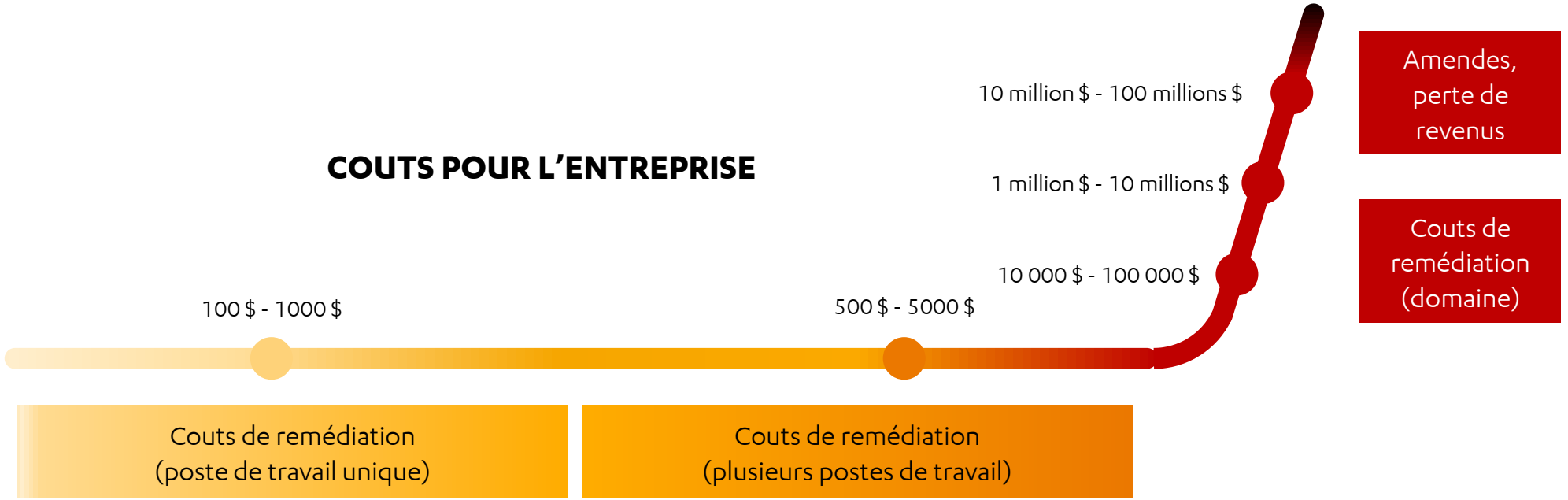
Nous fournissons des informations supplémentaires sur les découvertes au cours des 7 derniers jours. Cela comprend un résumé rédigé par un expert et une description de la détection, ainsi que toute autre donnée pertinente pour vous aider à déterminer si elle nécessite des actions de réponse.

INVESTIGATION

Nous menons une enquête très détaillée en exploitant toutes les données récentes et historiques. Cette option comprend également des conseils de réponse aux incidents exploitables de la part de nos experts en cybersécurité, ainsi qu'un rapport complet sur le type d'attaque détecté.

WITH secure

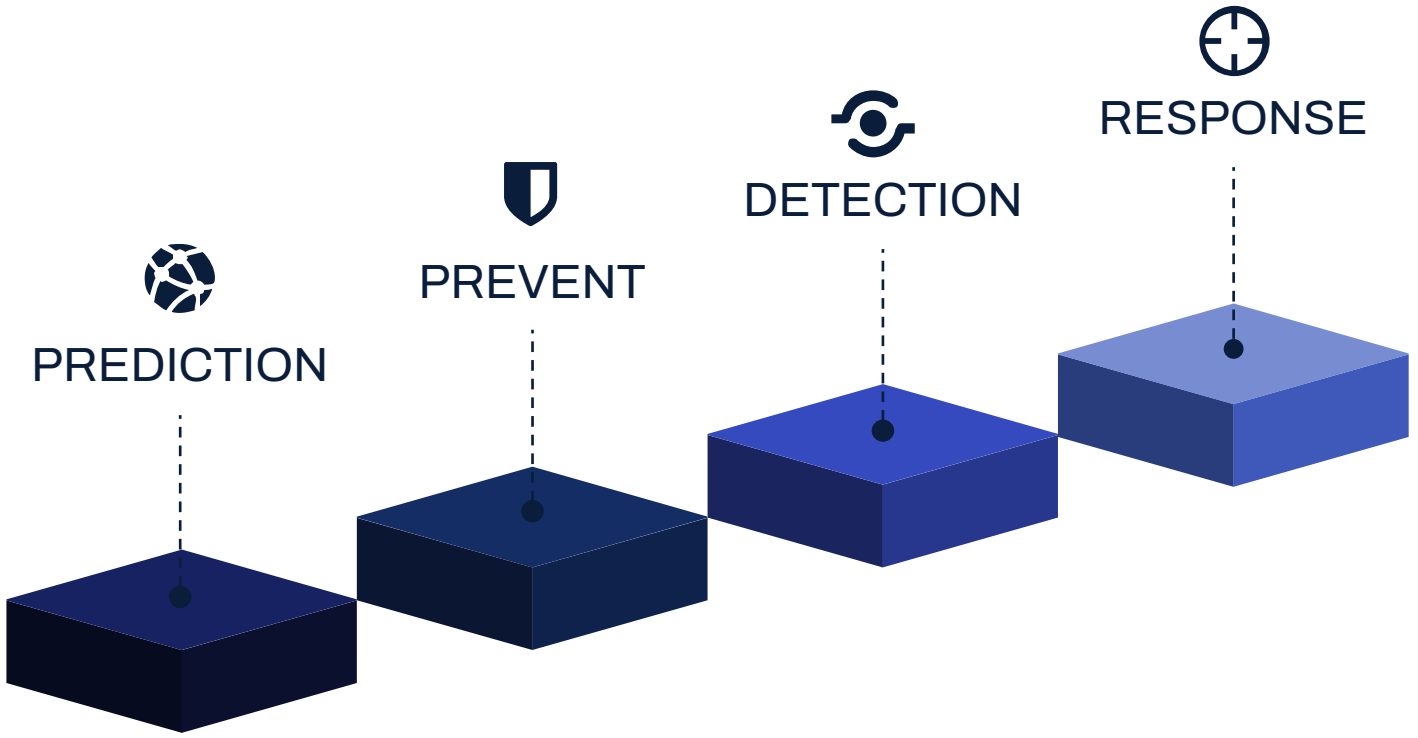
Progression de l'attaquant en 5 étapes



WITH secure

Notre approche

Live security



WITH secure

WithSecure™ Elements solutions

WithSecure™ Elements
One client

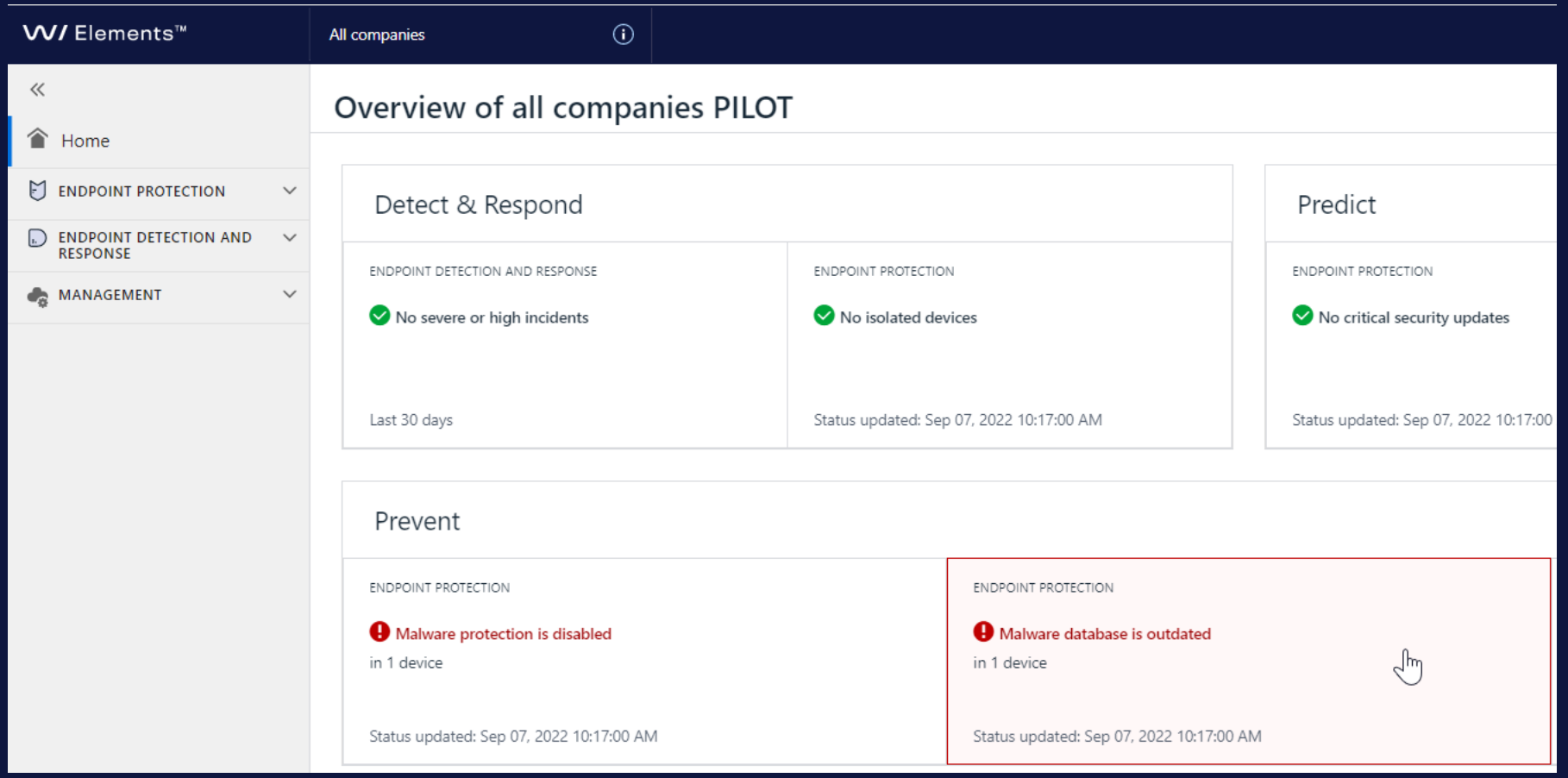
WithSecure™ Elements Vulnerability Management

WithSecure™ Elements EPP

WithSecure™ Elements for Microsoft 365

WithSecure™ Elements EDR

Console Elements : Une seule pour les gouverner toutes !!!



WITH secure

Demo live

Elements Platform