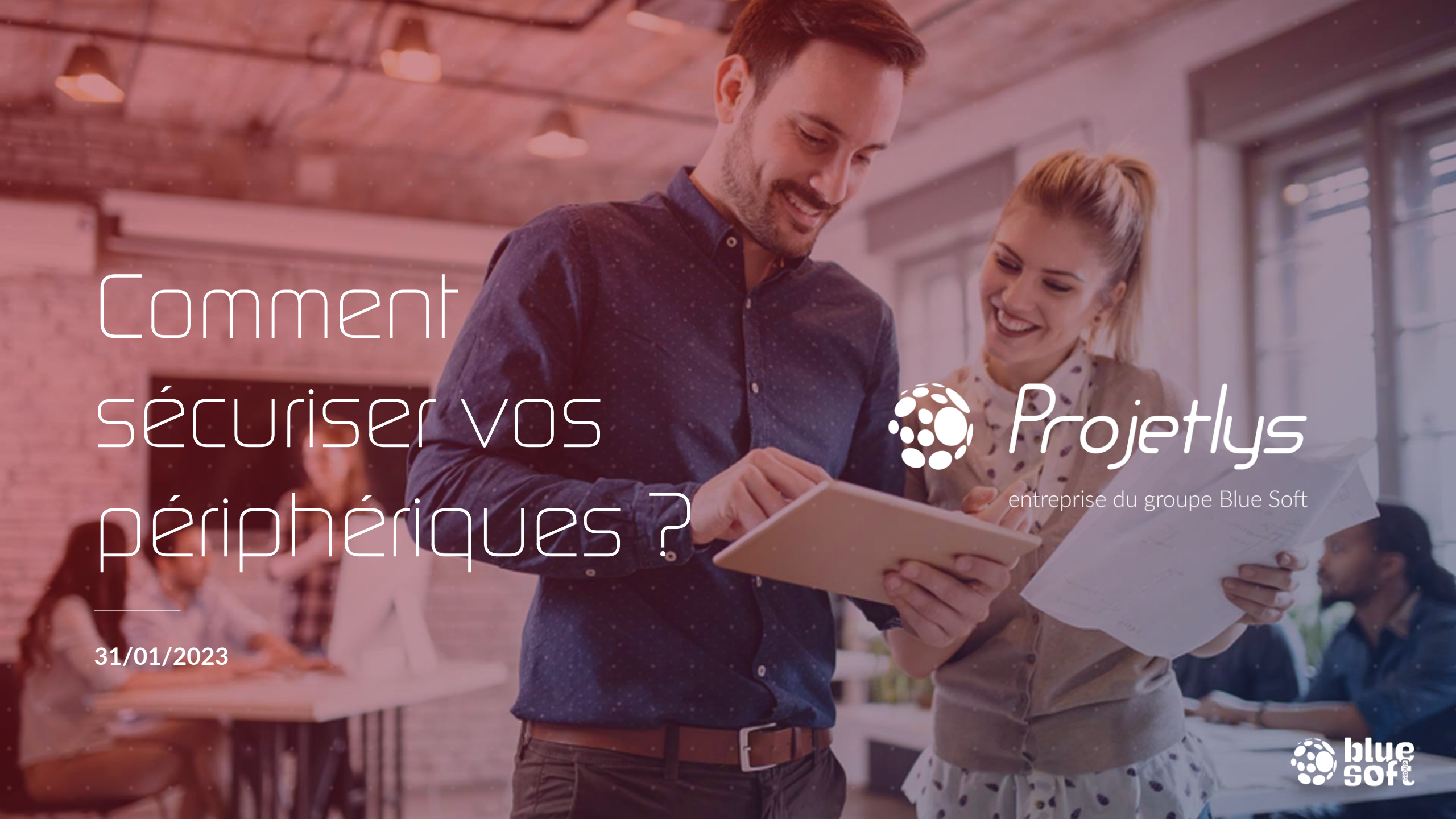


Comment sécuriser vos périphériques ?

31/01/2023

Projetlys

entreprise du groupe Blue Soft

blue soft

Les intervenants

Romaric MAHUT
Chef de projets Marketing

Antoine LOREAU
Consultant Avant-vente

Jean-Noël LETORD
Directeur des opérations adjoint

Sommaire

01.
La cybersécurité en quelques mots

Définitions

« La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. »

Source Kaspersky

« La cybersécurité est la pratique consistant à protéger les systèmes, les réseaux et les programmes contre les attaques numériques. Ces cyberattaques visent généralement à accéder à des informations sensibles, à les modifier ou à les détruire, à extorquer de l'argent aux utilisateurs, ou à interrompre les processus normaux de l'entreprise. »

Cisco

« Il faut rendre la sécurité numérique sexy, c'est-à-dire compréhensible et mettre dans la tête de nos dirigeants que ce n'est pas un mal nécessaire mais absolument indispensable pour le développement de l'entreprise »

Guillaume Poupard, ancien directeur général de l'ANSSI

Nouveau paradigme

La sécurisation des systèmes d'information est une guerre incessante qui **nécessite de se préparer aux attaques**.

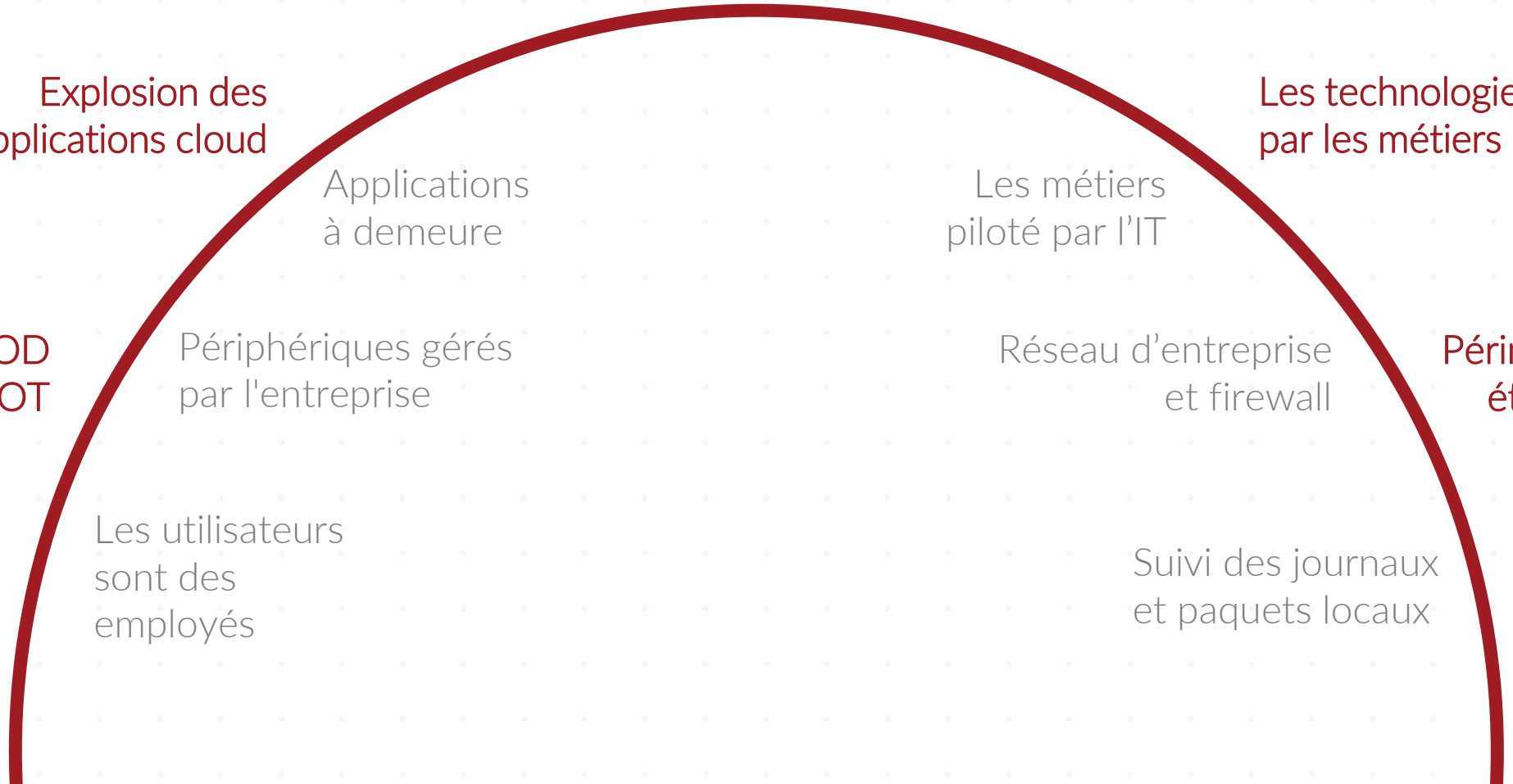
La sécurité consiste a **comprendre les menaces** et à faire le nécessaire pour **les atténuer**, mais il est impossible de parer toutes les attaques.

C'est pourquoi, il est important **d'adopter une stratégie** et une **approche de défense** en profondeur fondées sur le risque.

Changement d'usage

Maintenant

Avant



Changement d'environnement

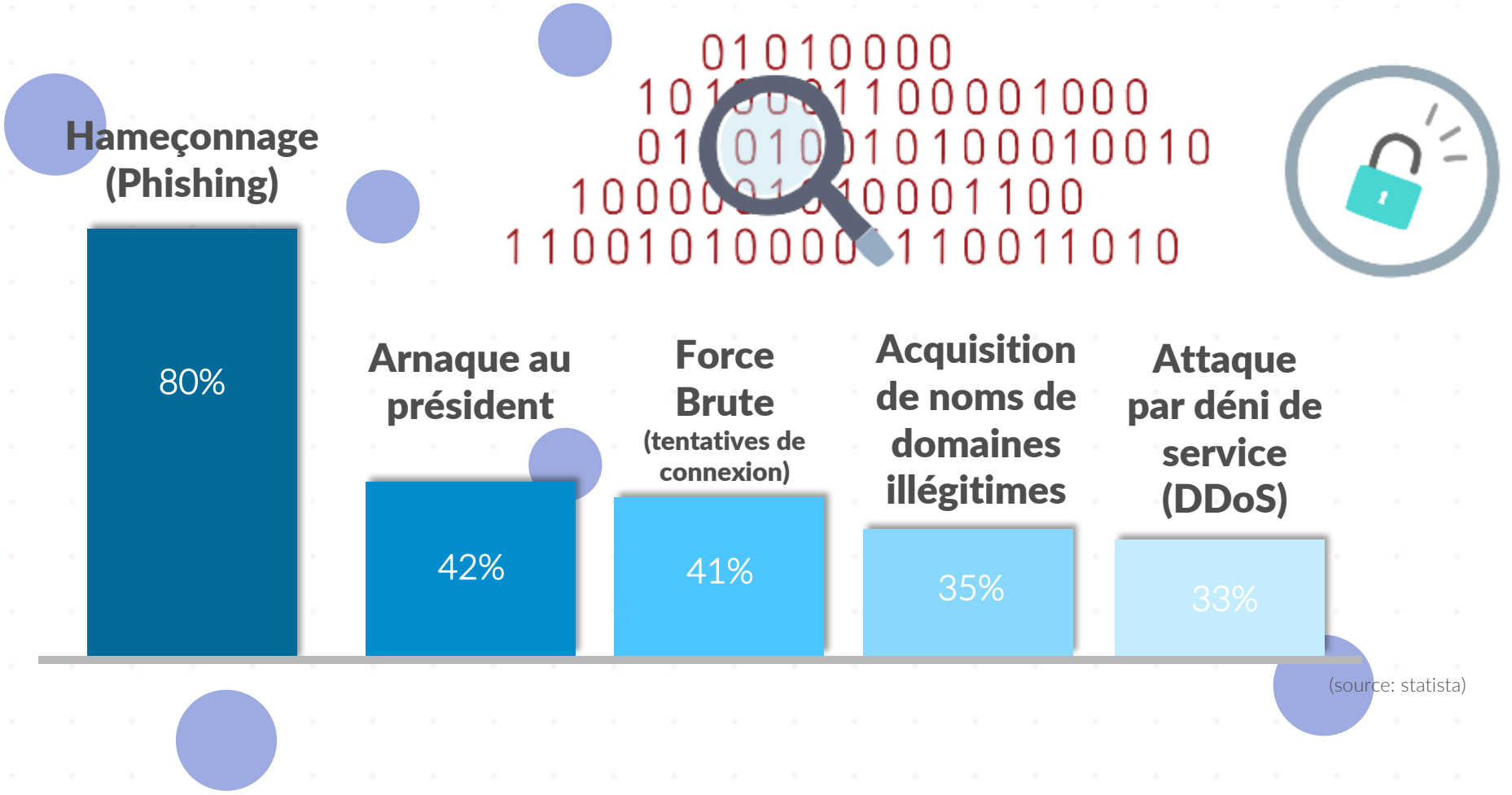
Outils de sécurité conventionnels
n'ont pas suivi le rythme

Les attaques se multiplient
plus sophistiquées

Paysage réglementaire
devenant plus complexe

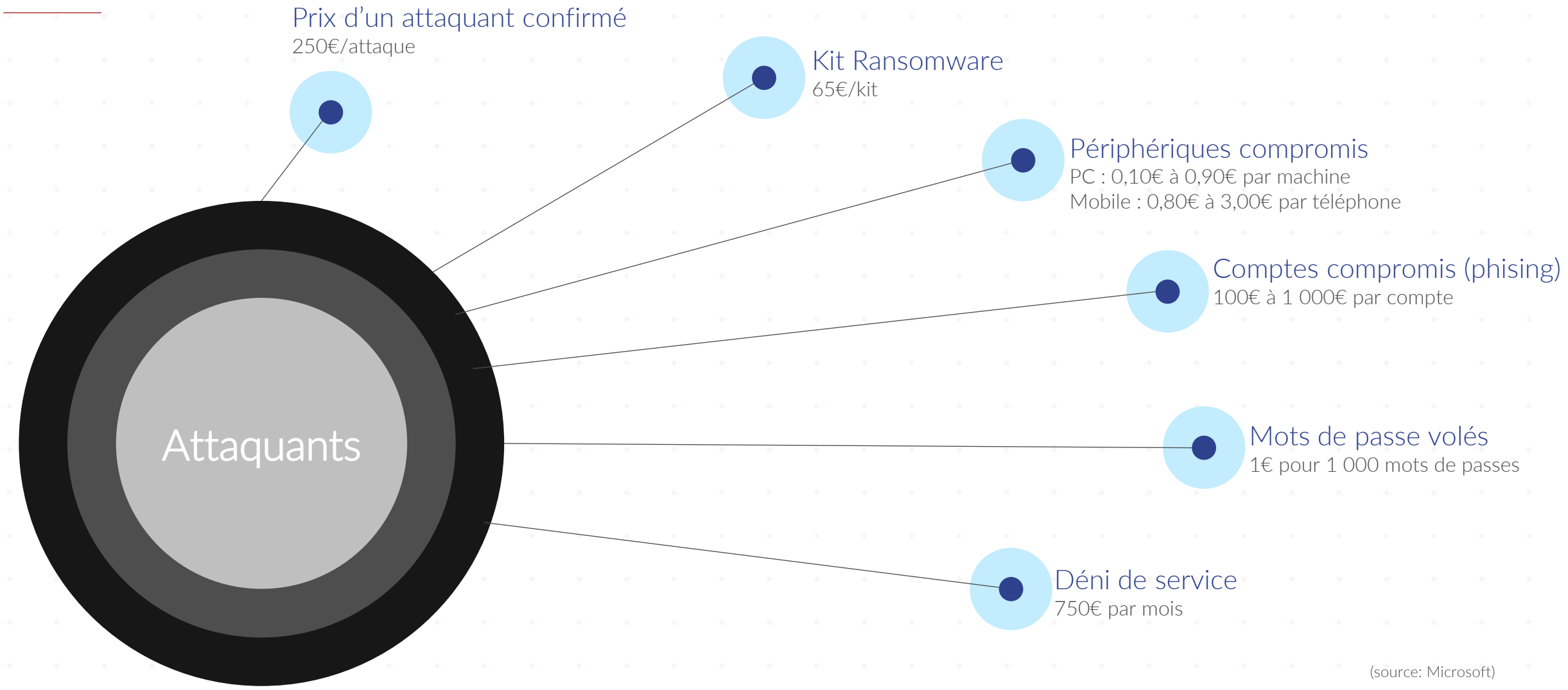
Les cyberattaques

Les plus courantes contre les entreprises en 2021



(source: statista)

Produits d'attaque en vente sur Internet



Prix d'un attaquant confirmé
250€/attaque

Kit Ransomware
65€/kit

Périphériques compromis
PC : 0,10€ à 0,90€ par machine
Mobile : 0,80€ à 3,00€ par téléphone

Comptes compromis (phising)
100€ à 1 000€ par compte

Mots de passe volés
1€ pour 1 000 mots de passes

Déni de service
750€ par mois

(source: Microsoft)

02. Defender for Endpoint

Protection contre les menaces

Cloud App Security

Étendre la protection et l'accès conditionnel à d'autres applications cloud (CASB)

Microsoft Defender for O365

Anti-phishing, pieces-jointes et liens sécurisés

Azure AD Premium Plan 1 and 2

Identity protection & accès conditionnel

Attaque par force brute ou utilisation d'identifiants volés

Exfiltration

L'attaquant accède aux données sensibles

L'attaquant collecte : **reconnaissance & données de configuration**

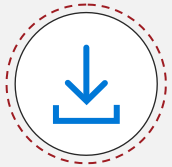
Phishing mail

Ouverture de pièce jointe

Clic sur un lien

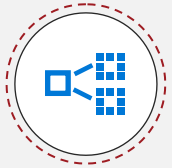
Parcours de site Web

Exploitation & Installation



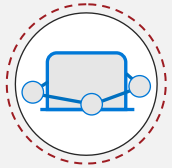
Commande & Contrôle

Compte utilisateur **compromis & persistant**



Tentative d'attaques **mouvement latéral**

Compte à privilège **compromis**



Domaine **compromis**

Endpoint Detection and Response (EDR)
Endpoint Protection (EPP)
Gestion des menaces et des vulnérabilités

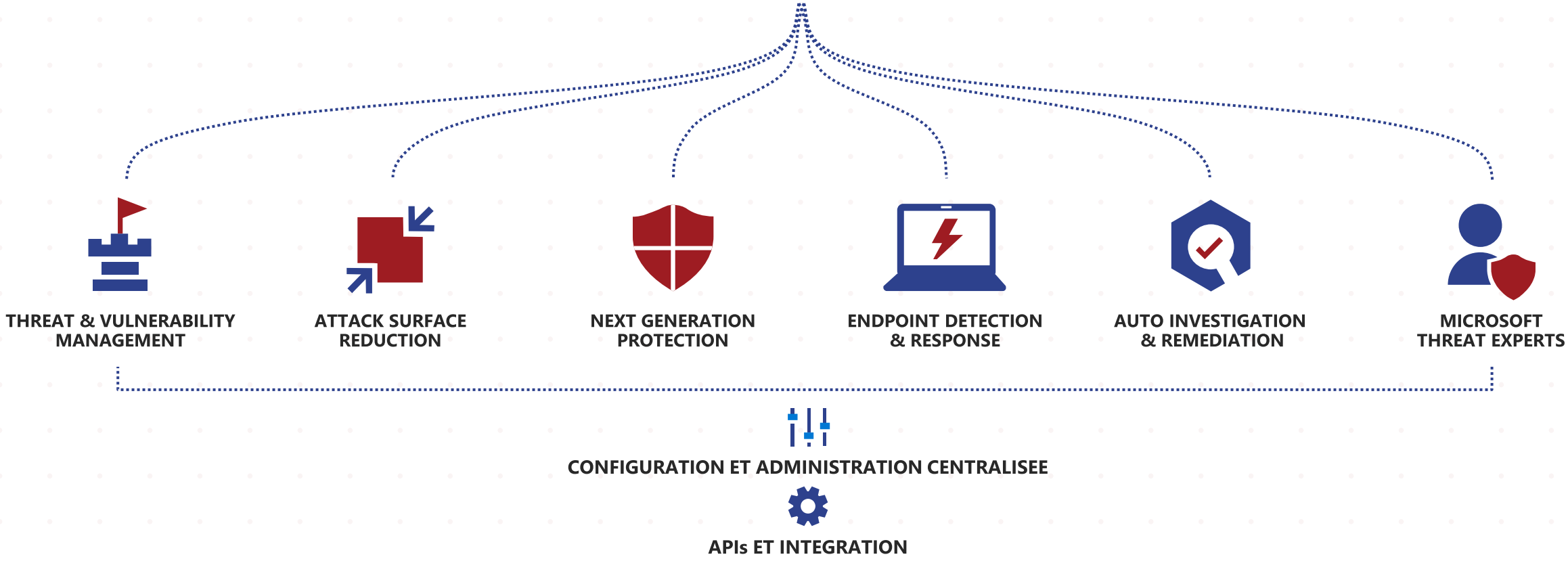
Microsoft Defender for Endpoint

Protection de l'Active Directory
Analyse du comportement des utilisateurs

Microsoft Defender for Identity

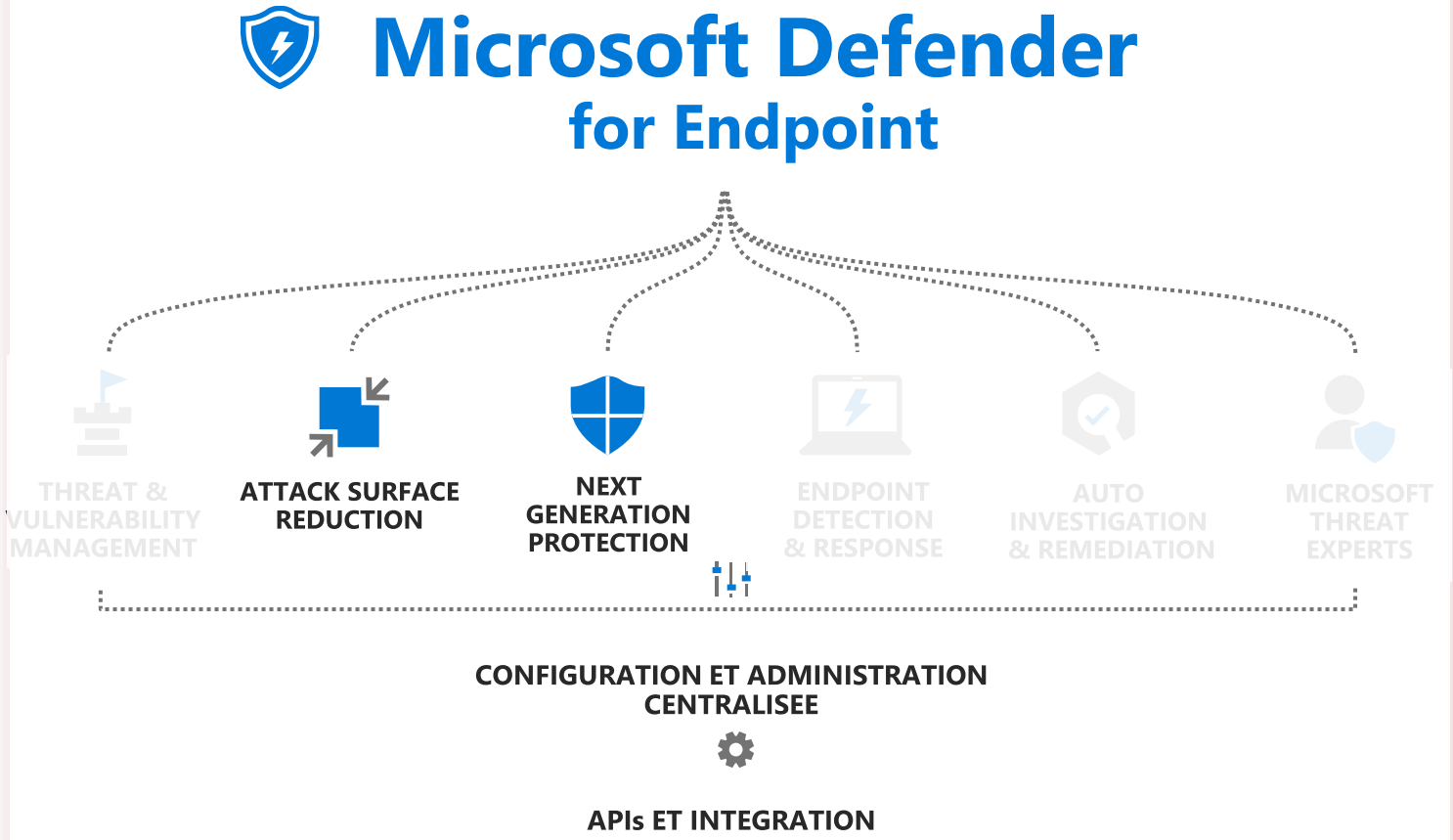
Projetlys
entreprise du groupe Blue Soft

Microsoft Defender
for Endpoint



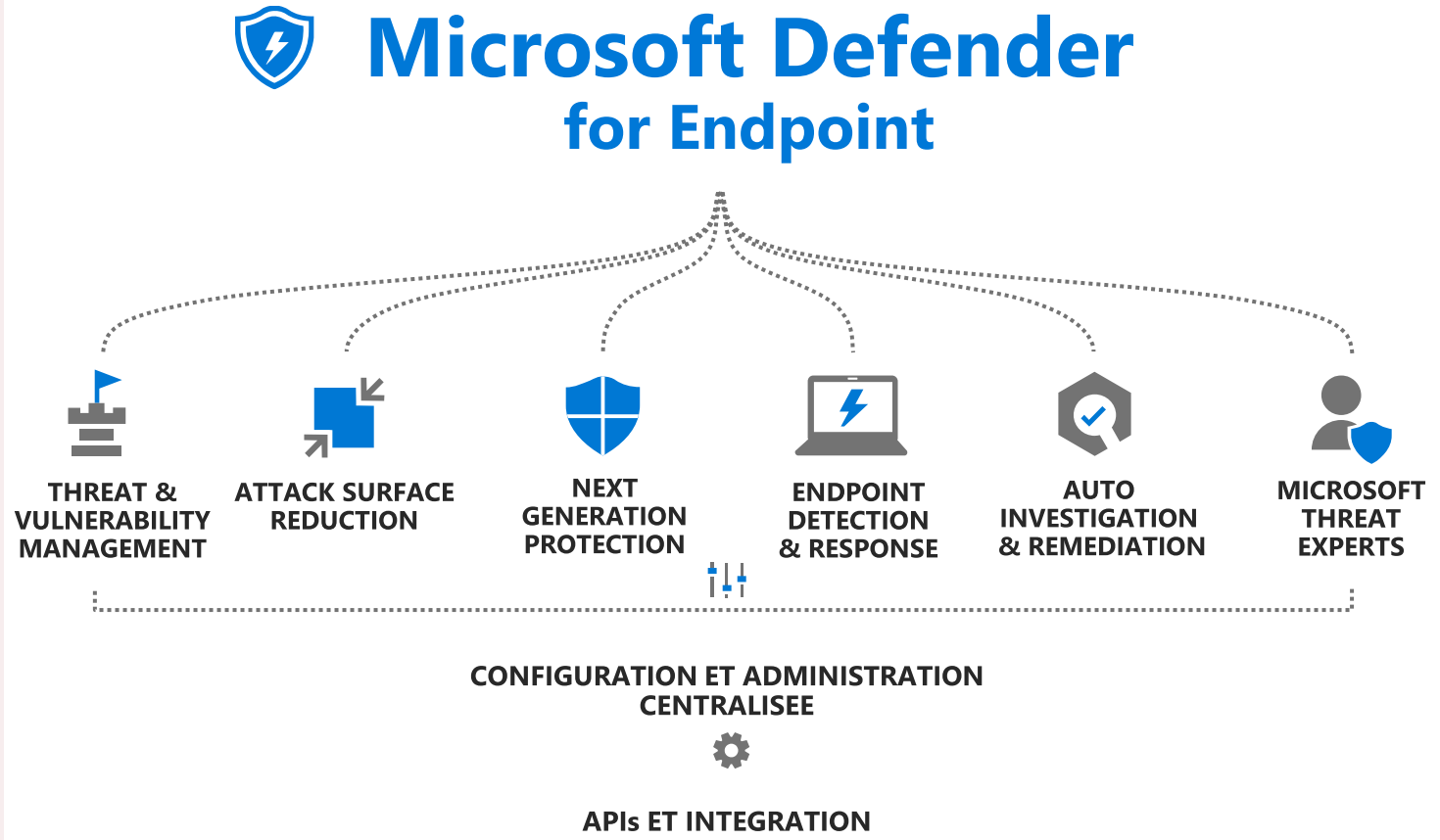
Defender for Endpoint Plan 1

Fonctionnalités inclues dans le Plan 1



Defender for Endpoint Plan 2

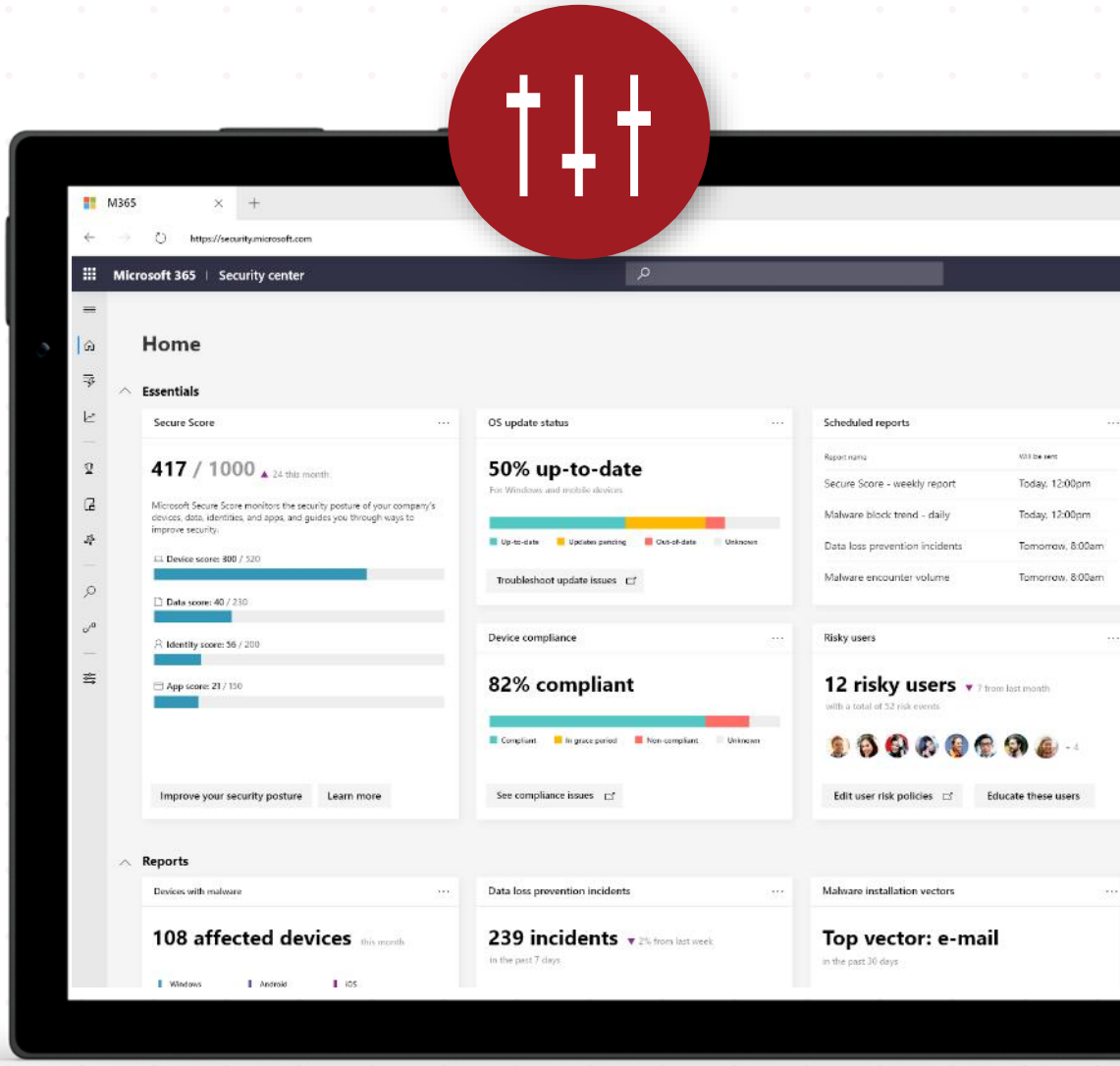
Fonctionnalités inclues dans le Plan 2



Gestion de la sécurité

Analyse, configure et répond aux changements dans l'environnement

- Analyse et gestion centralisée de la sécurité
- Une multitude de rapports et dashboards pour un monitoring et une visibilité détaillée
- Integration totale des outils (analyse des menaces et déploiement des strategies)

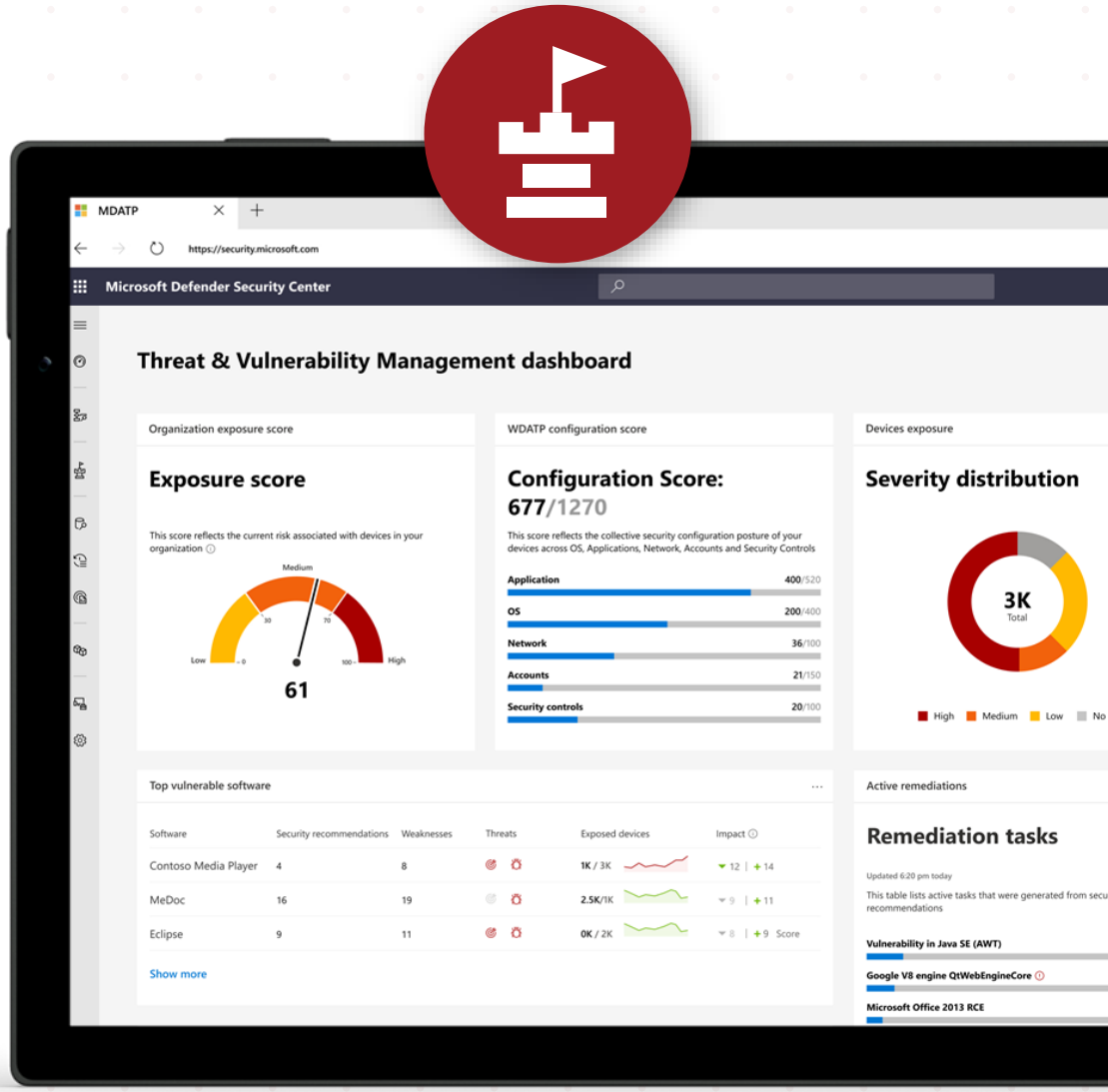


Projetlys
entreprise du groupe Blue Soft

Gestion des menaces et des vulnérabilités

Une approche basée sur le risque pour évaluer le niveau de gestion

1. Découverte en temps réel
2. Priorisation en fonction du contexte
3. Process de remediation construit de bout en bout



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

Projetlys
entreprise du groupe Blue Soft

Réduction de la Surface d'Attaque

Éliminer les risques en réduisant la surface d'attaque

- Durcissement du système, sans interruption
- Personnalisation adaptée à votre organisation
- Visualisez l'impact et activez-le simplement

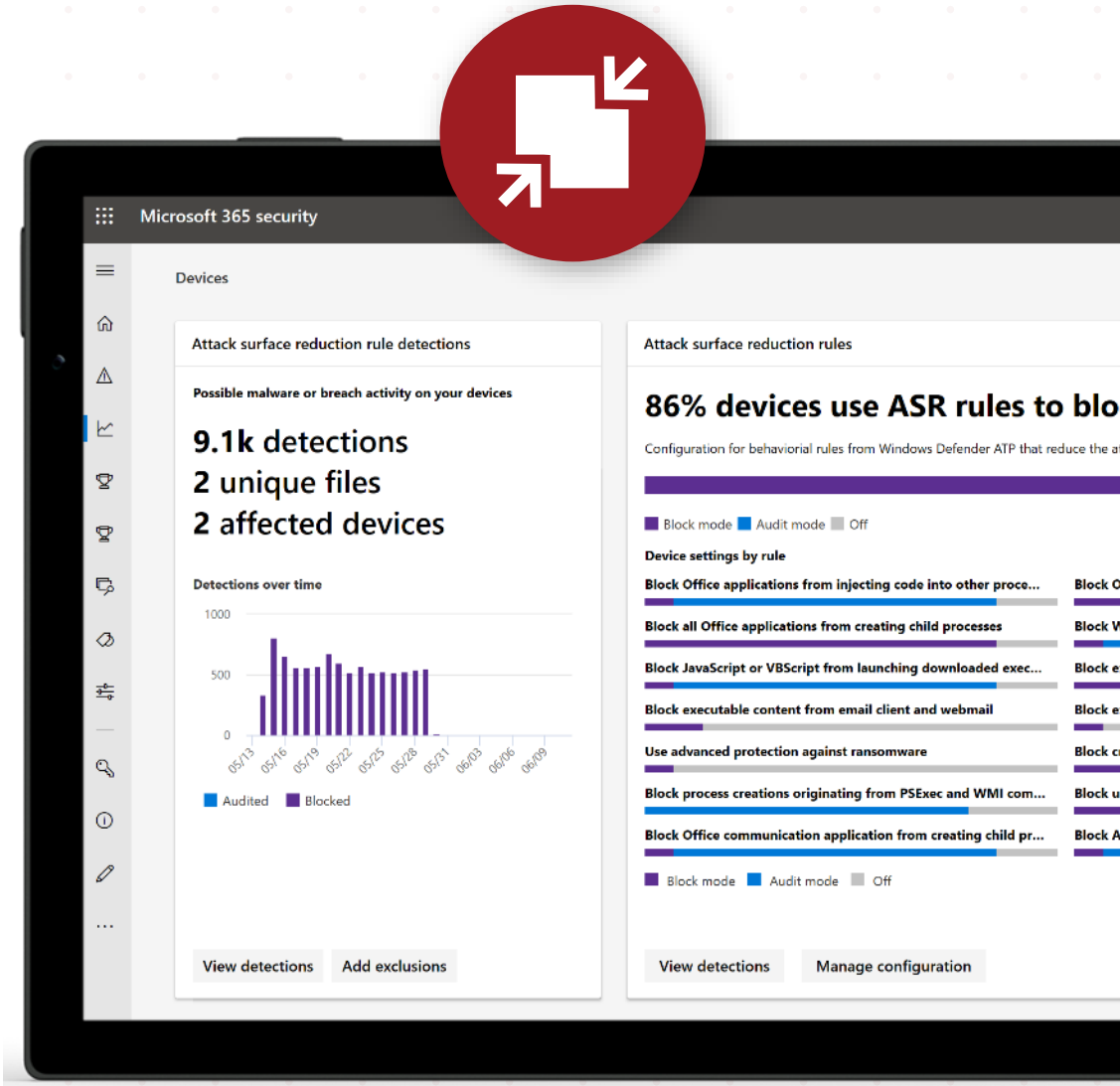
THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

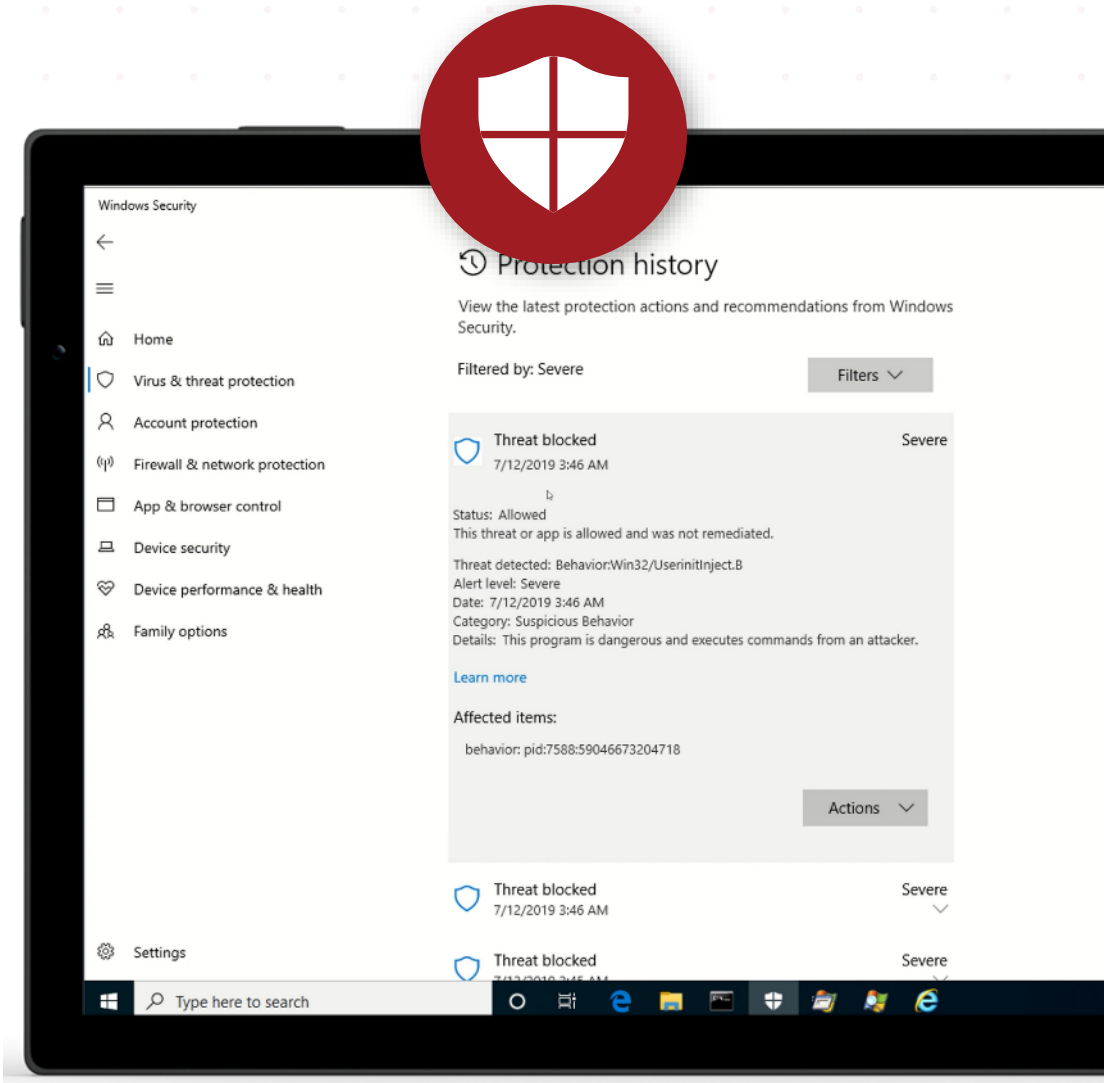


Projetlys
entreprise du groupe Blue Soft

Protection Next Generation

Bloque et s'attaque aux menaces sophistiquées et aux logiciels malveillants

- Protection comportementale en temps réel
- Bloque les logiciels malveillants
- Arrête les activités malveillantes provenant d'applications fiables et non fiables



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

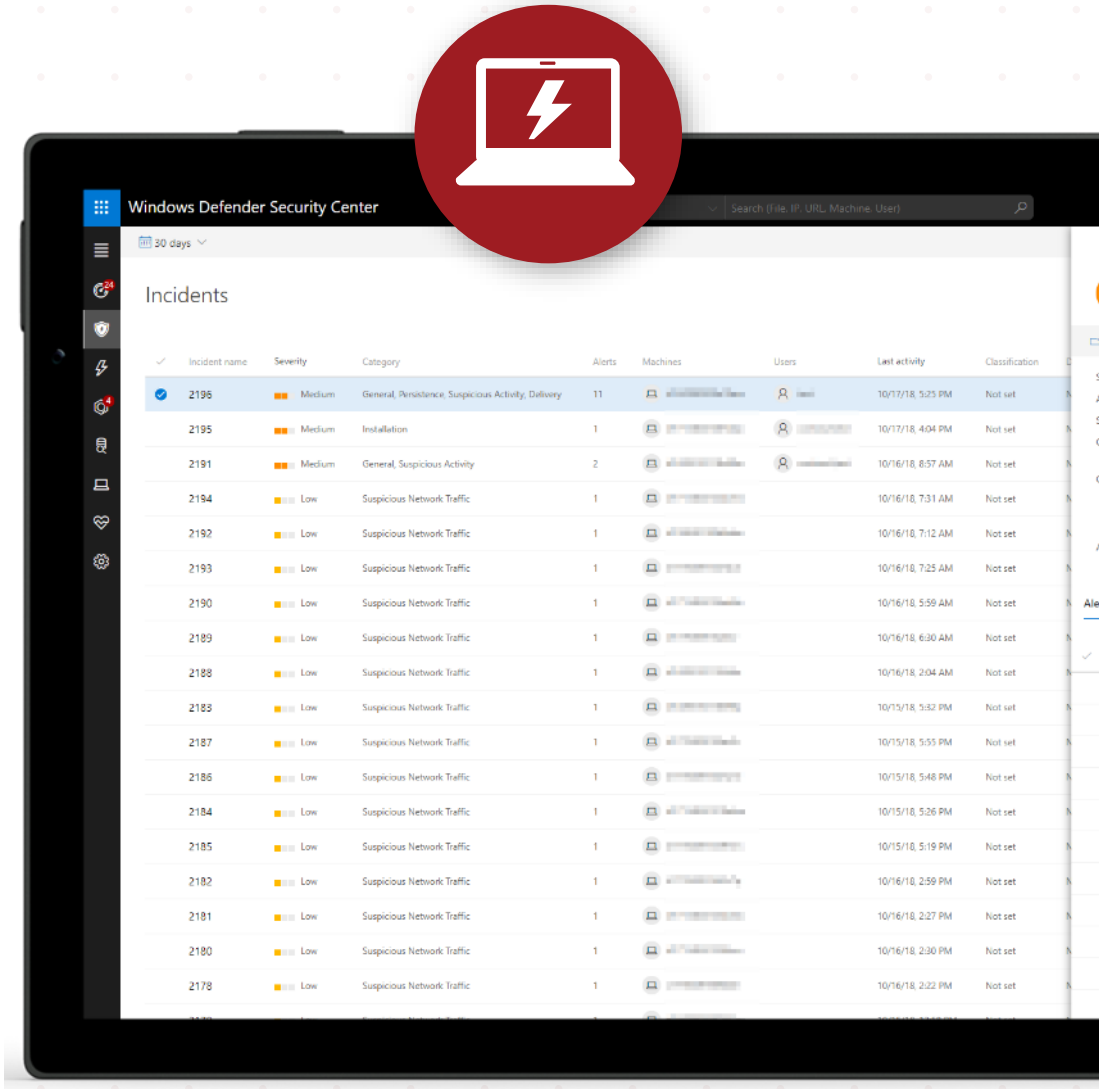
AUTO INVESTIGATION & REMEDIATION

Projetlys
entreprise du groupe Blue Soft

Endpoint Detection & Response

Détection et analyse avancée des attaques

- Correlation des alertes
- Investigation et “chasse” (Hunting)
- Variété étendue d’actions de rémédiation



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

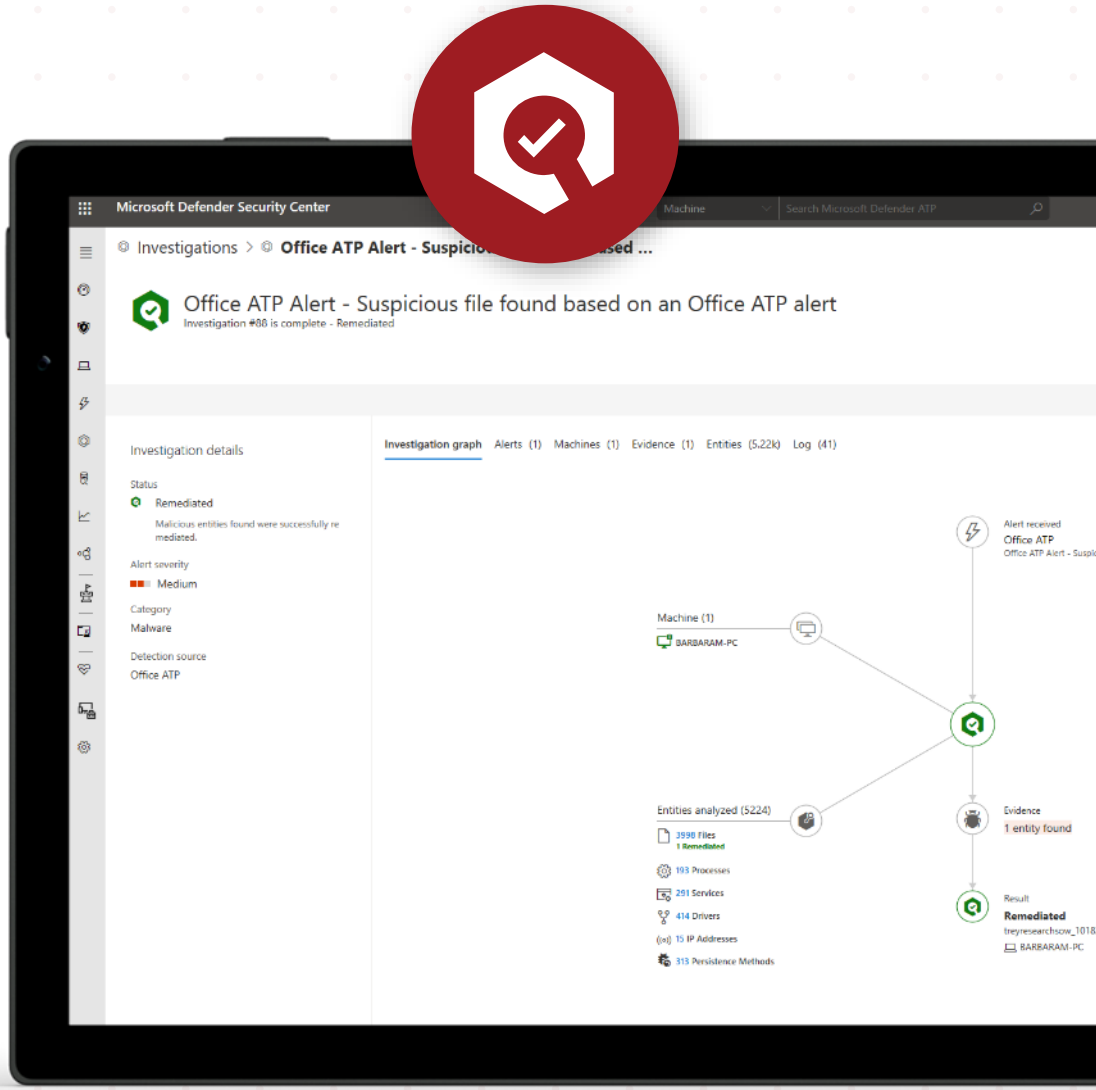
AUTO INVESTIGATION & REMEDIATION

Projetlys
entreprise du groupe Blue Soft

Auto Investigation & Remediation

Investigation automatique des menaces complexes en quelques minutes

- Reproduit les actions qu'un analyste ferait
- Gère les attaques par fichiers et attaques basées sur la mémoire
- Fonctionne en 24x7, sans limitation de capacité



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

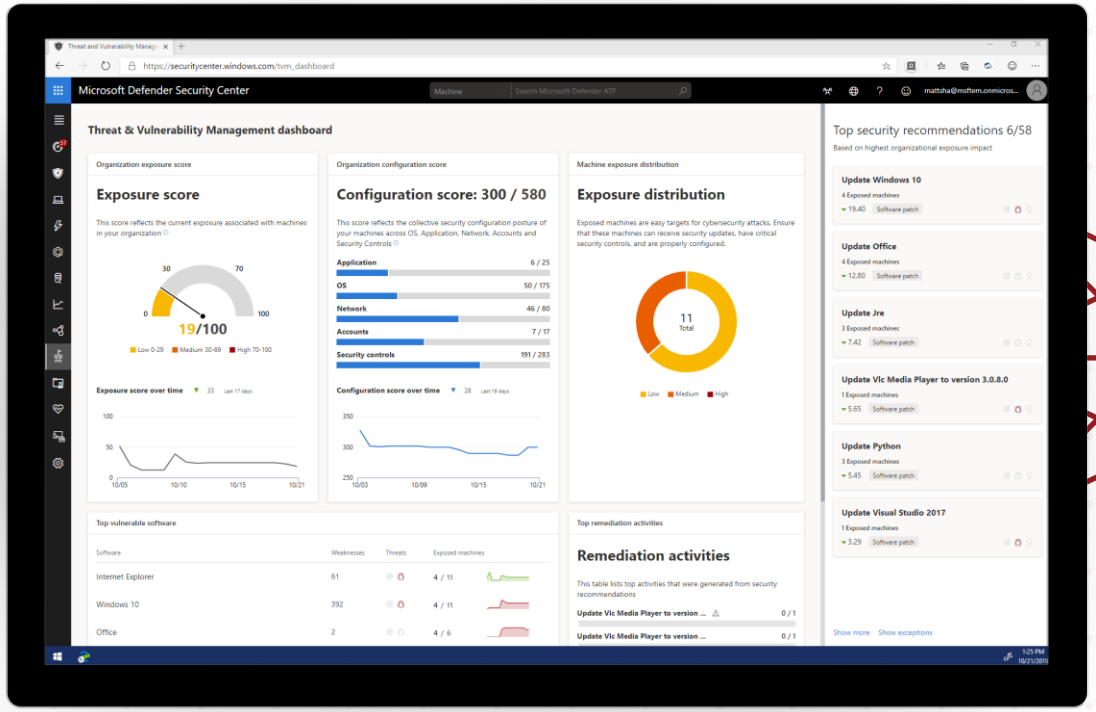
NEXT GENERATION PROTECTION

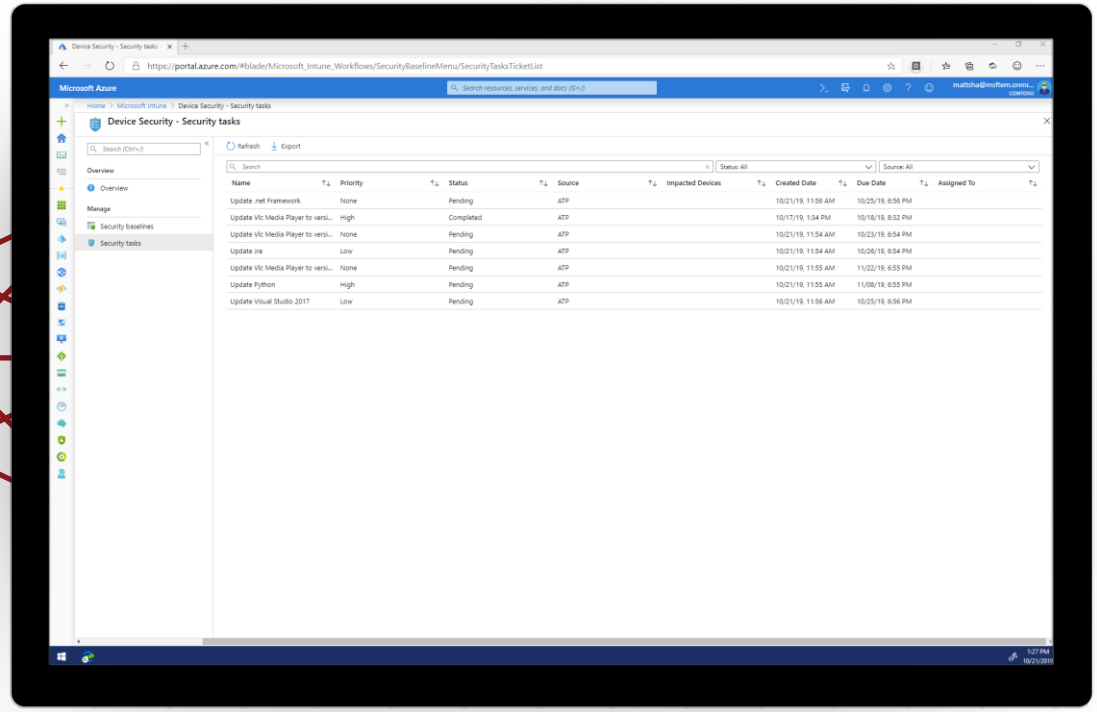
ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

Projetlys
entreprise du groupe Blue Soft

Totalement intégré à l'écosystème de gestion des terminaux





Microsoft Defender for Endpoint

Evaluation des menaces

Microsoft Endpoint Manager

Application des stratégies

03.
Déploiement poste utilisateurs et serveurs

Projetlys
entreprise du groupe Blue Soft

Onboarding des machines

L'intégration des machines à Defender for Endpoint se nomme « onboarding » ou « intégration ».

Windows Defender se *connecte* à Defender for Endpoint et remonte les données d'investigation des machines vers Microsoft Azure.

Intégration des Clients :

Windows 10 + :

+ Par Script
+ Par GPO (via fichier d'onboarding)
+ Par Microsoft Intune
+ Par SCCM

MacOS :

+ Par Script
+ Par Microsoft Intune

Intégration des Serveurs :

Windows Serveur 1809 et supérieur :

+ Par Script (pour test)
+ Par GPO (via fichier d'onboarding)
+ Par Microsoft Intune
+ Par SCCM

Windows Serveur 2012^{R2} et 2016 :

+ Par Script (pour test)
+ Par GPO (mdw4s.msi + onboarding)
+ Par SCCM

Windows Serveur 2008$^{R2\ sp1}$ et 2012 :

+ Par Script (pour test)
+ Par GPO (Microsoft Monitoring Agent)
+ Par SCCM

Linux :

+ Par Script

Configuration de Microsoft Defender for Endpoint

Après avoir intégré des machines, il faut configurer l'agent.

Configuration des Clients :

Windows 10 + :

+ Par Script Powershell
+ Par GPO
+ Par Microsoft Intune
+ Par SCCM

MacOS :

+ Par Script
+ Par Microsoft Intune

Configuration des Serveurs :

Windows Serveur 2012R2 et supérieur :

+ Par Script Powershell
+ Par GPO
+ Par Microsoft Intune
+ Par SCCM

Linux :

+ Déploiement de fichiers de config (via Ansible ou tout autre outil de déploiement)

04. Déploiement périphériques mobile

Projetlys
entreprise du groupe Blue Soft

Onboarding des périphériques mobiles et configuration de Microsoft Defender for Endpoint

L'intégration des machines à Defender for Endpoint se nomme « onboarding » ou « intégration ».

Windows Defender se *connecte* à Defender for Endpoint et remonte les données d'investigation des machines vers Microsoft Azure.

Intégration des Clients :

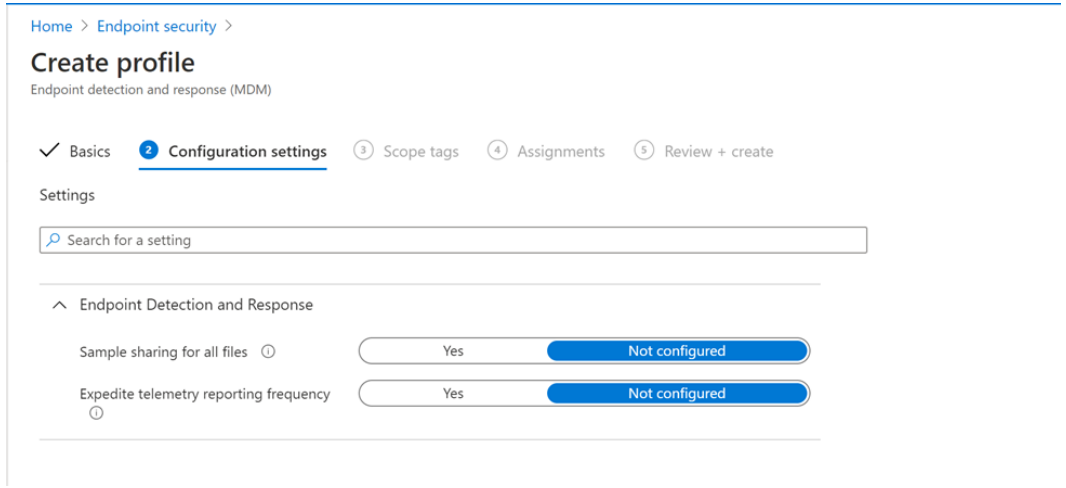
iOS et Android :

+ Par Microsoft Intune (via application)

Configuration de l'agent

iOS et Android :

+ Par Microsoft Intune (via application)



Recommandations

Nos recommandations de configuration

- **Postes utilisateurs**
- **Serveurs**
- **Périphériques mobiles**

Configuration des paramètres « de base » de Defender (Scans et fréquence, exclusions, mises à jour de l'agent et des définitions)

Configuration des « Règles de Réduction de Surface d'Attaque » (ASR)

Activation des fonctionnalités de sécurité basés sur la virtualisation

Renforcement de la sécurité des Endpoints (via Baseline de sécurité ou via référentiel)

Comparaison des paramètres de sécurité avec les référentiels publics (ex: CIS)

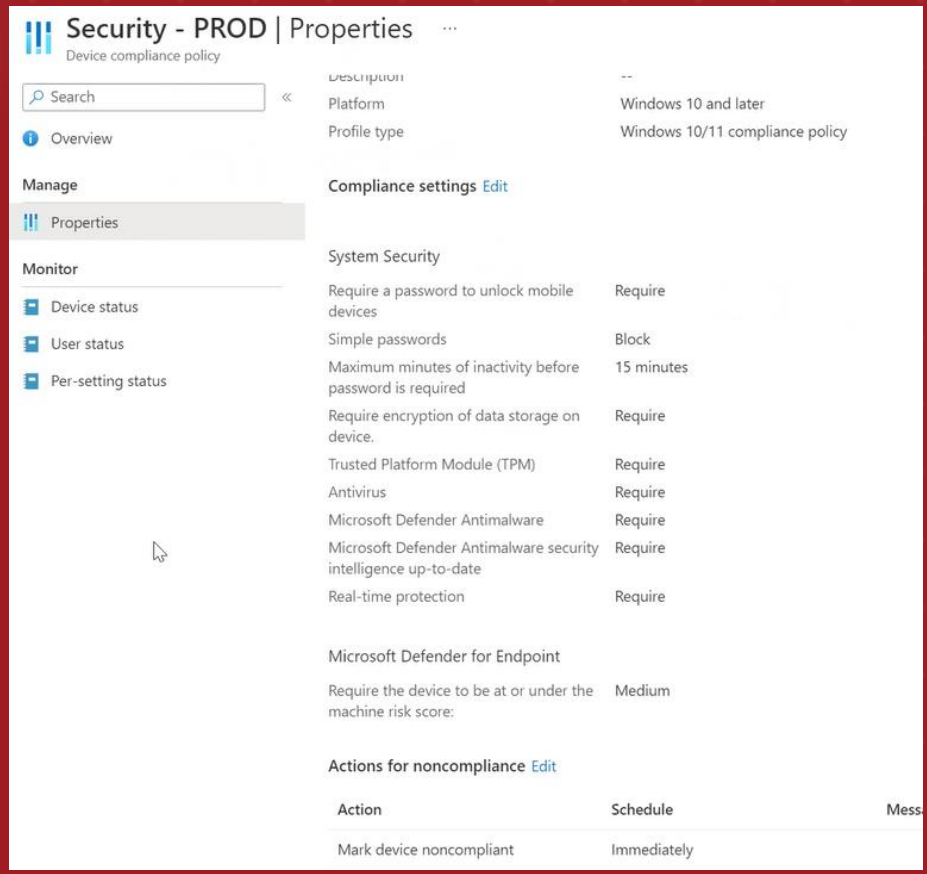
Activation du « filtrage web »

Nos recommandations pour la conformité des périphériques

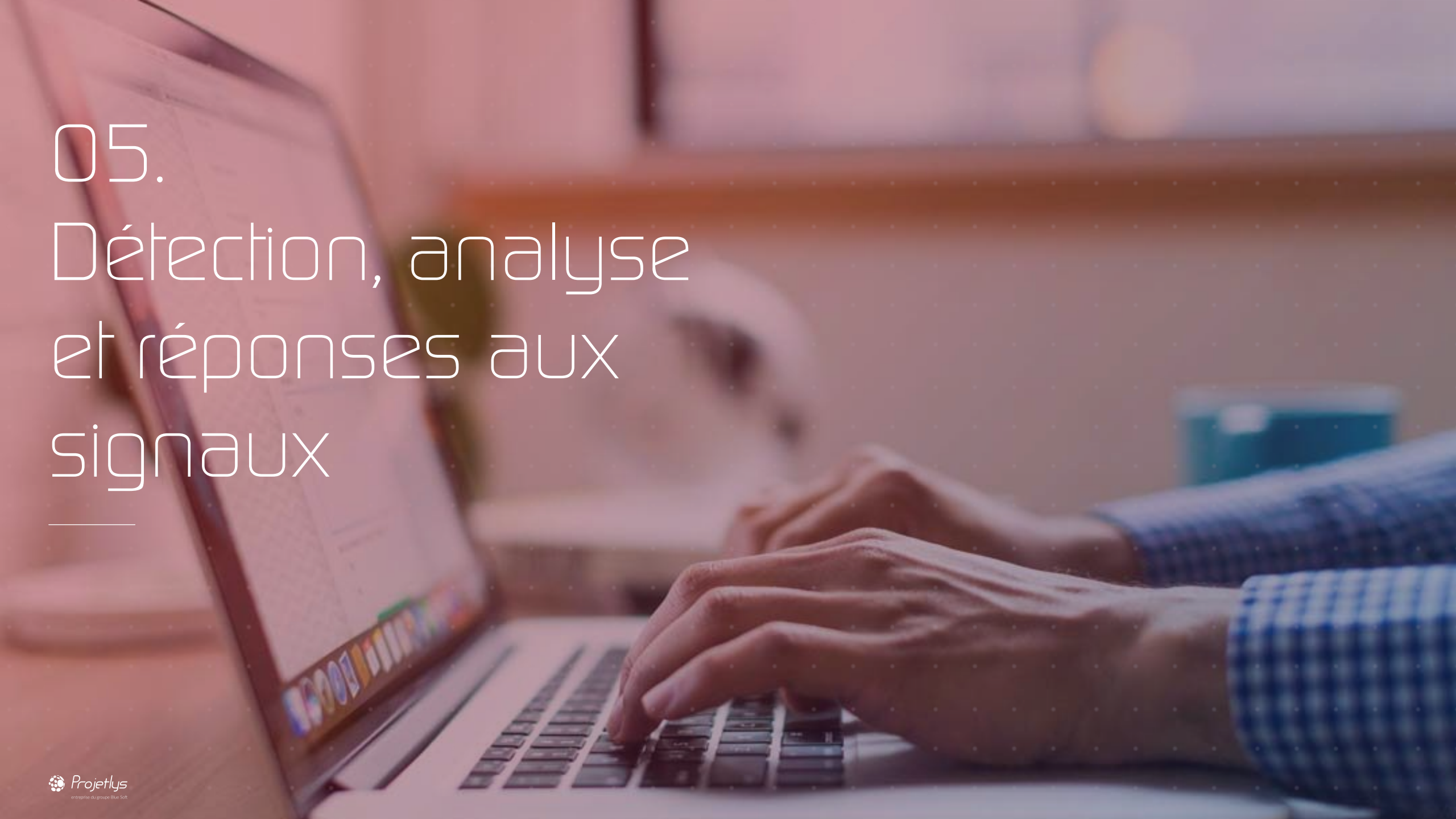
Création d'une stratégie de conformité basée sur le « niveau de risque » des périphériques

En plus : ajouter à la stratégie de conformité les paramètres relatifs à Defender (Présence de Defender, protection en temps réel activée, définitions à jour)

Créer une stratégie d'accès conditionnel pour refuser l'accès aux données de l'entreprise depuis une machine « à risque » (basée sur la conformité des périphériques)



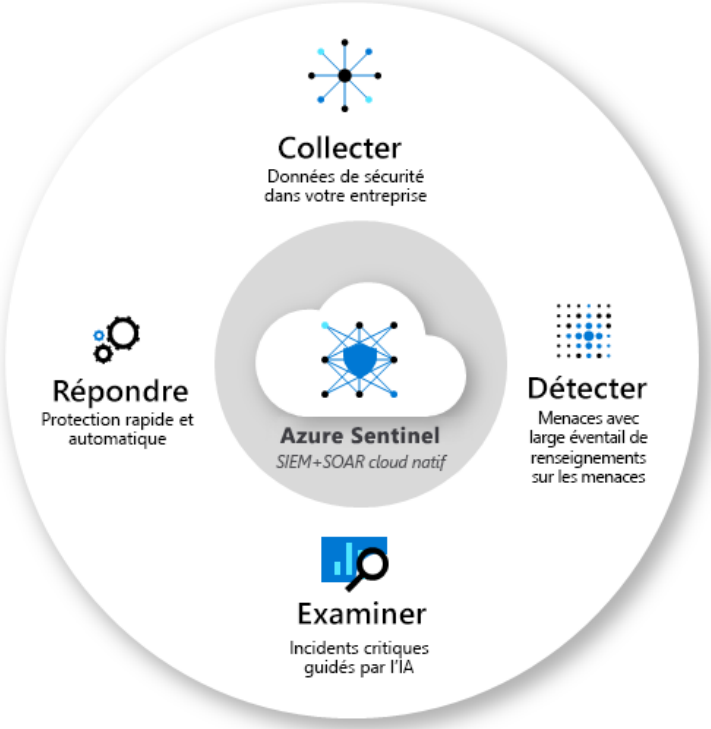
05.
Détection, analyse et réponses aux signaux



Azure Sentinel

SIEM (Security Information and Event Management)

SOAR (Security Orchestrated Automated Response)



Solution « SOC » de bout en bout

Collecte

Visibilité

Détection

Analytique
Analytics

Chasse
Hunting

Investigation

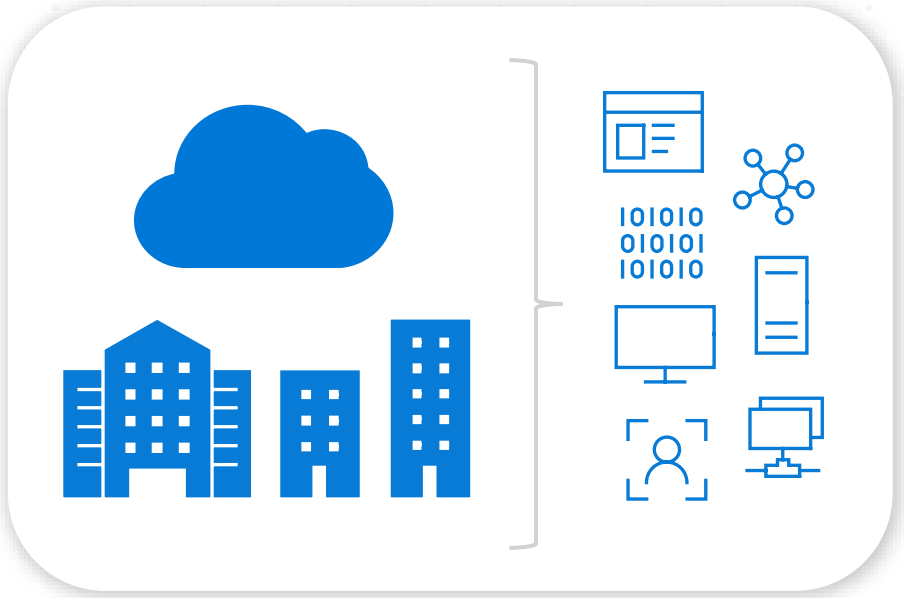
Incidents

Réponse

Automatisation

Communauté + experts sécurité Microsoft

Collecte : n'importe quelle source, à l'échelle du cloud



AZURE + MICROSOFT 365
Security Alerts, Activity Data

COLLECTORS
CEF, Syslog, Windows, Linux

TAXII + MS Graph
Threat Indicators

APIs
Custom Logs

AZURE SENTINEL

AZURE MONITOR LOG ANALYTICS

06. Accompagnement des utilisateurs à la cybersécurité

Projetlys
entreprise du groupe Blue Soft

L'adoption des bonnes pratiques de sécurité passe en premier lieu par de la **sensibilisation**

Sensibilisation
aux enjeux de la cybersécurité à l'échelle de l'entreprise

Volonté
de changer, pourquoi est-ce important de me protéger y compris à titre individuel, quels sont les risques encourus à ne pas le faire

Apprentissage
des bonnes pratiques en matière de cybersécurité, Posture à adopter face à une menace

Capacité
à mettre en œuvre les bonnes pratiques en matière de cybersécurité et comportement requis quelque soit l'environnement dans lequel je me trouve

Ancrage
des bonnes pratiques dans le temps et évolution de mon comportement en fonction des nouvelles menaces

Sensibilisation des utilisateurs

LIVRABLES PEDAGOGIQUES

Mise à disposition de
4 fiches « Bonnes pratiques »

CAMPAGNE DE SENSIBILIATION

1 newsletter général et 10
« flashsécu' » à envoyer

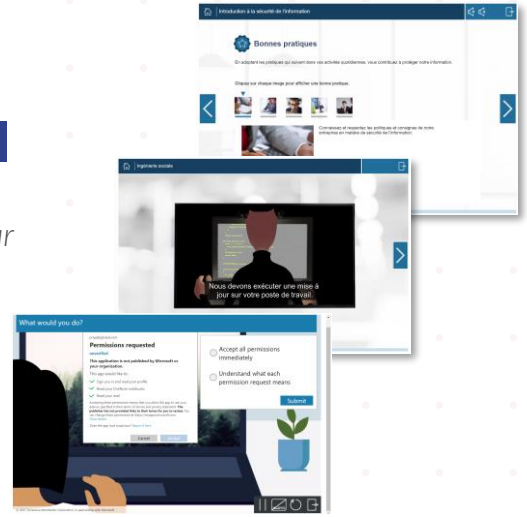
WEBINAIRES D'INFORMATION

3 webinars d'information à distance avec l'ensemble des utilisateurs sur les enjeux, les risques, les retours des campagnes et les bonnes pratiques à adopter

Quizz final

MODULES DE FORMATION

Tutoriels vidéos interactifs
Livrables existants disponibles sur Microsoft Defender
(26 modules disponibles)



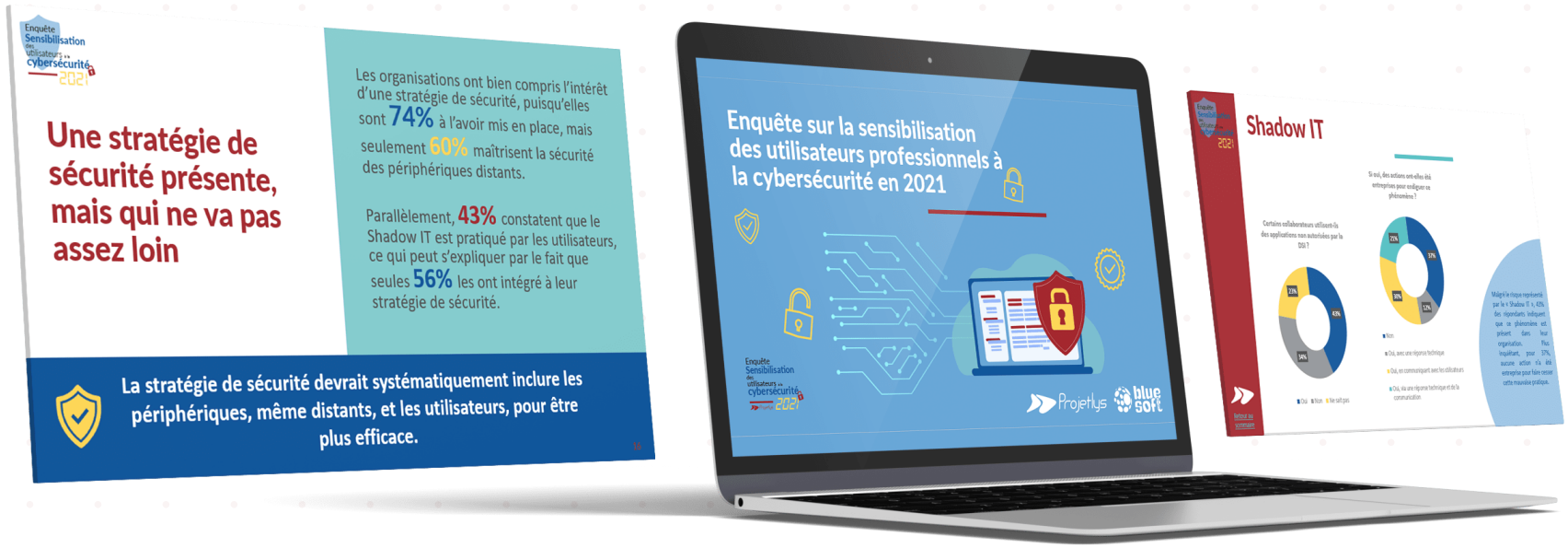
ATELIERS « Usages »

Travailler avec une équipe sur leurs pratiques à risques, proposer des solutions plus sécurisées
OPTION

Enquête sur la sensibilisation des utilisateurs à la cybersécurité

Cette enquête couvre :

- la stratégie de sécurité déployée
- les types de cyberattaques subies et la période
- le rôle des utilisateurs dans la lutte contre les cyberattaques
- les actions de sensibilisation menées
- les statistiques par secteur (privé, public, santé)
- les tendances et les conclusions



Projetlys
entreprise du groupe Blue Soft

Projetlys
entreprise du groupe Blue Soft

Projetlys

entreprise du groupe Blue Soft

Merci !

www.bluesoft-group.com

www.projetlys.com

blue soft