tv

Le live !

Un webinar by koesio

Le SOC en service managé de Sophos

# L’atout sécurité, à la portée de votre entreprise

SOPHOS koesio

# Intervenants

## Joris DI MARCANTONIO

Sales Engineer

Sophos

## David PIROCCHI

Directeur Technique Régional

Koesio Corporate IT

© Koesio Corporate IT tous droits réservés

tv

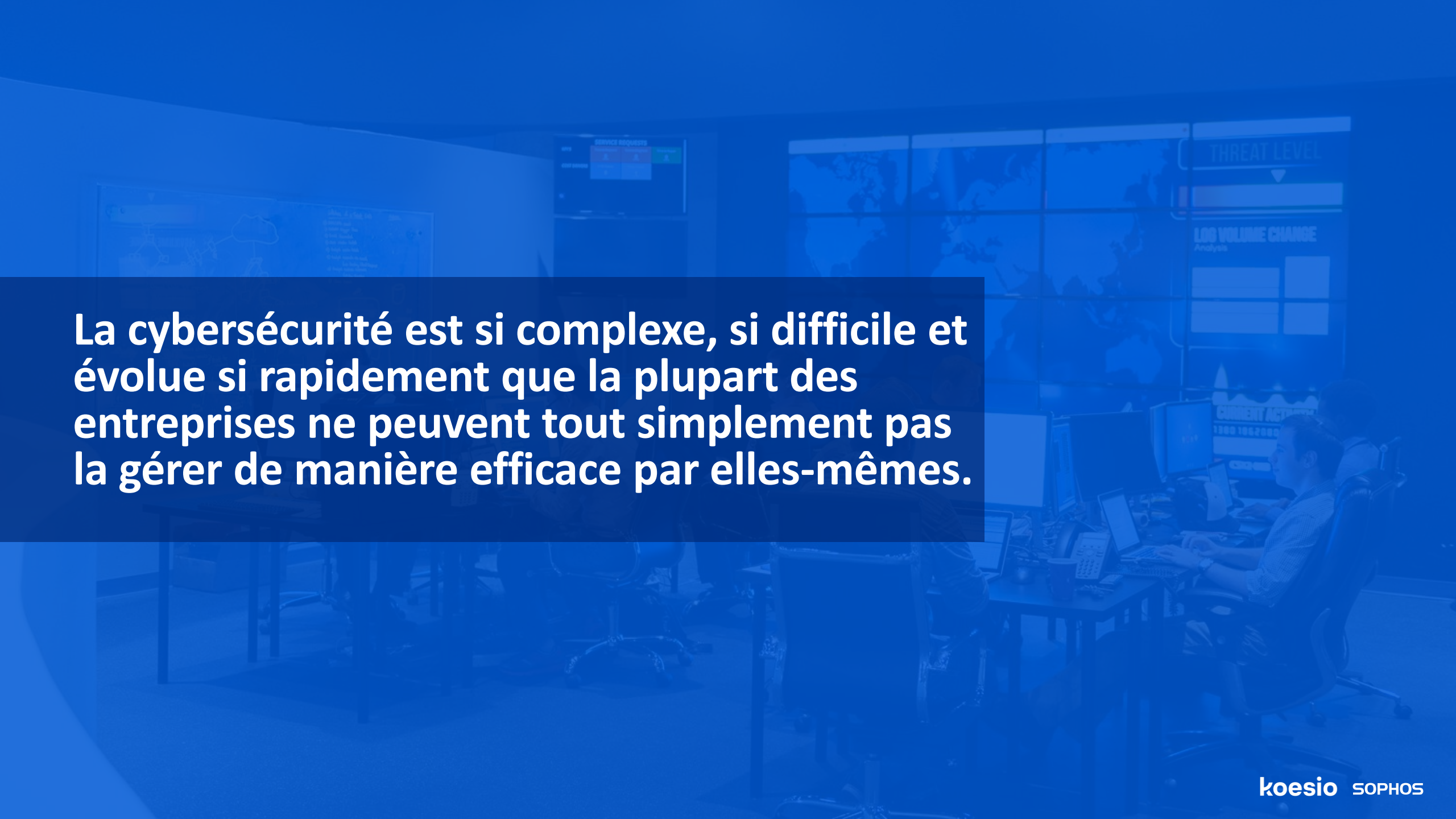
Le live !

Un webinar by koesio

Le SOC en service managé de Sophos

# L’atout sécurité, à la portée de votre entreprise

SOPHOS koesio




**La cybersécurité est si complexe, si difficile et évolue si rapidement que la plupart des entreprises ne peuvent tout simplement pas la gérer de manière efficace par elles-mêmes.**

koesio SOPHOS

# L’état de la cybersécurité pour les entreprises

# Les ransomwares sont la menace numéro un

**63 %**

des entreprises ont été touchées par ransomware en 2022

**1,66 M $**

coût moyen pour les entreprises pour remédier à l'impact de ransomware

Source : L'état des ransomwares 2023, Sophos Enquête indépendante menée auprès de 3 000 professionnels de l'informatique, dont 272 issus de entreprises (100 et 250 employés).

# Les entreprises sont particulièrement vulnérables

## Manque de ressources et d'expertise

Classé l'un de leurs **trois principaux risques de sécurité** par les entreprises[1]

Les opérations de sécurité 24/7 **nécessitent généralement 5 ou 6 employés** au minimum

Le coût moyen de maintenance d'un SOC est de **près de 3 M$**[2]

## Complexité des technologies de cybersécurité

**La mauvaise configuration des outils de sécurité** est considérée **comme le premier risque de sécurité** pour les entreprises[1]

En moyenne, une entreprise dispose de plus **de 46 outils de surveillance de la cybersécurité**

Les entreprises enquêtent **sur 48 % de leurs alertes de sécurité** pour détecter des signes d'activité malveillante[1]

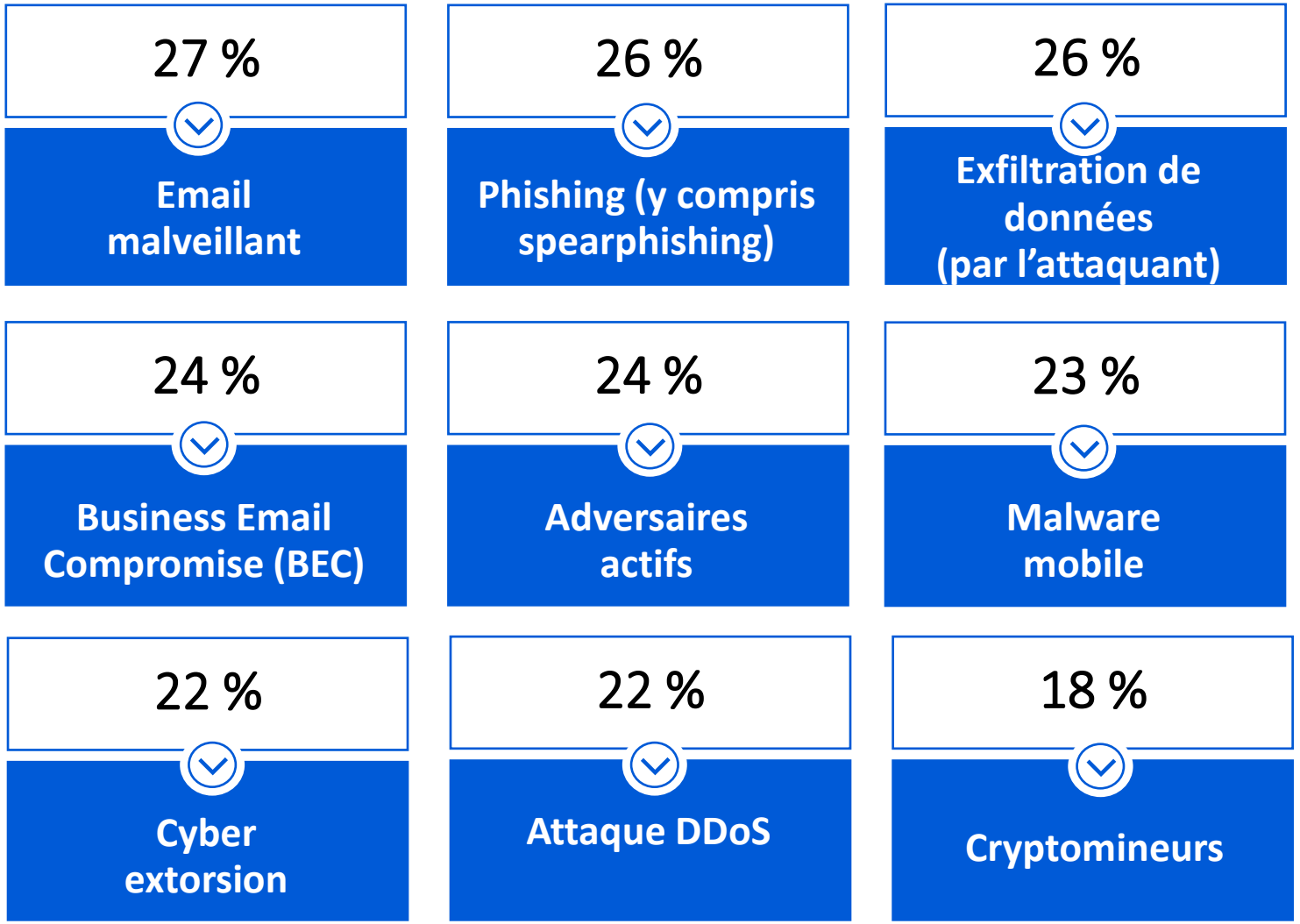
[1] *L'état de la cybersécurité en 2023 : L'impact commercial des adversaires, Sophos*

[2] *Ponemon Institute : « The Economics of Security Operations Centers: What Is the True Cost for Effective Results? »*

koesio SOPHOS

# Les entreprises sont confrontées à un large éventail de menaces

**L'année dernière, 90% des entreprises ont subi au moins une cyberattaque**




Source : L'état de la cybersécurité en 2023 : L'impact commercial des adversaires, Sophos. Enquête indépendante menée auprès de 3 000 professionnels de l'informatique, dont 271 issus de entreprises (100 et 250 employés).

koesio SOPHOS

# Managed Detection and Response (MDR)

Un service entièrement managé, disponible 24 h/24 et 7 j/7, fourni par des experts spécialisés dans la détection et la réponse aux cyberattaques que les solutions technologiques seules ne peuvent empêcher.

koesio SOPHOS

# Humain + Intelligence Artificielle = MDR

## Outils de détection et de réponse sur les terminaux

1. InterceptX avec XDR
Surveille les menaces

2. Intelligence Artificielle priorise les activités suspectes

3. Les activités néfastes sont automatiquement stoppées

## Analystes de menaces et réponses effectuées par des experts

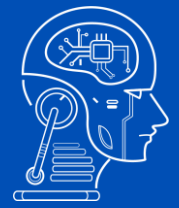
4. Un humain analyse les évènements suspects

5. Une traque des menaces est conduites pour en découvrir de nouvelles

6. Des experts interviennent pour neutraliser les menaces.

# Pourquoi associer les humains et les machines ?

## Intelligence Artificielle



Traiter rapidement d’énormes quantités de données pour détecter les activités potentiellement malveillantes

Effectue des corrélations en fonction de comportements couramment associés à une activité malveillante

Effectue des actions automatiques presque en temps réel pour bloquer ou mettre fin aux activités malveillantes confirmées (signaux forts)

Formule des conclusions en se basant sur les données précédemment introduites dans le système

## Intelligence Humaine

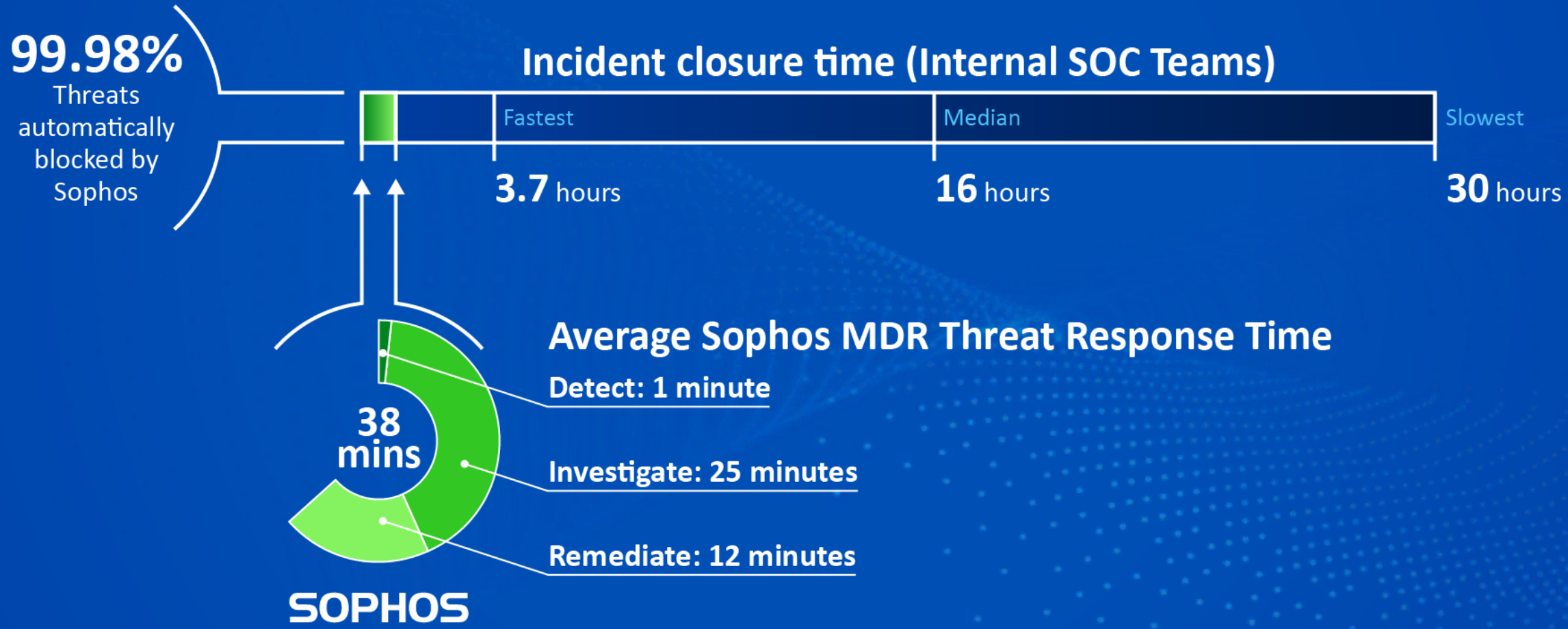
Utilise des techniques d'enquêteur(s) pour déterminer si une activité suspecte est malveillante ou bénigne

Adapte sa stratégie d’investigation en fonction des motivations de l’attaquant (type de données, type d’entreprises etc..)

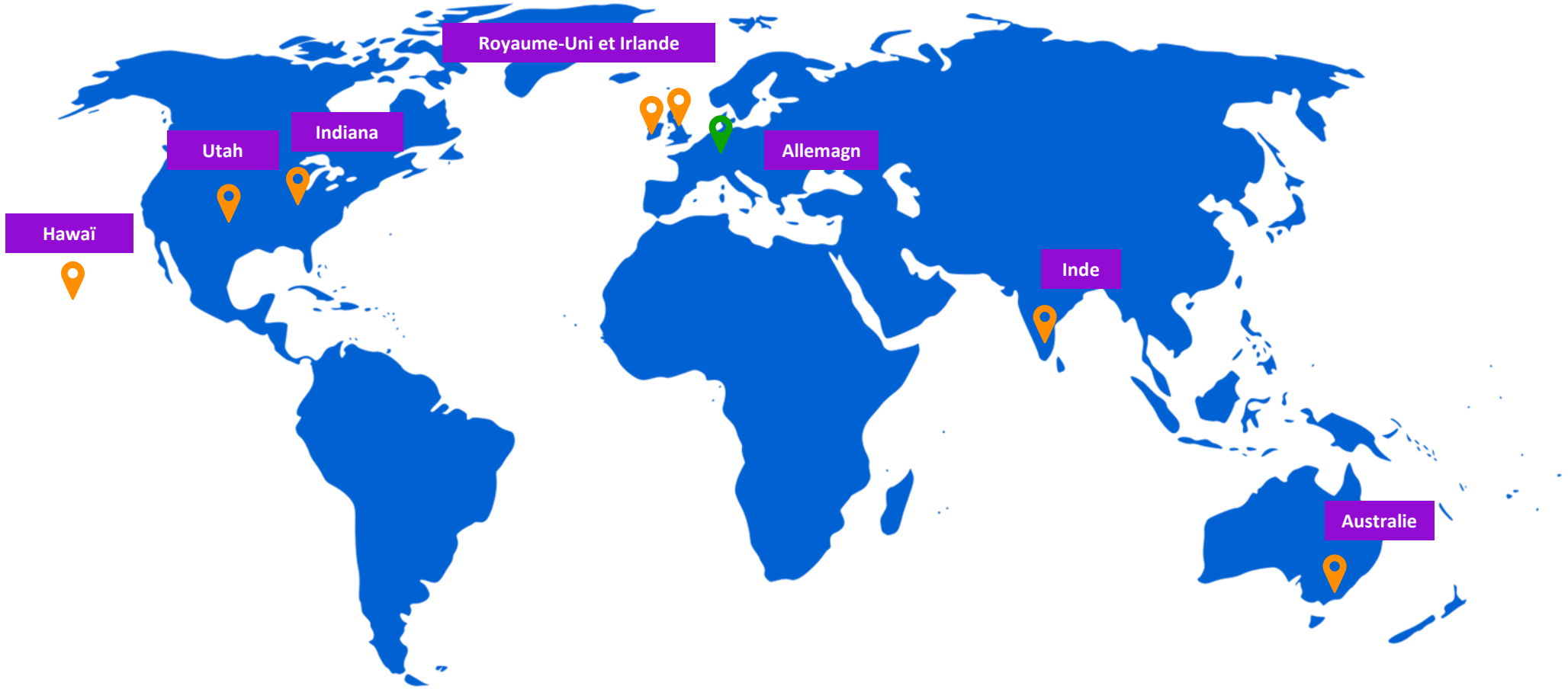
Identifie les signaux faibles pour découvrir de Nouvelles menaces qui étaient auparavant impossibles à détecter

Évalue les résultats de multiples sources et fait appel à l’intelligence Humaine pour prendre des décisions

# Temps d’investigation et de réponse de premier ordre



# Couverture 24/7 grâce à nos six SOC mondiaux



# Solution MDR pour tous les environnements

## Sophos

- Cld — Sophos Cloud
- Ep — Sophos Endpoint
- Fw — Sophos Firewall
- XDR — Sophos XDR
- Em — Sophos Email
- NDR — Sophos NDR

## Endpoint

Microsoft, CROWDSTRIKE, McAfee, SentinelOne, CHECK POINT, TREND MICRO, Malwarebytes, BlackBerry CYLANCE

## Firewall

paloalto NETWORKS, FORTINET, CHECK POINT, CISCO, SONICWALL

## Cloud SaaS

aws, Azure, Google Cloud, orca security

## Messagerie

Microsoft 365, mimecast, proofpoint.

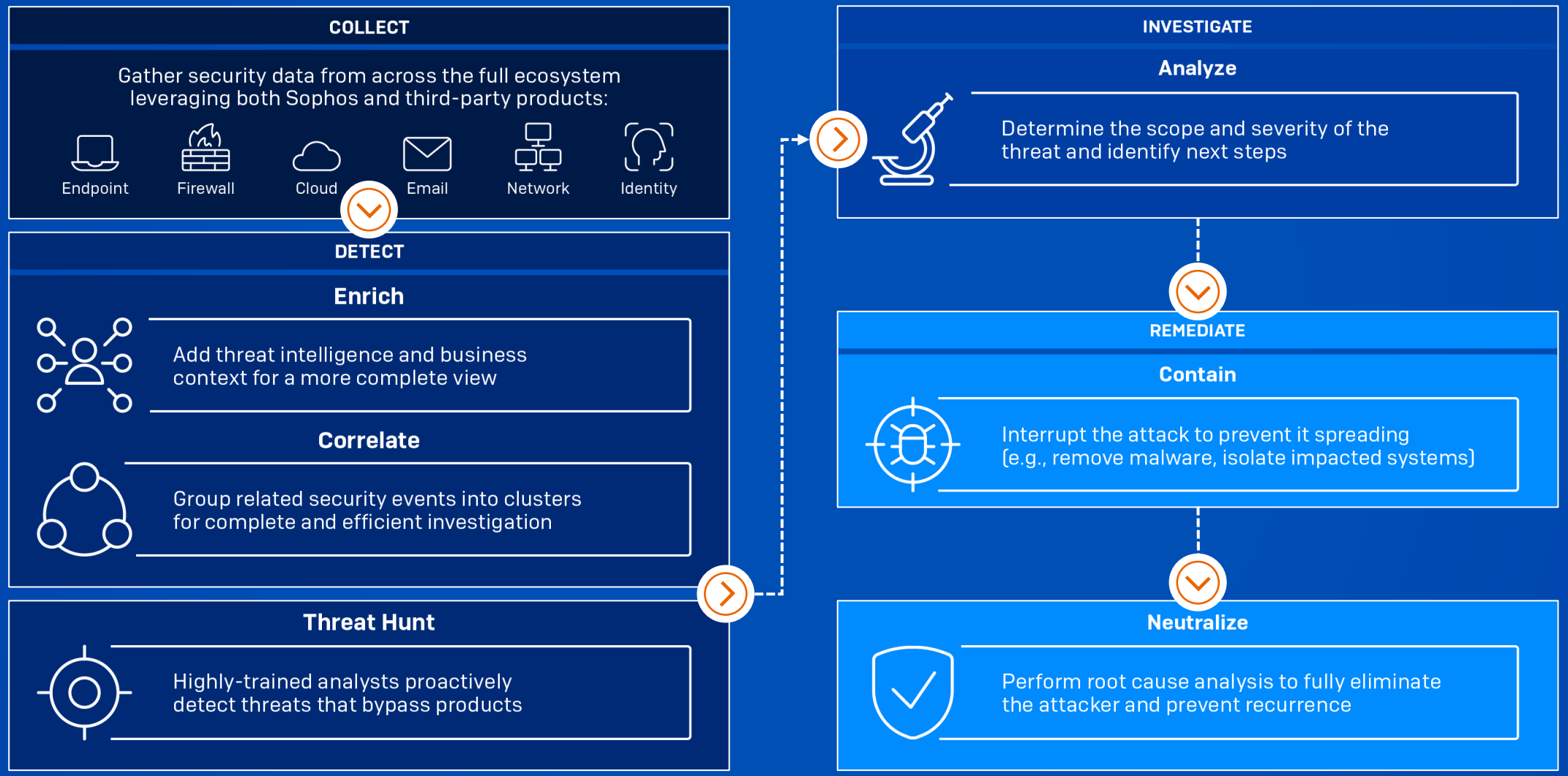
## Gestion d'identité

Microsoft [Azure IDP, ATA], okta, DUO

## Réseau

DARKTRACE, Forcepoint

# Le processus de détection et de réponse




koesio SOPHOS

# Types d’actions menées par nos experts

| Actions | Description |
|---|---|
| Changement des stratégies de sécurité | Ajustez les configurations pour mieux gérer la menace active. Peut inclure l'ajustement des politiques de menace, l'activation de l’XDR sur les appareils non protégés, l'ajustement des exclusions. |
| Isolation des terminaux. | Tirez parti de la fonctionnalité d’isolation des terminaux et serveurs depuis Central pour limiter l'exposition qu'un actif compromis pourrait avoir. |
| Blocage fichiers | Bloquer les fichiers identifiés par somme SHA256 pour empêcher l'exécution de contenu malveillant |
| Contrôle AV de la machine | Lancer l’analyse du système |
| Blocage sites/IPs/CIDR | Bloquer un site Web ou une adresse IP spécifique via le contrôle Web |
| Blocage applicatif | Bloquer une application spécifique via le contrôle applicatif |
| Utilisation d’une session ‘Live Terminal’ | Si toutes les actions précédentes ne sont pas efficaces, l'utilisation d’une session ‘Live Terminal’ nous donne un accès direct à l'hôte. Nécessite l'approbation du client |

# Détection d’un incident par l’outil de sécurité

Organisation de 200 employés dans le secteur manufacturier aux États-Unis

| Début | Étape 1 | Étape 2 | Étape 3 | Fin |
|---|---|---|---|---|
| Observation d’outils suspects | Alerte du client | Confirmation de l’entrée d’un attaquant | Neutralisation de l’attaquant | Le client reçoit des conseils sur la manière de prévenir les attaques futures |
| | Partage d’échantillons avec Sophos X-Ops | Identification du probable ransomware Cuba | Ejection de l’attaquant | |

# Incident de sécurité avec chasse aux menaces proactive

## Nouveau client Sophos

### Début

Un nouveau client nous contacte

### 15 min

Investigation d'une potentielle attaque de la supply chain

Identification des fichiers suspects

### 38 min

Partage du fichier avec Sophos X-Ops pour analyse

### 1 h 22 min

Identification d'un cheval de Troie bancaire historique

Ejection de l'attaquant

### 2 h 6 min

Le client reçoit des conseils sur la manière de prévenir les attaques futures

# Les avantages de Sophos MDR pour les entreprises

koesio

# Prévention des ransomwares et des violations 24/7/365

**Playbook des menaces**

- TTP
- IOC pertinents
- Preuve de concepts
- Requêtes utiles

Volume et variété d'attaques

**Expertise inégalée**

Investigation et réponse au quotidien

**Plus grande maîtrise des outils**

Enseignements partagés

**Accélérer la réponse**

Expérience client partagée

**Immunité communautaire**

# Libérez vos ressources informatiques pour vos initiatives stratégiques

« Nous n'avons pas besoin de passer du temps à combattre les incendies ou à nous inquiéter à propos des violations ou des menaces de sécurité. Cela nous permet de passer plus de temps à travailler sur les priorités stratégiques. »

- Forest Traffic Services, United Kingdom

« Nous apprécions que Sophos maîtrise parfaitement les dernières activités et menaces, nous permettant de nous concentrer sur la fourniture de services sécurisés et de qualité à nos clients et nos artistes. »

—CD Baby, US

# Améliorez le coût total de possession (TCO) de la cybersécurité

- Les coûts de prévention sont bien moins élevés que les coûts de remédiation
- Coût réduit de la sécurité 24 h/24 et 7 jours/7
- Accélérer la mise en œuvre des initiatives stratégiques
- Augmenter le ROI de vos investissements existants
- Améliorer votre position en matière de cyberassurance

« Sophos MDR est rentable à plus d'un titre. S'il permet d'éviter un incident majeur par an, il est rentabilisé dix fois, voire plus. »
—*Hammondcare*

« Sophos propose une couverture et une charge de travail équivalentes à six employés à temps plein pour un coût inférieur à celui d'une seule personne ».
—*Detmold Group*

« Nous avons gagné 15 heures par semaine et multiplié notre productivité par un facteur de 2,6. »
—*Tourism Finance Corporation of India*

# Sophos est le premier service MDR sur le marché

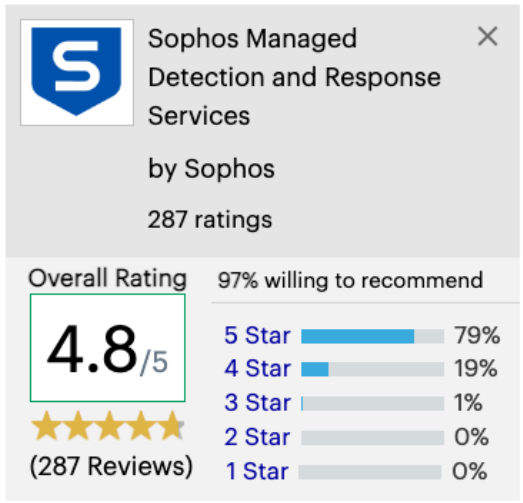
## Le plus fiable

**> 17 500 clients**

Plus d'entreprises font confiance à Sophos pour son service MDR qu'à tout autre éditeur.

## Le mieux noté

Gartner Peer Insights™




## Leader du marché

Sophos MDR est un **Leader** dans les segments Overall, Mid-Market et Enterprise

Classé **Top Vendor** dans le G2 Grid® 2022 pour les services MDR servant le midmarket.

*Le contenu de Gartner Peer Insights est constitué d'avis d'utilisateurs individuels basés sur leurs propres expériences avec les éditeurs répertoriés sur la plateforme. Ces avis ne doivent pas être interprétés comme des déclarations de faits et ne représentent pas les opinions de Gartner ou de ses affiliés. Gartner ne recommande aucun éditeur, produit ou service décrit dans ce contenu et ne donne aucune garantie, expresse ou implicite, concernant ce contenu, quant à sa précision ou son exhaustivité, y compris toutes garanties de qualité et de pertinence de la solution choisie.*

koesio SOPHOS

# THANK YOU

## MERCI.

# Questions / Réponses

**Joris DI MARCANTONIO**

Sales Engineer

Sophos

**David PIROCCHI**

Directeur Technique Régional

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**

© Koesio Corporate IT tous droits réservés