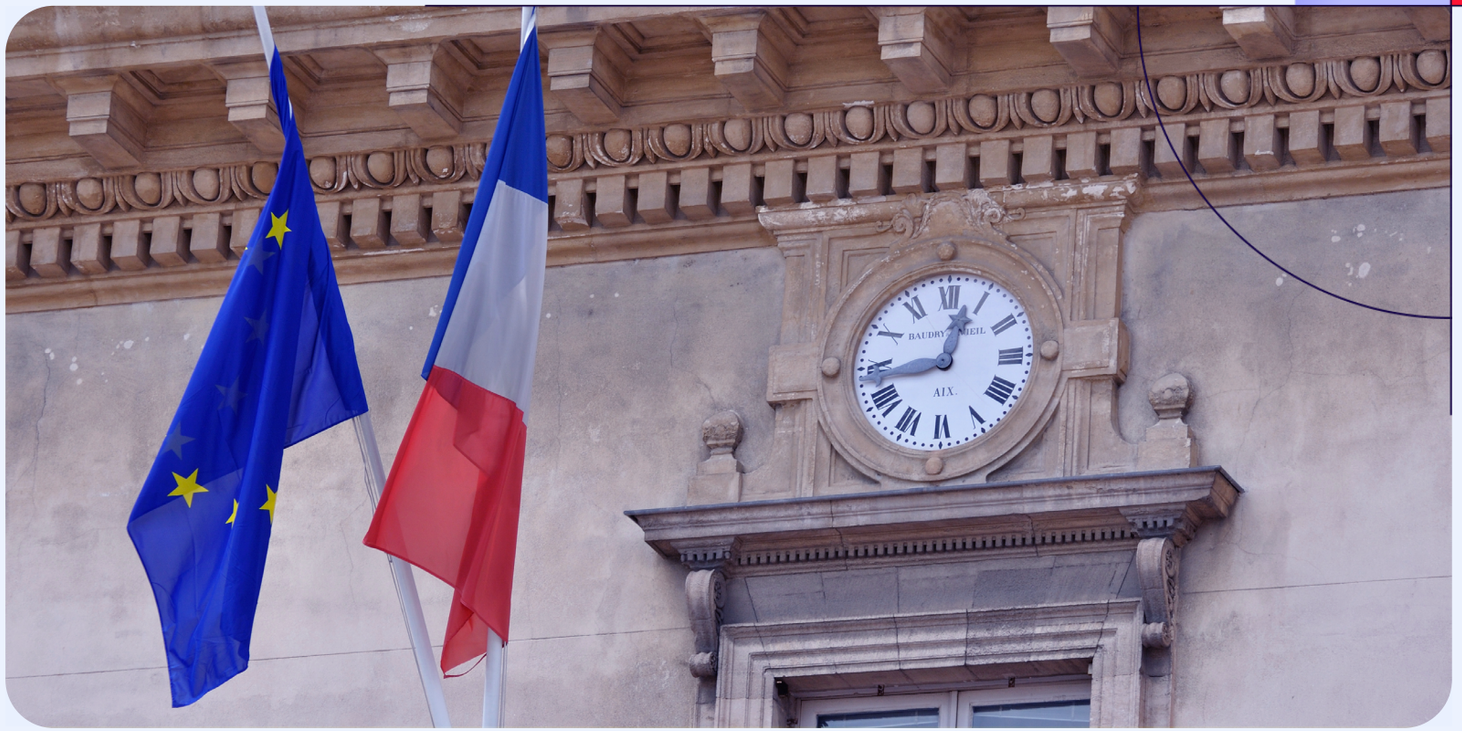
CUSTOMER STORY

VILLE DE CHELLES



Le NDR nous a permis d'identifier des comportements et des usages qui passaient inaperçus avec nos autres outils de sécurité, soit parce qu'ils ne relevaient pas de leur périmètre, soit parce que certaines configurations, volontairement permissives pour des raisons de production, les laissaient passer.

Antoine Trillard - DSI de la Ville de Chelles et Président du CoTer Numérique & **Julien Fargeix** - ingénieur sécurité

#COLLECTIVITÉ TERRITORIALE #NDR #VISIBILITÉ #OPTIMISATION RESSOURCES

01

POUVEZ-VOUS NOUS PRÉSENTER VOTRE COLLECTIVITÉ ET LES DÉFIS SPÉCIFIQUES QUE VOUS RENCONTREZ EN MATIÈRE DE CYBERSÉCURITÉ ?

La Ville de Chelles se situe en Région Parisienne, forte d'environ 55000 habitants, ce qui en fait la seconde commune de Seine-et-Marne. La DSI (Direction des Systèmes d'Information) gère un **parc de 900 équipements, ainsi qu'environ 70 sites, pour près de 1100 utilisateurs** - agents administratifs et enseignants inclus. Ce large périmètre implique une grande diversité de profils et de niveaux de maturité numérique, notamment sur les aspects de cybersécurité. **Le défi principal consiste à maintenir un système d'information opérationnel, sécurisé, et cohérent malgré cette hétérogénéité, tout en respectant les contraintes budgétaires fortes du secteur public.** Cela nécessite beaucoup d'agilité, d'ingéniosité, et de pragmatisme au quotidien.

ANTOINE TRILLARD_

DSI de la Ville de Chelles & Président du CoTer Numérique

02

QUELS RISQUES CYBER CONSIDÉREZ-VOUS AUJOURD'HUI COMME LES PLUS CRITIQUES POUR UNE COLLECTIVITÉ COMME LA VÔTRE ?

Tous les risques cyber doivent être considérés comme critiques car aujourd'hui **les menaces sont devenues multiformes et imbriquées.**

Alors qu'auparavant l'explosion d'une charge malveillante se déroulait rapidement après l'infection, les attaquants prennent maintenant le temps d'étudier leurs cibles, de bien préparer le terrain, d'échanger les informations avec d'autres pirates, afin de faire le plus de dégâts possibles dans le but d'obliger les victimes à céder au chantage financier. Il se passe parfois plusieurs mois avant qu'un opérateur malveillant ne décide de prendre le contrôle de votre SI. Même si nous ne manipulons pas de secrets industriels, **nous détenons un actif très convoité : la donnée personnelle,** qu'il s'agisse de celles de nos agents ou de nos administrés. Nous nous devons donc d'en assurer la protection, en couvrant un spectre de risque le plus large possible tout en le pondérant avec sa vraisemblance.

*Enjeux cybersécurité_*

Garantir
la continuité des services publics malgré des ressources limitées

Protéger
les données personnelles des agents et des citoyens

Détecter et identifier
toutes typologies d'attaques de plus en plus furtives et sophistiquées

Réduire
les angles morts induits par l'hétérogénéité des outils

Anticiper
les risques dans un contexte de compétences rares

Ainsi, peu importe le vecteur d'attaque, même si nous savons parfaitement que les programmes malveillants, les phishing ou encore tentatives d'usurpation d'identité sont légion dans les collectivités, **il est nécessaire de surveiller toute la surface du SI et de détecter les premiers signaux faibles,** ces comportements isolés qui, mis en relation, révèlent une menace bien plus large. **La surveillance doit donc être continue, complète et intelligente.**

GATEWATCHER

03

QUELLES SONT VOS PRINCIPALES CONTRAINTES TECHNIQUES ET OPÉRATIONNELLES EN MATIÈRE DE CYBERSÉCURITÉ ?

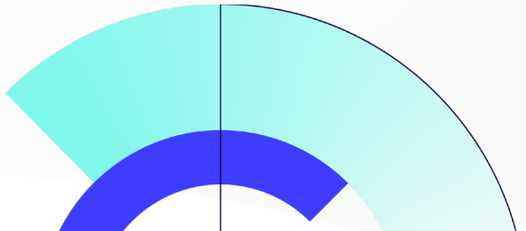
Les collectivités font aujourd'hui face à une double contrainte:

> Un **manque d'attractivité pour les talents** de la cybersécurité

> Des **budgets limités**

La fonction publique n'attire pas facilement les jeunes diplômés du secteur, et cela complique le renforcement des équipes avec des experts. En parallèle, les agents en poste doivent souvent être polyvalents, ce qui limite le temps qu'ils peuvent consacrer à la cybersécurité.

La question des budgets alloués à la cybersécurité est aussi une part intégrante du problème. En effet, même si la conscience des risques progresse chez les décideurs, et notamment grâce aux retours d'expériences de nos pairs, **les besoins de sécurité augmentent plus vite que les moyens.** C'est pourquoi nous privilégions des **solutions capables de consolider plusieurs fonctions dans un seul outil,** avec une interface claire. C'est un **levier de rationalisation efficace, autant pour l'analyse que pour la réponse.**



04

QUELLES LIMITES RENCONTRIEZ-VOUS DANS VOTRE PROTECTION AVANT DE DÉPLOYER UN NDR ?

La principale limite que nous rencontrions se situait dans la **multiplication des outils et des sources d'alertes**. Chaque solution avait sa propre console, ses propres alertes, et son propre périmètre de détection. Cela rendait la supervision globale complexe et parfois incomplète. Même avec des réglages affinés, une mauvaise configuration ou un oubli humain (comme un agent non installé, un filtrage trop permissif, etc.) pouvait créer une faille. **Les outils déployés en silo,** aujourd'hui considérés comme «obligatoires», **ne permettent pas toujours une vision transversale des flux réseau, ni une corrélation efficace entre signaux faibles.**

05

QU'EST-CE QUI VOUS A CONVAINCU D'INTÉGRER UNE PLATEFORME NDR À VOTRE DISPOSITIF DE CYBERSÉCURITÉ? ET COMMENT AVEZ-VOUS MESURÉ LE SUCCÈS DE SON INTÉGRATION ?

La plateforme NDR vient en complément de tous nos autres outils, elle participe de fait **au renforcement global de la sécurisation de notre SI en scrutant et détectant des menaces que nos autres outils auraient pu ne pas voir.** Si nous avions déjà la ceinture et les bretelles, notre pantalon cybersécurité possède maintenant aussi un élastique invisible dans sa doublure.

On parle beaucoup aujourd'hui de logique XDR, la plateforme NDR en est une partie intégrante, car comme je le disais précédemment, si l'EDR a été oublié, mal configuré ou désactivé sur un poste, la sonde NDR reste elle pleinement active et permettra une détection des menaces.

Le NDR nous a permis d'identifier des comportements et des usages qui passaient inaperçus avec nos autres outils de sécurité, soit parce qu'ils ne relevaient pas de leur périmètre, soit parce que certaines configurations, volontairement permissives pour des raisons de production, les laissaient passer. S'ils ne représentaient pas un risque immédiat, ces comportements auraient toutefois pu être exploités à des fins malveillantes.

NOM DE LA COLLECTIVITÉ
Chelles

TYPE DE COLLECTIVITÉ
Commune

NOMBRE DE COLLABORATEURS
> 800 agents + 450 enseignants

NOMBRE DE SITES SUPERVISÉS
70

PARC INFORMATIQUE
900 dont 125 serveurs virtuels

PÉRIMÈTRE FONCTIONNEL COUVERT PAR LE DSI/RSSI
SIG, Smart city, Infra, SSI, poste de travail, une centaine de progiciel

> *C'est pourquoi nous privilégions des solutions capables de consolider plusieurs fonctions dans un seul outil, avec une interface claire. C'est un levier de rationalisation efficace, autant pour l'analyse que pour la réponse.*

06

COMMENT S'EST PASSÉE LA PHASE DE DÉPLOIEMENT DE LA PLATEFORME NDR ?

Nous avons la chance d'avoir des compétences en cybersécurité en interne, elles-mêmes associées à l'envie de maitriser les solutions que nous mettons en œuvre dans notre SI. **La phase de POC a été une étape clé : elle nous a permis de comprendre la logique de la solution, son fonctionnement intrinsèque, ses capacités de personnalisation et de flexibilité, et ses cas d'usage concrets.**

Ces discussions techniques, avec des équipes compétentes, ont permis une intégration et une mise en œuvre facilitée et très fluide. Depuis le déploiement, **nous affinons régulièrement les règles d'alerte avec leur support,** afin d'obtenir un niveau de précision parfaitement adapté à notre contexte.

07

POURQUOI AVOIR CHOISI GATEWATCHER PLUTÔT QU'UN AUTRE ACTEUR DU MARCHÉ ?

Nous avons été sollicités par plusieurs éditeurs, mais ce sont à la fois les spécificités techniques de la solution et sa souveraineté qui ont fait pencher la balance en faveur de Gatewatcher. **Le fait qu'il s'agisse d'un acteur français,** proposant également des solutions qualifiées par l'ANSSI, **constitue un atout important pour une collectivité :** cela garantit un meilleur alignement avec nos exigences réglementaires et une maîtrise locale et souveraine des données sensibles.

L'interface intuitive et entièrement personnalisable a été tout aussi déterminante. Les briques de gestion intelligente et de réponse ciblée aux menaces/incidents avec Reflex et Cockpit apportent des capacités de tri, de contextualisation et de réponse aux incidents qui nous font gagner en efficacité au quotidien.

> *Les briques de gestion intelligente et de réponse ciblée aux menaces/incidents avec Reflex et Cockpit apportent des capacités de tri, de contextualisation et de réponse aux incidents qui nous font gagner en efficacité au quotidien.*

08

AVEZ-VOUS UN EXEMPLE CONCRET D'ALERTE OU D'ATTAQUE DÉTECTÉE GRÂCE À GATEWATCHER ? QUELS RÉSULTATS VOUS SEMBLENT LES PLUS PARLANTS ?

Par chance, nous n'avons pas encore eu de détection d'attaque, mais la solution NDR nous a permis de découvrir les alertes suivantes :

>**L'utilisation de réseau P2P:** des ordinateurs personnels connectés sur un réseau un peu plus ouvert pour des raisons de production se connectaient au moyen de protocoles P2P. Cette détection nous a permis de restreindre ces usages qui auraient pu devenir dangereux par rebond.

>**Des requêtes DNS vers des sites suspicieux:** certains ordinateurs du réseau effectuaient des requêtes DNS vers des sites suspicieux, parfois bloqués par le filtrage, parfois non. Cette détection nous a permis de renforcer nos filtrages et de spécifiquement nettoyer les fichiers temporaires des postes correspondants.

>**Du bruit sur le réseau:** de nombreuses requêtes transitaient sur le réseau (broadcast en particulier) ajoutant du bruit et une consommation de bande passante sur le réseau. Cette détection nous a permis de désactiver des services inutilisés, mais générant du trafic, sur certains de nos outils.

09

AVEC VOTRE REGARD TRANSVERSAL AU SEIN DU COTER NUMÉRIQUE, DANS QUELS CAS D'USAGE FRÉQUENTS OBSERVEZ-VOUS UNE RÉELLE VALEUR AJOUTÉE DE LA PLATEFORME NDR POUR LES COLLECTIVITÉS ?

Pour adopter une approche réellement proactive de la cybersécurité, la plateforme NDR permet d'obtenir une visibilité et des informations sur tout ce qui transite sur le réseau. En remontant des alertes à un niveau différent des autres produits de sécurité, **elle offre la possibilité aux collectivités de mieux maitriser leur exposition aux risques.**

Dans les structures disposant de ressources et de compétences internes, le NDR affine la détection et la configuration des différents composants du SI, en permettant d'aller au-delà des standards pour cibler les zones les plus sensibles.

Pour une collectivité dont les ressources et les compétences sont plus restreintes, **le NDR constitue un levier de centralisation et d'automatisation qui offre à la fois une vision globale des menaces et une feuille de route sur les sécurisations à mettre en œuvre.**

Bénéfices clés de la plateforme NDR_

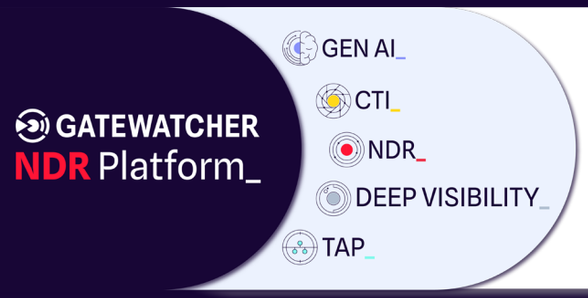
Surveiller
l'ensemble du trafic réseau pour une visibilité continue et complète

Unifier
la détection, l'identification et la priorisation sur une interface unique, personnalisable et claire

Déployer
une solution flexible et hybride (non cloud native) garantissant souveraineté et contrôle des données

Automatiser et optimiser
la remédiation avec une réponse ciblée, complète et adaptée à votre contexte

Prioriser
les investigations pour valoriser le travail des analystes sur des alertes critiques

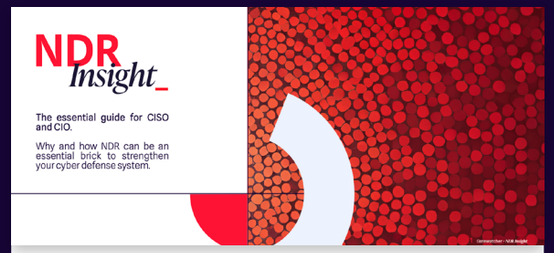


La plateforme NDR de Gatewatcher offre une cartographie et une analyse comportementale des cybermenaces pour obtenir une détection augmentée sur les attaques ciblées, y compris en cas de flux chiffrés. Elle associe machine learning, analyses statique et dynamique.

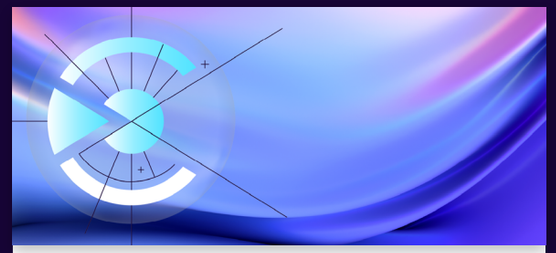
GATEWATCHER

Envie d'en *savoir plus* sur le sujet ?_

[VIDEO]
Easy as NDR:
Le R de NDR, qu'est-ce que c'est?



[GUIDE]
L'essentiel du NDR
dans un guide pratique.



[USE CASE]
Révéler des zones de faiblesses
dans mon dispositif

*Easy as_*

NDR_ CTI_ TAP_ GEN AI_ DEEP VISIBILITY_

Contactez-nous ! ⟶