Sophos MDR : Le SOC 24x7 démocratisé.

Bechtle-IT Forum | 13.06.2023 | SwissTech Convention Center Lausanne

Michel Rueger, Senior Sales Engineer, Sophos
Renaud Schweigruber, Entreprise Account Executive, Sophos

Sophos en quelques chiffres

1985
FONDÉ A
OXFORD,
Royaume-Uni

1’200 M$
VENTES ANNEE FISCALE 2022

4’100+
EMPLOYES
(APPROX.)

Siège
OXFORD,
Royaume-Uni

554’000+
CLIENTS

100M+
D'UTILISATEURS

70’000+
PARTENAIRES
REVENDEURS

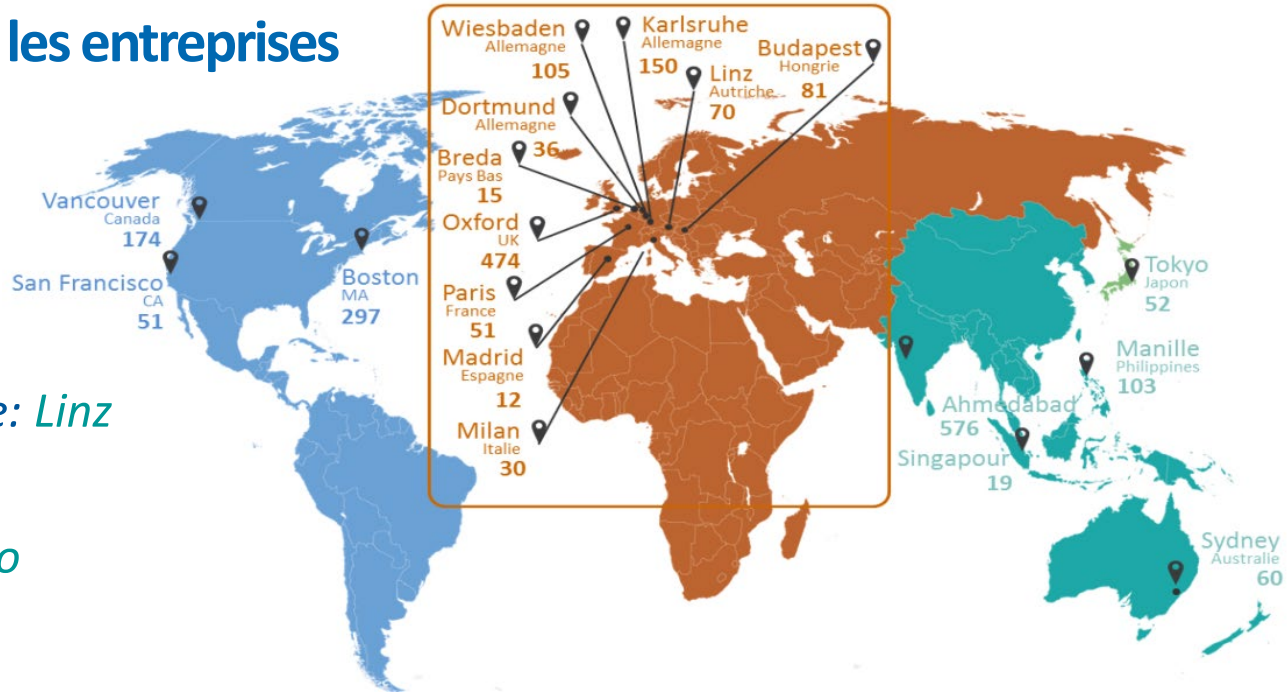
1er éditeur européen de solutions de sécurité pour les entreprises

- **4 SophosLabs** dont **2 en Europe**

  Oxford, Budapest, Vancouver, Sydney

- **12 Centres de R&D** dont **7 en Europe**

  UK: Oxford Allemagne: Dortmund, Karlsruhe Autriche: Linz
  Hongrie: Budapest Irlande: Cork Pays-Bas: Hengelo
  Canada: Vancouver USA: Boston, Fairfax, San Francisco
  Inde: Ahmedabad



Team Sophos Switzerland FY 2024

Mirko Casarico
Country Manager Switzerland

Michael Kretschmann
Snr. Manager Channel

Neslihan Cellek-Gargiulo
Snr. Territory Account Executive
Mid Market 101-1000 Users
PLZ 80.. – 85.. /5

Michael Fenyves
Enterprise Account Executive
EAST >1001 Users
PLZ 8../9../LI

Sascha Paris
Snr. Sales Engineer
D/I – CH

Patrik Rohrer
Channel Account Executive

Thorsten Mangei
Territory Account Executive
Mid Market 101-1000 Users
PLZ 60-64../7../86..- 89/9../LI

Renaud Schweingruber
Enterprise Account Executive
WEST >1001 Users
PLZ 1../2../3962-3982

Yannick Escudero
Snr. Sales Engineer
D/I – CH

Terek Moumene
Snr. Channel Account Executive F – CH

Sabrina Sbaffoni
Territory Account Executive
Mid Market 101-1000 Users
PLZ 1../2../3../4../65-69..

Solveig Barrand
Enterprise Account Executive
Central >1001 Users
PLZ 3../4../5../6../7..

Michel Rueger
Snr. Sales Engineer
F – CH

Patrizia Raso
Sales Specialist
SMB Market 1-100 Users
CH / AUT

Cybermenaces en 2023

Résultat d’enquête auprès de professionnels de l’IT

3’000
répondants

100-5’000
employés

14
pays

<$10M - $5B+
Revenu annuel

Jan/Fev 23
Période d’enquête

Top 3 des principales cybermenaces pour 2023

Cybermenace	% qui estiment être une topmenace
Data exfiltration (theft by an external attacker)	**41%**
Phishing (including spear phishing)	**40%**
Ransomware	**35%**
Cyber extortion	**33%**
Denial of Service attacks (DDoS)	**32%**
Business email compromise	**31%**
Active adversaries (human hands-on-keyboard attackers)	**30%**
Mobile malware	**30%**
Cryptominers	**22%**
Wipers	**16%**
Other	**0%**
I am not concerned about any cyber threats affecting my organisation in 2023	**1%**
Don’t know	**0%**

Temps moyens de détection, investigation et réponse

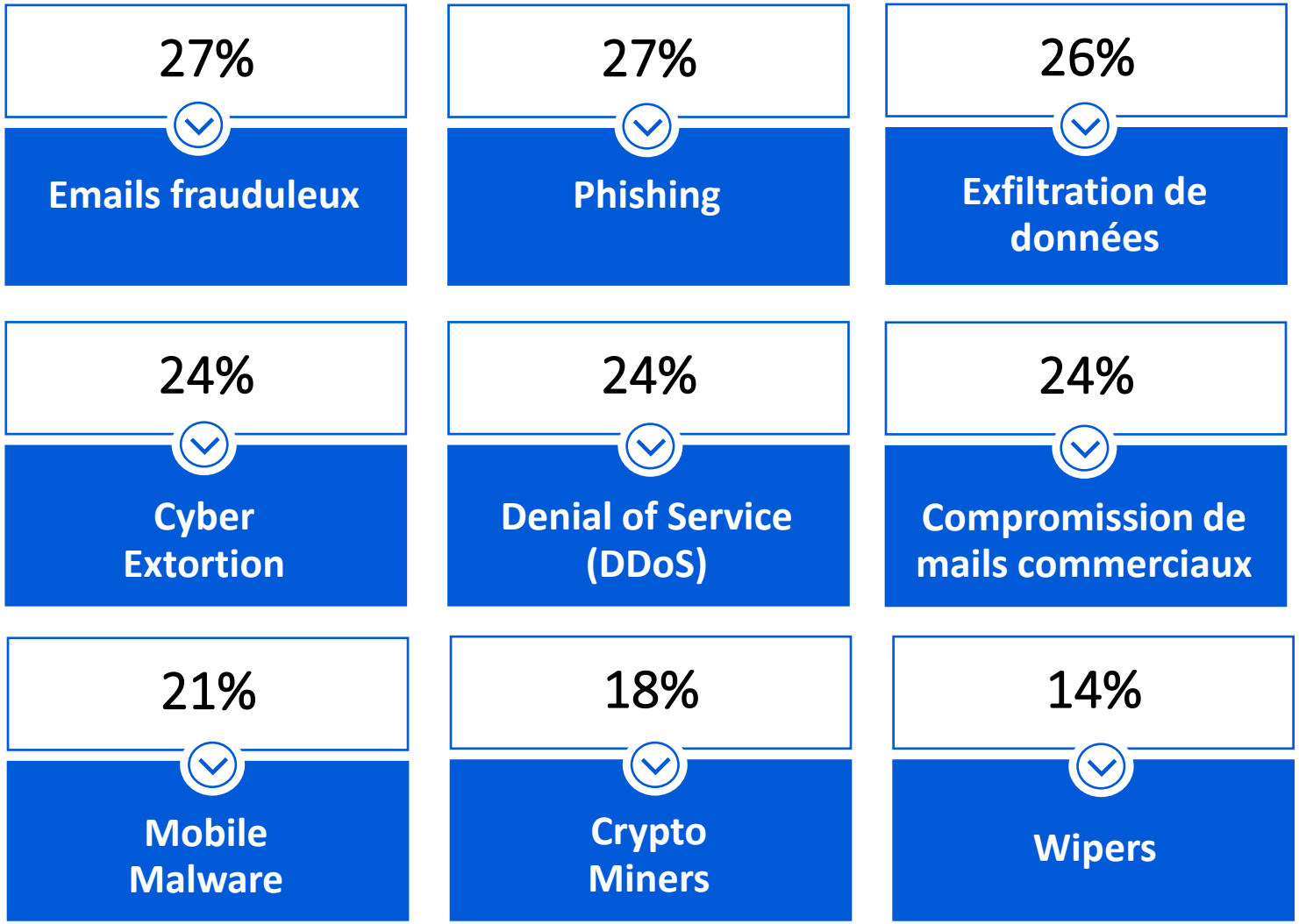
Activité	100-3,000 employés (n=2,460)	3,001-5,000 employés (n=350)	IT, technologie et télécoms (n=98)	Production et fabrication (n=331)	Energie, pétrole/gaz et services publics (n=66)
Détection	3 heures	3 heures	1.5 heures	3 heures	6 heures
Investigation	3 heures	6 heures	2.25 heures	6 heures	6 heures
Réponse	3 heures	6 heures	3 heures	6 heures	6 heures
Total	**9 heures**	**15 heures**	**6.75 heures**	**15 heures**	**18 heures**

Temps médian de détection, d'investigation et de réponse à une alerte de sécurité.

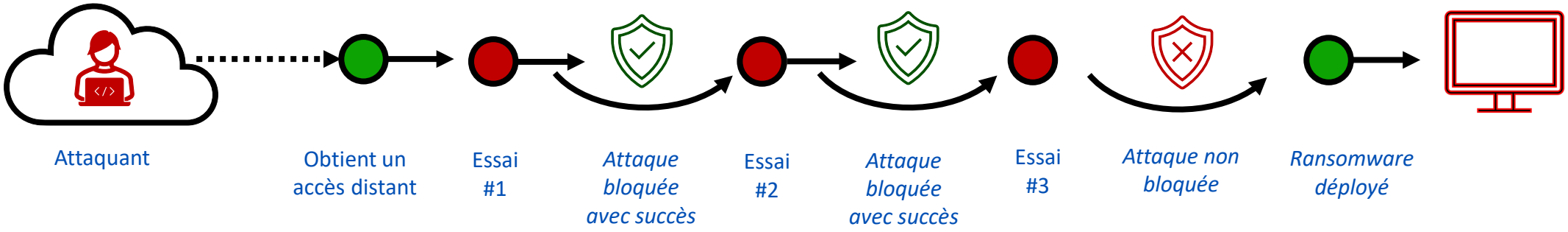
Combien de temps faut-il à votre organisation pour détecter, enquêter et, le cas échéant, remédier à un incident potentiel ?
Médiane (n=2 812 répondants qui enquêtent sur les alertes en interne)

Les adversaires exécutent une myriade d'attaques à grande échelle

94%
des organisations ont fait l'objet d'au moins une cyberattaque l'année passée



Comprendre les attaquants actifs



- Les attaquants actifs utilisent de multiples techniques, tactiques et procédures, notamment :
  - Exploiter les faiblesses de la sécurité pour pénétrer dans les organisations et se déplacer latéralement.
  - Abuser des outils informatiques légitimes utilisés par les défenseurs pour éviter de déclencher des détections.
  - Modifier leurs attaques en temps réel en réponse aux contrôles de sécurité
  - Passer à de nouvelles techniques jusqu'à ce qu'ils trouvent un moyen d'atteindre leurs objectifs.

Situation en Suisse romande

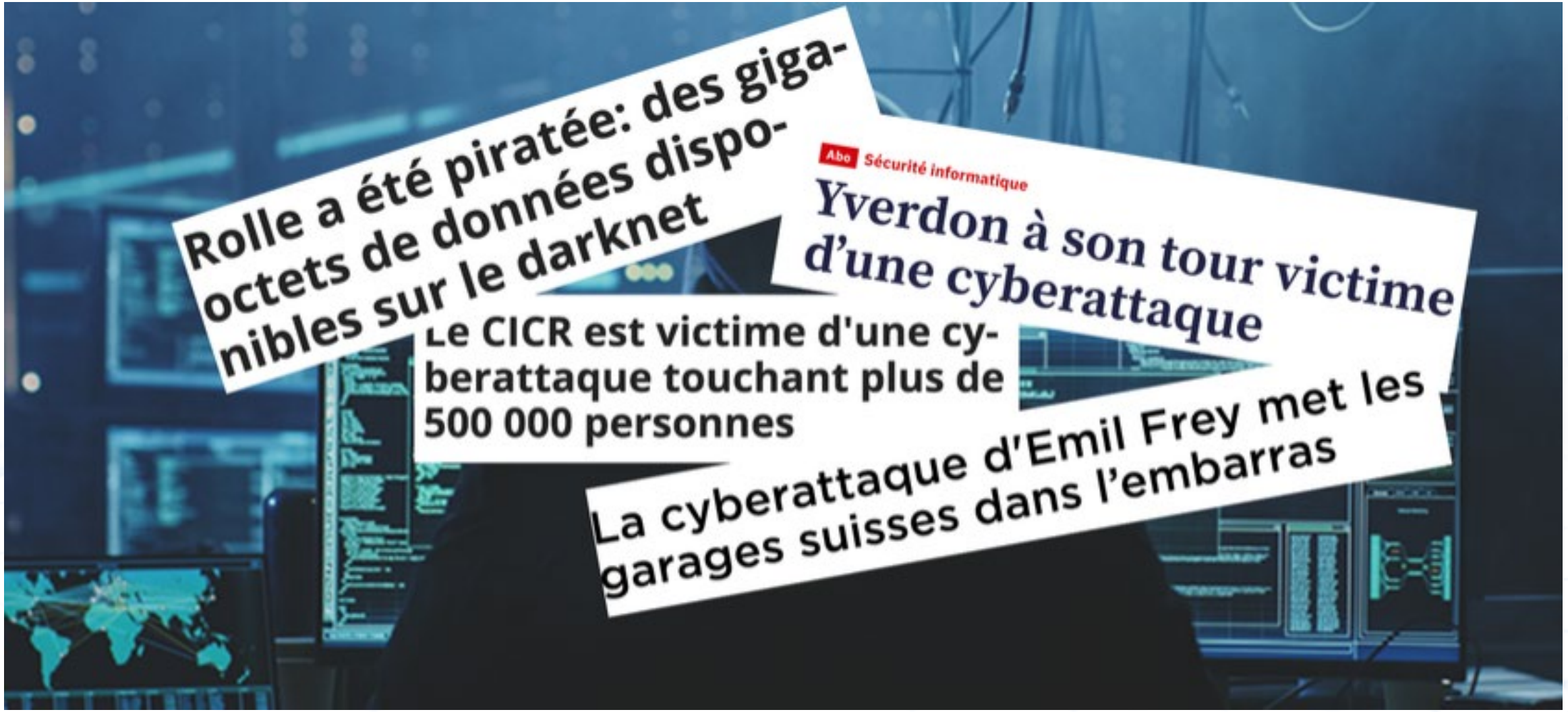
Menaces en Suisse romande

Ingénierie sociale
- Méthode éprouvée
- La technologie seule ne suffit pas.

Ransomware
- Rapportent moins qu'auparavant
- Personnalisé pour chaque cible
- La revente des données est donc désormais un vrai sujet
- Cryptolockers toujours d'actualité, mais utilisés comme moyen de pression.

Cibles
- PME confrontées aux mêmes cybermenaces que les grandes organisations

Menaces en Suisse romande



Menaces en Suisse romande

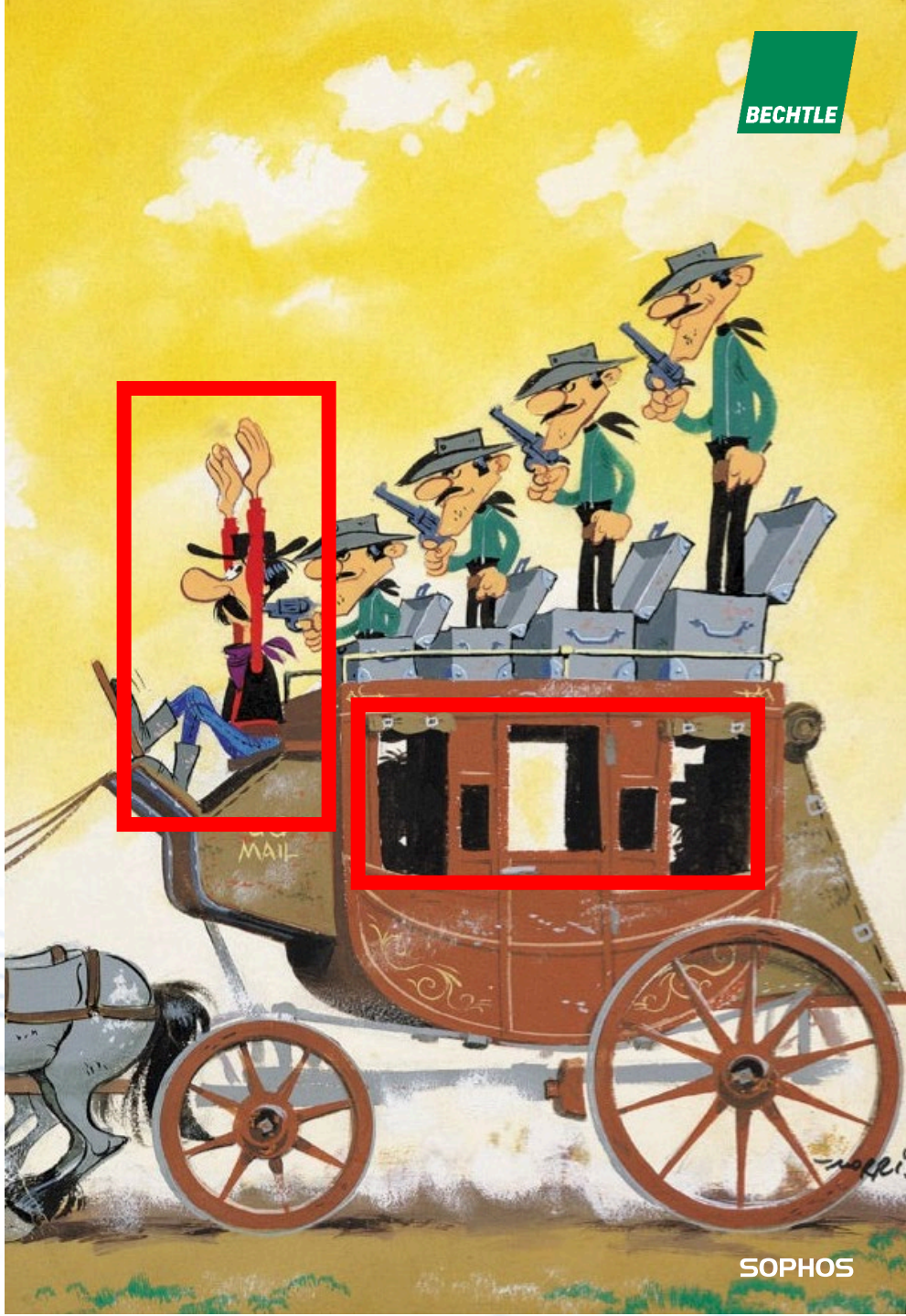
- Attaquer la chaîne d'approvisionnement
- Attaquer les fournisseurs de services managés (MSP)
- Attaquer les fournisseurs de Cloud

Infolog victime d'une cyberattaque

Des données volées à Infopro font l'objet d'une demande de rançon

log a fait les frais d'une cyberattaque. Les service
urs et aucune donnée n'aurait fuité.

Des pirates ciblent des centres de calcul pour dérober les données de leurs clients



Problématique majeure des équipes IT et de sécurité

Manque de visibilité

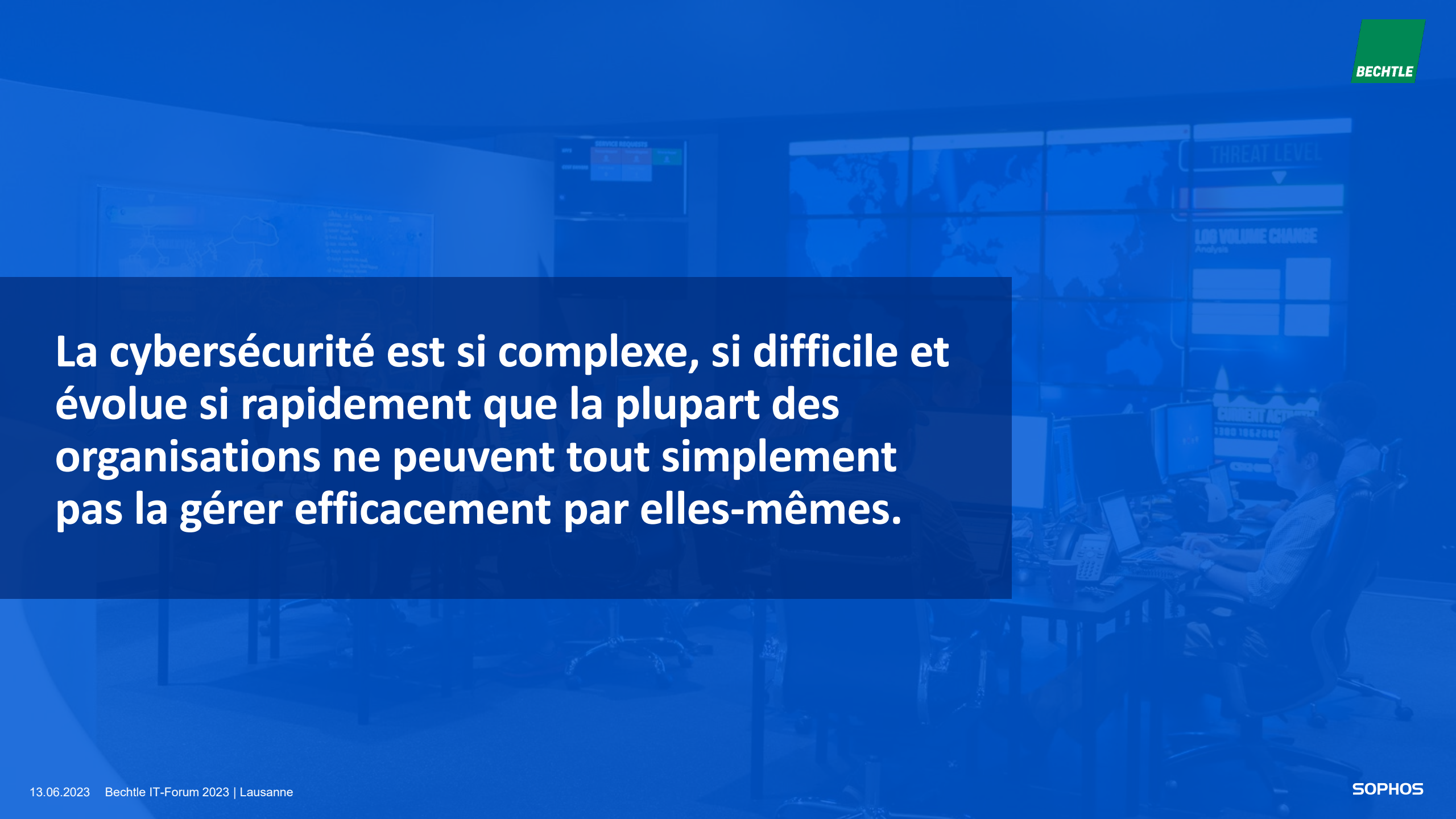
68% *des violations de sécurité sont détectées 30 jours après.*

Manque de temps

26% *du temps du team IT pour gérer des problèmes liés à la sécurité.*

Manque de resources

2/3 *mentionnent un budget de sécurité insuffisant.*

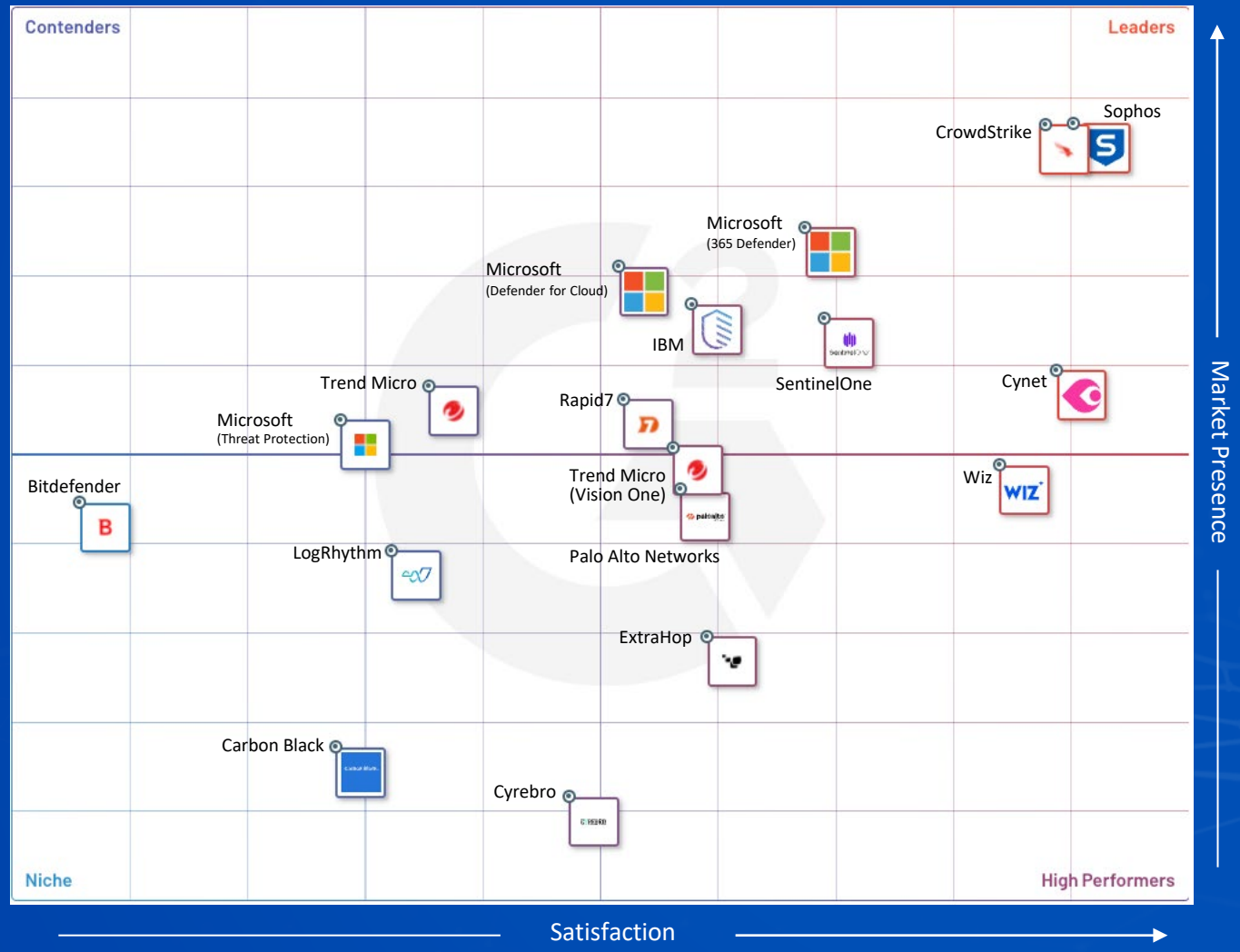


La cybersécurité est si complexe, si difficile et évolue si rapidement que la plupart des organisations ne peuvent tout simplement pas la gérer efficacement par elles-mêmes.

Gartner®

D'ici 2025, 60 % des entreprises utiliseront des services MDR **fournis directement par les éditeurs** de solution de sécurité.

2023 G2 Grid® for XDR Platforms

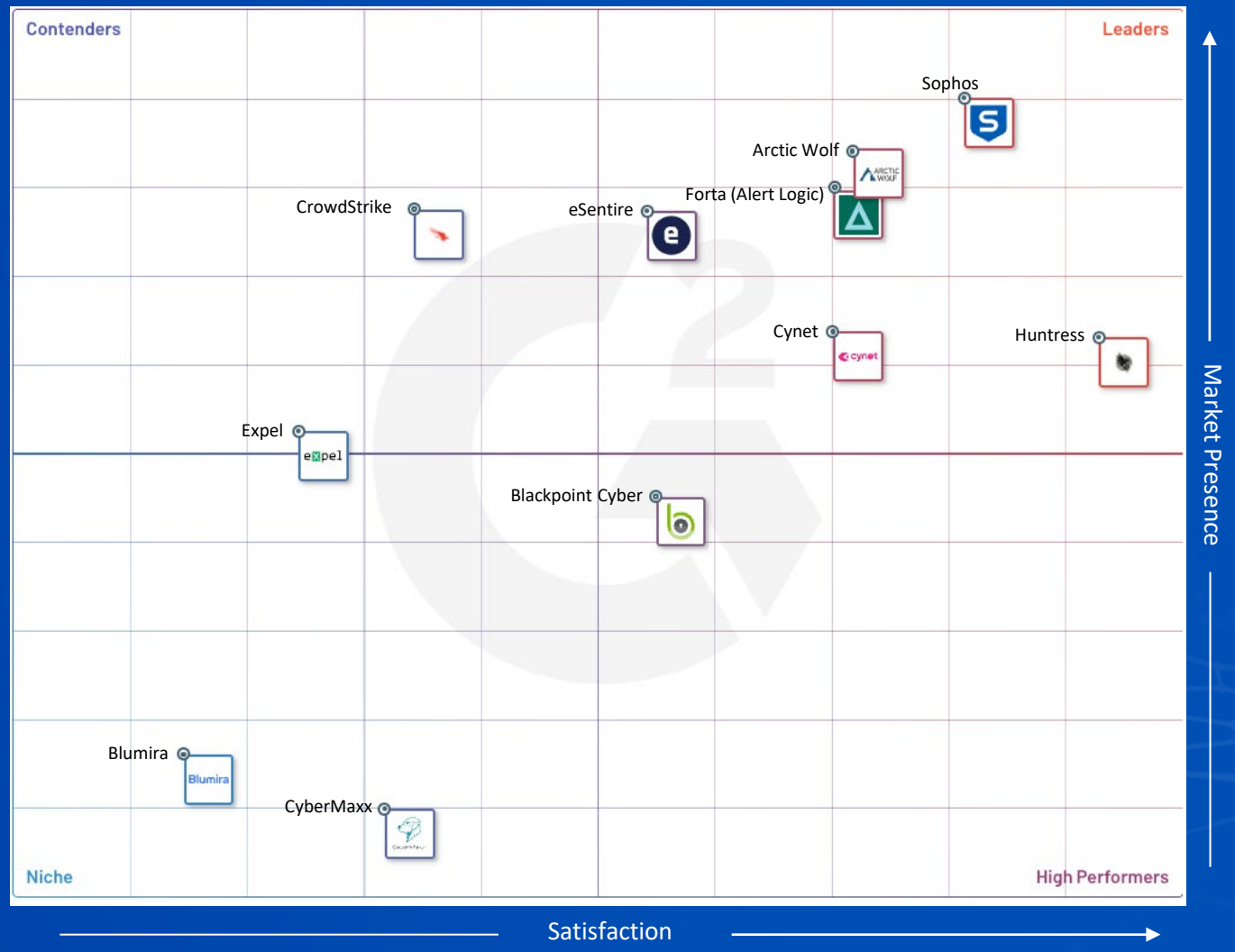


Sophos XDR is the **#1 XDR Platform** in the 2023 G2 Grid® for XDR Platforms.

Rated the **Top Vendor** in the 2023 G2 Grid® for XDR Services serving the midmarket.

2023 G2 Grid® for Extended Detection and Response (XDR) - Midmarket

2023 G2 Grid® for MDR Services

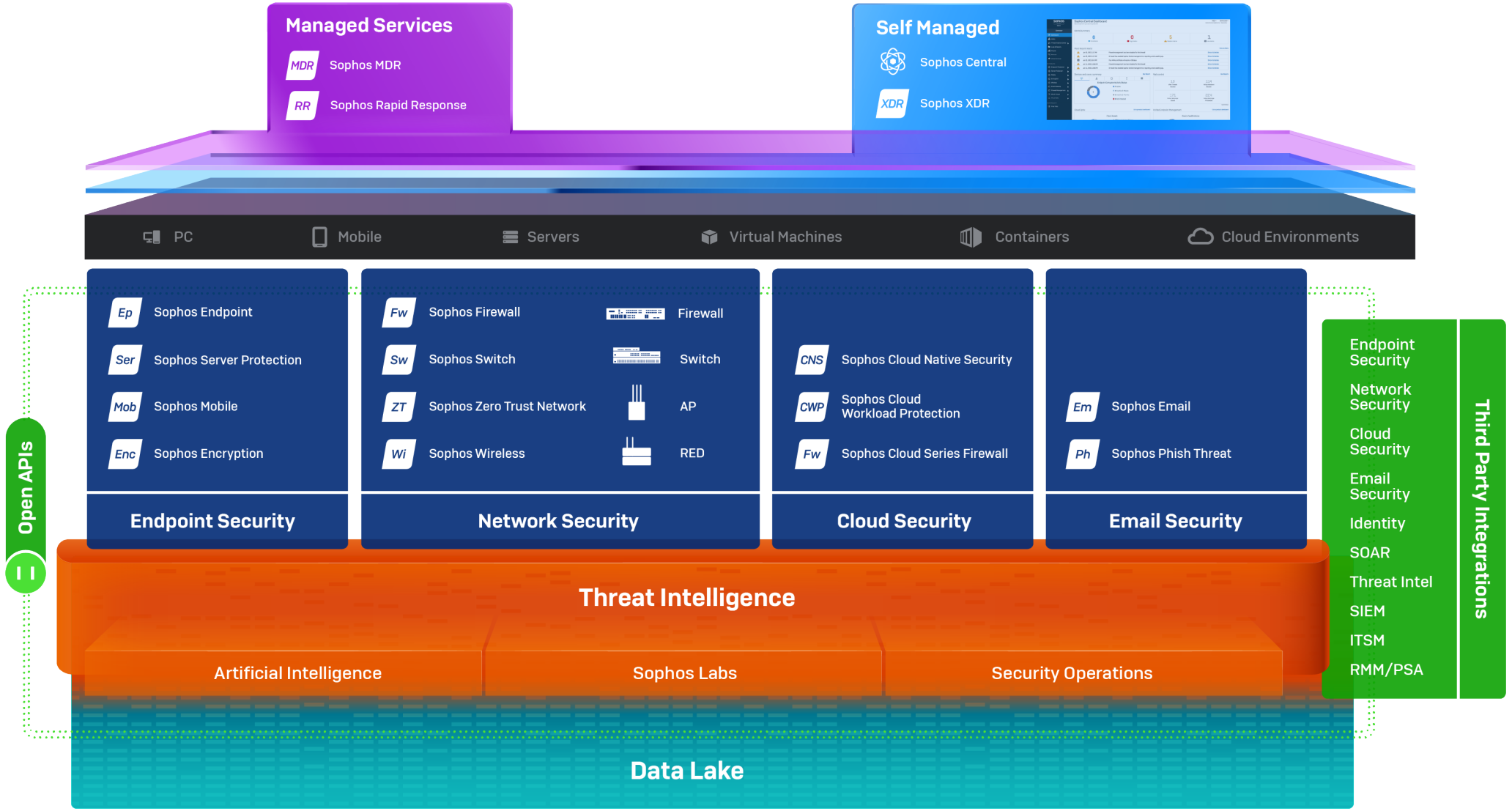


Sophos MDR is the **#1 MDR service** in the 2023 G2 Grid® for MDR Services.

Rated a Leader in the Overall, Enterprise, and Mid-Market categories.

2023 G2 Grid® for Managed Detection and Response (MDR) - Overall

Adaptive Cybersecurity Ecosystem



Protection des terminaux et serveurs

Intercept X Advanced

Intercept X Advanced for Server

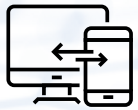
Ep Svr

Comprennent plusieurs technologies

Pour protéger les serveurs et les terminaux des menaces


Web Control


App Control


Peripheral Control


Windows Firewall Monitoring


Server Lockdown

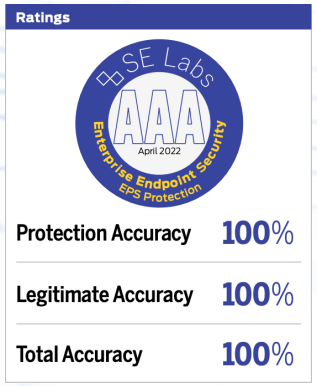

Anti Ransomware

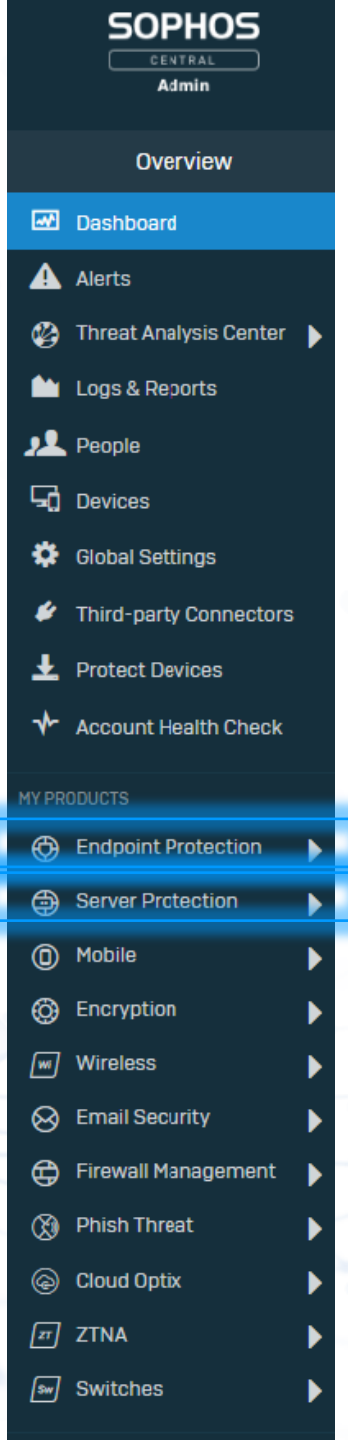

Exploit Prevention


Deep Learning


Server File Integrity Monitoring


Active Adversary Mitigations





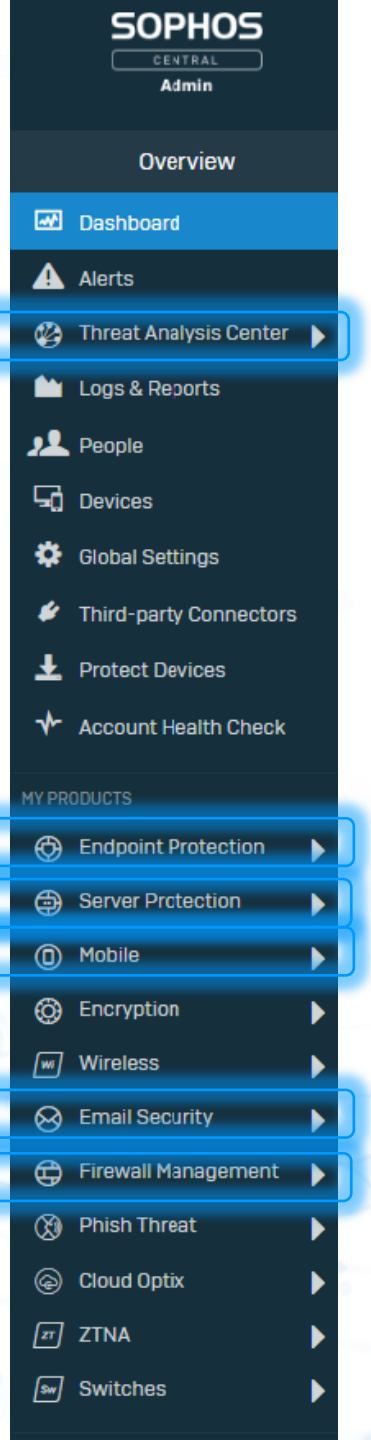
Protection maximale + détection + réponse

Intercept X Advanced with XDR

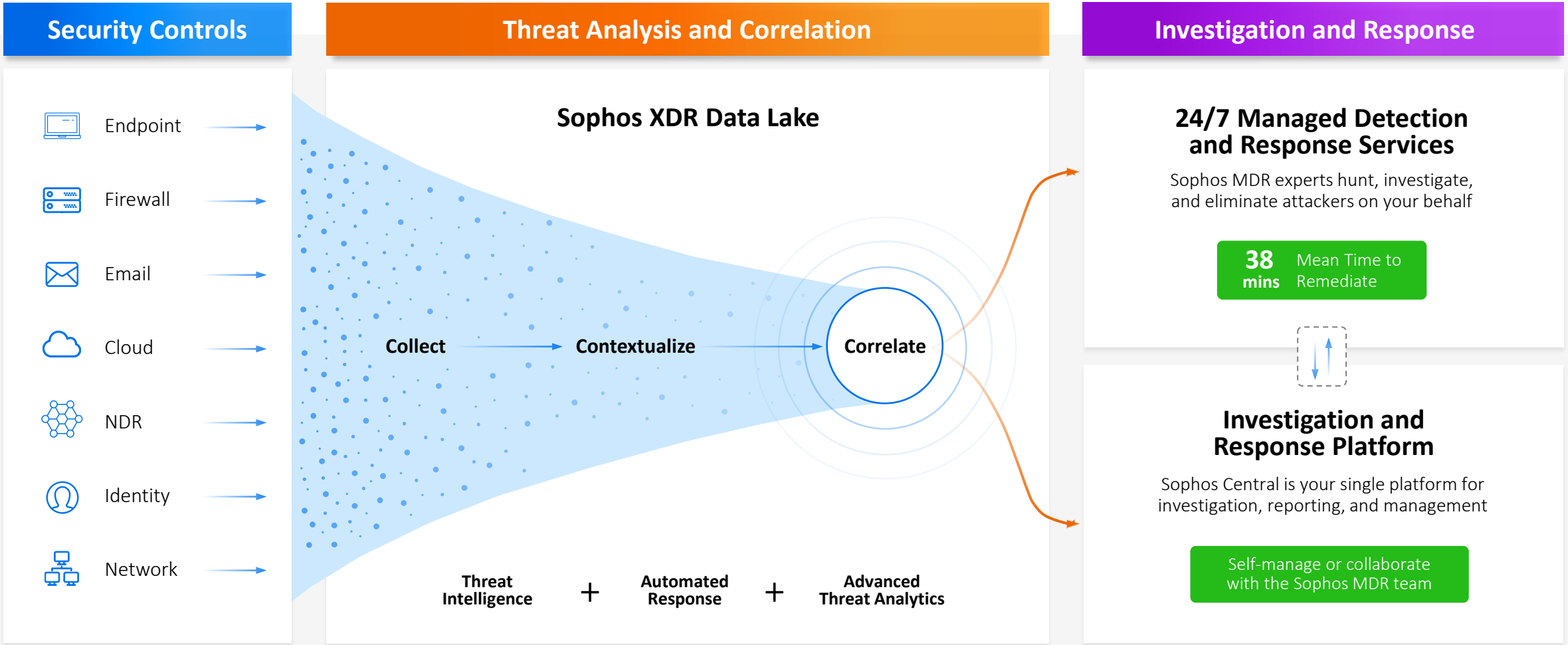
(eXtended Detection and Response)

est une **boîte à outils**

- pour détecter l'activité des pirates
- pour stopper et nettoyer les menaces
- en corrélant les événements sur de nombreux produits et technologies comme Endpoint, Server, Firewall, Mobile, Email, Microsoft 365, etc...



Détection et Réponse: Par vous ou par nous



L'exploitation de la télémétrie est complexe

FIREWALL TELEMETRY

<11>Aug 9 08:03:28 TDG-CDNDCFW01.CUSTOMER.ca CEF:0|VENDORA|VENDORA|9.1.10|MVPower DVR TV Shell Unauthenticated Command Execution Vulnerability(54553)|THREAT|**4**|rt=Aug 09 2022 13:03:27 GMT deviceExternalId=001701010750 src=45.58.21.70 dst=216.55.21.147 sourceTranslatedAddress=45.58.21.70 destinationTranslatedAddress=10.200.150.90 cs1Label=Rule cs1=Outside-DMZ1-chatbot.tdg-dsg.com suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Outside cs5Label=Destination Zone cs5=DMZ_01 deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ae2 cs6Label=LogProfile cs6=SOC.OS Agent cn1Label=SessionID cn1=447900 cnt=1 spt=36935 dpt=80 sourceTranslatedPort=36935 destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x80412000 proto=tcp act=alert request="shell" cs2Label=URL Category cs2=license-expired flexString2Label=Direction flexString2=client-to-server VENDORAActionFlags=0x20000000000000 externalId=12412496 cat=MVPower DVR TV Shell Unauthenticated Command Execution Vulnerability(54553) fileId=12075418355151190 VENDORADGl1=0 VENDORADGl2=0 VENDORADGl3=0 VENDORADGl4=0 VENDORAVsysName= dvchost=TDG-CDCFW01 VENDORASrcUUID= VENDORADstUUID= VENDORATunnelID=0 VENDORAMonitorTag= VENDORAParentSessionID=0 VENDORAParentStartTime= VENDORATunnelType=N/A VENDORAThreatCategory=code-execution VENDORAContentVer=AppThreat-8585-7440 VENDORAAssocID=0 VENDORAPPID=4294967295 VENDORAHTTPHeader= VENDORAURLCatList= VENDORARuleUUID=62dbe5-718d-401-aa37-b90540f748 VENDORAHTTP2Con=0 PanDynamicUsrgrp=

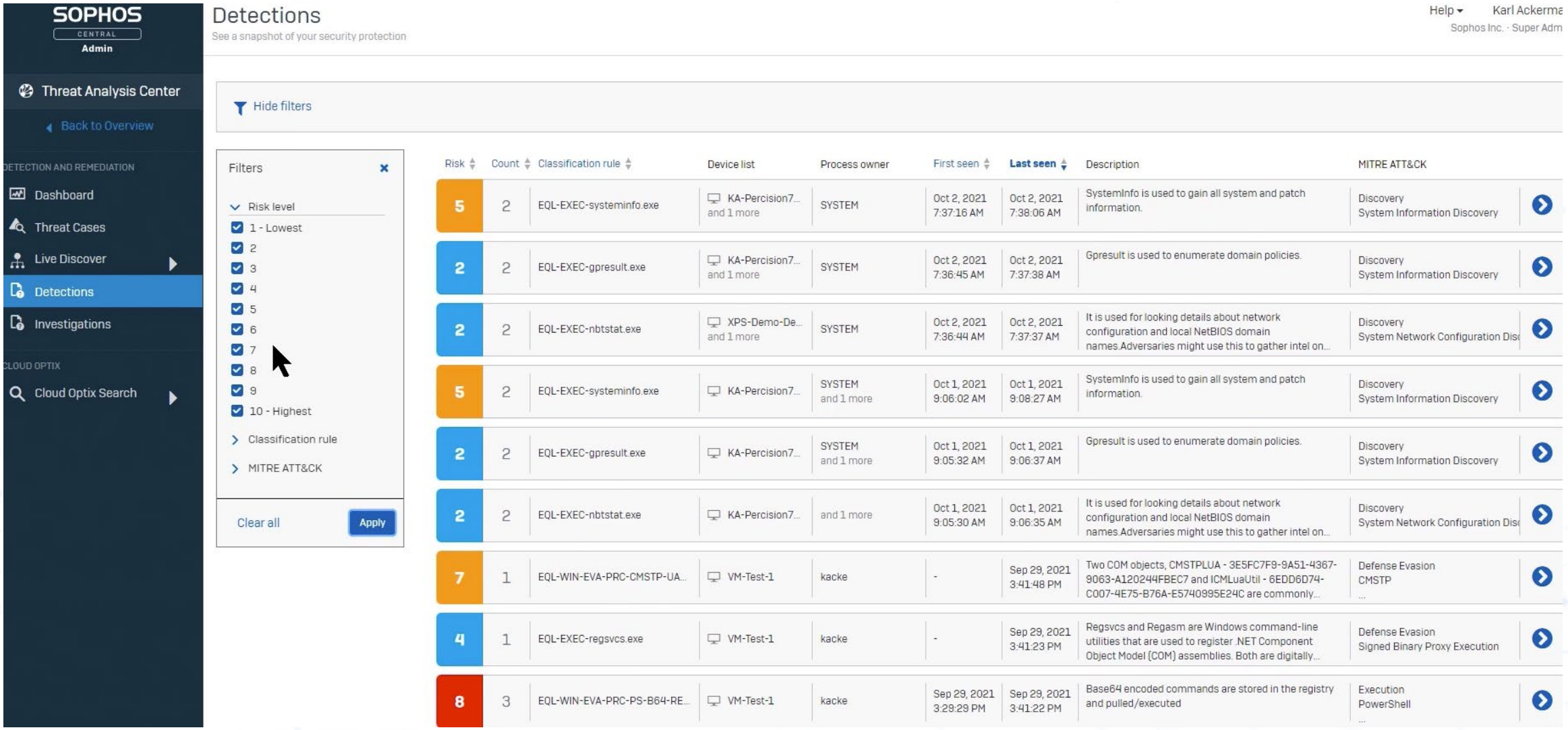
EMAIL TELEMETRY

{"senderAddress":"**SENDER.NAME@XXXX.com**","**recipientAddress":"FIRST.LAST@XXXXX.com**","**fileName":"Factura_RSS190815AN5_8613_XEXX010101000.pdf**","fileType":"application/pdf","result":"safe","**actionTriggered":"none, none**","date":"2022-10-06T03:09:12+0000","details":"Safe \r\nTime taken: 0 hrs, 0 min, 26 sec", "route":"inbound", "messageId":"<SA1PR13MB4976F328D68BF6D1B7560BA6845C9@SA1PR13MB4976.namprd13.prod.outlook.com>","subject":"ROCKA Specialty - Universal Lighting Virtual Septiembre 2022","fileHash":"9f1e0a25cb3b08d417bdced2ea226e010d76822420fd8265b8935668ddb4344a","**definition":"Default Attachment Protection**"}

IDENTITY TELEMETRY

{"access_device":{"browser":"Edge","browser_version":"18.19044","epkey":"EPQ0KD7N0H1AJJ5IZRS4","flash_version":"uninstalled","hostname":null,"**ip":"194.8.207.139**","is_encryption_enabled":"unknown","is_firewall_enabled":"unknown","is_password_set":"unknown","java_version":"uninstalled","location":{"city":"Hürth","country":"Germany","state":"North Rhine-Westphalia"},"os":"Windows","os_version":"10","security_agents":"unknown"}, "alias":"","application":{"key":"DIHUCR02IM4WOZQGGOEP","name":"Sophos Trusted Endpoint"},"auth_device" :{"ip":null,"location":{"city":null,"country":null,"state":null},"name":null},"**email":"FIRST.LAST@sophos.com**","event_type":"authentication","factor":"not_available","isotimestamp":"2022-06-09T11:59:24.424377+00:00","ood_software":null,"**reason":"endpoint_is_not_trusted**", "**result":"denied**","timestamp":1654775964,"trusted_endpoint_status":"not trusted","txid":"05558fa5-0145-4454-9aa5-8060493c41a2","user":{"groups":["AAD-DUOMFAUsers (from Azure sync \"Sophos Ltd\")"],"key":"DU9MZJV4IVSSZN49JGYT","**name":"FIRST.LAST**"}}

Détections


SOPHOS
CENTRAL
Admin
Threat Analysis Center
Back to Overview
DETECTION AND REMEDIATION
Dashboard
Threat Cases
Live Discover
Detections
Investigations
CLOUD OPTIX
Cloud Optix Search
Detections
See a snapshot of your security protection
Help
Karl Ackerma
Sophos Inc. · Super Adm
Hide filters
Filters
Risk level
1 - Lowest
2
3
4
5
6
7
8
9
10 - Highest
Classification rule
MITRE ATT&CK
Clear all
Apply
Risk
Count
Classification rule
Device list
Process owner
First seen
Last seen
Description
MITRE ATT&CK
5 2 EQL-EXEC-systeminfo.exe KA-Percision7... and 1 more SYSTEM Oct 2, 2021 7:37:16 AM Oct 2, 2021 7:38:06 AM SystemInfo is used to gain all system and patch information. Discovery System Information Discovery
2 2 EQL-EXEC-gpresult.exe KA-Percision7... and 1 more SYSTEM Oct 2, 2021 7:36:45 AM Oct 2, 2021 7:37:38 AM Gpresult is used to enumerate domain policies. Discovery System Information Discovery
2 2 EQL-EXEC-nbtstat.exe XPS-Demo-De... and 1 more SYSTEM Oct 2, 2021 7:36:44 AM Oct 2, 2021 7:37:37 AM It is used for looking details about network configuration and local NetBIOS domain names.Adversaries might use this to gather intel on... Discovery System Network Configuration Dis
5 2 EQL-EXEC-systeminfo.exe KA-Percision7... SYSTEM and 1 more Oct 1, 2021 9:06:02 AM Oct 1, 2021 9:08:27 AM SystemInfo is used to gain all system and patch information. Discovery System Information Discovery
2 2 EQL-EXEC-gpresult.exe KA-Percision7... SYSTEM and 1 more Oct 1, 2021 9:05:32 AM Oct 1, 2021 9:06:37 AM Gpresult is used to enumerate domain policies. Discovery System Information Discovery
2 2 EQL-EXEC-nbtstat.exe KA-Percision7... and 1 more Oct 1, 2021 9:05:30 AM Oct 1, 2021 9:06:35 AM It is used for looking details about network configuration and local NetBIOS domain names.Adversaries might use this to gather intel on... Discovery System Network Configuration Dis
7 1 EQL-WIN-EVA-PRC-CMSTP-UA... VM-Test-1 kacke - Sep 29, 2021 3:41:48 PM Two COM objects, CMSTPLUA - 3E5FC7F9-9A51-4367-9063-A120244FBEC7 and ICMLuaUtil - 6EDD6D74-C007-4E75-B76A-E5740995E24C are commonly... Defense Evasion CMSTP ...
4 1 EQL-EXEC-regsvcs.exe VM-Test-1 kacke - Sep 29, 2021 3:41:23 PM Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies. Both are digitally... Defense Evasion Signed Binary Proxy Execution
8 3 EQL-WIN-EVA-PRC-PS-B64-RE... VM-Test-1 kacke Sep 29, 2021 3:29:29 PM Sep 29, 2021 3:41:22 PM Base64 encoded commands are stored in the registry and pulled/executed Execution PowerShell ...

Problématique majeure des équipes IT et de sécurité

Manque de visibilité

68% *des violations de sécurité sont détectées 30 jours après.*

Manque de temps

26% *du temps du team IT pour gérer des problèmes liés à la sécurité.*

Manque de resources

2/3 *mentionnent un budget de sécurité insuffisant.*

Qu'est-ce MDR?

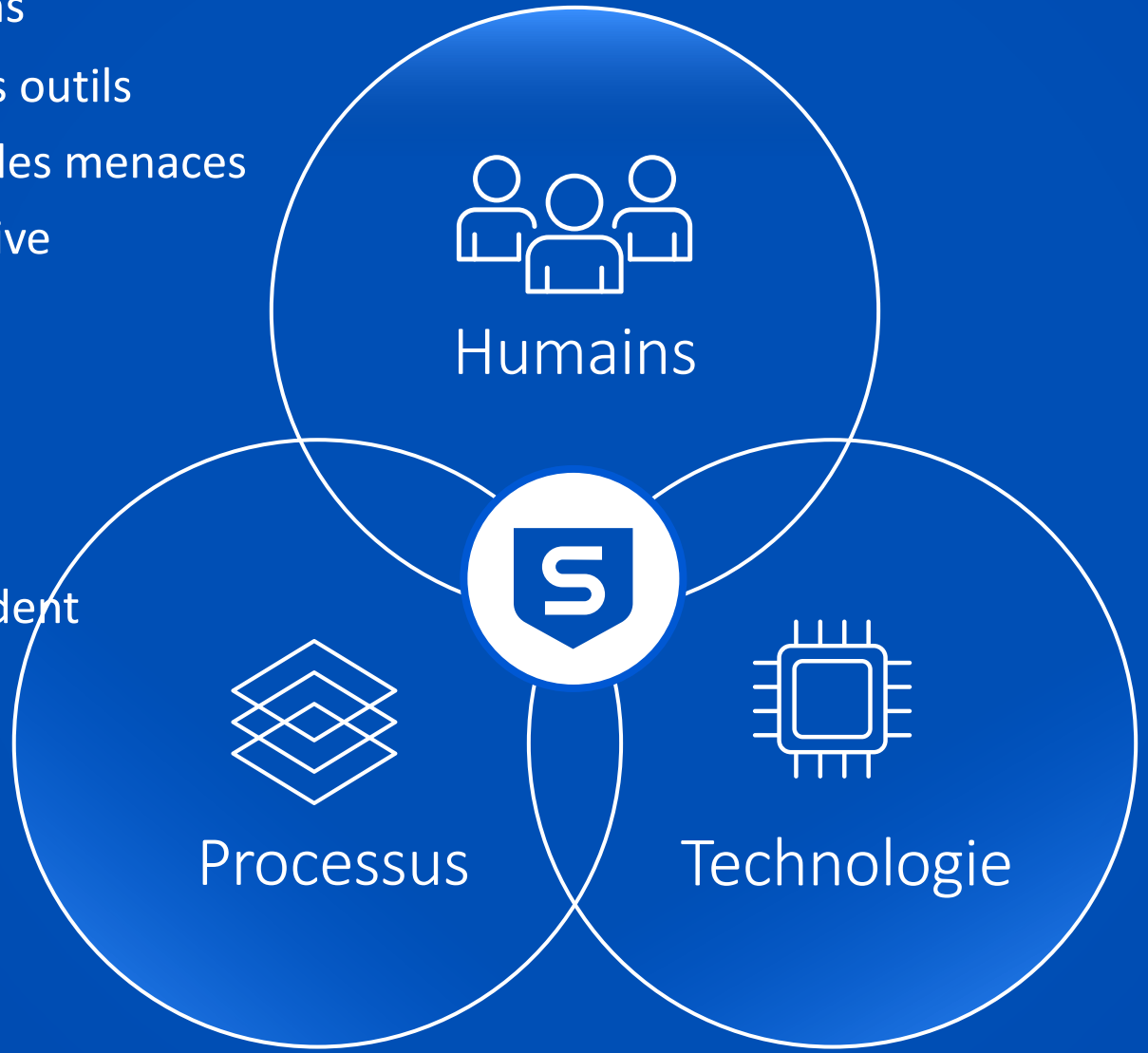
24/7 Security Operations

- **Chasse aux menaces**
- **Réponse à incident**
- **Amélioration proactive de la sécurité**

Sophos MDR

24/7 Security Operations

- Utilisation active des outils
- Recherche/analyse des menaces
- Amélioration proactive de la sécurité



Procédure en cas d'incident

- Incident/réponse
- Isolation
- Neutralisation
- Récupération

Minimum légal=
XDR écosystème

- Protection NextGen
- Télémétrie
- Détection + corrélation
- Réaction
- Automatisation

= Outils

Couverture 24x7 depuis 6 SOCs

Sophos MDR

Chasse aux menaces

Les recherches proactives de menaces effectuées par des analystes hautement qualifiés permettent de découvrir et d'éliminer rapidement plus de menaces que les produits de sécurité ne peuvent en détecter par eux-mêmes.

Détection des menaces

Les capacités étendues de détection et de réponse (XDR) permettent de détecter les menaces connues et les comportements potentiellement malveillants, quel que soit l'endroit où se trouvent vos données.

Réponse aux incidents

Nos analystes répondent aux menaces en quelques minutes, que vous ayez besoin d'une réponse complète à un incident ou d'une aide pour prendre des décisions plus précises.

Plus de 15 000 clients MDR

99,98 % des menaces sont automatiquement bloquées*

Temps de réponse moyen aux menaces de Sophos MDR

Temps de détection	Moins d'une minute
Il est temps d'enquêter	Moins de 25 minutes
Le temps de répondre	Moins de 12 minutes

Chaque outil joue un rôle important dans l'identification des menaces

ENDPOINT

Détecter les activités suspectes et les logiciels malveillants

FIREWALL

Détecter les tentatives d'intrusion et le balisage

IDENTITY

Détecter les entrées non autorisées sur le réseau et l'escalade des privilèges

EMAIL

Localisation de l'entrée initiale et des tentatives de vol de données d'accès

CLOUD

Indique un accès non autorisé au réseau et des efforts pour voler des données

NETWORK

Identifier les actifs indésirables, les dispositifs non protégés et les nouvelles attaques

SOPHOS MDR: Ouvert et flexible

MDR **Sophos MDR**

Compatible avec votre environnement

Compatible avec vos exigences

Compatible avec votre réseau

SOPHOS

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

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

Email

Microsoft 365, mimecast, proofpoint

Identity

Microsoft [Azure IDP, ATA], okta, DUO

Network

DARKTRACE, Forcepoint

Sophos MDR intègre ...

Sophos XDR

La seule plateforme qui intègre nativement l'intégration de la télémétrie issue de la protection des terminaux, des firewall, du cloud, du mobile et de microsoft

Sophos Firewall

Surveille et filtre le trafic entrant et sortant pour stopper les menaces avant qu'elle ne puisse causer des dégâts.

Microsoft Graph Securité

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Azure Active Directory
- Microsoft Defender for Cloud Apps
- Microsoft Sentinel
- Azure Information Protection
- Microsoft 365

Sophos Endpoint Protection

Bloque les menace et détecte les comportements malicieux, incluant les attaquants imitant l'activité d'utilisateurs légitimes

Sophos Email

Protège la BAL en bénéficiant d'une IA avancée qui stoppe les malwares, les impostures et les attaques par Phihsing.

Office 365 Activité de gestion

- Fournit des informations sur les utilisateurs, les tâches d'administration, les modifications de politiques de sécurité et les événements issus d'Office365 et les logs d'activité d'Azure Active Directory.

Sophos Cloud

Stoppe les failles et apporte la visibilité de l'ensemble des services Cloud critiques pour les plateformes AWS, Azure et Google Cloud Platform

Third-Party Endpoint Protection

Compatible avec ...

- Microsoft
- CrowdStrike
- SentinelOne
- Check Point
- Trend Micro
- BlackBerry (Cylance)
- McAfee
- Malwarebytes

90 jours consécutifs
Conservation des données

Sophos MDR Intégrations optionnelles

Firewall

Compatible avec ...

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall
- Stormshield

Public Cloud

Compatible avec ...

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud

Identity

Compatible avec ...

- Okta
- Duo

Network Security

Compatible avec ...

- Darktrace
- Forcepoint
- McAfee (web gateway)

Email

Compatible avec ...

- Proofpoint
- Mimecast

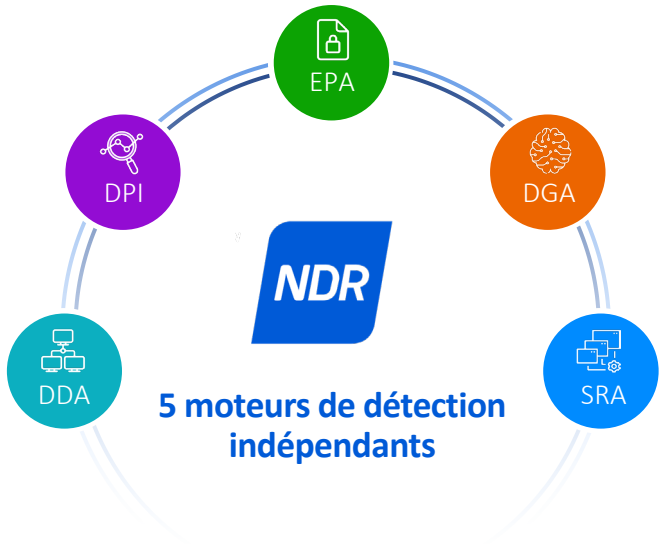
Sophos Network Detection and Response

Surveille en permanence l'activité réseau pour détecter les actions suspectes sur les périphériques.

1 an Conservation des données

Tous ces packs d'intégration sont disponibles pour Sophos MDR, Sophos MDR Complete, et Sophos Threat Advisor
Le Pack de conservation des données d'un an est disponible pour Sophos MDR and Sophos XDR
Chaque pack d'intégration doit être acquis en option et est comptabilisé par siège.

Détection de menaces réseau, génération de cas de suivi pour investigation et corrélation avec Sophos MDR



DDA **Device Detection Analytics**

Identifie la communication des équipements réseaux qui ne sont pas gérés par Sophos, ce qui inclue les périphériques non-autorisés et/ou potentiellement malveillants.

DGA **Domain Generation Algorithms**

Intelligence artificielle en 'deep learning' intégrant une mémoire à long terme pour prédire des noms de domaine générés automatiquement grâce à un algorithme.

DPI **Deep Packet Inspection**

Détecte les Indices de compromission (IOC) parmi le trafic en clair et le trafic chiffré afin d'identifier les acteurs et les TTP (Tactiques, Techniques et procédures)

SRA **Session Risk Analytics**

Moteur logique puissant qui utilise des règles qui alertent sur un facteur de risque basé sur des sessions (Certificats TLS auto-signé, transfert d'application binaire, etc.)

EPA **Encrypted Payload Analytics**

Détecte les serveurs de C&C zéro-Day et les nouvelles variantes de malware en se basant sur des patterns découverts dans les sessions réseaux (taille de paquets, sens du flux réseau et intervalles de temps).

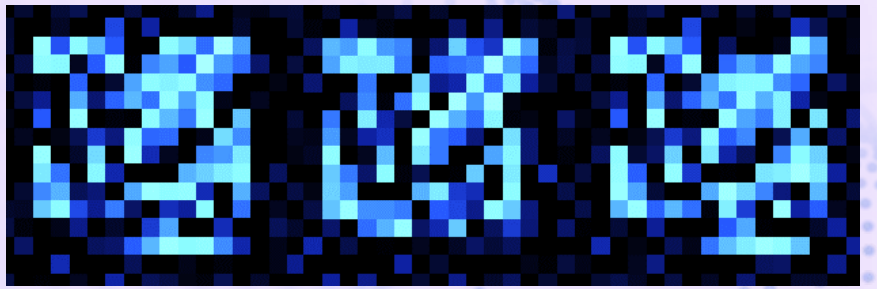
Sophos NDR

Encrypted Packet Analysis

EPA identifie les sessions de réseau générées par des familles de logiciels malveillants, sur la base de modèles trouvés dans la taille des paquets de la session, la direction et les temps de réponse.

Il s'agit d'un processus breveté de transformation et de présentation de ces caractéristiques à un réseau neuronal convolutif (CNN) à des fins de classification.

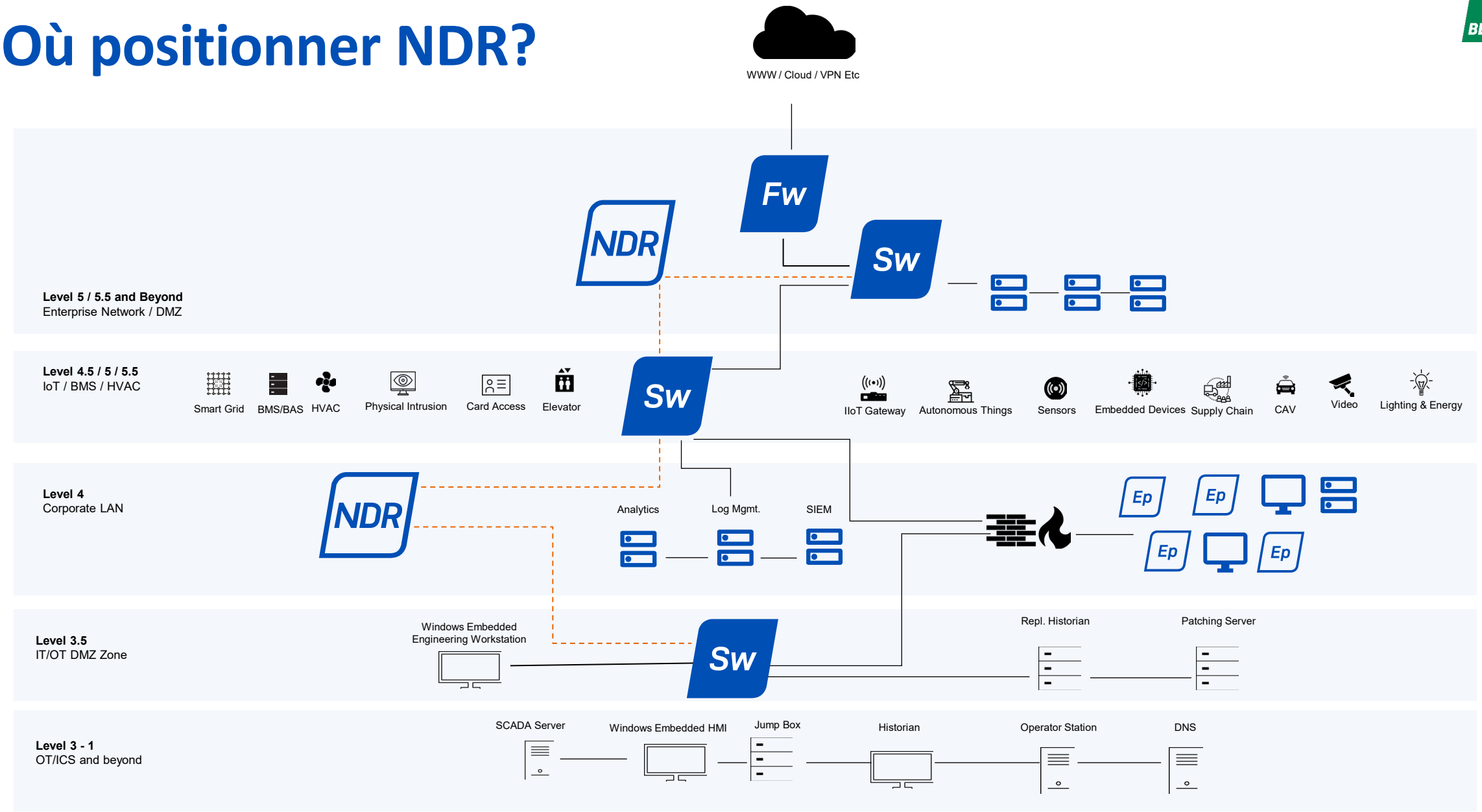
CobaltStrike sessions ready for EPA classification.



Les détections EPA sont basées sur la forme du flux du réseau, qui est une détection complètement indépendante.

(Limb, J. (2021). *Identifying Network Applications Using Images Generated from Payload Data and Time Data. US Patent 11,159,560.* Washington, DC: U.S.)

Où positionner NDR?



Détections et actions de réponses (à incident)

Répondre à une menace vs. Répondre à un incident

Réponse à menace	Réponse à incident
Action de **contenir** une menace pour **interrompre** une activité malveillante But: Empêcher la propagation de l'attaque et atténuer le risque qu'une menace se transforme en incident.	Action d'**éliminer un attaquant** d'un environnement et **remédier entièrement à la menace** But: Déterminer la cause racine, le calendrier et la portée de l'attaque afin de s'assurer que l'adversaire est totalement éliminé de l'environnement. Fournir des conseils pouvant être mis en œuvre pour atténuer le risque d'une attaque similaire à l'avenir.

Un incident critique est déclaré lorsque nous observons:

Exécution suspecte de code à partir d'un serveur web ou d'une application exploitée

- SolarWinds, ProxyShell, Confluence

Tentative réussie d'accès **aux identifiants** pour obtenir des informations d'authentification

Tentative de **désactivation** des solutions de protection Sophos

Mouvement latéral avec utilisation d'un compte privilégié pour effectuer d'autres actions sur les objectifs

- Impacket, activité suspecte liée à une connexion à distance à partir d'une adresse IP non gérée

Tentatives de **collecte** et/ou **d'exfiltration** de données

- Transferts de fichiers vers des sites d'hébergement

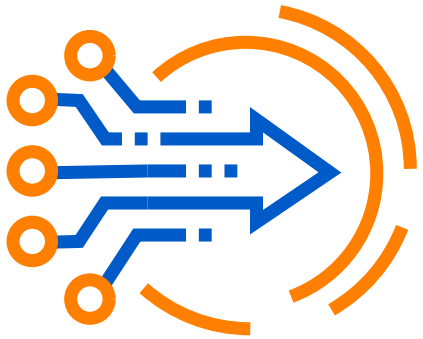
Tentatives de **cryptage** ou de **destruction** des données

- Ransomware, deleting files or systems

Travail collaboratif possible

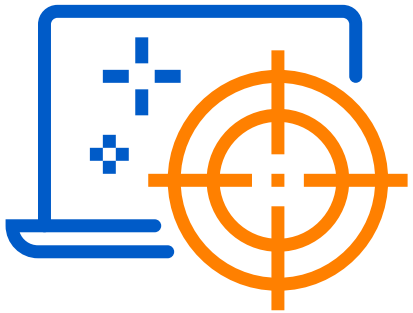
Notifier

Sophos: *„Sur ces 10 ordinateurs, nous avons constaté une attaque avec les activités suivantes.“*
Client: *„Merci, nous prenons le relais."*



Collaborer

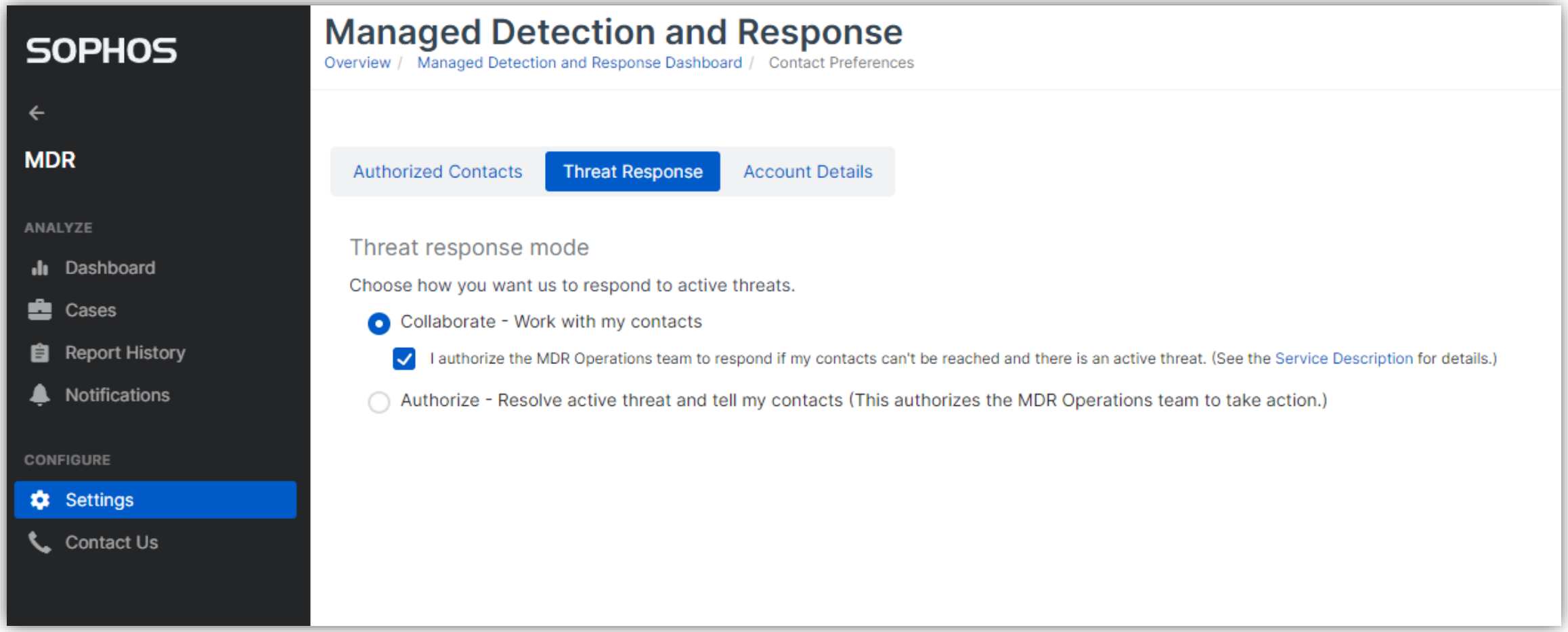
Sophos: *„Dans ce cas, devons-nous arrêter l'attaque?“*
Client: *„Oui, s'il vous plaît, mais demandez toujours pendant les heures de bureau, mais la nuit et le week-end, commencez immédiatement.!"*



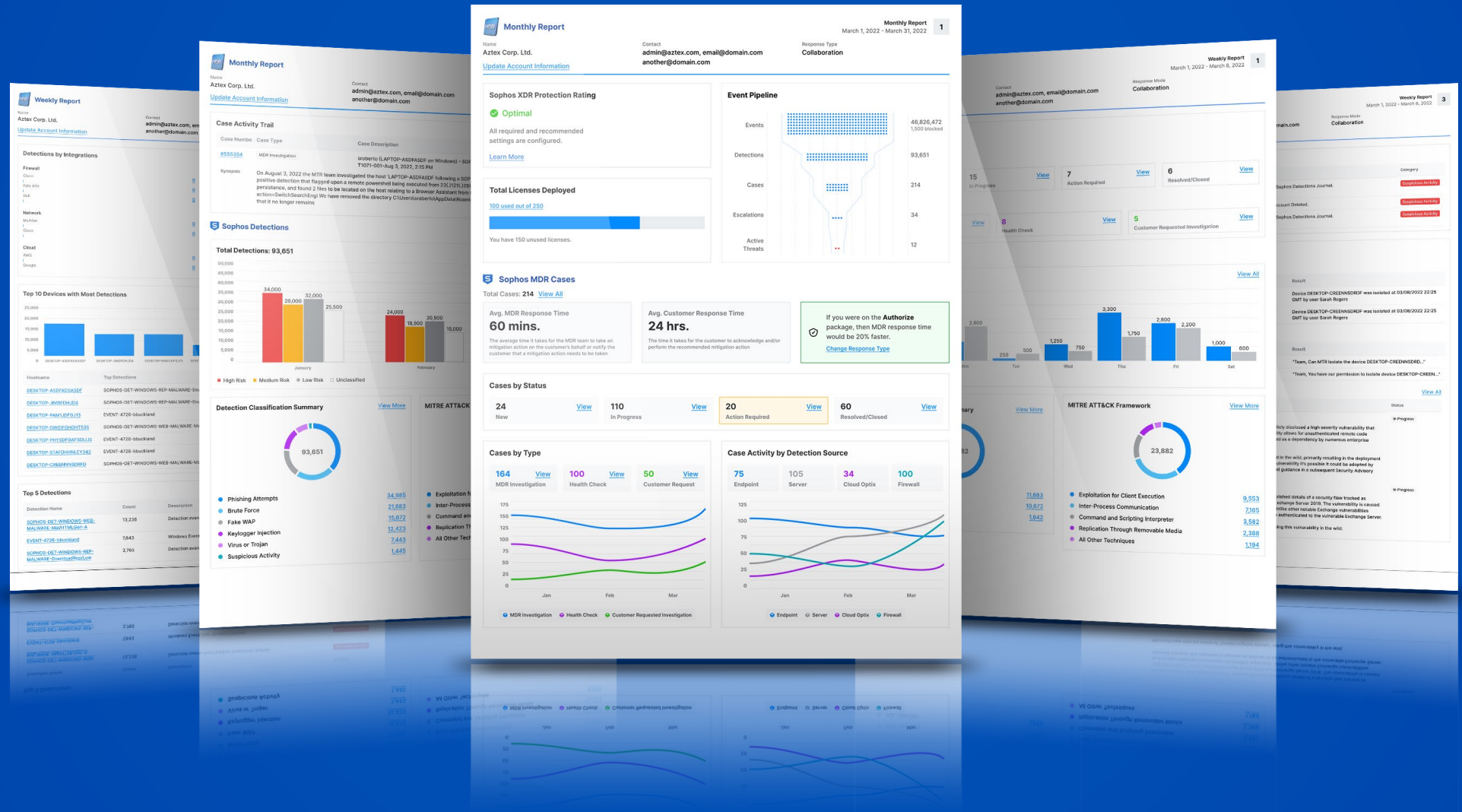
Autoriser

Client: *„SVP, neutralisez toute attaque avérée"*
Sophos: *„Ce sera fait."*

Travail collaboratif possible



Rapports hebdomadaires et mensuels



Sophos Endpoint Lineup

		Protection		Detection & Response	Managed Service
		Intercept X Essentials	Intercept X Advanced	Intercept X Advanced with XDR	MDR
Management	Multiple Policy Support	Single Policy	✓	✓	✓
Automated protection	Foundational techniques	✓	✓	✓	✓
	Deep learning malware detection	✓	✓	✓	✓
	Exploit and anti-ransomware	✓	✓	✓	✓
	Control Features (Web, App, Peripheral, DLP)		✓	✓	✓
	Threat Cases		✓	✓	✓
Detection & response	Live Discover and Live Response			✓	✓
	Sophos Data Lake retention			90+ days	90+ days
	On-device data retention			90 days	90 days
	Cross-product data sources			✓	✓
Managed detection & response	24/7 monitoring				✓
	Threat hunting				✓
	Incident response				✓
	Office 365 connector				

Sophos Service Tiers

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
24/7 expert-led threat monitoring and response	✓	✓	✓
Compatible with non-Sophos security products	✓	✓	✓
Weekly and monthly reporting	✓	✓	✓
Monthly intelligence briefing: “Sophos MDR ThreatCast”	✓	✓	✓
Sophos Account Health Check		✓	✓
Expert-led threat hunting		✓	✓
Threat Containment: attacks are interrupted, preventing spread Uses full Sophos XDR agent (protection, detection and response) or Sophos XDR Sensor (detection and Response)		✓	✓
Direct call-in support during active incidents		✓	✓
Full-scale Incident Response: threats are fully eliminated Requires full Sophos XDR agent (protection, detection and response)			✓
Root Cause Analysis: performed to prevent future recurrence			✓
Dedicated Incident Response Lead			✓
Breach Prevention Warranty			✓

BECHTLE

SOPHOS

The Sophos Breach Protection Warranty covers up to $1 million in response expenses

Included with new **Sophos MDR Complete** annual (term) subscriptions – at no additional cost

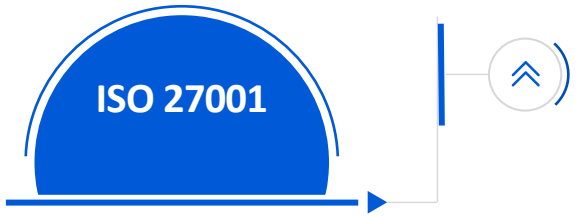
Built-in automatically with **1-, 2- and 3-year licenses**, both new customers and renewals

Comprehensive coverage: endpoints, servers, Windows, macOS, no geographic limits

Underwritten by Sophos, demonstrating our confidence in our protection

For full terms and conditions of the warranty see www.sophos.com/legal.

Sophos MDR Delivers to ISO 27001



By delivering 24/7 threat detection, investigation and response across the full security environment, Sophos MDR enables organizations to meet some of the security controls in Annex A of the ISO/IEC 27001:2013.

ISO 27001 Requirement		Sophos MDR
Operations Security	**A.12.2.1** Controls against malware	24/7 detection and neutralization of malicious attacks by human experts, leveraging AI, technologies and threat expertise
Information Security Incident Management	**A.16.1.2** Reporting information security events	Full incident response service including 24/7 coverage delivered by IR experts
	A.16.1.5 Response to information security incidents	Full incident response service including 24/7 coverage delivered by IR experts
	A. 16.1.6 Learning from information security incidents	Full root cause analysis post incident, enabling the identification of the underlying cause of the incident and for security posture weaknesses to be addressed
Information Security Aspects of Business Continuity Management	**A.17.1.2** Implementing information security continuity	24/7 detection of and response to security incidents across the IT environment, leveraging human expertise, AI, and advanced technologies

Aspects financiers

- Services de remédiation et investigations
- SOC externe (notification)
- EDR de l’éditeur Z
- Endpoint de l’éditeur Y
- Firewall du fabricant X

Coûts divisés par 3

Merci!

Des questions? Contactez-nous: it-forum.ch@bechtle.com

Plus d‘informations :
bechtle.com