SEE THE FUTURE
SOPHOS DISCOVER

Emotet et Matrix : Analyse, Protection Next-Gen, apports de l'IA et de l'EDR

Michel Lanaspèze
Directeur Marketing Europe de l'Ouest

SOPHOS

Agenda

- Introduction
- Emotet
- De SamSam à Matrix: ransomwares ciblés
- Protections Next-Gen
- Mieux répondre aux attaques: démocratiser l'EDR avec l'IA

Sophos en quelques chiffres

1985
FONDÉ À OXFORD
(Royaume-Uni)

770 M$
ANNÉE FISCALE 2018
(VENTES)

3 300+
EMPLOYÉS
(APPX.)

SIÈGE
ABINGDON, RU

300 000+
ENTREPRISES CLIENTES

100M+
UTILISATEURS

39 000+
PARTENAIRES CHANNEL

Premier éditeur d'origine européenne de solutions de sécurité pour les entreprises

- 5 SophosLabs dont **2 en Europe**

  Oxford, Budapest, Vancouver, Ahmedabad, Sydney

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

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

Sophos en quelques dates

Évolution vers une sécurité complète

- Société
- Protection Utilisateurs
- Protection Réseaux

1985 — Fondation à Abingdon (Oxford), Royaume-Uni

Peter Lammer
1985

Jan Hruska
1985

1988 — Premier logiciel d'antivirus à base de checksum

1989 — Premier logiciel antivirus à base de signatures

2003 — Acquisition ActiveState

2008 — Acquisition Utimaco Safeware AG

2011 — Acquisition Astaro

2012 — Acquisition Dialogs

2014 — IPO London Stock Exchange

2014 — Acquisition Cyberoam

2014 — Acquisition Mojave

2015 — Acquisition Reflexion

2015 — Lancement de Synchronized Security Security Heartbeat

2015 — Acquisition Surfright

2016 — Acquisition PhishThreat

2016 — Acquisition Barricade

2017 — Acquisition Invincea

2019 — Acquisition AVID

2019 — Acquisition DarkBytes

SOPHOS

Sophos: double Leader Réseaux + Endpoint

*Seul éditeur double leader des Magic Quadrants **UTM** + **Endpoint Protection***

Gartner Magic Quadrant
UNIFIED THREAT MANAGEMENT

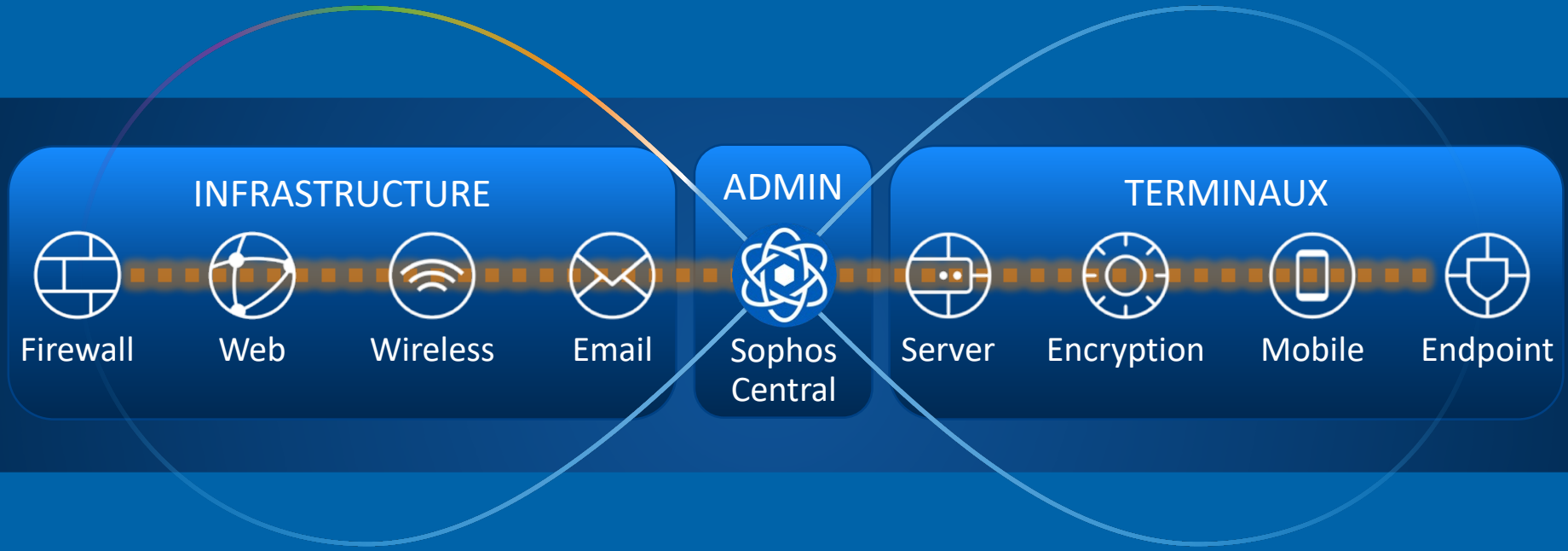
Magic Quadrant for Unified Threat Management
Rajpreet Kaur, Claudio Neiva - 20 septembre 2018

Gartner Magic Quadrant
ENDPOINT PROTECTION PLATFORMS

Magic Quadrant for Endpoint Protection Platforms
Ian McShane, Avivah Litan, Eric Ouellet, Prateek Bhajanka - 24 janvier 2018

Sécurité Synchronisée

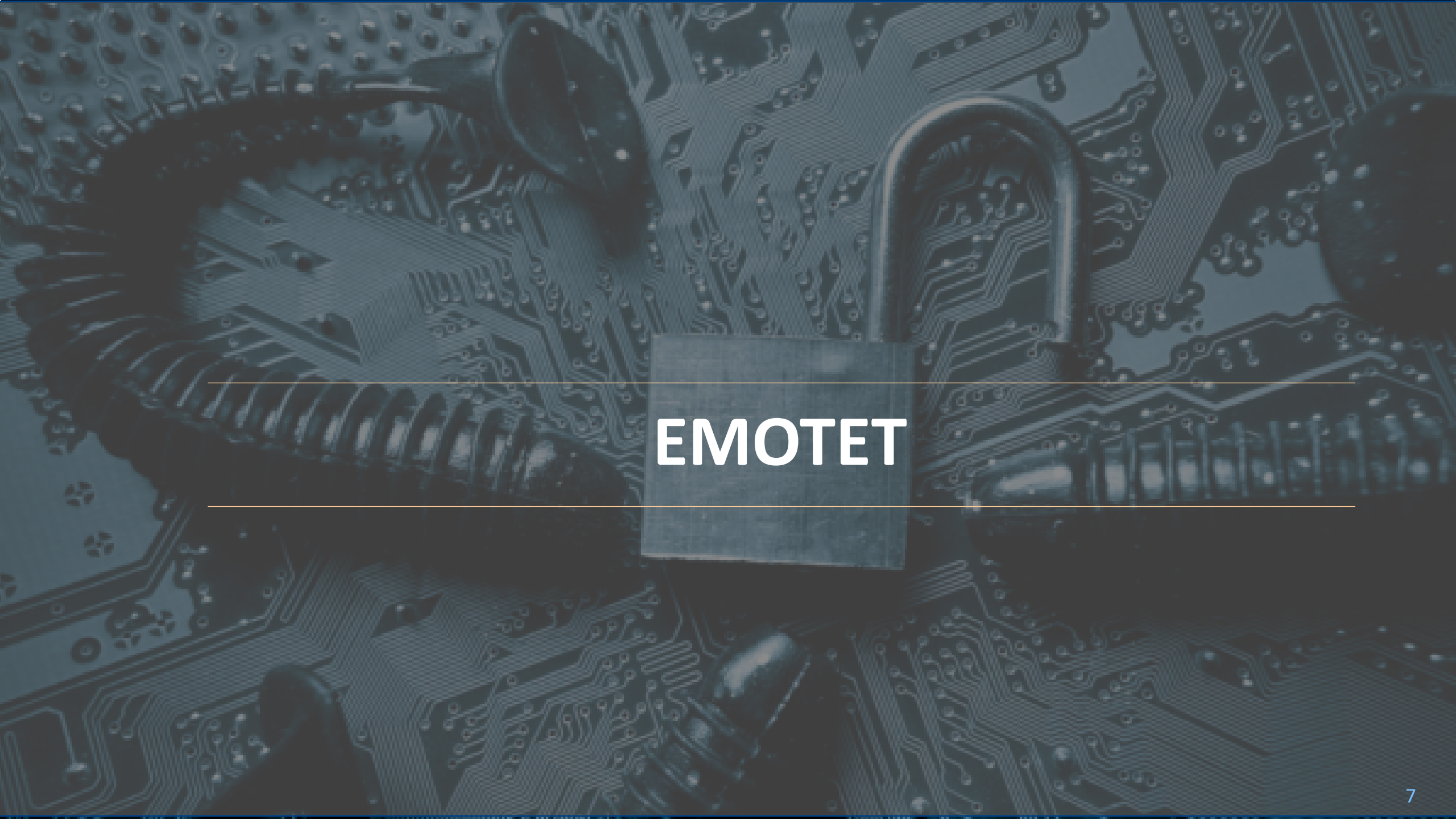
Analytics | Analyse les données provenant de tous les produits Sophos pour une meilleure visibilité, corrélation et automatisation



Sophos Labs | Réseau d'analystes mondial 24x7x365 | URL Database | Malware Identities | File Look-up | Genotypes | Reputation | Behavioural Rules | APT Rules Apps | Anti-Spam | Data Control | SophosID | Patches | Vulnerabilities | Sandboxing |

2015	2016	2017	2018
• Endpoint + Firewall • Security Heartbeat ™ • Isolement Automatique	• Endpoint + Chiffrement • Heartbeat ™ Destination • Absence d'état Heartbeat ™	• Contrôle applicatif synchronisé • Heartbeat ™ sur Linux • Heartbeat ™ sur Mac Os	• Endpoint & Mobile + WiFi • Endpoint & Email + PhishThreat • Blocage des attaques latérales

SOPHOS



EMOTET

EMOTET

"Amongst the most costly and destructive threats to U.S. businesses right now"

U.S. Department for Homeland Security, 2018

Cheval de Troie dérobant silencieusement les informations de compte bancaire des victimes

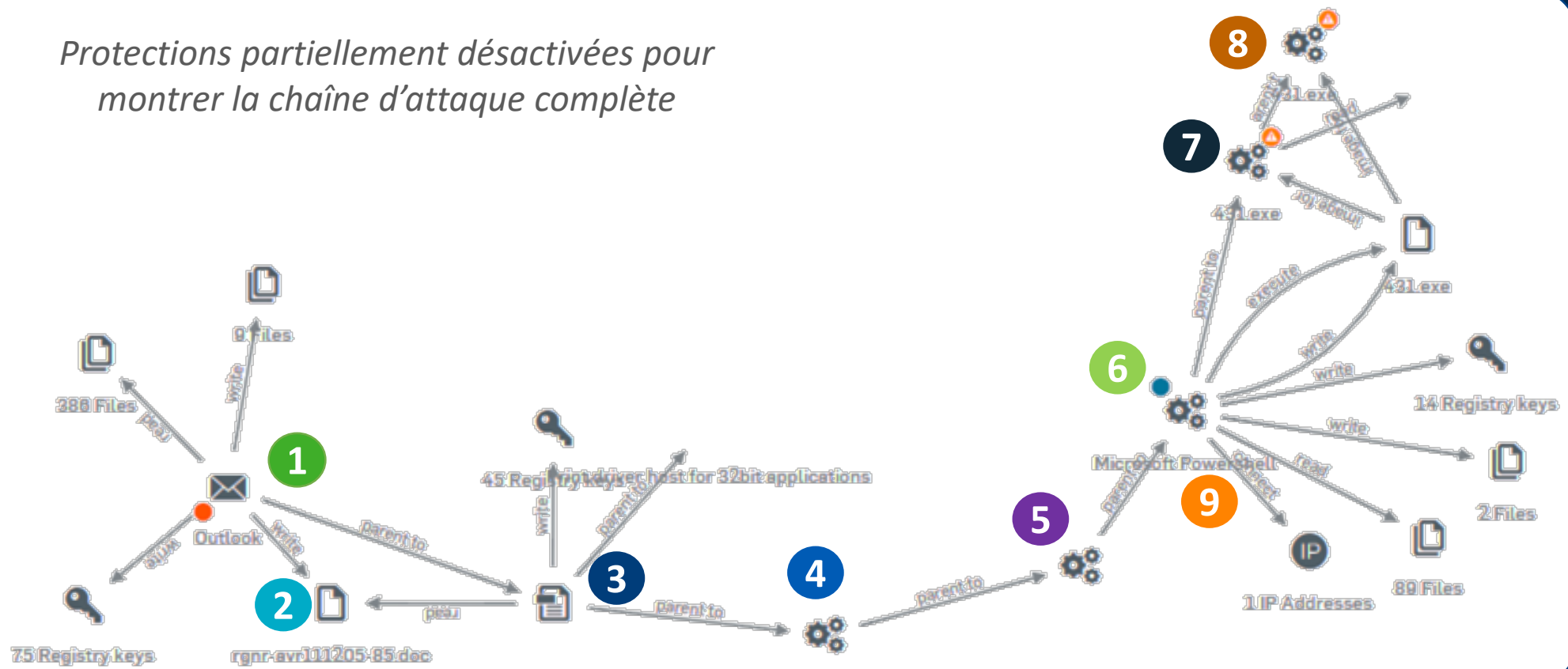
Ver réseaux hautement sophistiqué distribuant d'autres malwares, en particulier des Chevaux de Troie bancaires

2014

2019

EMOTET : Chaîne d'attaque

Protections partiellement désactivées pour montrer la chaîne d'attaque complète



1. L'utilisateur reçoit un email malveillant (malspam)
2. L'utilisateur clique sur une pièce jointe malveillante: rgnr-avr111205-85.doc
3. L'utilisateur active des macros malveillantes dans le document
4. La macro utiliset CMD (Command Prompt) pour exécuter un code obfusqué
5. CMD lance une deuxième copie de CMD
6. La seconde copie lance Microsoft Powershell.
7. Powershell se connecte à une adresse IP et télécharge un fichier appelé 431.exe
8. Powershell exécute 431.exe
9. Sophos HIPS détecte la connection Powershell vers une adresse IP suspecte avec téléchargement d'exécutable de reputation douteuse, et intervient

EMOTET : Quels sont ses buts ?

Se diffuse à travers le réseau

Ecran de fumée pour des attaques de ransomware ciblées

Infections secondaires

Envoie du spam pour infecter d'autres organisations

Atteinte à la réputation

Vole les historiques des navigateurs, noms et mots de passe

Violations de sécurité

Télécharge une charge virale

Infection primaire

Recherche les addresses emails et les contacts

Atteintes aux données personnelles

EMOTET : Pourquoi est-il si dangereux ?

Une machine suffit

Evolution continue

Réinfections incessantes

De SamSam à Matrix: ransomware ciblé

Du ransomware de masse … au ransomware ciblé

WannaCry, NotPetya etc…		SamSam, Matrix …
Diffusion explosive		Quelques attaques par jour
Attaques indiscriminées	vs.	Attaques ciblées
Quelques semaines		Perdurent des années

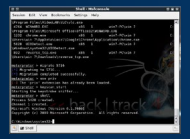
Des familles nombreuses et anciennes

	SamSam	Dharma	Matrix	BitPaymer	Ryuk	GandCrab
Active	No	Yes	Yes	Yes	Yes	Yes
First appeared	2015	2016	2016	2017	2018	2018
Type	Targeted	Targeted	Targeted	Targeted	Targeted	Targeted
Infection vector	RDP Exploit	RDP	RDP Exploit	RDP	RDP	RDP Email Exploit
Victim size	Med/large	Small/med	Med/large	Med/large	Med/large	Any
computers targeted	Servers/ endpoints	Servers	Any	Servers	Servers	Any
Attack frequency	Med	High	Low	Med	Med	High
Regions affected	All	All	All	All	All	All
Decryption available	No	No	No	No	No	Some variants
Ransom currency	Bitcoin	DASH	Bitcoin	Bitcoin	Bitcoin	Bitcoin
Avg.ransom	$50k	$5k	$3.5K	$500k	$100k	$800
Payment method	Dark Web	Email	Email	Email Dark Web	Email	Dark Web

Persistence

Techniques d'attaques de style APT

- Choix et étude minutieuse de la victime
- Infiltration + Expansion *« Land + Expand »*
- Persistence + Progression silencieuse et manuelle



MIGRATION DE PROCESSUS MALVEILLANT

ÉLÉVATION DE PRIVILÈGES DE PROCESSUS

VOL D'IDENTIFIANTS

MODIFICATIONS DE LA BASE DE REGISTRES

CODE CAVE

VIOLATION APC ATOM BOMBING

MAN-IN-THE-BROWSER

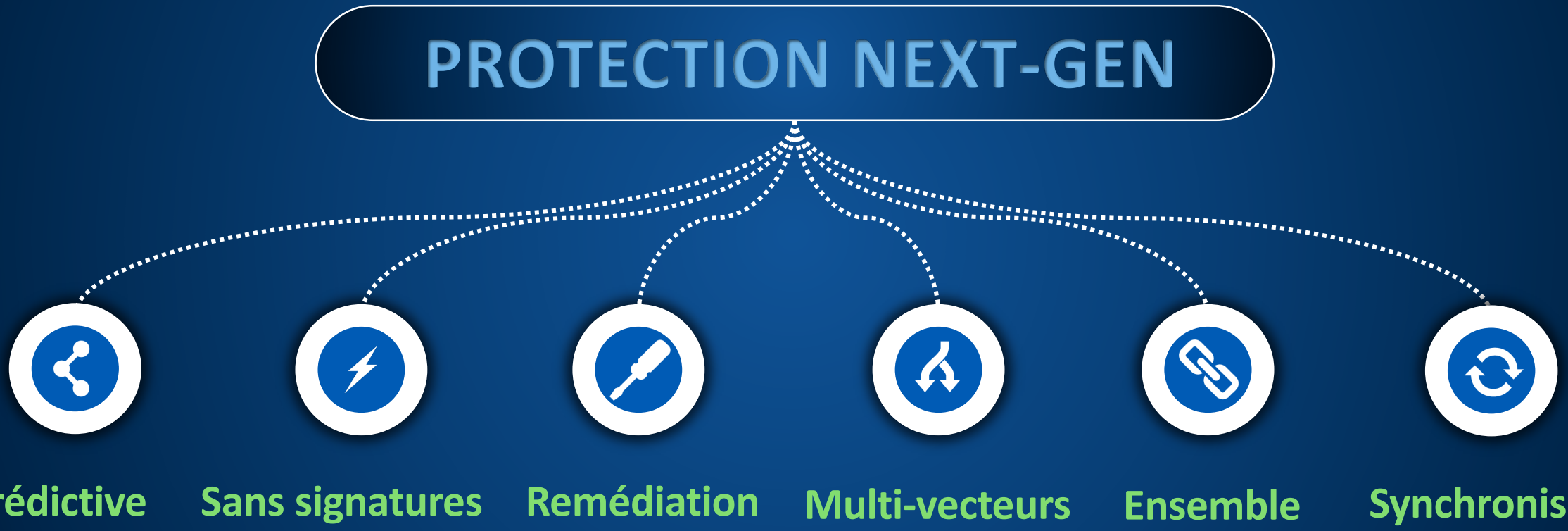
- Recherche des ressources les plus sensibles (serveurs)
- Frappe brutale et ciblée

Protection Next-Gen

Protection Next-Gen

Une nouvelle approche de la sécurité

SOPHOS | discover
This is NEXT-GEN



Protection Réseaux
Next-Gen

XG FIREWALL

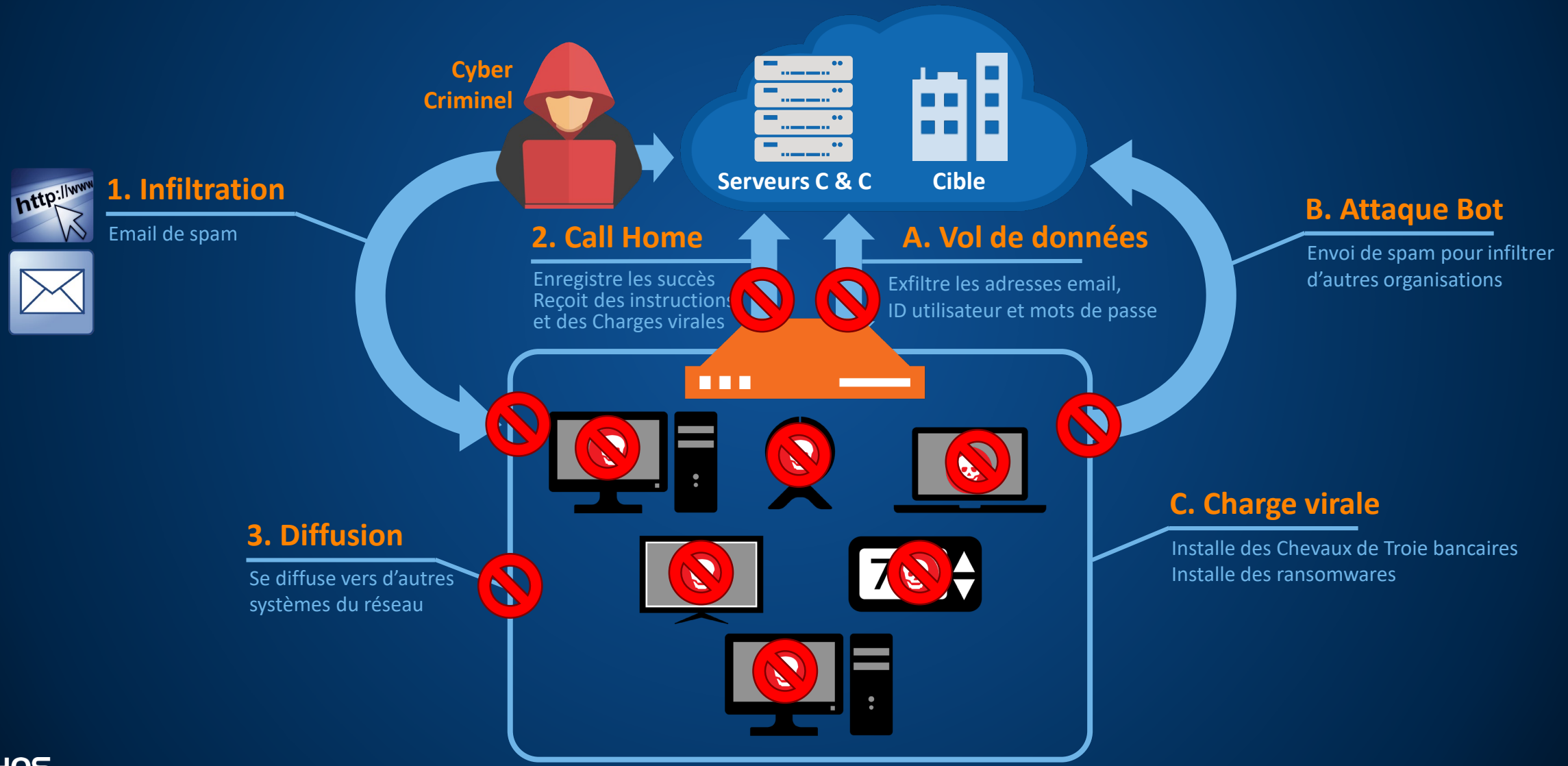
Protection Endpoint
Next-Gen

SOPHOS INTERCEPT X

Sécurité
Synchronisée

Intervenir à tous les niveaux de l'attaque

L'exemple d'EMOTET

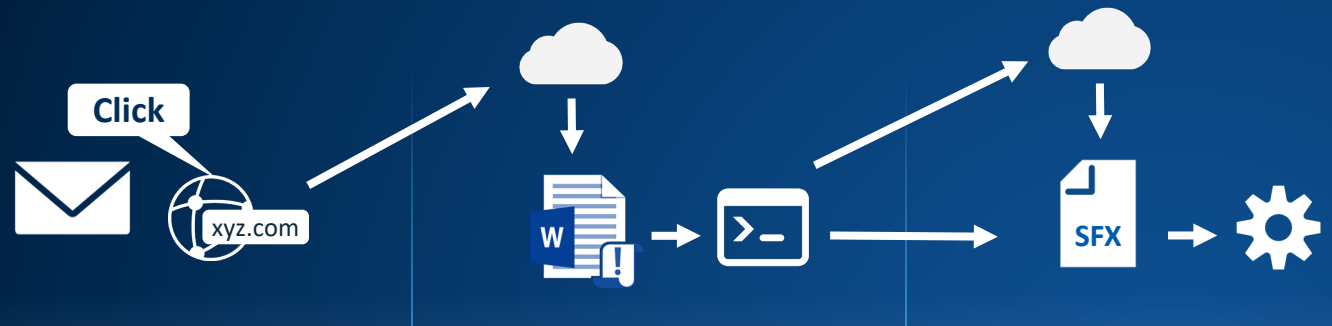


Intervenir à tous les niveaux

L'exemple d'EMOTET

XG FIREWALL

SOPHOS INTERCEPT X



Livraison	Exploitation	Installation	Commande & Contrôle	Actions sur la cible
WEB PROTECTION	CODE/MEMORY/APC MITIGATIONS APPLICATION LOCKDOWN LOCAL PRIVILEGE MITIGATION APPLICATION CONTROL	DEEP LEARNING HIPS	NETWORK THREAT PROTECTION	ANTI-RANSOMWARE CREDENTIAL THEFT PROTECTION RUNTIME HIPS THREAT CASE (RCA) & EDR

SOPHOS

Protection Endpoint Next-Gen

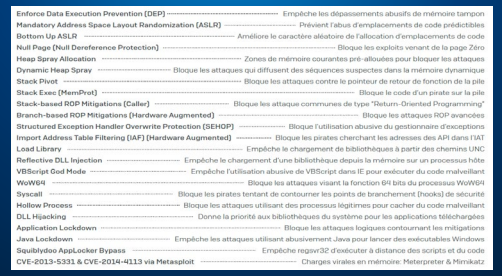
Protections avancées sans signatures

INTERCEPT X NOW WITH EDR

Anti-Exploit

Blocage des techniques utilisées par les exploits

- 24+ techniques bloquées
- Protection Zero-Day
- Bloque les attaques en mémoire sans fichiers
- 10+ ans d'expertise en R&D et de technologies SurfRight



Anti-piratage (APT) & Anti-ransomware

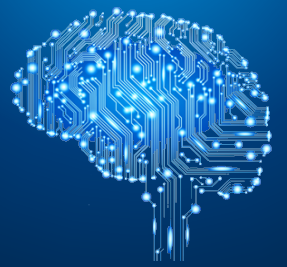
Détection des menaces avancées

- **Anti-piratage (APT)**
  - Credential Theft, Code Cave Utilization, Malicious Process Migration, Process Privilege Escalation, APC violation, Registry modification, Process Lockdown
- **Anti-Ransomware**
  - Blocage du chiffrement malveillant
  - Analyses comportementales
  - Restitution des fichiers originels

Deep Learning

Anti-malware à base de Deep Learning

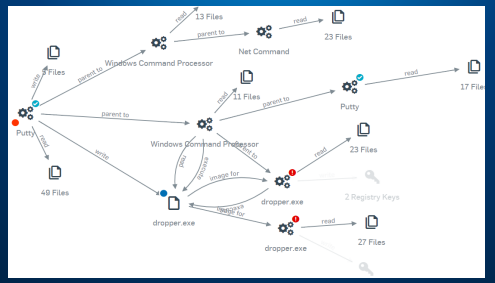
- Sans signatures
- Fiable et éprouvé
- 10+ ans d'expertise en R&D et de technologies Invincea
- Enrichi de l'expertise et des données des SophosLabs



EDR Endpoint Detection & Response

Détection, analyse et réponses automatisées

- Détection des menaces latentes infiltrées dans la chaîne d'attaque
- Analyse détaillée assistée par Deep Learning et les SophosLabs
- Remédiation automatisée
- Nettoyage avancé



SOPHOS

Anti-Exploit: des vulnérabilités toujours plus présentes

Un des principaux risques en matière de sécurité

Source: NIST National Vulnerability Database
https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

Anti-Exploit: protection à large spectre

10+ années d'expertise anti-exploit | 25+ techniques d'exploit bloquées

Enforce Data Execution Prevention (DEP)	Empêche les dépassements abusifs de mémoire tampon
Mandatory Address Space Layout Randomization (ASLR)	Prévient l'abus d'emplacements de code prédictibles
Bottom Up ASLR	Améliore le caractère aléatoire de l'allocation d'emplacements de code
Null Page (Null Dereference Protection)	Bloque les exploits venant de la page Zéro
Heap Spray Allocation	Zones de mémoire courantes pré-allouées pour bloquer les attaques
Dynamic Heap Spray	Bloque les attaques qui diffusent des séquences suspectes dans la mémoire dynamique
Stack Pivot	Bloque les attaques contre le pointeur de retour de fonction de la pile
Stack Exec (MemProt)	Bloque le code d'un pirate sur la pile
Stack-based ROP Mitigations (Caller)	Bloque les attaque communes de type "Return-Oriented Programming"
Branch-based ROP Mitigations (Hardware Augmented)	Bloque les attaques ROP avancées
Structured Exception Handler Overwrite Protection (SEHOP)	Bloque l'utilisation abusive du gestionnaire d'exceptions
Import Address Table Filtering (IAF) (Hardware Augmented)	Bloque les pirates cherchant les adresses des API dans l'IAT
Load Library	Empêche le chargement de bibliothèques à partir des chemins UNC
Reflective DLL Injection	Empêche le chargement d'une bibliothèque depuis la mémoire sur un processus hôte
VBScript God Mode	Empêche l'utilisation abusive de VBScript dans IE pour exécuter du code malveillant
WoW64	Bloque les attaques visant la fonction 64 bits du processus WoW64
Syscall	Bloque les pirates tentant de contourner les points de branchement (hooks) de sécurité
Hollow Process	Bloque les attaques utilisant des processus légitimes pour cacher du code malveillant
DLL Hijacking	Donne la priorité aux bibliothèques du système pour les applications téléchargées
Application Lockdown	Bloque les attaques logiques contournant les mitigations
Java Lockdown	Empêche les attaques utilisant abusivement Java pour lancer des exécutables Windows
Squiblydoo AppLocker Bypass	Empêche regsvr32 d'exécuter à distance des scripts et du code
CVE-2013-5331 & CVE-2014-4113 via Metasploit	Charges virales en mémoire: Meterpreter & Mimikatz

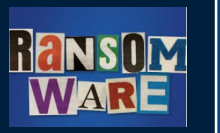
SOPHOS

Protection contre attaques avancées et APT

Protection contre les techniques d'attaques ciblées

INTERCEPT X NOW WITH EDR

ANTI-RANSOMWARE



Stoppe les techniques d'attaque par ransomware

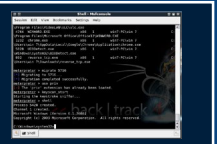
VOL D'IDENTIFIANTS

Stoppe les techniques qui collectent les identifiants utilisateur

ÉLÉVATION DE PRIVILÈGES DE PROCESSUS

Détecte l'insertion d'un jeton de noyau pour élever les privilèges

MIGRATION DE PROCESSUS MALVEILLANT

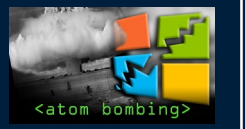


Empêche le mouvement vers des processus distants pour persistance

CODE CAVE

Détecte le code caché dans des applications légitimes

VIOLATION APC et ATOM BOMBING



Détecte les violations APC et les abus sur la table ATOM

MODIFICATIONS DE LA BASE DE REGISTRES

Empêcher l'exécution de code arbitraire via la base de registres

VERROUILLAGE DE PROCESSUS

Bloque le lancement de Powershell, de macros … pour injecter du code

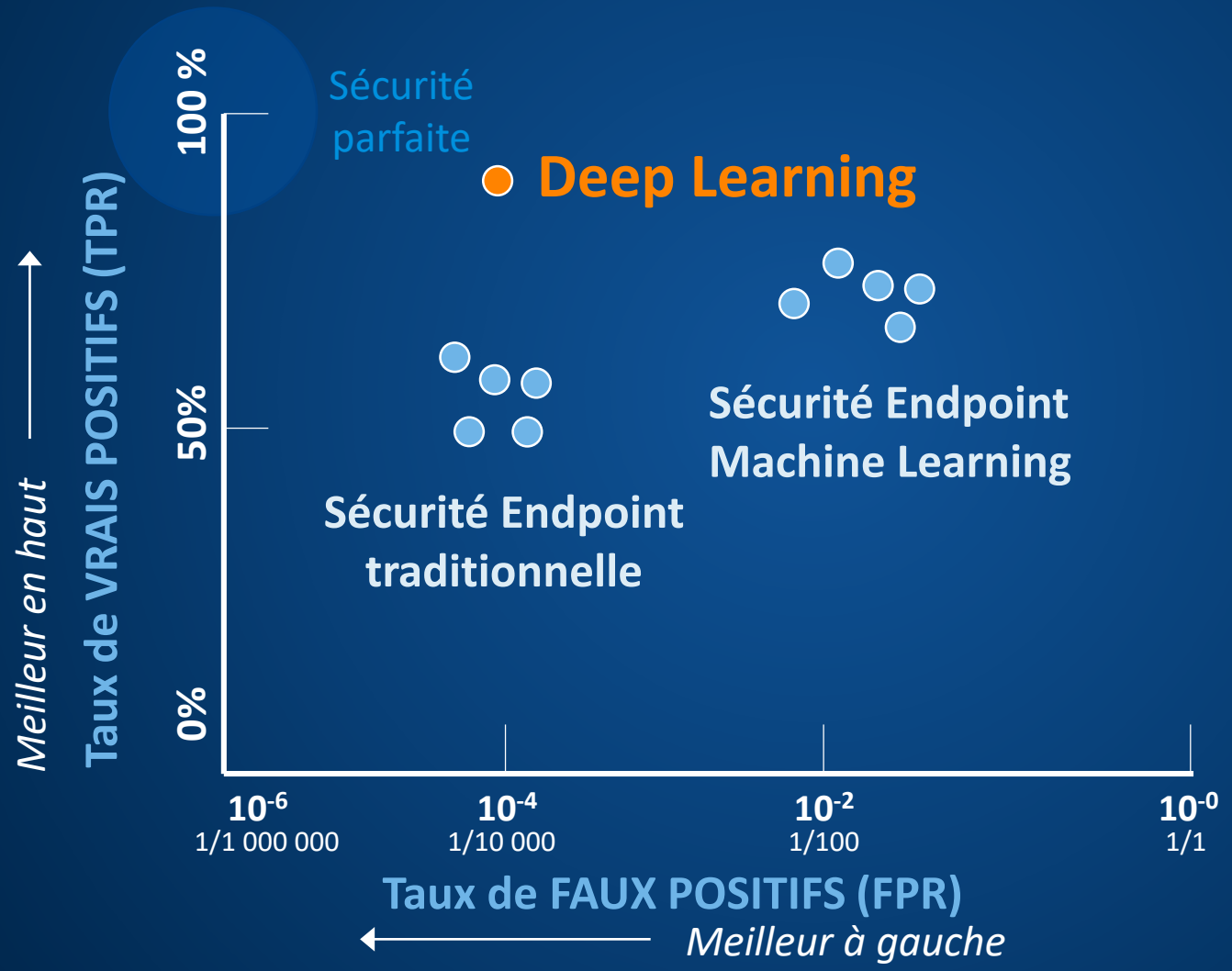
MAN-IN-THE-BROWSER

Prévient les modifications illicites du browser pouvant conduire à des attaques

SOPHOS

Deep-Learning: bloquer les menaces inconnues

Meilleure protection, meilleure précision, meilleures performances



Meilleure protection

Meilleure précision

Meilleures performances

SOPHOS

Deep-Learning: bloquer les menaces inconnues

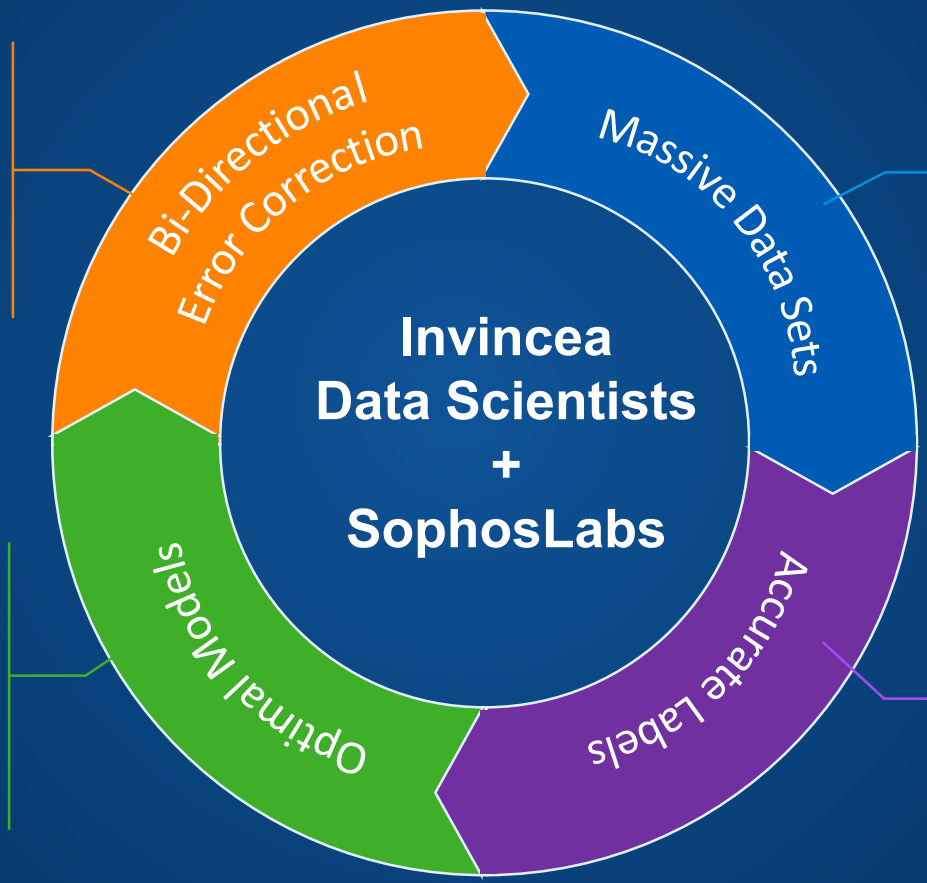
L'union fait la force: Data Scientists Invincea + SophosLabs

DATA SCIENTISTS + SOPHOS LABS:

Intègrent en continu les retours d'expérience pour améliorer la precision et le pouvoir prédictif

DATA SCIENTISTS:

Créent les algorithmes les plus efficaces pour résoudre les problems de cybersécurité les plus complexes



SOPHOS LABS:

Collectent des centaines de millions d'échantillons pour permettre la meilleure prédiction possible

SOPHOS LABS:

Utilisent les systèmes et processus éprouvés des Labs pour réaliser une catégorisation précise

"Pour la première fois, nous pouvons prendre en compte tout l'univers des données observables."

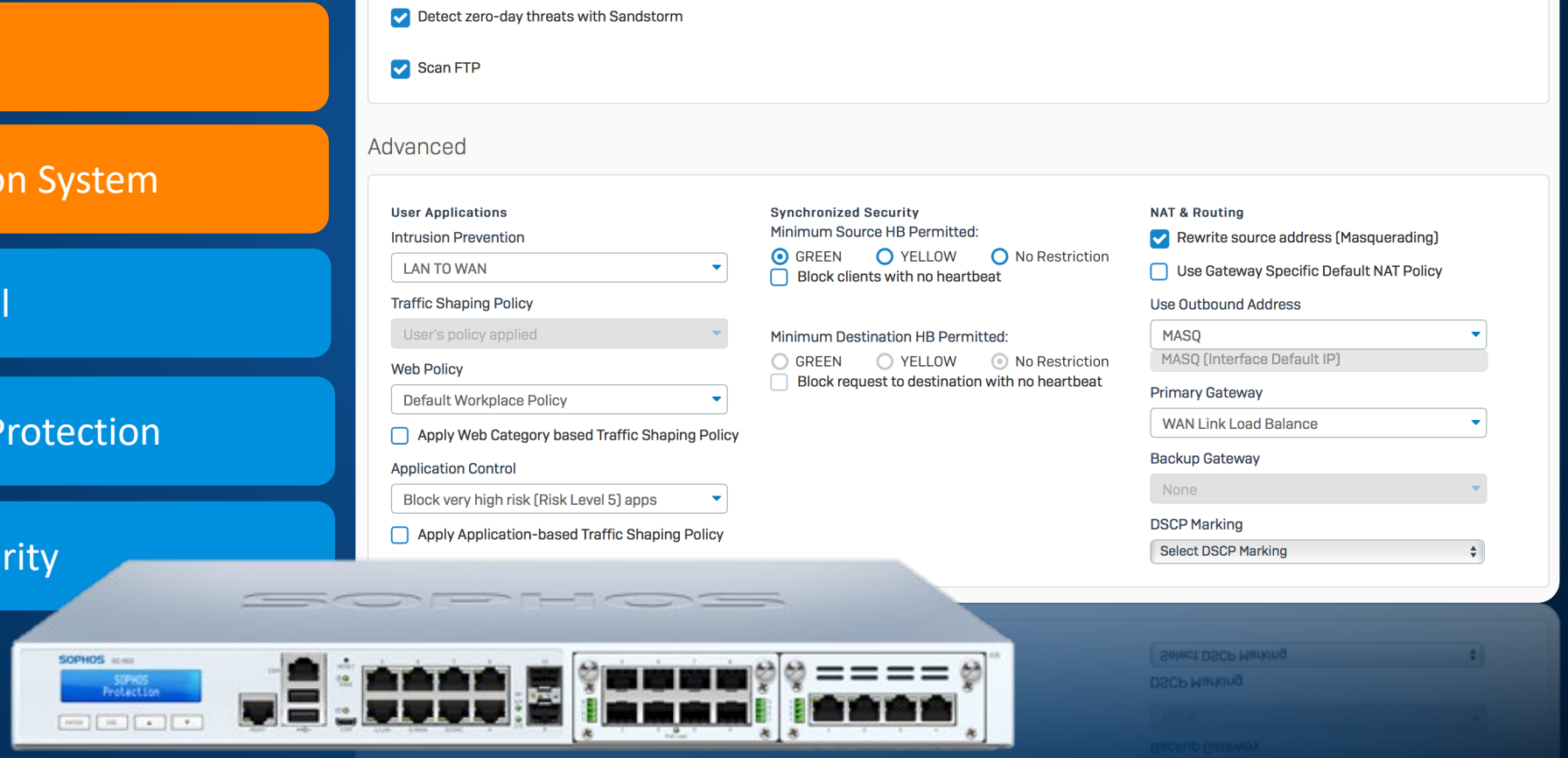
SOPHOS

XG Firewall – Bloquer l'infiltration

Bloque Emotet avant qu'il n'atteigne le réseau

XG FIREWALL

- Web and Email Protection
- Sandboxing
- Intrusion Prevention System
- Application Control
- Advanced Threat Protection
- Synchronized Security



SOPHOS

Sophos Sandstorm Sandboxing

Protection contre les menaces Zero Day et les menaces avancées

XG FIREWALL

Deep Memory Analysis		Deep Behavioural Analysis		Deep Network Analysis		Deep Learning Analysis	
Initial & Post Execution Memory Inspection & Analysis	Frequent & Aggressive Run-Time Analysis	Sandbox Evasion Techniques, API & File System Behavior	Intercept X Exploit Detection & CyrptoGuard	Full port and protocol analysis	IPS detections	Analysis of all dropped executables	Continuously adaptive learning model

Sophos Sandstorm

SOPHOS

Intrusion Prevention System (IPS)

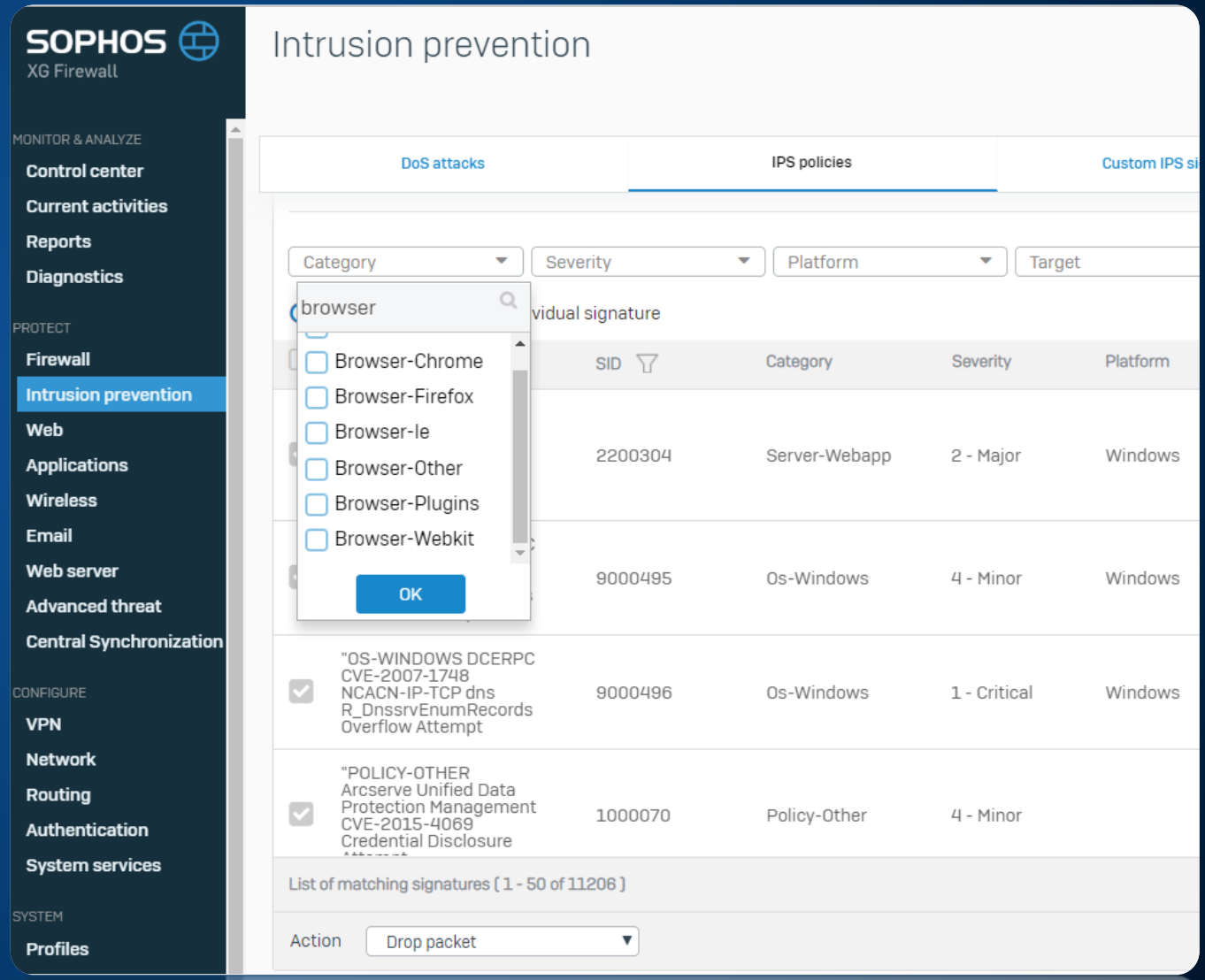
L'équivalent réseaux de la détection des Exploits

Comment cela fonctionne-t-il ?

- Inspecte le traffic réseaux
  à la recherche d'exploits
- Détecte les exploits sur les systèmes
  d'exploitation, les piles réseaux, les serveurs,
  les systèmes Endpoints, les navigateurs,
  les applications, etc ….

Pourquoi Sophos ?

- NSSLabs:
  Top 3 pour l'Efficacité sécurité et la Performance
- Granularité des catégories
  pour optimiser la performance et la protection



Advanced Threat Protection (ATP)

Bloque la communication avec les pirates et l'exfiltration de données

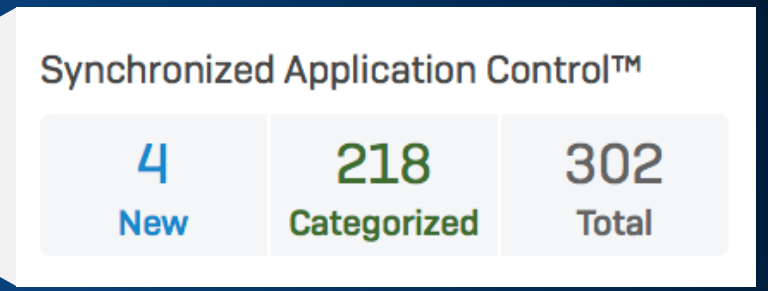
XG FIREWALL

- Web and Email Protection
- Sandboxing
- Intrusion Prevention System
- Advanced Threat Protection
- Application Control
- Synchronized Security

SOPHOS

Contrôle des Applications

Visibilité complete sur la totalité du traffic applicatif



DES CENTAINES

D'APPS NON VISIBLES AUPARAVANT

INCLUANT DES APPLICATIONS

MALVEILLANTES

PRÉSENTES

SUR VOTRE RÉSEAU

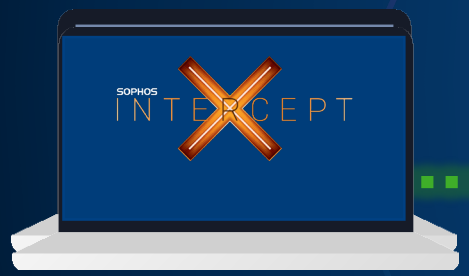
Sécurité Synchronisée

Automatisation de la corrélation et de la remédiation

1 Détection
Intercept X détecte l'exécution d'Emotet

2 Communication Endpoint-Firewall
Intercept X informe immédiatement XG Firewall du système sur lequel il a détecté Emotet

3 Isolement du poste infecté
XG Firewall isole automatiquement les systèmes infectés par Emotet.
- Isolement du monde extérieur
- Isolement des autres Endpoint



Security Heartbeat™

5 Accès restauré automatiquement
XG Firewall restaure automatiquement l'accès réseaux. L'investigation guidée fournit une analyse détaillée de toute les séquences de la chaîne d'attaque.

4 Nettoyage
Intercept X nettoie automatiquement l'infection. Une fois Emotet éradiqué, Intercept X partage cette information d'état avec XG Firewall

Démocratiser l’EDR avec l’IA

Endpoint Detection & Response + Deep Learning

Détecter et éradiquer les menaces latentes

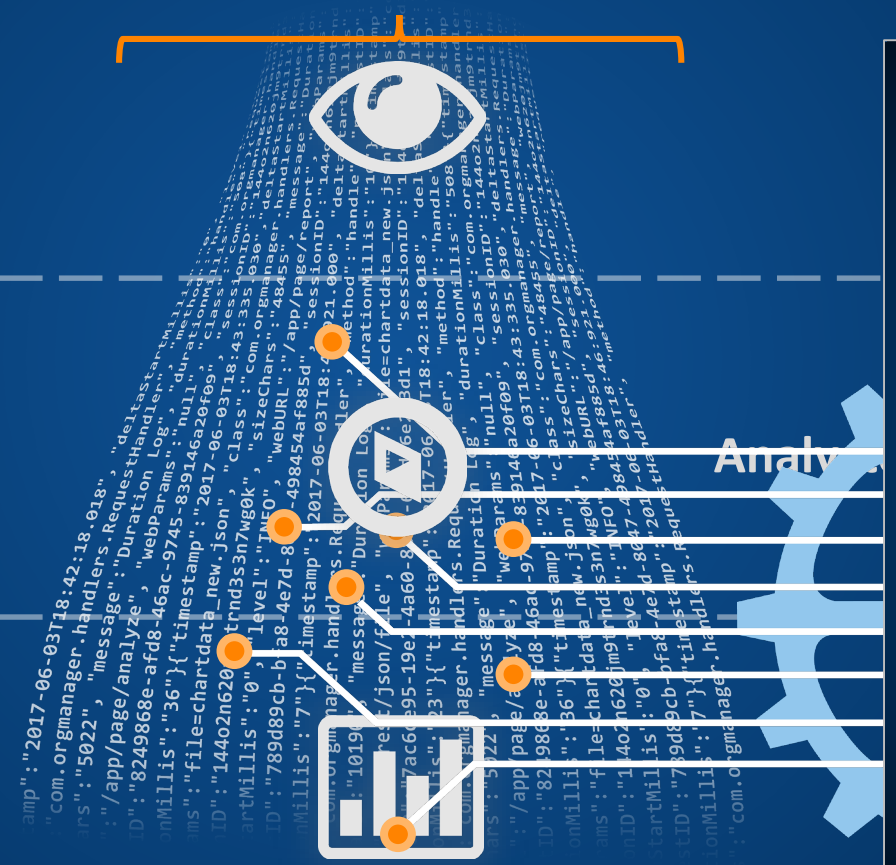
INTERCEPT X NOW WITH EDR

Visibilité
Compréhension, priorités et actions à mener

Explorer
Identifier, enquêter et rechercher

Données
Corrélées, contextualisées et organisées

Expertise augmentée par l'IA



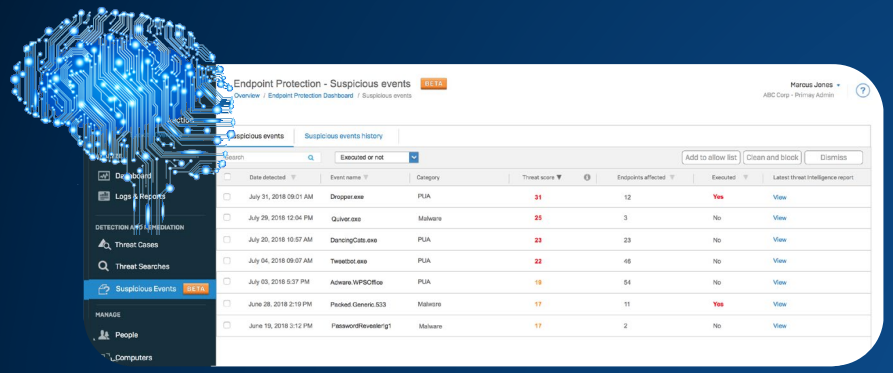
- ***Expertise d'identification et de gestion des priorités***
  Bloquer les menaces avant qu'elles ne frappent
- ***Expertise d'analyse***
  Comprendre et circonscrire le risque
- ***Réponse guidée aux incidents***
  Activation des réponses sur un simple clic

Expertise cybersécurité augmentée par l'IA

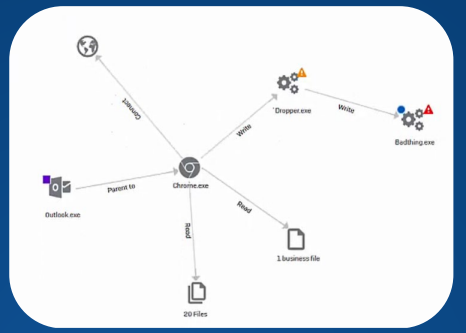
SOPHOS

EDR: contribution du Deep Learning

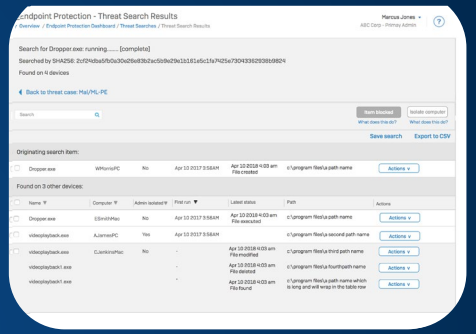
Une journée dans la vie d'un analyste EDR



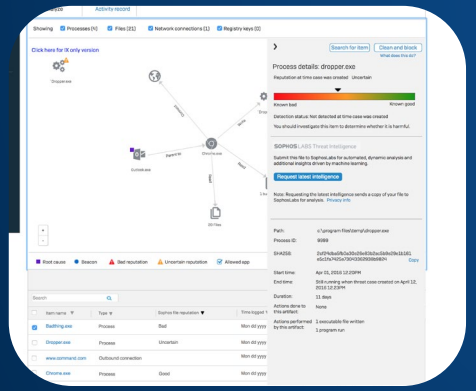
Identifier les "événements" suspects à examiner, tels que Dropper.exe



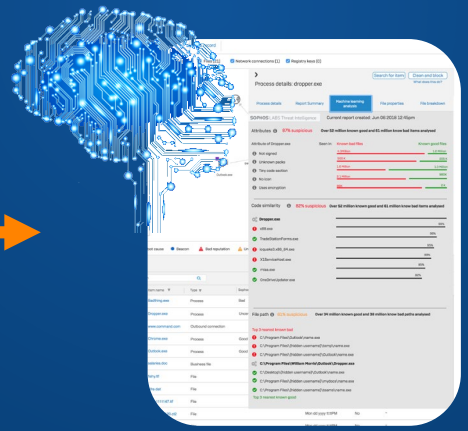
Examiner la chaîne d'attaque ayant mené à l'identification de Dropper.exe



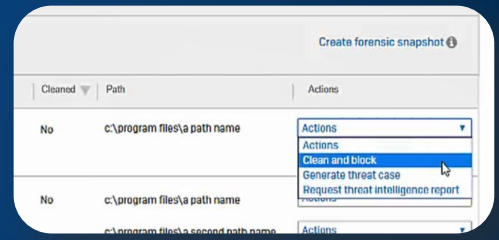
Trouver tous les endroits où Dropper.exe est présent



Obtenir une analyse détaillée des SophosLabs



Analyser le code pour déterminer si le fichier est malveillant

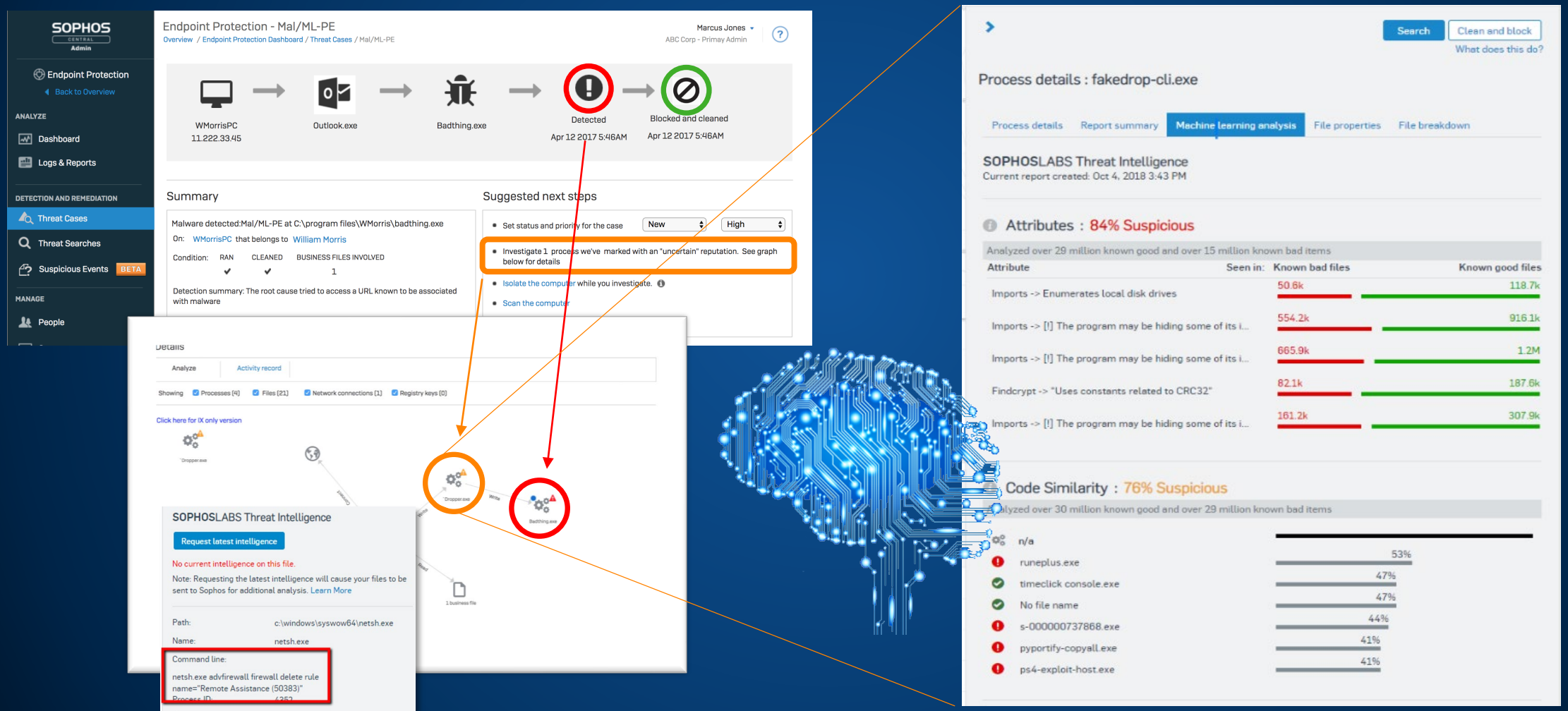


Remédier à la menace: bloquer, nettoyer et prévenir

SOPHOS

Démocratiser l'EDR avec le Deep learning

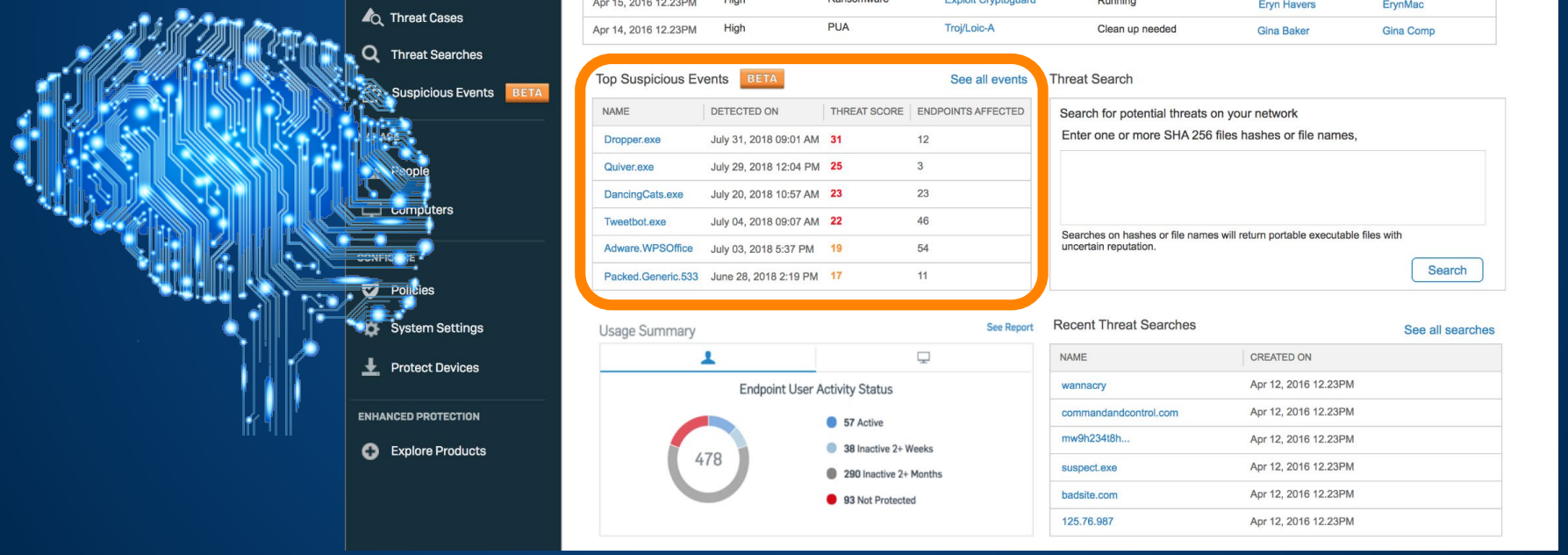
Investigation guidée et analyse détaillée grâce au Deep Learning



SOPHOS

Démocratiser l'EDR avec le Deep learning

Détection et organisation des priorités grâce au Deep Learning



Un seul agent … pour une protection complète

Agent Endpoint unique = Protections classiques + Next-Gen

INTERCEPT X NOW WITH EDR

Prévenir

*Corréler les indicateurs de menaces pour bloquer les menaces web, les applications illégitimes, les URLs dangereuses et les codes malicieux **avant exécution**.*

Détecter

*Analyser le comportement **à l'exécution** des codes et du trafic réseau, vous alertant en cas de menaces cachées.*

Répondre

Supprime les malwares, isoler les systèmes compromis, rechercher les menaces latentes, remédier et prévenir les attaques

Technologies classiques

- Contrôle des périphériques
- Contrôle des apps
- Contrôle de contenu
- Contrôle du Web
- Réputation des téléchargement
- Analyse statique des fichiers
- Analyse génotype
- Analyse dynamique des fichiers
- Détection du trafic malveillant
- Analyse comportementale
- Security Heartbeat ™
- Blocage
- Quarantaine
- Verrouillage des clés
- Alertes
- Logs et rapports
- Sécurité Synchronisée

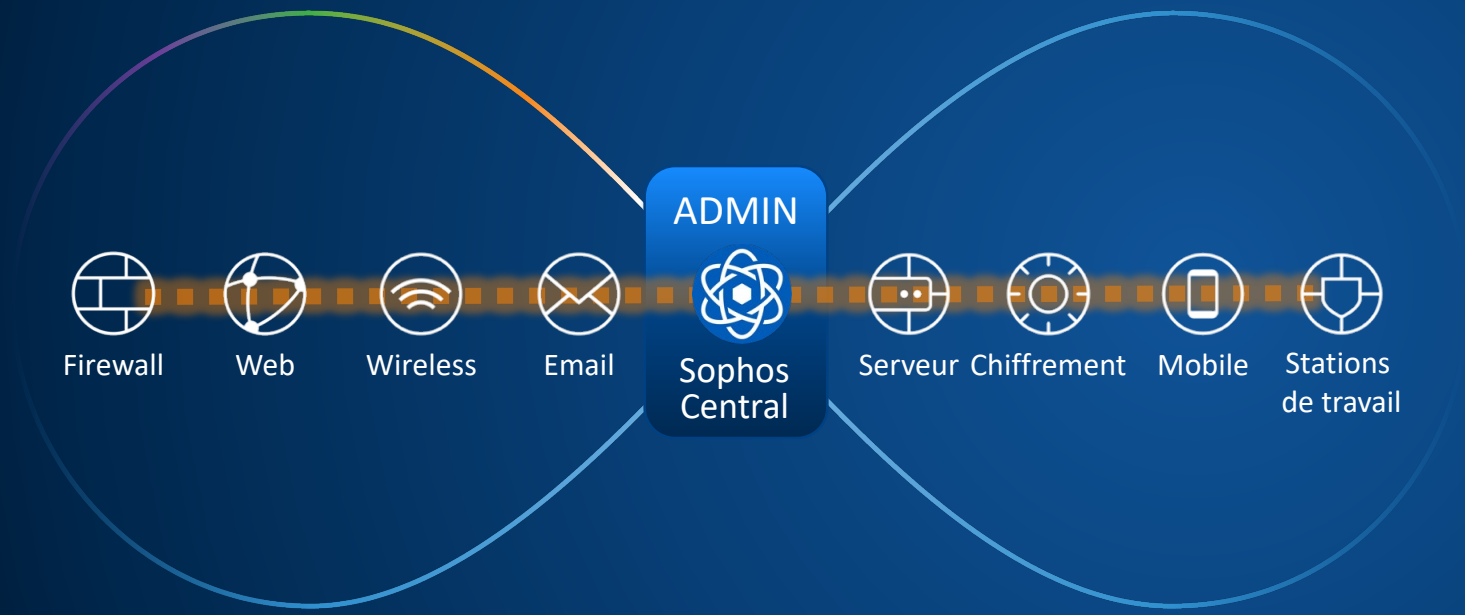
Technologies Next-Gen

- Deep Learning
- Anti Exploit
- Anti Piratage
- Anti Ransomware
- Wipe Guard
- EDR
- Restauration
- Nettoyage avancé

SOPHOS

Un seul agent … synchronisé

Sécurité synchronisée avec l'ensemble de l'infrastructure



Firewall + Endpoint
Isole les systèmes compromis
Bloque l'accès aux systèmes compromis
Bloque la propagation latérale
Identifie et contrôle les applications
Accélère l'analyse et la remédiation

WiFi + Endpoint
Bloque l'accès des postes infectés

Email + Endpoint
Scanne les postes émetteurs de spam

PhishThreat + Endpoint
Enrôle dans un cours de sensibilisation un utilisateur au comportement risqué

Chiffrement + Endpoint
Suspend les clés des postes infectés

SOPHOS

SOPHOS

Cybersecurity made simple.