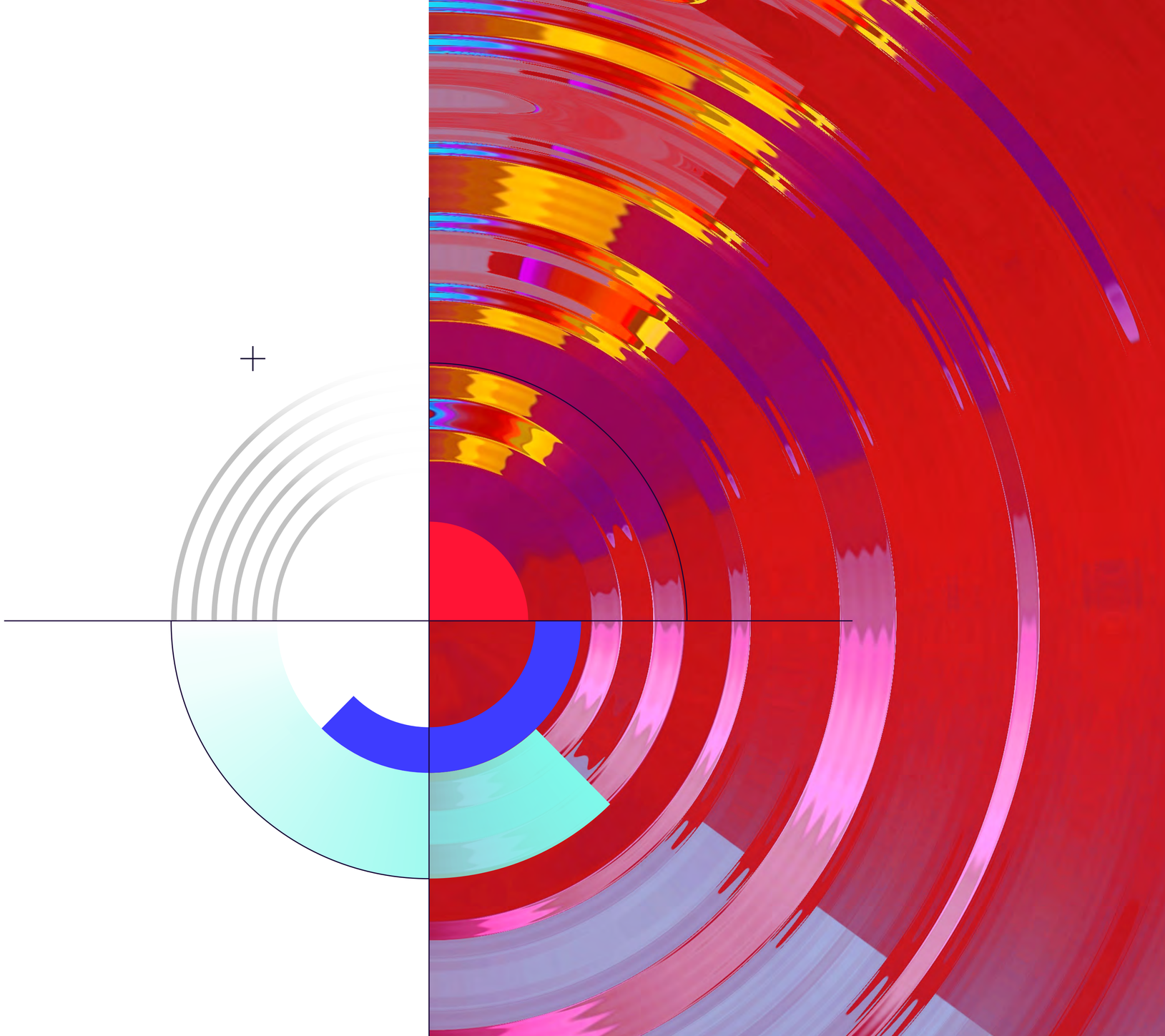
NDR *insights_*

POURQUOI LA TECHNOLOGIE NDR CONSTITUE UNE BRIQUE ESSENTIELLE POUR LE RENFORCEMENT DE VOTRE CYBERDÉFENSE ?

L'ESSENTIEL SUR LE NDR DANS UN GUIDE PRATIQUE POUR LES RSSI ET LES DSI

GATEWATCHER



Sommaire_

01

LES CYBERATTAQUES MODERNES EXPLOITENT UNE SÉCURITÉ INFORMATIQUE OBSOLÈTE_

Aujourd'hui, les cyberattaques des systèmes informatiques et réseaux de certaines entreprises sont plus devenues la règle plus que l'exception. D'après l'ANSSI, les TPE, PME et ETI ont été particulièrement visées en 2022 par les cyberattaques. Elles représentent 40 % des attaques par rançongiciel et selon le CESIN, une entreprise française sur deux a été victime d'une cyberattaque en 2022.

En effet, les possibilités des cybercriminels, et donc des cyberattaques, ont évolué mais pas les mesures de sécurité des entreprises. Dans la plupart des cas, leur version remonte à 15 ans en arrière.

Exploitez les renseignements fournis dans cette fiche d'informations pour en savoir plus sur les menaces, leurs évolutions et les tendances dans le cyberespace, et la façon dont votre entreprise peut prendre des mesures de sécurité adaptées contre les cyberattaques les plus récentes grâce aux solutions Network Detection and Response, qui interviennent au niveau des flux réseau, utilisés dans la majorité des attaques.

> “En effet, les possibilités des cybercriminels, et donc des cyberattaques, ont évolué mais pas les mesures de sécurité des entreprises.”

02

LA SÉCURITÉ INFORMATIQUE AVEC DES SOLUTIONS NETWORK DETECTION AND RESPONSE (NDR)_

De nombreux systèmes, avant tout des pare-feux, des programmes antivirus, des systèmes de détection et de prévention des intrusions, traitent les effets, mais jamais la cause, et dans le cas de cyberattaques innovantes il est souvent déjà trop tard. Dès lors que les agresseurs sont dans le système, les dommages sont présents et souvent irréversibles.

La détection des menaces au niveau du réseau n'est pas une approche récente mais, bien que les solutions NDR puissent au premier abord être perçus comme une simple évolution de technologies de détection et de prévention des intrusions existantes, elles s'en distinguent en de nombreux points à commencer par leur capacité à détecter et neutraliser les attaques dès leur mise en place.

En effet, contrairement aux technologies réactives traditionnelle, les solutions NDR interviennent dès la détection d'anomalies grâce à une cartographie et une surveillance contextuelle de l'intégralité de l'activité au niveau des flux réseau ce qui leur permet de déployer des contre-mesures automatisées avant qu'un vecteur d'attaque puisse déployer ses effets malfaisants.

> “Dès lors que les agresseurs sont dans le système, les dommages sont présents et souvent irréversibles.”

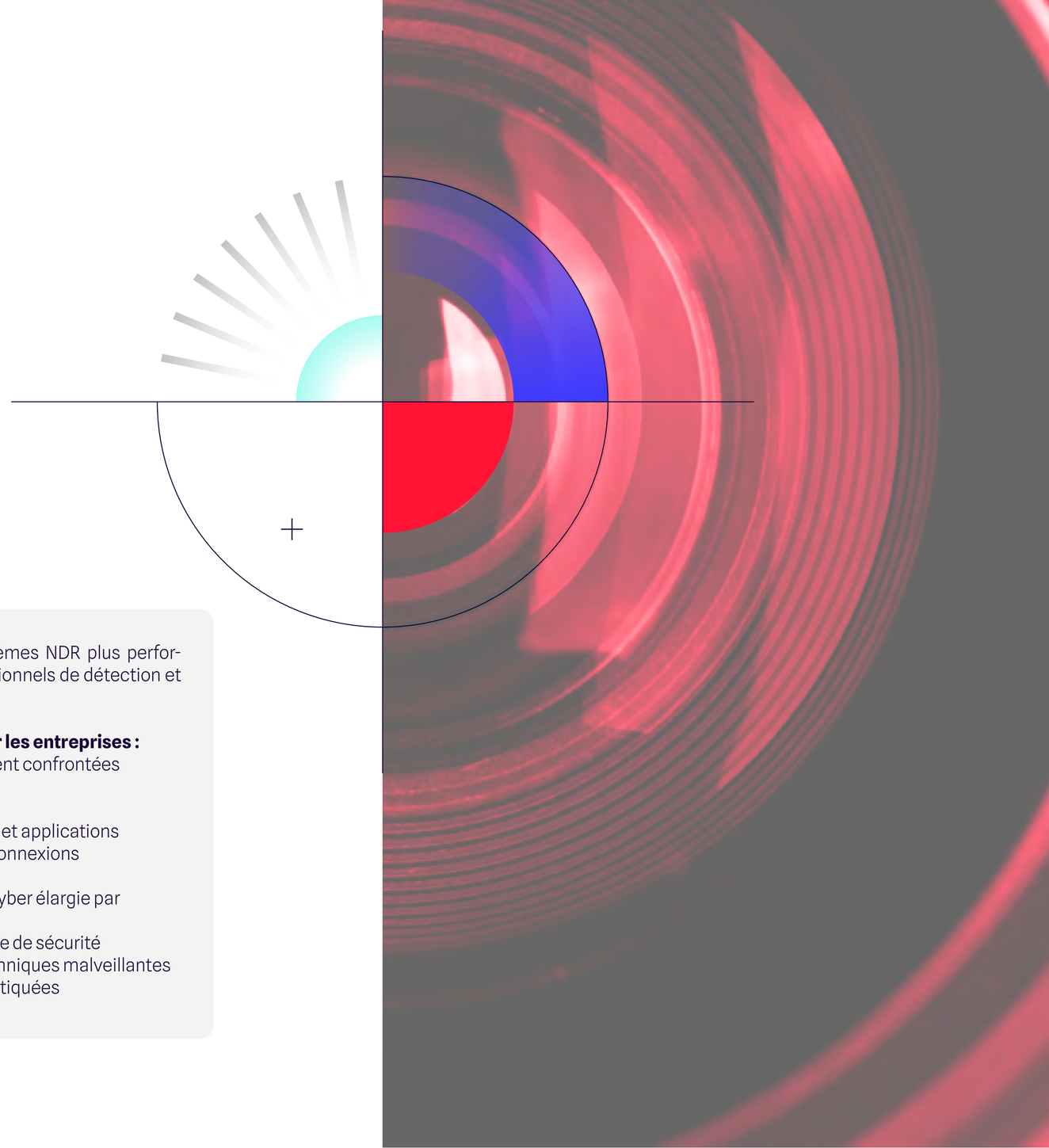
Méthodes de détection des menaces employées par des solutions NDR

1 > Analyse du comportement
Les systèmes NDR surveillent le comportement d'appareils, d'utilisateurs et d'applications sur le réseau pour y détecter toute anomalie. Grâce à l'analyse des activités et des données transitant sur le réseau, les systèmes NDR peuvent détecter si un appareil ou un utilisateur agit en dehors du modèle comportemental normal.

2 > Machine Learning
Les systèmes NDR exploitent des algorithmes d'intelligence artificielle pour analyser le comportement sur le réseau et détecter les menaces. Grâce à l'analyse de grandes quantités de données, les systèmes NDR peuvent repérer des menaces qui ne peuvent pas être détectées habituellement sur la base de signatures ou de modèles.

3 > Automatisation et orchestration
Les systèmes NDR proposent des réactions automatisées aux menaces détectées. Ils peuvent, par exemple, isoler automatiquement un hôte ou un utilisateur, ou envoyer un avertissement à l'équipe chargée de la sécurité.

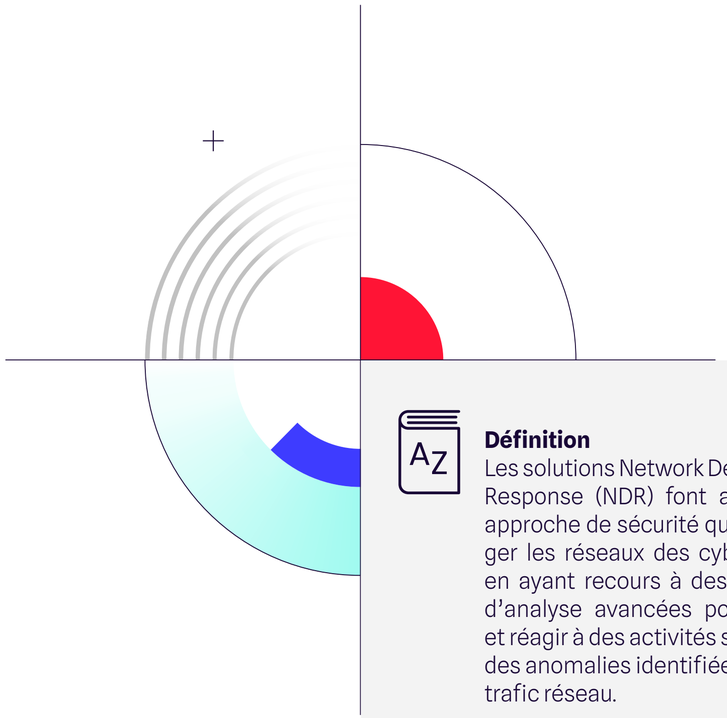
4 > Surveillance en temps réel
Les systèmes NDR offrent une surveillance en temps réel des activités sur le réseau afin de détecter rapidement les menaces et d'y réagir.



Ces méthodes innovantes rendent les systèmes NDR plus performants et plus précis que des systèmes traditionnels de détection et de prévention des intrusions.

Les enjeux actuels de la cybersécurité pour les entreprises :
Les défis actuels auxquels les sociétés se voient confrontées concernent surtout :

- La complexité grandissante des réseaux et applications
- L'augmentation de terminaux IoT et de connexions (mot-clé OT)
- une surface d'exposition aux menaces cyber élargie par le cloud computing
- Le manque d'experts qualifiés en matière de sécurité
- Une évolution quasi quotidienne des techniques malveillantes avec des attaques de plus en plus sophistiquées



Définition
Les solutions Network Detection and Response (NDR) font appel à une approche de sécurité qui doit protéger les réseaux des cybermenaces en ayant recours à des techniques d'analyse avancées pour détecter et réagir à des activités suspectes et des anomalies identifiées au sein du trafic réseau.

Les solutions NDR combinent analyse du trafic réseau, détection des menaces et réactions automatisées afin de réagir rapidement aux menaces connues et inconnues, et de minimiser les éventuels dommages.

Contrairement aux solutions de sécurité traditionnelles basées sur des signatures et des règles prédéfinies, les solutions NDR exploitent l'intelligence artificielle et le machine learning pour détecter continuellement et en temps réel des modèles d'attaque et des anomalies comportementales, et y réagir.

Les étapes exécutées par les systèmes NDR pour détecter des menaces sont les suivantes

1 > Collecte de données
Les systèmes NDR collectent des données en continu sur le trafic réseau, y compris les données de protocole, les métadonnées et les données utiles.

2 > Analyse des données
Les données collectées sont analysées afin de détecter des activités suspectes et des anomalies sur le trafic réseau. Pour ce faire, des algorithmes et des modèles de machine learning sont utilisés pour identifier les modèles comportementaux d'applications et d'appareils dans le réseau.

3 > Détection des menaces
Lorsqu'une activité suspecte ou une anomalie est détectée, un avertissement est distribué pour attirer l'attention dessus. Il est également possible de combiner les systèmes NDR à d'autres outils de sécurité tels que des SIEM (Security Information and Event Management) et des solutions EDR (Endpoint Detection and Response). Cela permet de garantir une surveillance et une protection complètes de la sécurité du réseau.

4 > Réponse aux incidents
Les systèmes NDR peuvent aussi réagir automatiquement à des menaces en bloquant le trafic ou en prenant d'autres mesures, par ex. pouvoir rédiger une nouvelle règle sur le pare-feu grâce à un playbook pour arrêter l'attaque.

5 > Analyse post-mortem (Forensics)
Après la détection d'une menace, les systèmes NDR peuvent faciliter la réponse aux incidents en mettant à disposition des informations supplémentaires sur la menace. Les équipes chargées de la réponse à un incident peuvent ainsi réagir de manière plus rapide et plus efficace.

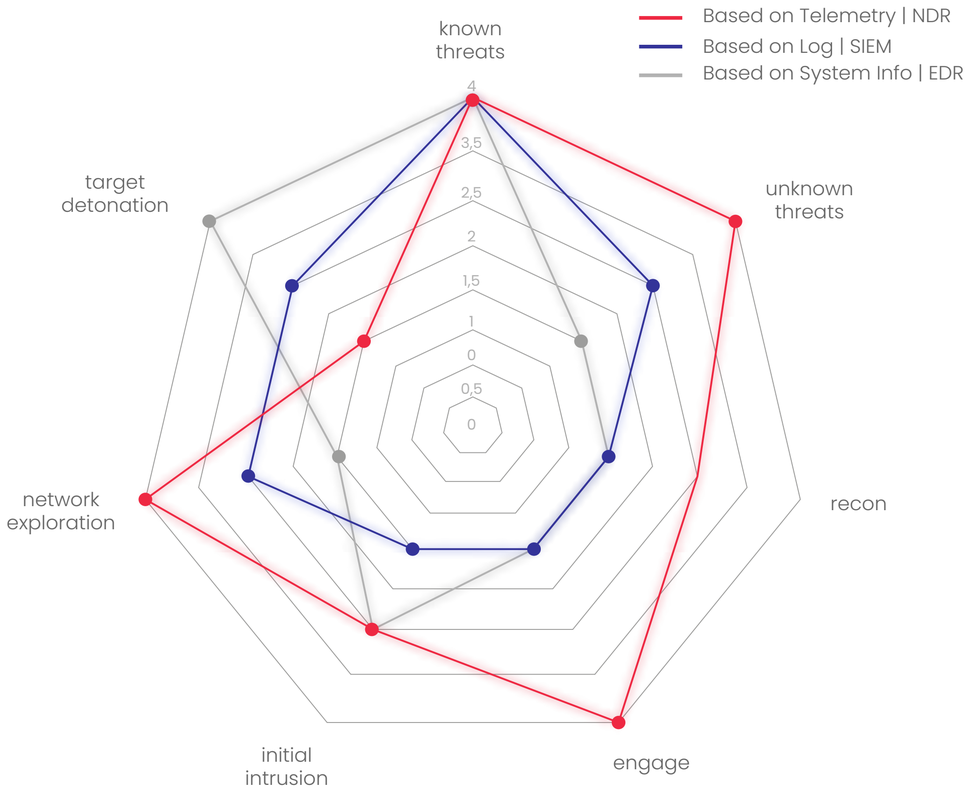
03

EDR ET NDR, QUELLES DIFFÉRENCES ?_

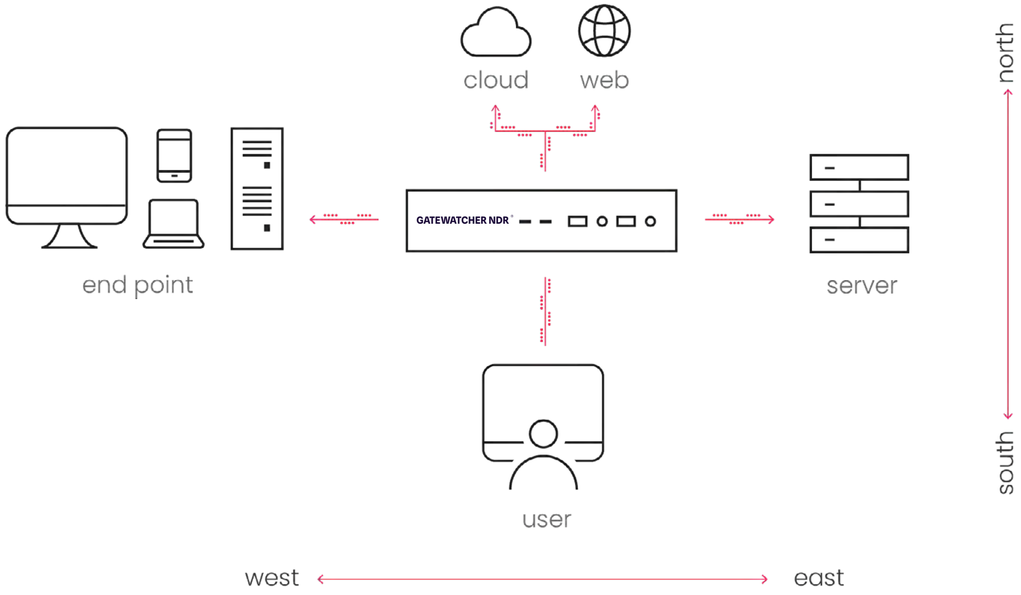
Définition
Tout comme les systèmes NDR, les solutions EDR sont une nouvelle technologie, qui garantit l'amélioration continu de la protection des terminaux, telle que les logiciels antivirus locaux ou les pare-feu personnels sur des terminaux comme les ordinateurs portables, les ordinateurs de bureau et les serveurs.

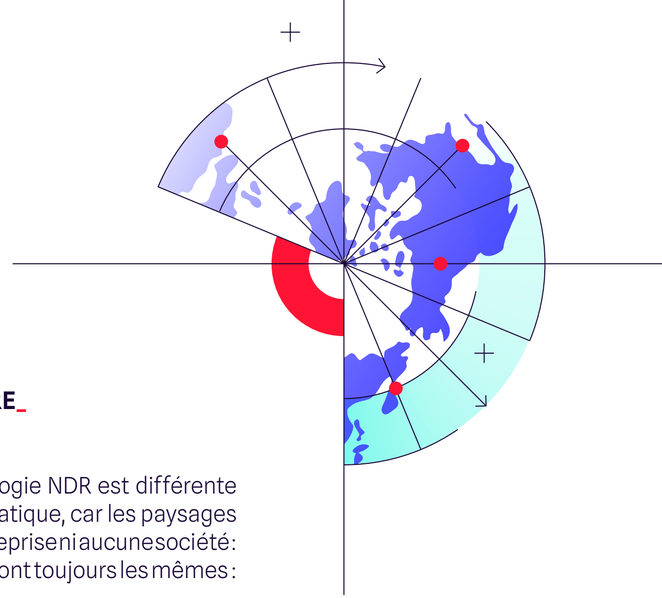
Les solutions EDR collectent des données en continu sur ces appareils et les analysent pour détecter toute menace en temps réel, mais seulement lorsqu'elles arrivent sur le terminal. Or, il est souvent déjà trop tard.

La principale différence entre les solutions EDR et NDR tient dans le type de données collectées et analysées par ces technologies. Les systèmes EDR collectent les données de terminaux, tandis que les systèmes NDR se concentrent sur le trafic réseau. Ces deux systèmes se complètent et peuvent être utilisés en combinaison afin de garantir une surveillance et une protection complètes contre les menaces cyber.



> Les systèmes EDR collectent les données de terminaux, tandis que les systèmes NDR se concentrent sur le trafic réseau.





04

LA TECHNOLOGIE NDR ET SON ARCHITECTURE_

L'implémentation et l'architecture d'une technologie NDR est différente dans l'environnement de chaque système informatique, car les paysages informatiques ne sont identiques dans aucune entreprise ni aucune société : ils sont uniques. Cependant, les aspects suivants sont toujours les mêmes :

1 >Cartographie des données
En se basant sur les communications entre les différents composants du réseau les systèmes NDR collectent des informations de façon passive, donc sans impact sur les performances et l'activité. Ces informations sont variées : paquets de données, informations sur les flux (NetFlow, sFlow, IPFIX,..), les TAP réseau, les ports SPAN et les fichiers journaux. Elles offrent un aperçu exhaustif du trafic réseau et permettent l'analyse des activités et modèles comportementaux.

2 > Traitement et stockage de données
Les données collectées sont traitées, agrégées, et stockées dans une base de données centrale ou un data lake. Cet emplacement de stockage central permet une analyse simple et rapide, et assiste l'équipe chargée de la sécurité dans la recherche d'incidents (analyse forensique, voir ci-contre).

3 > Analyse des données
Les données stockées sont analysées en permanence afin d'identifier des anomalies, des activités suspectes et des menaces. Des technologies telles que l'intelligence artificielle (IA), le machine learning (ML) et les analyses des big data sont exploitées à cet effet.

4 > Détection des menaces
Les solutions NDR ont recours à des méthodes de détection basées sur les signatures ainsi que les comportements afin de repérer des menaces connues et inconnues.

05

L'INTELLIGENCE ARTIFICIELLE ET LE MACHINE LEARNING DANS LA TECHNOLOGIE NDR_

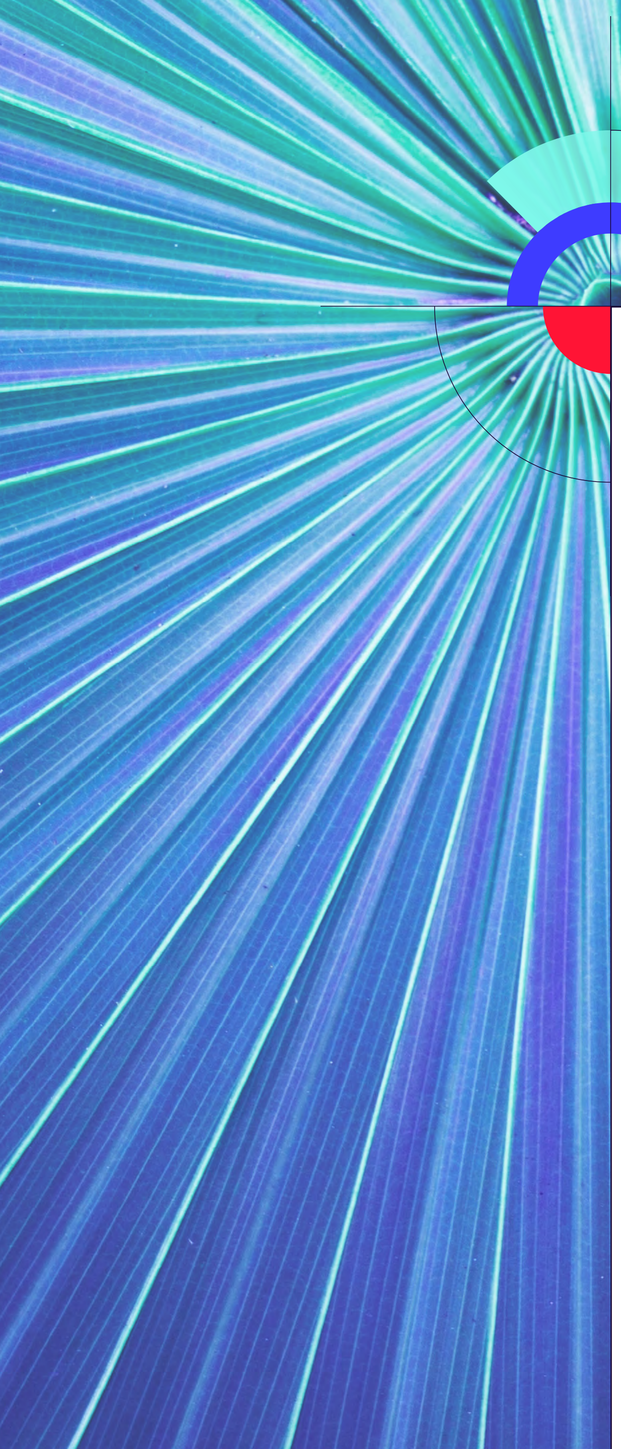
L'intelligence artificielle (IA) et le machine learning (ML) jouent un rôle décisif dans les solutions Network Detection and Response car ils permettent des méthodes d'analyse innovantes et des réactions automatisées.

Ils sont notamment utilisés dans les cas de figure suivants :

1 > Détection d'anomalies
Le machine learning permet aux systèmes NDR d'identifier des modèles et tendances dans le trafic réseau, et d'identifier des anomalies ou activités suspectes annonciatrices de menaces potentielles. Pour cela, des modèles de ML sont entraînés à détecter un comportement normal pour pouvoir repérer des modèles inhabituels ou déviation de comportement, annonciateurs d'une attaque ou d'une atteinte à la sécurité.

2 > Réactions automatisées
L'IA et le ML permettent des réactions automatisées en temps réel aux menaces détectées. Le blocage d'adresses IP, l'isolement des appareils concernés, l'utilisation de patchs de sécurité ou la mise à jour des règles du pare-feu font partie de ces mesures. L'automatisation des réactions permet de raccourcir le temps de réaction et de minimiser les éventuels dommages.

3 > Apprentissage continu et ajustements permanents
L'IA et le ML amènent les systèmes NDR à apprendre en continu du trafic réseau analysé et à s'adapter aux changements qui interviennent dans le paysage des menaces. Cela aide dans la détection de nouvelles menaces en cours d'évolution que les méthodes de détection traditionnelles basées sur les signatures peuvent ignorer.



Dans l'ensemble, l'IA et le ML améliorent l'efficacité des systèmes NDR en permettant une détection plus précise, des réactions plus rapides et une plus grande capacité d'adaptation aux menaces. Grâce à l'utilisation de l'IA et du ML dans les systèmes NDR, les entreprises peuvent bénéficier d'un certain nombre d'avantages :

1 > Détection plus précise
L'IA et le ML permettent aux systèmes NDR de mieux détecter les modèles et anomalies dans le trafic réseau en analysant de larges volumes de données et en identifiant les relations complexes. Ces techniques d'analyse avancées permettent une détection plus précise des menaces, y compris celles que les systèmes traditionnels basés sur des règles statiques ignorent.

2 > Réactions plus rapides
Grâce à l'automatisation des processus de détection et de réaction, les systèmes NDR qui font appel à l'IA et au ML peuvent réagir beaucoup plus rapidement aux menaces potentielles. Cela permet de réduire le temps nécessaire pour réagir aux incidents et de minimiser les impacts business.

3 > Meilleur ajustement aux paysages de menaces en évolution
Étant donné que les modèles d'IA et de ML apprennent et s'ajustent en continu, ils sont en mesure de s'adapter aux modèles d'attaque changeants et aux nouveaux vecteurs de menace. Cela permet aux systèmes NDR de tenir efficacement la cadence des cybermenaces dynamiques par nature et de protéger les sociétés en permanence contre de nouvelles attaques en cours d'évolution.

4 > Réduction des fausses alertes
En faisant appel à l'IA et au ML, les systèmes NDR sont en mesure de mieux distinguer les modèles comportementaux normaux de ceux qui ne le sont pas au sein du réseau. Cela entraîne une réduction des fausses alertes (False Positives), et permet d'alléger le travail des équipes chargées de la sécurité et d'améliorer l'efficacité des opérations de sécurité dans leur ensemble.

5 > Investigation cyber proactive
Les systèmes NDR basés sur l'IA et le ML peuvent aider les experts en sécurité à rechercher d'éventuelles menaces dans le réseau de manière proactive avant qu'elles ne causent de quelconques dommages. Cela permet aux équipes chargées de la sécurité de détecter toute menace à temps et de prendre des contre-mesures avant que cela ne dégénère.

6 > Réactions automatisées et mesures défensives
Lorsqu'une menace ou une anomalie est détectée, les systèmes NDR peuvent déclencher des réactions automatisées et des mesures défensives en ayant recours à l'IA et au ML. Ces actions automatisées peuvent inclure, par exemple, le blocage d'adresses IP, l'isolement de certains appareils ou l'application de patchs de sécurité. L'automatisation de ces réactions permet aux équipes chargées de la sécurité de réagir rapidement et efficacement aux incidents, et de réduire le risque de dommages et de pertes de données.

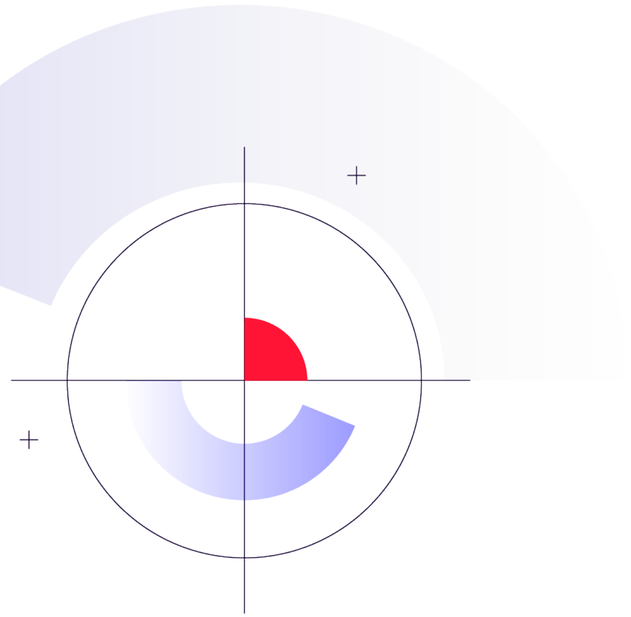
7 > Amélioration de la réponse aux incidents
Les systèmes NDR basés l'IA et le ML peuvent aider les équipes chargées de la sécurité à rechercher des incidents en mettant automatiquement à leur disposition des données et informations pertinentes concernant tout incident de sécurité détecté. Ces connaissances permettent aux équipes de mieux comprendre l'étendue et la cause d'un incident, et de prendre les mesures appropriées en termes de correction et de restauration.

06

LES AVANTAGES DES SOLUTIONS NDR PAR RAPPORT AUX APPROCHES DE SÉCURITÉ TRADITIONNELLES_

La solution NDR la mieux adaptée à une entreprise dépend de plusieurs facteurs, dont les exigences en matière de sécurité, l'infrastructure réseau, le budget, etc.

Il est donc recommandé de mener des recherches approfondies sur différentes solutions NDR et de les comparer pour trouver celle qui répond le mieux aux exigences spécifiques à l'entreprise.



L'avancée technologique d'une solution NDR lui confère un certain nombre d'avantages par rapport aux solutions de sécurité réactives comme les pare-feux, et les systèmes de détection (IDS) et de prévention des intrusions (IPS). Elles comprennent :

1 > La détection de menaces inconnues
Alors que d'autres approches de sécurité s'appuient, en général, sur des méthodes basées sur les signatures pour détecter des menaces inconnues, les solutions NDR repèrent les anomalies basées sur le comportement à l'aide de l'IA et du ML. Cela permet aux solutions NDR d'identifier aussi des menaces inconnues et « zero-days » qui pourraient être ignorées par des systèmes de sécurité traditionnels.

2 > Une connaissance totale du réseau
Les solutions NDR donnent une visibilité sur le trafic réseau plus détaillée et plus complète que des approches de sécurité traditionnelles. Cela permet aux équipes chargées de la sécurité de détecter des activités suspectes et des anomalies dans tout le réseau, et d'y réagir.

3 > Une réaction plus rapide aux incidents
Grâce à l'automatisation et à l'analyse en temps réel, les solutions NDR peuvent réagir aux incidents de sécurité plus vite que des solutions de sécurité traditionnelles. Cela permet de réduire le délai entre la détection et la réaction, et de minimiser le risque de dommages et de perte de données.

4 > Une réduction des faux positifs
Le recours à l'IA et au ML permet aux solutions NDR de faire une distinction efficace entre des modèles comportementaux normaux et anormaux. Cela entraîne une réduction des fausses alertes et permet aux équipes chargées de la sécurité de se concentrer sur de vraies menaces.

5 > Une capacité d'adaptation
Les systèmes NDR peuvent s'adapter aux modèles d'attaque polymorphes et aux nouveaux vecteurs de menace grâce à l'IA et au ML. Cela permet à ces systèmes de rester efficaces également dans des paysages de menaces en évolution.

6 > Une traque proactive des menaces
Contrairement aux approches de sécurité traditionnelles plutôt passives et réactives, les solutions NDR permettent aux équipes chargées de la sécurité de rechercher des menaces dans le réseau de manière proactive et de prendre des mesures préventives.

7 > Une amélioration de la réponse aux incidents
Les systèmes NDR aident les équipes chargées de la sécurité à rechercher et à réagir aux incidents en mettant automatiquement à leur disposition des données et informations pertinentes sur un incident de sécurité détecté en particulier. Grâce à l'analyse en temps réel du trafic réseau et à la surveillance continue des anomalies et des menaces, les équipes chargées de la sécurité sont en mesure de mieux comprendre l'étendue, la cause et les impacts d'un incident. Cela permet une réaction plus rapide et plus efficace afin de minimiser les éventuels dommages, et d'accélérer la restauration des systèmes et services concernés.

De plus, les systèmes NDR offrent aux équipes chargées de la sécurité des possibilités d'analyse forensique pour reconstituer et rechercher des événements et tentatives d'attaque ultérieurs. Cela entraîne une meilleure identification des points faibles et vecteurs d'attaque, qui peuvent ensuite être atténués pour améliorer encore la sécurité du réseau.

07

L'IMPLÉMENTATION DES SOLUTIONS NDR DANS VOTRE ENTREPRISE_

L'implémentation des solutions Network Detection and Response dans votre entreprise nécessite une planification, la sélection des bonnes technologies et une étroite collaboration entre les équipes impliquées. Les étapes suivantes sont importantes :

1 > Analyse des besoins
Identifiez les points faibles de votre système de sécurité actuel et déterminez la façon dont les solutions NDR peuvent contribuer à les combler.

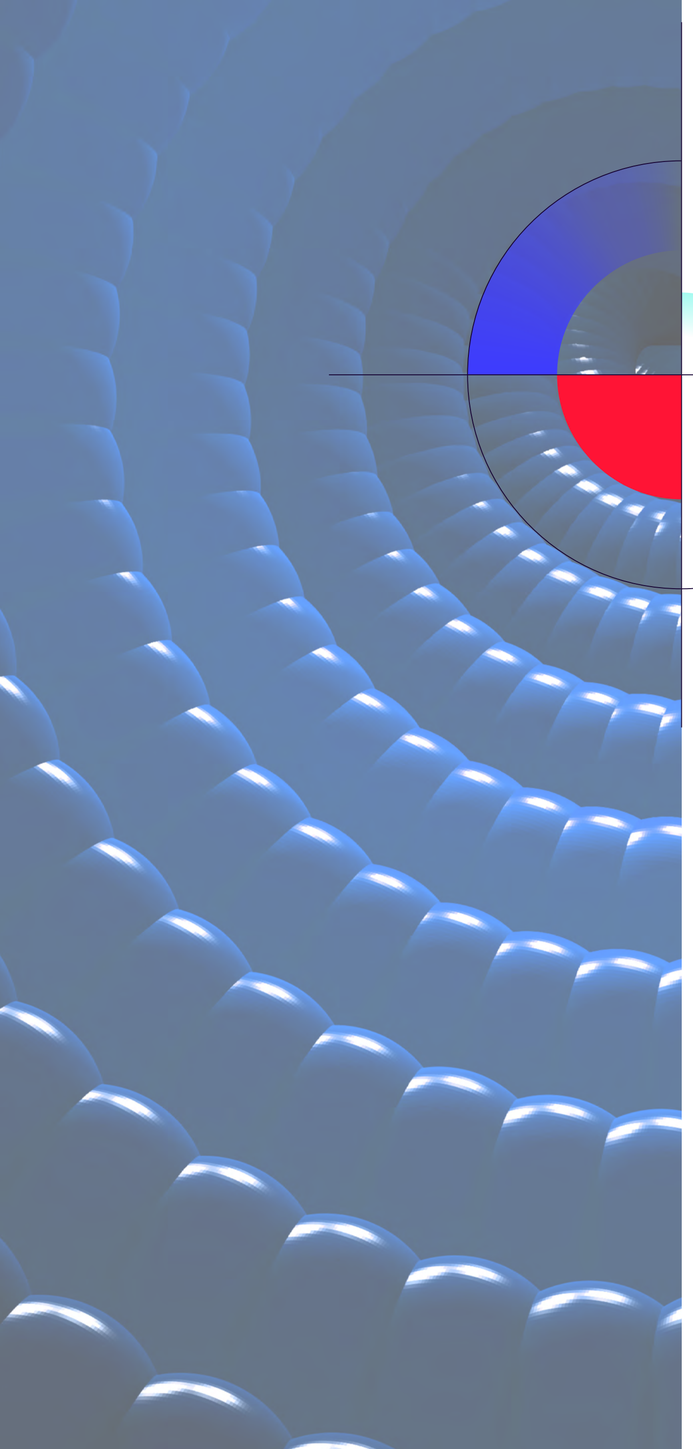
2 > Évaluation de la technologie
Tenez compte des facteurs tels que la scalabilité, l'intégration avec les systèmes existants, le TCO, la convivialité de déploiement, la personnalisation du paramétrage.

3 > Implication des équipes interne
Afin de garantir une implémentation réussie de la solution, définissez les rôles et responsabilités, et assurez-vous que toutes les équipes concernées au sein de la SSI disposent des connaissances et ressources nécessaires pour utiliser efficacement la solution NDR.

4 > Formation et transmission des connaissances
Pour vous assurer de conserver une efficacité opérationnelle, favorisez la transmission des connaissances et la formation continue pour garantir que votre équipe reste au courant des dernières évolutions, notamment après une mises à niveau majeure par le fournisseur de votre solution NDR.

5 > Intégration et configuration
Intégrez la solution NDR choisie dans l'infrastructure existante de votre réseau et de votre sécurité. Configurez les systèmes NDR conformément à vos exigences et directives spécifiques, et assurez-vous qu'ils collaborent efficacement avec vos solutions de sécurité existantes.

6 > Surveillance et optimisation
Surveillez les performances de votre système NDR en permanence pour vous assurer qu'il détecte efficacement les menaces et qu'il y réagit. Exploitez les connaissances acquises pour continuer à optimiser vos pratiques en matière de sécurité et améliorer constamment la sécurité de votre réseau.



07 > Plan de réponse aux incidents

Établissez un plan de réponse aux incidents qui tient compte du rôle de la solution NDR en cas d'incident de sécurité. Ce plan doit contenir les éléments suivants :

- **Détection :** définissez la façon dont votre système NDR fonctionne lors de la phase de détection, y compris l'identification des anomalies, des activités suspectes et des menaces potentielles dans le trafic réseau.
- **Recherche :** définissez la façon dont votre équipe chargée de la sécurité utilise les informations mises à disposition par le système NDR afin d'analyser la cause, l'étendue et les impacts d'un incident de sécurité.
- **Communication :** élaborez un plan de communication qui définit comment et où les informations sur un incident de sécurité sont retransmises aux acteurs concernés, comme les équipes de direction, les collaborateurs et, le cas échéant, les clients.
- **Réaction :** décrivez le rôle de votre système NDR quant à la réaction à un incident de sécurité, y compris les mesures automatisées telles que le blocage d'adresses IP, l'isolement de certains appareils ou l'utilisation de patchs de sécurité.
- **Restauration :** planifiez la façon dont votre entreprise va restaurer les systèmes et services concernés afin de rétablir ses activités normales aussi vite que possible. Pour cela, tenez compte du rôle du système NDR dans la surveillance et la protection du réseau pendant le processus de restauration.
- **Suivi et amélioration :** après un incident de sécurité, vous devez procéder à un suivi pour analyser l'incident et en tirer des connaissances. Exploitez ces connaissances pour améliorer votre plan de réponse aux incidents et l'implémentation du système NDR pour pouvoir mieux maîtriser les futurs incidents.

L'intégration d'un système NDR à votre plan de réponse aux incidents permet de garantir que votre société soit en mesure de réagir rapidement et efficacement aux incidents de sécurité, et de minimiser les éventuels dommages.

08

SOLUTIONS NDR ET EXPLOITATION DES TRACES D'ATTAQUE POST INCIDENT (ANALYSE FORENSIQUE)_

Les systèmes NDR jouent un rôle important dans l'investigation criminelle cyber, car les équipes char-gées de la sécurité offrent des informations ainsi qu'une visibilité précieuse en termes d'incidents de sécurité et d'attaques. Voici quelques éléments qui éclairent la façon dont les systèmes NDR permettent l'analyse forensique :

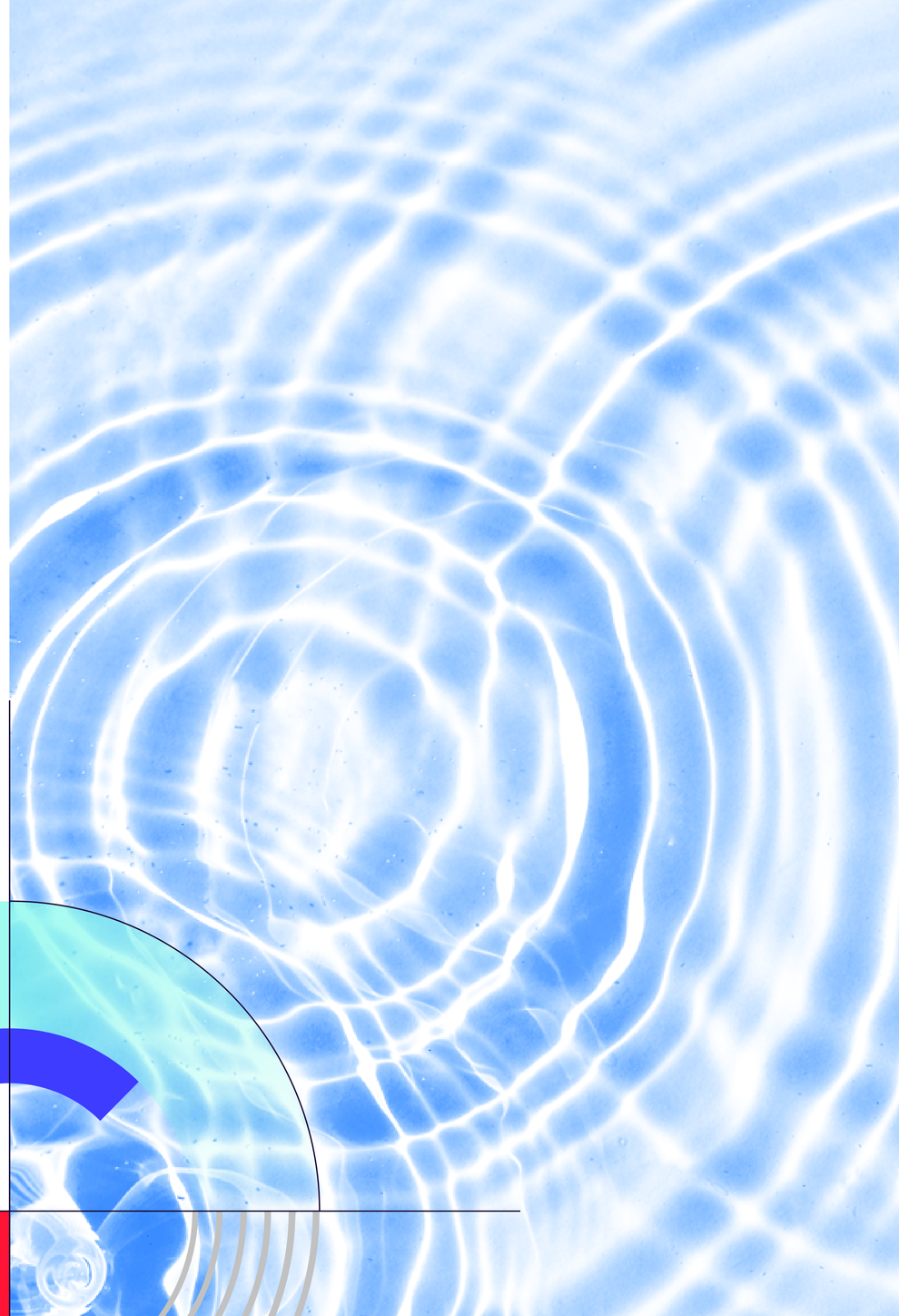
- **Données sur le trafic réseau**
  Les systèmes NDR collectent des données en continu sur le trafic réseau, qui peuvent être exploitées lors d'une analyse forensique des incidents de sécurité. Ces données comprennent des données en paquets, des protocoles, des informations sur les flux et d'autres données pertinentes qui permettent d'obtenir une connaissance détaillée sur les événements avant, pendant et après un incident.

- **Détection d'anomalies et de menaces**
  L'utilisation de l'IA et de technologies de ML permettent aux systèmes NDR de détecter des anomalies et des menaces dans le trafic réseau, prémices d'activités malveillantes ou d'atteintes à la sécurité. Ces informations peuvent être exploitées pour l'analyse des vecteurs d'attaque, des techniques utilisées et des systèmes concernés.

- **Chronologie et relations**
  Les systèmes NDR peuvent aider à établir des chronologies et à comprendre les relations entre différents événements au sein d'un incident de sécurité. Cela permet aux équipes en charge de la sécurité de mieux comprendre les chaînes de causalité et l'évolution d'une attaque, et d'identifier les éventuels points faibles de l'architecture de la sécurité.

- **Profilage des auteurs**
  Grâce à l'analyse de modèles comportementaux et d'indicateurs d'activités malveillantes, les systèmes NDR peuvent contribuer à déterminer l'identité ou le contexte dans lequel évoluent les agresseurs. Ces informations peuvent être utiles dans la lutte et la poursuite des cybercriminels ainsi que dans la prévention de futures attaques.

- **Extraction des preuves**
  Les systèmes NDR peuvent contribuer à collecter et protéger des preuves en lien avec un incident de sécurité. Cela peut s'avérer d'une importance capitale dans la poursuite judiciaire des cybercriminels, dans le respect des réglementations ou dans la revendication de droits en matière d'assurance.



09

ÉTUDES DE CAS D'APPLICATION RÉUSSIE DE SOLUTIONS NDR_

Ces deux études de cas démontrent des applications intéressantes et réussies de solutions NDR :

- **Détection précoce de code malveillant exécuté à distance**
  Une grande entreprise industrielle a implémenté une solution NDR pour améliorer la sécurité de son réseau et garantir la disponibilité de ses services métiers. Cela lui a permis solution d'identifier différents scripts PowerShell malveillants utilisés lors de la phase initiale d'une attaque notamment via des macros-office. Par son analyse temps réel des données par IA et apprentissage machine, la solution NDR a pu identifier les adresses IP concernées et de les bloquer automatiquement avant que l'attaquant n'ai pu s'introduite sur d'autres composants IT,OT et IoT dans l'infrastructure via des mouvements latéraux avec élévation de privilège. L'équipe en charge de la sécurité (SOC) a pu repousser cette attaque à ses prémices et maintenir la continuité de ses activités en s'appuyant uniquement sur la solution NDR en place.

- **Découverte d'une Advanced Persistant Threat (APT)**
  Une entreprise de prestation de services financiers a eu recours à une solution NDR pour améliorer sa cybersécurité et protéger les données confidentielles de ses clients. La solution NDR a identifié un modèle comportemental anormal dans le trafic réseau, annonciateur d'une éventuelle menace. Une recherche a révélé qu'il s'agissait d'une attaque persistante avancée (APT) par laquelle l'agresseur tentait de pénétrer lentement et discrètement dans le réseau afin d'accéder à des informations confidentielles. Grâce à la solution NDR, l'équipe chargée de la sécurité a pu détecter l'attaque à temps et prendre des mesures pour isoler les systèmes concernés et les rectifier. L'analyse forensique des données NDR a donc permis d'identifier les points faibles dans l'architecture de la sécurité et de repousser de futures attaques.

> “Ces études de cas montrent de quelle façon les systèmes NDR peuvent aider les entreprises à détecter des cybermenaces à temps et d'y réagir efficacement afin de minimiser les dommages, et de garantir la sécurité de leurs réseaux et de leurs données.”

10

CONCLUSION ET PERSPECTIVES FUTURES_

Dans un monde connecté menacé par des risques cyber de plus en plus sophistiqués, les solutions Network Detection and Response s'affirment peu à peu comme une composante essentielle des stratégies de sécurité mises en place par les entreprises en permettant une meilleure visibilité sur l'activité réseau, une détection précoce des incidents de sécurité et un délai de remédiation plus court.

En interaction avec d'autres technologies spécifiques à la sécurité telles que les solutions EDR, SIEM et pare-feux, les systèmes NDR constituent une ligne de défense solide contre les cyberattaques.

En ce qui concerne les perspectives d'avenir, nous nous attendons à ce que les technologies NDR gagnent en importance, car les entreprises et les sociétés recherchent des solutions de sécurité plus efficaces et évolutives. Les avancées en matière d'IA et de ML contribueront à rendre les systèmes NDR encore plus performants et encore plus précis dans la détection et la réaction aux menaces. De plus, l'intégration de solutions NDR dans une architecture informatique plus détaillée en matière de sécurité des entreprises, y compris la sécurité du cloud et la sécurité des terminaux IoT, est d'une importance capitale.

En conclusion, il est essentiel que les entreprises et les sociétés comprennent l'importance des systèmes NDR dans leur stratégie en matière de cybersécurité et prennent des mesures proactives pour protéger leurs réseaux, leurs données et leurs ressources des cybermenaces. En ayant recours à des technologies NDR, les entreprises peuvent consolider leur sécurité et se préparer à affronter les défis d'un paysage de menaces en constante évolution.

Comment fonctionne la solution NDR de GATEWATCHER

Notre solution NDR fonctionne par une approche multifactorielle qui associe l'analyse comportementale par machine learning à des techniques poussées de détection du trafic réseau sur les flux Est-Ouest et Nord-Sud ainsi que des flux d'information sur les menaces provenant de notre propre plateforme de Cyber threat Intelligence (CTI). Elle permet une cartographie de 100 % des assets présents sur le SI et l'analyse contextuelle pour une détection en amont du déclenchement de l'attaque ainsi qu'une visibilité à 360° de l'activité au sein du SI organisations

Un exemple d'application

Lorsque la solution Gatewatcher NDR détecte une anomalie éventuellement causée par un fichier ou un shellcode, elle peut la déplacer automatiquement dans une sandbox interne, où elle est isolée dans un environnement séparé de celui de la production, afin d'observer la façon dont le fichier ou le code se comporte. Si, par exemple, un comportement qui exploite un point faible est observé (conformément à la synchronisation avec la base de données des CVE, et qu'il représente une menace critique (conformément à la synchronisation par le biais du Common Vulnerability Scoring System, base de données CVSS), il est alors classifié comme tel et l'alerte correspondante est déclenchée.

La solution NDR invoque simultanément des informations depuis le flux CTI afin de détecter également des malwares inconnus, les attaques de type «zero-days» par exemple en détectant une relation avec un serveur de commande et de contrôle (C2) ou parce que le code a déjà été détecté comme étant malveillant dans d'autres cas, mais n'est pas encore enregistré dans une base de données ou une signature officielle.