SOPHOS

Sophos Network Detection and Response

# Renforcer les opérations de sécurité avec Sophos Network Detection and Response (NDR)

*Un livre blanc Sophos. Avril 2023*

# Introduction

Dans le paysage en constante évolution des menaces, les entreprises doivent adopter une démarche proactive pour identifier et répondre aux cyberattaques potentielles. La technologie Network Detection and Response (NDR) joue un rôle essentiel dans cette stratégie.

La technologie NDR s'appuie sur le Deep Learning, des correspondances traditionnelles basées sur des règles, et des statistiques de flux basées sur des risques, afin d'analyser le trafic brut et d'identifier les activités suspectes et potentiellement malveillantes sur le réseau. Tout ce travail permet aux équipes de sécurité d'adopter des mesures proactives pour empêcher les attaques et, le cas échéant, minimiser leur impact.

Le problème, cependant, provient du fort taux de faux positifs, un défi courant et inhérent à la technologie NDR. La solution Sophos NDR apporte une réponse à cette problématique, en utilisant une technologie brevetée de clustering et de scoring qui recoupe les preuves issues de multiples moteurs de détection des menaces.

Si la technologie NDR existe depuis les années 1990, elle varie d'un fournisseur à l'autre en termes de complexité et de précision. Il est essentiel pour les entreprises d'envisager une solution NDR robuste telle que Sophos NDR, qui offre des niveaux avancés de détection des menaces et permet d'obtenir des verdicts tout en minimisant les faux positifs. Ce livre blanc présente les fonctionnalités et les avantages de Sophos NDR, et il explique pourquoi il devrait faire partie intégrante des opérations de sécurité de toute entreprise.

# Sommaire

## Évolution de la surveillance de la sécurité réseau : chronologie de la technologie NDR

Sophos NDR est aujourd'hui un composant essentiel des opérations de sécurité modernes, mais la technologie NDR remonte aux années 1990, lorsque les systèmes de détection d'intrusion réseau (ou NIDS pour Network Intrusion Detection System) ont fait leur apparition. À leurs débuts, les systèmes NIDS visaient avant tout à identifier et à bloquer les attaques au niveau du réseau, mais ils n'étaient pas capables de corréler plusieurs événements ou de détecter les menaces avancées qui s'étendaient sur plusieurs systèmes.

Au début des années 2000, la technologie NDR a évolué pour remédier à ces limites. Au lieu de simplement repérer les attaques au niveau du réseau de façon isolée, les solutions NDR ont commencé à analyser le trafic réseau et à corréler les événements sur de multiples systèmes pour identifier les menaces avancées. Sophos NDR est une solution NDR leader sur le marché, qui s'appuie sur le Deep Learning, les correspondances traditionnelles basées sur des règles, et les statistiques de flux basées sur des risques, afin d'analyser le trafic brut et d'identifier les activités suspectes et potentiellement malveillantes sur le réseau.

Au fil du temps, la technologie NDR a gagné en sophistication, offrant une visibilité en temps quasi réel sur les activités réseau et s'intégrant de manière transparente aux autres solutions de sécurité. Le tableau chronologique suivant présente les principales étapes de l'évolution de la technologie NDR :

| ANNÉE(S) | ÉTAPE |
|---|---|
| Années 1980 | Les produits de sécurité réseau commencent à émerger, la technologie des pare-feux (Firewall) étant largement adoptée. |
| Années 1990 | Les systèmes NIDS (Network Intrusion Detection System) font leur apparition, marquant le début de la surveillance de la sécurité réseau. |
| Années 2000 | La technologie NDR (Network Detection and Response) évolue pour analyser le trafic réseau et corréler les événements entre plusieurs systèmes. |
| Années 2010 | Des algorithmes avancés de Machine Learning sont intégrés aux solutions NDR afin d'identifier les menaces complexes et de réduire les faux positifs. |
| 2016 | Le botnet Mirai, qui exploite les appareils connectés (IoT), lance l'une des plus grandes attaques par déni de service distribué (DDoS) de l'histoire, soulignant le besoin de renforcer la sécurité réseau. |
| 2019 | Gartner introduit l'expression Network Detection and Response (NDR) pour remplacer le terme précédent Network Traffic Analysis (NTA). |
| Années 2020 | Les solutions NDR offrent une visibilité en temps réel et des options de déploiement flexibles, permettant aux entreprises de les déployer dans n'importe quel environnement. |

Les solutions NDR telles que Sophos NDR fournissent aux entreprises un outil efficace de détection et de réponse aux menaces avancées.

# Sophos NDR : surveillance réseau avancée pour les menaces modernes

Sophos NDR est une solution avancée de surveillance du réseau conçue pour répondre à la complexité et à l'évolution du paysage des menaces.

Contrairement aux solutions NDR classiques, Sophos NDR associe plusieurs moteurs de détection propriétaires à des analyses de Deep Learning, ce qui permet d'obtenir des informations en temps réel et exploitables sur un large éventail de menaces réseau.

Les moteurs de détection propriétaires de Sophos NDR classent le trafic réseau en fonction de plus de 330 protocoles, 50 risques de flux et des milliers d'indicateurs de compromission (IOC). Ces moteurs intègrent également les prédictions de multiples modèles de Deep Learning, offrant ainsi un niveau de précision sans précédent dans la détection des menaces tout en minimisant les faux positifs.

Ces améliorations sont particulièrement utiles pour la technologie NDR car elles permettent à Sophos NDR d'identifier et de répondre avec précision aux menaces réseau sans générer un nombre excessif de faux positifs. Grâce à sa rapidité, sa précision et sa capacité à traiter le trafic chiffré sans avoir à le déchiffrer, Sophos NDR est aujourd'hui un outil indispensable à toute stratégie de sécurité qui se veut intégrale.

Sophos NDR offre aux entreprises une solution de surveillance réseau avancée, conçue pour détecter les menaces et y répondre efficacement dans un cyber environnement en constante mutation. En combinant de multiples moteurs de détection propriétaires à des analyses de Deep Learning, Sophos NDR fournit des informations exploitables, à la fois précises et pertinentes, pour faire face aux menaces modernes.

**Avantages clés de Sophos NDR :**

| NDR TRADITIONNEL | SOPHOS NDR | AMÉLIORATION |
|---|---|---|
| Nombre limité de protocoles | Plus de 330 protocoles réseau | Sophos NDR classe le trafic en utilisant plus de 330 protocoles. Il obtient ainsi une vue plus complète du trafic réseau, condition indispensable pour identifier les menaces nouvelles et émergentes. Voir l'Annexe B pour une liste complète des protocoles. |
| IOC de base | Des milliers d'IOC | Sophos NDR utilise des milliers d'IOC (indicateurs de compromission), se traduisant par un niveau accru de précision dans la détection des menaces. |
| Identification minimale des risques de flux | 50 risques de flux | Sophos NDR intègre 50 risques de flux dans ses moteurs de détection propriétaires, ce qui permet de détecter des menaces plus complexes qui pourraient passer inaperçues aux yeux d'autres solutions NDR. Voir l'Annexe A pour une liste complète des risques de flux. |
| Correspondance basée sur des règles | Analyses de Deep Learning | Sophos NDR utilise l'analyse de Deep Learning pour fournir un niveau de précision sans précédent dans la détection des menaces tout en minimisant les faux positifs. |
| Taux de faux positifs élevés | Technologie brevetée de clustering et de scoring | Sophos NDR utilise une technologie brevetée de clustering et de scoring pour réduire les faux positifs et fournir des informations exploitables sur un large éventail de menaces réseau. |

## Architecture conceptuelle du capteur NDR

La solution Sophos NDR se déploie comme un outil de surveillance du trafic passif inspectant un port SPAN/Miroir. Elle n'ajoute aucune latence au trafic et ne crée pas de point d'échec dans le réseau si celui-ci devient surchargé ou hors ligne.

À mesure que les données entrent dans le capteur, des métadonnées sont collectées et les détails du flux réseau sont envoyés à une série de moteurs de détection avant d'être regroupés et notés. Les résultats des flux réseau regroupés sont envoyés au Data Lake de Sophos et présentés dans le tableau de bord des détections de Sophos Central.

## Traitement des paquets réseau (NPP pour Network Packet Processing)

La collecte efficace des métadonnées sur les flux réseau est un élément essentiel au succès des solutions NDR. Ce processus implique d'agréger les paquets réseau en une seule communication ou flux, et de recueillir les métadonnées de chaque paquet réseau grâce au moteur DPI (Inspection approfondie des paquets). Les métadonnées collectées sont ensuite enrichies d'informations de géolocalisation et d'autres mesures, telles que les destinations impopulaires, la périodicité et la dynamique des paquets. L'étape finale consiste à détecter les indicateurs de risque tels que les mauvaises informations TLS, le trafic unidirectionnel, les paquets DNS volumineux, etc.

Pour mieux comprendre les informations « En-tête des paquets » et « Couche applicative » collectées pendant cette phase, les tableaux suivants donnent des exemples, en expliquant à quoi elles correspondent et pourquoi elles sont importantes dans la chasse aux menaces.

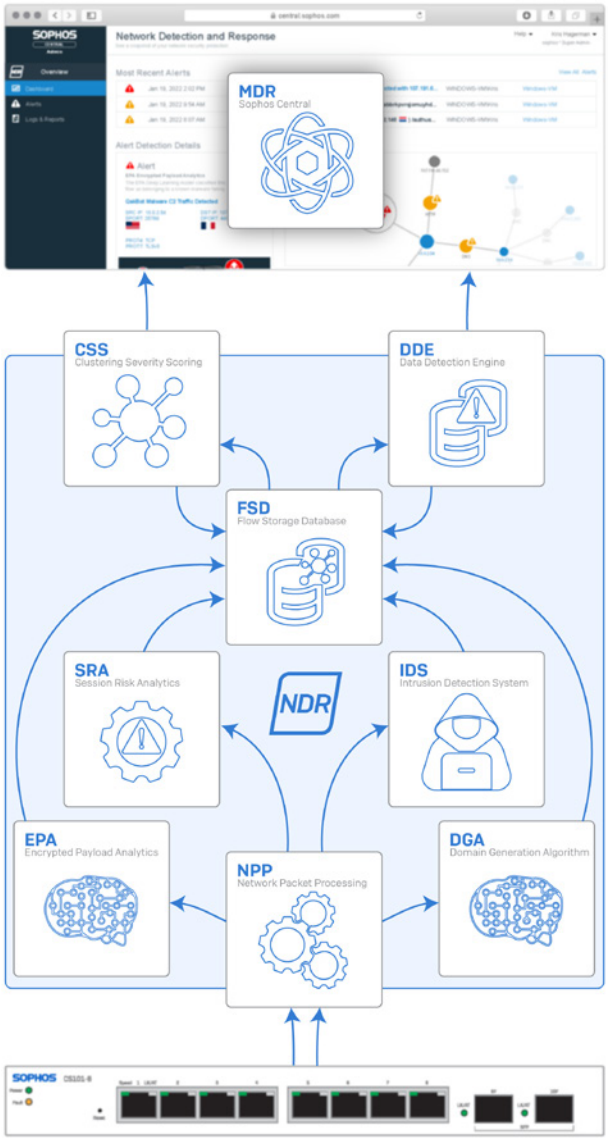


Figure 1 : Schéma architectural de Sophos NDR

## NPP : Données 'En-tête des paquets'

Les données En-tête des paquets fournissent des informations sur la communication réseau, telles que les adresses source et destination, le protocole de transport, la durée et la taille. Elles aident les solutions NDR à identifier la source de la communication et la menace potentielle qu'elle peut représenter. Voici quelques-unes des informations pouvant être tirées des données 'En-tête des paquets' :

| DONNÉES 'EN-TÊTE DES PAQUETS' | DESCRIPTION | IMPORTANCE DANS LA CHASSE AUX MENACES NDR |
|---|---|---|
| IP source | L'adresse IP de l'expéditeur | Identifie la source de la communication, qui peut être utilisée pour suivre les activités suspectes ou localiser les hôtes infectés. |
| Adresse MAC de la source | L'adresse MAC (Media Access Control) de l'expéditeur | L'adresse MAC peut permettre d'identifier l'appareil physique associé au trafic réseau et être utilisée avec d'autres informations du capteur pour corréler les alertes provenant de plusieurs capteurs sur un périphérique spécifique. |
| Port source | Le port utilisé par l'expéditeur pour la communication | Aide à identifier le service ou l'application spécifique associé à la communication, ce qui peut être utilisé pour détecter une activité suspecte ou non autorisée. |
| IP de destination | L'adresse IP du destinataire | Aide à identifier la cible de la communication, ce qui peut être utilisé pour repérer des sources de menaces externes. |
| Adresse MAC de destination | L'adresse MAC du destinataire | Aide à identifier l'appareil physique associé à la communication, ce qui peut être utilisé pour suivre les activités suspectes ou localiser les hôtes infectés. |
| Port de destination | Le port utilisé par le destinataire pour la communication | Aide à identifier le service ou l'application spécifique associé à la communication, ce qui peut être utilisé pour détecter une activité suspecte ou non autorisée. |
| Indicateurs TCP | Indiquent l'état d'une connexion TCP, telle que SYN, ACK, FIN, RST, etc. | Peuvent être utilisés pour détecter des activités suspectes ou des attaques sur le réseau, telles que le contrôle des ports ou les attaques par déni de service. |
| Durée de la communication | Le temps que la communication a duré | Aide à identifier les activités suspectes comme les connexions qui durent plus longtemps que prévu, les connexions anormalement courtes ou encore les communications périodiques liées au balisage. |
| Octets reçus | Quantité de données reçues pendant la communication | Peuvent être utilisés pour détecter des activités suspectes ou des attaques, telles que l'exfiltration de données ou le téléchargement de malware. |
| Protocoles de la couche 3 (réseau) et de la couche 4 (transport) | Les protocoles utilisés pour la communication tels que IP, OSPF, ICMP, TCP ou UDP | Aident à identifier le type de trafic et les services associés, information pouvant être utilisée pour détecter des activités suspectes ou non autorisées. |
| ID du réseau VLAN (Virtual Local Area Network) | La balise VLAN associée à la communication | Aide à identifier le segment de réseau spécifique associé à la communication. |

## NPP : Données 'Couche applicative'

Les données de la couche applicative donnent un aperçu du contenu de la communication réseau, ce qui permet aux solutions NDR d'identifier les menaces potentielles pouvant s'y cacher. Elles fournissent des informations sur les applications et les services utilisés dans les communications réseau et aident à identifier les noms d'utilisateur et les mots de passe en clair. Voici quelques exemples d'informations déterminables à partir des données de la couche applicative :

| DONNÉES 'COUCHE APPLICATIVE' | EXPLICATION | IMPORTANCE POUR LA CHASSE AUX MENACES NDR |
|---|---|---|
| Protocole de la couche applicative | Le protocole utilisé au niveau de la couche applicative, tel que HTTP, TLS ou SMB (Server Message Block) | Le fait de connaître le protocole de la couche applicative utilisé peut aider à identifier le trafic potentiellement malveillant ou tout comportement anormal pour ce protocole. |
| Noms d'hôte source et de destination | Les noms d'hôtes associés aux adresses IP source et de destination, résolus via DNS ou d'autres moyens | Cette information peut aider à identifier un trafic potentiellement malveillant ou un comportement anormal associé à des hôtes ou à des domaines. |
| Type de contenu HTTP | Le type de contenu transféré via HTTP, par ex. texte, image ou vidéo | Cette information peut aider à identifier un trafic potentiellement malveillant ou un comportement anormal associé à des types de contenu. |
| Code de réponse | Le code d'état HTTP renvoyé par le serveur en réponse à une requête HTTP | Cette information peut aider à identifier un trafic potentiellement malveillant ou un comportement anormal associé à des codes de réponse particuliers tels que « 404 Not Found » ou « 500 Internal Server Error ». |
| URL | L'URL complète demandée ou consultée | Cette information peut aider à identifier un trafic potentiellement malveillant ou un comportement anormal associé à des URL ou à des domaines. |
| Agent utilisateur | L'agent logiciel utilisé par le client pour effectuer la requête, tel qu'un navigateur web ou une application mobile | Cette information aide à identifier le trafic potentiellement malveillant ou les comportements anormaux associés aux agents utilisateurs, comme on peut les voir dans certains malwares connus. |
| Noms d'utilisateur et mots de passe en clair | Tout nom d'utilisateur ou mot de passe transmis en texte lisible, comme dans une requête HTTP non chiffrée | Cette information peut aider à identifier des problèmes de sécurité potentiels ou des tentatives d'accès non autorisé. |
| Informations sur le certificat TLS | Les données sur le certificat TLS utilisé dans une connexion sécurisée, y compris les hachages JA3 | Ces informations peuvent aider à identifier des certificats potentiellement malveillants ou usurpés, et informer sur la nature du trafic chiffré. |
| Client et serveur SSH HASSH | Une méthode d'empreinte digitale pour l'identification des clients et serveurs SSH | Cette information aide à identifier le trafic SSH potentiellement malveillant ou détecter les tentatives d'accès SSH non autorisées. |
| Encapsulation CAPWAP | Le protocole CAPWAP (Control and Provisioning of Wireless Access Points) est utilisé pour la gestion des points d'accès sans fil | Cette information aide à identifier les tentatives d'accès sans fil potentiellement malveillantes ou non autorisées, ainsi que les activités inhabituelles du réseau sans fil. |

Pour conclure, la collecte des métadonnées sur les flux réseau constitue une composante essentielle des solutions NDR, car elle permet de mieux analyser les communications réseau en vue de détecter les menaces potentielles. Toutes ces données recueillies sur l'en-tête des paquets et la couche applicative fournissent des informations précieuses qui aident à identifier la source, le type et le risque potentiel de la communication. En exploitant ces informations, les solutions NDR parviennent à mieux détecter les menaces qui pèsent sur le réseau et à y répondre efficacement.

## Moteurs de détection de Sophos NDR

Sophos NDR intègre cinq moteurs de détection afin de fournir un ensemble de fonctionnalités complet pour la détection des menaces. Ces moteurs travaillent en synergie pour identifier et corréler les différents indicateurs de compromission, qui sont ensuite notés et présentés sous forme de renseignements sur les menaces exploitable dans Sophos Central pour les clients et les analystes

Pour des performances accrues, les moteurs de détection basés sur le Machine Learning (EPA - Encrypted packet Analytics et DGA - Domain Generation Algorithm) ne sont pas exécutés sur tous les flux réseau, mais plutôt déclenchés en fonction des résultats obtenus par les autres moteurs de détection. Permettre aux moteurs de détection de collaborer pour la classification est essentiel si l'on veut maintenir les performances et réduire le nombre de faux positifs.

Les résultats des moteurs de détection sont ensuite intégrés dans un algorithme de clustering et de scoring de la gravité (ou CSS pour Clustering and Severity Scoring) afin de générer une note globale pour la menace qui apparaîtra ensuite à l'administrateur comme une détection dans le tableau de bord des détections de Sophos Central. Le rapport de détection contient les résultats de la contribution de chaque moteur.

# IDS – Moteur du système de détection des intrusions

Ce moteur IDS (Intrusion Detection System) propriétaire est un moteur optimisé et plus efficace, capable d'identifier les indicateurs de compromission dans le trafic non chiffré. De nombreux fournisseurs de solutions de sécurité continuent d'utiliser des systèmes de correspondance de contenu trop robustes, et ce même avec la perte de visibilité due au chiffrement.

Sophos NDR utilise des renseignements sur les menaces rigoureusement élaborés pour créer des règles IDS classées en six groupes, en fonction du type d'indicateur de compromission. Voici ci-dessous les classifications de ces règles ainsi que leurs descriptions :

### Activité diverse

La classification de cette règle correspond à un niveau de « Gravité faible ». Elle est utilisée pour détecter le trafic réseau qui n'appartient à aucune autre classification. On trouvera ici le trafic vers les serveurs DNS publics, le trafic vers les réseaux de diffusion de contenu ou le trafic vers les services Cloud de confiance. Identifier les activités diverses permet d'établir une base de référence du trafic réseau normal et de mettre en évidence tout écart par rapport à cette base.

### Violation de la politique

La classification de cette règle correspond à un niveau de « Gravité faible ». Elle est utilisée pour détecter le trafic qui viole potentiellement une politique de sécurité de l'entreprise. On trouvera ici le trafic vers des sites web ou des services non autorisés, ou du trafic provenant d'appareils non autorisés. Détecter les violations de politiques aide les entreprises à renforcer l'application de leurs politiques de sécurité et à prévenir les accès non autorisés ou l'exfiltration de données.

### Inconnu malveillant

La classification de cette règle correspond à un niveau de « Gravité moyenne ». Elle est utilisée pour identifier les communications réseau dont la destination est potentiellement malveillante. Il peut s'agir de communications avec une adresse IP ou un domaine malveillants connus, ou de communications avec un domaine Sinkhole utilisé pour rediriger le trafic vers une infrastructure malveillante. Détecter un trafic inconnu malveillant peut aider à identifier les postes de travail compromis et à empêcher l'exfiltration de données ou davantage de compromission.

### Téléchargement de malware

La classification de cette règle correspond à un niveau de « Gravité élevée ». Elle est utilisée pour identifier les communications réseau avec une source connue de distribution de malware. Il peut s'agir de communications avec un serveur de commande et contrôle (C&C) connu, utilisé pour télécharger ou distribuer des malwares, ou de communications avec un site de diffusion de malware connu. Détecter les téléchargements de malware permet aux entreprises d'identifier et d'isoler les postes de travail infectés afin d'empêcher leur propagation.

### Activité de cheval de Troie

La classification de cette règle correspond à un niveau de « Gravité élevée ». Elle est utilisée pour identifier les communications réseau avec un serveur C&C de malware connu. Il peut s'agir de communications avec un serveur C&C utilisé pour prendre le contrôle à distance d'un système compromis ou de communications avec un serveur C&C utilisé pour l'exfiltration de données. Détecter les activités de type cheval de Troie aide les organisations à identifier et à isoler les postes de travail compromis et à empêcher l'exfiltration de données ou davantage de compromission.

### Liste de blocage TLS

La classification de cette règle correspond à un niveau de « Gravité critique ». Elle est utilisée pour identifier les communications réseau avec un acteur malveillant connu sur la base d'une correspondance de certification TLS. Il peut s'agir de communications avec un domaine malveillant connu utilisant un certificat TLS compromis ou de communications avec un domaine malveillant connu n'utilisant pas de certificat TLS valide. Détecter le trafic TLS sur liste de blocage aide les organisations à empêcher la communication avec des infrastructures malveillantes connues et à se protéger contre les cyberattaques.

## SRA - Moteur d'analyse du risque de la session

Le moteur SRA (Session Risk Analytics) détecte les cas où le trafic réseau dévie des normes protocolaires définies, ce qui pourrait indiquer une activité suspecte ou comportant des risques. C'est un outil important dans la chasse aux menaces, car il permet d'identifier les comportements non standard pouvant être le signe d'une attaque. Lorsque le moteur SRA observe une telle activité, il ajoute des informations sur le comportement aux métadonnées du flux. Ces risques de flux ne sont pas considérés comme des indicateurs de compromission en soi, mais corrélés aux détections provenant d'autres moteurs, ils peuvent aider à identifier des activités malveillantes.

Voici ci-dessous une liste des risques de flux généraux que l'on peut retrouver dans de nombreux protocoles et ce qu'ils indiquent :

| TYPE | RISQUE DE FLUX | DESCRIPTION |
|---|---|---|
| Général | Exploit potentiel | Indique qu'un exploit potentiel a été détecté, tel que Log4J/Log4Shell. Important pour détecter toute activité liée aux exploits et prévenir/limiter les attaques. |
| Général | Protocole connu sur un port non standard | Indique qu'un protocole est utilisé sur un port non standard, comme HTTP sur TCP/8000 au lieu du port standard TCP/80. Important pour détecter les attaquants qui utilisent des ports non standard pour échapper à la détection. |
| Général | ASN à risque | Indique que du trafic réseau a été échangé avec un serveur appartenant à un ASN (Autonomous System Number) considéré comme comportant des risques. Important pour identifier les hôtes ou les réseaux malveillants. |
| Général | Trafic unidirectionnel | Indique qu'une session est unidirectionnelle, ce qui pourrait indiquer une activité C&C vers un serveur qui ne fonctionne plus à l'adresse en question. Important pour identifier les hôtes ou les serveurs C&C compromis. |
| Général | Session de partage de bureau ou de fichiers | Indique que le flux contient des données de partage de bureau ou de fichiers, telles que TeamViewer ou AnyDesk. Important pour détecter les attaquants qui utilisent ces outils pour contrôler à distance un hôte compromis. |
| Général | Protocole non sécurisé | Indique que le protocole utilisé n'est pas sûr et ne devrait pas être utilisé, par exemple Telnet au lieu de SSH. Important pour détecter les attaquants qui peuvent intercepter et lire le trafic envoyé via des protocoles non sécurisés. |
| Général | Identifiants en texte clair | Indique que les identifiants ont été transmis en texte clair via un protocole connu, tel que FTP, HTTP, IMAP, POP3 ou SMTP. Important pour détecter les attaquants qui peuvent intercepter et lire les identifiants en texte clair. |
| Général | Paquet mal formé | Indique qu'un paquet a un format inattendu, ce qui peut indiquer une erreur de protocole ou la prise de contrôle d'un protocole valide pour transporter un autre type de données. Important pour détecter les attaques qui ont recours à la manipulation de paquets ou à une utilisation abusive de protocoles. |
| Général | Problèmes de TCP | Indique que des problèmes ont été identifiés dans les paramètres TCP de la session réseau. Important pour détecter les attaquants qui utilisent les problèmes de TCP dans leurs attaques pour entraver la détection ou y échapper. |
| Général | Flux périodique | Indique que la session réseau se répète à un intervalle programmé, ce qui pourrait indiquer une activité C&C d'un cheval de Troie ou d'un botnet. Important pour détecter les attaquants qui utilisent des communications périodiques pour garder le contrôle des hôtes compromis. |

Pour une liste complète des risques de flux, voir l'annexe A.

# EPA – Moteur d'analyse des charges utiles chiffrées et Machine Learning [ML]

Le Machine Learning est de plus en plus utilisé dans les solutions de détection et de réponse (NDR) pour détecter le trafic suspect sur les réseaux d'entreprise. Selon Gartner, les outils NDR analysent en permanence le trafic brut ou les enregistrements de flux, comme dans le cas de NetFlow, afin d'entraîner des modèles qui reflètent le comportement normal du réseau. Le Deep Learning va plus loin dans cette approche, car il permet de détecter des modèles à travers de multiples attributs. La détection peut ainsi s'effectuer sans les renseignements sur les menaces basés sur les indicateurs de compromission.

Sophos a développé une solution spécifique appelée Analyse des charges virales chiffrées (EPA pour Encrypted Payload Analytics) pour résoudre ce problème de détection dans le trafic chiffré utilisant des technologies plus anciennes. Les flux de réseau sont constitués de paquets avec des données d'en-tête et de charge utile, et lors de l'inspection d'une communication chiffrée, seules les données de charge utile sont chiffrées, et il est donc impossible de connaître le contenu sans déchiffrent. Le moteur EPA est un modèle de prédiction par Deep Learning multi-classes entraîné pour détecter des modèles dans les flux réseau en fonction de la séquence SPLIT (Sequence of Packet Length and Interarrival Time). Simples à calculer, ces attributs SPLIT sont utilisés pour entraîner un réseau neuronal convolutif (CNN) pour la classification. Sophos NDR utilise un processus breveté pour normaliser, transformer et présenter ces données au CNN à des fins de classification.

Figure 2 : Séquence SPLIT (Sequence of Packet Length and Interarrival Time)

En utilisant des échantillons de malwares, le modèle EPA peut identifier les activités malveillantes en temps réel, y compris les variantes de malwares zero-day ou inconnus, ainsi que les serveurs C&C, en se basant sur les modèles de flux réseau entre eux. Le moteur EPA enrichit également les métadonnées des flux avec la famille de malware détectée et un indice de fiabilité afin de réduire le nombre de faux positifs. En conclusion, il permet aux entreprises de détecter et de répondre aux menaces chiffrées qui n'auraient pas été détectées auparavant. Cette approche est particulièrement utile lorsque les postes de travail ne peuvent pas exécuter une solution classique de sécurité Endpoint et lorsque les communications réseau ne doivent pas être déchiffrées en raison de l'obligation de protéger les données personnelles identifiables (PII).

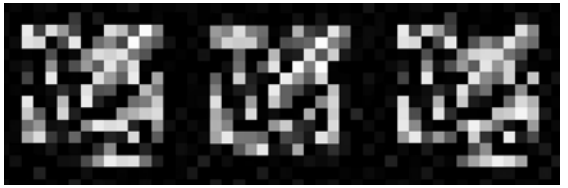

Figure 3 : Variant de Cobalt Strike après traitement en tant qu'image pour le réseau CNN du moteur EPA.

Le moteur EPA enrichit les métadonnées de flux en identifiant la famille de malware (comme Bumblebee, Cobalt Strike, Emotet, Dridex, QakBot) et fournit un indice de fiabilité allant de 0 à 100. Pour réduire le nombre de faux positifs, le modèle comprend également une classification « Inconnu ».

## DGA – Moteur d'algorithme de génération de domaines

Les algorithmes de génération de domaines (Domain Generation Algorithms ou DGA) sont utilisés par les acteurs malveillants pour générer des noms de domaines exploitables à des fins de commande et de contrôle (C&C) sans être mis sur liste de blocage. En utilisant ces algorithmes, le malware peut générer une liste de noms de domaines potentiels sur lesquels le serveur C&C pourra être hébergé. Après de nombreuses tentatives, l'algorithme trouvera un domaine qui existe et établira une connexion.

husbbrkpvrqjomuyhdpd[.]com

Figure 4 : Exemple de domaine DGA

Les DGA ont déjà été utilisés par le passé dans plusieurs attaques de haut niveau. Par exemple, dans l'épidémie du ver Conficker en 2008, les DGA ont servi à générer quotidiennement une liste de plus de 50 000 noms de domaines qui pouvaient être utilisés comme serveurs C&C. Il a donc été extrêmement difficile pour les experts en sécurité d'interrompre le réseau C&C du ver. Autre exemple : l'utilisation de DGA dans le malware Gameover Zeus, qui a été utilisé pour générer jusqu'à 1 000 noms de domaines par jour à des fins de C&C. On estime que le botnet Gameover Zeus a fait perdre à ses victimes dans le monde entier plus de 100 millions de dollars.

Le moteur de détection DGA de Sophos NDR est un outil essentiel pour identifier les activités malveillantes en temps réel. Au cœur de ce moteur, se trouve un réseau neuronal de Deep Learning de type LSTM (Long Short-Term Memory) qui évalue chaque nom de domaine demandé et consulté. Notons cependant que toutes les activités des DGA ne sont pas malveillantes. De nombreux services légitimes utilisent régulièrement les algorithmes de génération de domaines, ce qui explique que Sophos NDR ne génère pas d'alerte chaque fois qu'un DGA est détecté. À la place, un indice de fiabilité (de 0 à 100) est attribué aux métadonnées du flux et il est utilisé par le moteur CSS (Clustering and Severity Scoring) pour déterminer si l'activité impliquant des détections DGA est véritablement malveillante.

## DDE - Moteur de détection des données

Le moteur de détection des données (Data Detection Engine ou DDE) est un composant de Sophos NDR exécuté sur chaque capteur. Il s'agit d'un moteur de corrélation léger qui utilise le stockage de la base de données embarquée des flux réseau et des clusters de flux. Le moteur DDE effectue du dataminig programmé sur ces informations afin d'identifier les menaces réseau complexes telles que les activités d'énumération. Ces renseignements sont ensuite envoyés à Sophos Central et utilisés pour générer des rapports d'informations sur le réseau.

De plus, les données collectées par le moteur DDE peuvent être mises en corrélation avec les données des capteurs Endpoint de Sophos XDR (Extended Detection & Response) pour identifier les actifs non gérés sur le réseau. Cette corrélation s'effectue dans le Data Lake de Sophos et fournit une vue d'ensemble complète du réseau, permettant aux administrateurs d'identifier les risques de sécurité potentiels et de prendre les mesures appropriées. Il est important de noter que le moteur DDE effectue des activités de datamining sur un intervalle défini et non en temps réel.

## CSS – Clustering et scoring de la gravité

La fonction CSS (Clustering and Severity Scoring) joue un rôle majeur dans le travail de détection des menaces de Sophos NDR. Au cours des sessions réseau entre clients et serveurs, le système observe un large éventail d'indicateurs de menaces. Ces indicateurs, s'ils étaient analysés de manière isolée, pourraient ne pas signaler un problème ou une activité malveillante. C'est pourquoi Sophos NDR utilise un processus breveté qui regroupe (d'où le terme anglais « clustering ») ces indicateurs dans le temps, permettant ainsi d'obtenir un indice de fiabilité accrue dans l'identification des menaces.

Le processus de clustering regroupe les flux réseau en se basant sur des informations réseau basiques telles que l'IP/Port source et de destination, ainsi que les informations de protocole. En regroupant les différents flux qui ont eu lieu dans le temps, le système est capable de générer une vue plus complète des activités suspectes et d'agréger les flux réseau connexes en un seul événement de détection où la corrélation entre les flux permet de mieux comprendre l'activité suspecte.

Une fois ces groupes créés, ils sont notés (d'où le terme anglais « scoring ») sur la base des informations recueillies par chacun des moteurs de détection. L'algorithme CSS évalue toutes les activités au sein d'un cluster afin de fournir un contexte supplémentaire, d'améliorer la précision et de réduire les faux positifs.

Le système de scoring CSS repose sur différents facteurs, notamment le niveau de gravité et les indicateurs de menace identifiés par les différents moteurs de détection. En combinant ces informations, Sophos NDR attribue une score ou indice à chaque cluster, reflétant le risque potentiel posé par l'activité réseau. Ce système de scoring fournit aux administrateurs réseau des informations précieuses sur les menaces potentielles, leur permettant de prioriser leurs réponses en fonction de la gravité du risque.

# ANNEXES

### ANNEXE A : Risques du flux SRA

| PROTOCOLE | RISQUE DE FLUX | DESCRIPTION |
|---|---|---|
| GÉNÉRAL | Exploit potentiel | Un exploit potentiel a été détecté (par ex. Log4J/Log4Shell). |
| GÉNÉRAL | Protocole connu sur un port non standard | Le protocole est utilisé sur un port non standard (par ex. HTTP sur TCP/8000, le protocole standard étant TCP/80). |
| GÉNÉRAL | ASN à risque | Une session réseau a été échangée avec un serveur appartenant à un ASN (Autonomous System Number) à risque. |
| GÉNÉRAL | Trafic unidirectionnel | La session n'est établie que dans une seule direction. Cela pourrait indiquer une activité C&C vers un serveur qui ne fonctionne plus à l'adresse en question. |
| GÉNÉRAL | Session de partage de bureau ou de fichiers | Le flux transporte des données de partage de bureau ou de fichiers (par ex. TeamViewer, AnyDesk). |
| GÉNÉRAL | Protocole non sécurisé | Le protocole utilisé n'est pas sécurisé et ne devrait pas être utilisé (par ex. Telnet vs SSH). |
| GÉNÉRAL | Identifiants en texte clair | Les identifiants ont été transmis en texte clair via un protocole connu (par ex. FTP, HTTP, IMAP, POP3 ou SMTP). |
| GÉNÉRAL | Paquet mal formé | Le paquet réseau a un format inattendu. Cela peut indiquer une erreur de protocole ou la prise de contrôle d'un protocole valide pour acheminer un autre type de données |
| GÉNÉRAL | Problèmes de TCP | Des problèmes ont été identifiés dans les paramètres TCP de la session réseau |
| GÉNÉRAL | Abonné anonyme | L'adresse IP source a été anonymisée et ne peut pas être utilisée pour identifier l'abonné (par ex. flux généré par un nœud de sortie iCloud-private-relay). |
| GÉNÉRAL | Flux périodique | Une session réseau se répète à un intervalle programmé. Cela peut indiquer une activité C&C d'un cheval de Troie ou d'un botnet. |
| TLS, HTTP, DNS | Domaine DGA suspect | Le nom de domaine peut être un DGA, qui est utilisé pour générer des noms de domaines souvent exploités par des malwares. |
| TLS, HTTP, DNS | Domaine à risque | Le trafic réseau a eu lieu avec un domaine considéré à risque. |
| TLS, HTTP, DNS | Caractères non valides | Le protocole décodé contient des caractères non autorisés dans ce champ de protocole (par ex. un nom d'hôte DNS ne doit contenir qu'un sous-ensemble de tous les caractères imprimables). |
| TLS, HTTP, DNS | IDN en punycode | Le nom de domaine a été observé au format IDN. Les domaines IDN encodés en punycode IDN peuvent indiquer une attaque de phishing par homographe. |
| HTTP, DNS | Code d'erreur détecté | Erreur détectée dans le protocole |

| PROTOCOLE | RISQUE DE FLUX | DESCRIPTION |
|---|---|---|
| DNS | Trafic suspect | Type d'enregistrement DNS inattendu ou obsolète observé |
| DNS | Paquet volumineux | Le paquet DNS sur UDP a dépassé la taille limite de 512 octets. Cela peut indiquer un tunneling DNS ou une exfiltration |
| DNS | Fragmenté | Les DNS sur UDP a été fragmenté. Cela peut indiquer un tunneling DNS ou une exfiltration |
| SSH | Chiffrement ou version du client obsolète | Le client SSH utilise une version de protocole obsolète ou des algorithmes de chiffrement peu sûrs. |
| SSH | Chiffrement ou version du serveur obsolète | Le serveur SSH utilise une version de protocole obsolète ou des algorithmes de chiffrement peu sûrs. |
| SMB | Version non sécurisée | Une version non sécurisée de SMB a été observée (par ex. SMBv1). |
| ICMP | Entropie suspecte | Une entropie suspecte a été observée dans les paquets ICMP. Cela peut indiquer une exfiltration de données via ICMP |
| TLS | Certificat auto-signé | Un certificat auto-signé a été utilisé |
| TLS | Certificat SHA1 malveillant | Le certificat TLS observé a été trouvé sur un certificat malveillant |
| TLS | Certificat non correspondant | Le certificat TLS ne correspond pas au nom d'hôte auquel on accède. |
| TLS | SNI manquant | Le SNI du serveur auquel on accède est manquant. |
| TLS | Utilisation suspecte de l'ESNI | Un SNI chiffré a été observé. Cela peut indiquer une attaque de type « domain fronting ». |
| TLS | Ne transporte pas le HTTPS | Le flux TLS n'a pas été utilisé pour transporter le HTTPS. |
| TLS | Empreinte digitale JA3 malveillante | L'empreinte digitale JA3 a été trouvée sur une liste de blocage JA3 malveillante |
| TLS | Extension suspecte | Le nom de domaine dans l'extension SNI n'est pas imprimable. |
| TLS | ALPN peu courant | Une extension APLN peu courante a été observée dans le flux TLS (ex. : HTTP/1.1). |
| TLS | Certificat expiré | Le certificat TLS utilisé dans le flux est expiré. |
| TLS | Certificat prêt à expirer | Le certificat TLS utilisé dans le flux est sur le point d'expirer. |
| TLS | Validité du certificat trop longue | Le certificat TLS utilisé dans le flux a une durée de vie supérieure à 13 mois. |
| TLS | Version obsolète | La version TLS est antérieure à 1.1. |
| TLS | Chiffrement faible | Un algorithme de chiffrement TLS peu sûr a été utilisé lors de la configuration du flux. |
| TLS | Alerte fatale | Le protocole TLS a fait l'objet d'une alerte fatale dans le flux. |

| PROTOCOLE | RISQUE DE FLUX | DESCRIPTION |
|---|---|---|
| HTTP | Hôte IP numérique | On a accédé au serveur web en utilisant son adresse IP à la place du nom d'hôte. |
| HTTP | URL suspecte | L'URL d'accès est suspecte. (Exemple : http://127.0.0.1/ msadc/..% 255c../..%255c../winnt/system32/cmd.exe.). |
| HTTP | En-tête suspecte | L'en-tête HTTP contient des entrées suspectes inhabituelles. (Exemple : UUID, version TLS version, nom de l'OS). |
| HTTP | Agent utilisateur suspect | La chaîne de l'agent utilisateur contenait des caractères ou un formatage suspects. (Exemple : <?php something ?>). |
| HTTP | Contenu suspect | Le flux HTTP transportait un contenu dans un format inattendu. (Exemple : l'en-tête HTTP indique que le contexte est au format text/html, mais le contenu n'est pas lisible car il s'agit de données binaires). |
| HTTP | Transfert d'application binaire | Une application binaire est en train d'être téléchargée ou uploadée. Les fichiers détectés comprennent des binaires Windows, des exécutables Linux, des scripts Unix et des applications Android. |
| HTTP | URL potentiel XSS | Une possible attaque XSS (Cross Site Scripting) a été observée. |
| HTTP | Injection SQL possible | Une attaque par injection SQL possible a été observée. |
| HTTP | Injection RCE possible | Une attaque RCE (Remote Code Execution) possible a été observée. |
| HTTP | Bot Crawler | Un crawler/bot/robot a été détecté. |
| HTTP | Serveur obsolète | Une session réseau avec un serveur Apache ou Nginx obsolète a été détectée. |

**ANNEXE B : Protocoles NPP**

| | | | |
|---|---|---|---|
| 1KXUN | GIT | MICROSOFT_365 | SPOTIFY |
| ACCUWEATHER | GITHUB | MICROSOFT_AZURE | SSDP |
| ACTIVISION | GITLAB | MINING | SSH |
| ADS_ANALYTICS_TRACK | GMAIL | MODBUS | STARCRAFT |
| ADULT_CONTENT | GNUTELLA | MONGODB | STEAM |
| AFP | GOOGLE | MPEGDASH | STUN |
| AJP | GOOGLE_CLASSROOM | MPEGTS | SYNCTHING |
| ALIBABA | GOOGLE_CLOUD | MQTT | SYSLOG |
| ALICLOUD | GOOGLE_DOCS | MS_ONE_DRIVE | TAILSCALE |
| AMAZON | GOOGLE_DRIVE | MS_OUTLOOK | TARGUS_GETDATA |
| AMAZON_ALEXA | GOOGLE_MAPS | MSSQL_TDS | TEAMSPEAK |
| AMAZON_AWS | GOOGLE_PLUS | MSTEAMS | TEAMVIEWER |
| AMAZON_VIDEO | GOOGLE_SERVICES | MUNIN | TELEGRAM |
| AMONG_US | GOTO | MYSQL | TELNET |
| AMQP | GTP | NATPMP | TENCENT |
| ANYDESK | GTP_C | NATS | TENCENTVIDEO |
| APPLE | GTP_PRIME | NEST_LOG_SINK | TEREDO |
| APPLE_ICLOUD | GTP_U | NETBIOS | TFTP |
| APPLE_ITUNES | GUILDWARS | NETFLIX | THREEMA |
| APPLE_PUSH | H323 | NETFLOW | TIDAL |
| APPLE_SIRI | HALFLIFE2 | NFS | TIKTOK |
| APPLESTORE | HANGOUT_DUO | NINTENDO | TINC |
| APPLETVPLUS | HBO | NOE | TIVOCONNECT |
| ARMAGETRON | HOTSPOT_SHIELD | NTOP | TLS |
| AVAST | HPVIRTGRP | NTP | TOCA_BOCA |
| AVAST_SECUREDNS | HSRP | OCS | TOR |
| BADOO | HTTP | OCSP | TPLINK_SHP |

| | | | |
|---|---|---|---|
| BGP | HTTP_CONNECT | OOKLA | TRUPHONE |
| BITTORRENT | HTTP_PROXY | OPENDNS | TUENTI |
| BJNP | HULU | OPENVPN | TUMBLR |
| BLOOMBERG | I3D | ORACLE | TUNEIN |
| CACHEFLY | IAX | PANDORA | TUNNELBEAR |
| CAPWAP | ICECAST | PASTEBIN | TUYA_LP |
| CASSANDRA | ICLOUD_PRIVATE_RELAY | PINTEREST | TVUPLAYER |
| CHECKMK | IEC60870 | PLAYSTATION | TWITCH |
| CISCOVPN | IFLIX | PLAYSTORE | TWITTER |
| CITRIX | IHEARTRADIO | PLURALSIGHT | UBNTAC2 |
| CLOUDFLARE | IMO | POSTGRES | UBUNTUONE |
| CLOUDFLARE_WARP | INSTAGRAM | PPSTREAM | ULTRASURF |
| CNN | IP_EGP | PPTP | USENET |
| COAP | IP_GRE | PSIPHON | VEVO |
| COLLECTD | IP_ICMP | QQ | VHUA |
| CORBA | IP_ICMPV6 | QUIC | VIBER |
| CPHA | IP_IGMP | RADIUS | VIMEO |
| CRASHLYSTICS | IP_IP_IN_IP | RAKNET | VK |
| CROSSFIRE | IP_OSPF | RDP | VMWARE |
| CRYNET | IP_PGM | REDDIT | VNC |
| CSGO | IP_PIM | REDIS | VUDU |
| CYBERSECURITY | IP_SCTP | RIOTGAMES | VXLAN |
| DAILYMOTION | IP_VRRP | RPC | WARCRAFT3 |
| DATASAVER | IPP | RSH | WAZE |
| DAZN | IPSEC | RSYNC | WEBEX |
| DEEZER | IRC | RTCP | WEBSOCKET |
| DHCP | JABBER | RTMP | WECHAT |
| DHCPV6 | KAKAOTALK | RTP | WHATSAPP |

| | | | |
|---|---|---|---|
| DIAMETER | KAKAOTALK_VOICE | RTSP | WHATSAPP_CALL |
| DIRECTV | KERBEROS | RX | WHATSAPP_FILES |
| DISCORD | KISMET | S7COMM | WHOIS_DAS |
| DISNEYPLUS | KONTIKI | SALESFORCE | WIKIPEDIA |
| DNP3 | LASTFM | SAP | WINDOWS_UPDATE |
| DNS | LDAP | SD_RTN | WIREGUARD |
| DNSCRYPT | LIKEE | SFLOW | WORLD_OF_KUNG_FU |
| DOFUS | LINE | SHOWTIME | WORLDOFWARCRAFT |
| DOH_DOT | LINE_CALL | SIGNAL | WSD |
| DRDA | LINKEDIN | SIGNAL_VOIP | XBOX |
| DROPBOX | LISP | SINA | XDMCP |
| DTLS | LIVESTREAM | SIP | XIAOMI |
| EAQ | LLMNR | SIRIUSXMRADIO | YAHOO |
| EBAY | LOTUS_NOTES | SKINNY | YANDEX |
| EDGECAST | MAIL_IMAP | SKYPE_TEAMS | YANDEX_CLOUD |
| EDONKEY | MAIL_IMAPS | SKYPE_TEAMS_CALL | YANDEX_DIRECT |
| ELASTICSEARCH | MAIL_POP | SLACK | YANDEX_DISK |
| ETHERNET_IP | MAIL_POPS | SMBV1 | YANDEX_MAIL |
| FACEBOOK | MAIL_SMTP | SMBV23 | YANDEX_MARKET |
| FACEBOOK_VOIP | MAIL_SMTPS | SMPP | YANDEX_METRIKA |
| FASTCGI | MAPLESTORY | SNAPCHAT | YANDEX_MUSIC |
| FIX | MDNS | SNAPCHAT_CALL | YOUTUBE |
| FORTICLIENT | MEGACO | SNMP | YOUTUBE_UPLOAD |
| FTP_CONTROL | MEMCACHED | SOAP | Z3950 |
| FTP_DATA | MERAKI_CLOUD | SOCKS | ZABBIX |
| FTPS | MESSENGER | SOFTETHER | ZATTOO |
| FUZE | MGCP | SOMEIP | ZMQ |
| GENSHIN_IMPACT | MICROSOFT | SOUNDCLOUD | ZOOM |

## Pour en savoir plus sur Sophos NDR, rdv sur www.sophos.com/ndr

Les déclarations contenues dans ce document sont basées sur des informations disponibles au public au 30 mars 2023. Ce document a été préparé par Sophos seul et non pas par les autres éditeurs listés. Les fonctionnalités ou caractéristiques des produits comparés dans ce document, qui pourraient avoir un impact direct sur la précision ou la validité d'une comparaison, sont susceptibles de changer. Les informations contenues dans cette comparaison sont destinées à favoriser la compréhension et la connaissance d'informations factuelles sur divers produits et elles pourraient ne pas être exhaustives. Toute personne utilisant ce document devrait prendre ses propres décisions d'achat basées sur ses besoins, et devrait également faire des recherches en se basant sur les sources originales des informations et ne pas se baser uniquement sur cette comparaison pour choisir un produit. Sophos ne garantit pas la fiabilité, la précision, l'utilité ou l'exhaustivité de ce document. Les informations contenues dans ce document sont fournies « en tant que telles », sans garantie d'aucune sorte, expresse ou tacite. Sophos se réserve le droit de modifier ou de retirer ce document à tout moment.



2023-03-29 (WP-NP)

SOPHOS