CUSTOMER STORY

RENFORCER LA CYBERSÉCURITÉ DANS LE SECTEUR DE L'ÉDUCATION_

“

Avec un budget IT réduit, nous devons faire des choix difficiles. Mais une attaque pourrait coûter bien plus cher que la prévention.

Directeur Cybersécurité & DPO
d'un établissement d'enseignement supérieur

#NDR #ÉDUCATION #OPTIMISATIONBUDGET

01

QUELS SONT LES PRINCIPAUX DÉFIS DE CYBERSÉCURITÉ RENCONTRÉS DANS LE SECTEUR DE L'ÉDUCATION ?

La cybersécurité dans le secteur éducatif va bien au-delà de la simple protection des ordinateurs. **Le secteur de l'éducation est devenu une cible privilégiée des cybercriminels,** avec une augmentation des cyberattaques ces trois dernières années. Notre établissement gère **des milliers de dossiers d'étudiants, de données financières, et une infrastructure numérique complexe** qui s'étend des **systèmes de gestion scolaire aux plateformes d'apprentissage en ligne.** Avec un écosystème aussi fragmenté, sécuriser chaque point d'entrée représente un défi majeur.

Protéger **les données des étudiants** et du personnel est une priorité absolue. Nos plateformes d'apprentissage en ligne, systèmes de notes, et portails administratifs traitent d'énormes quantités d'informations personnelles sensibles ; au-delà des simples bulletins ou dossiers d'inscription, on parle par exemple de plans d'accompagnement handicap / dossiers médicaux (PAI), coordonnées bancaires ou RIB pour les frais de scolarité et bourses, évaluations disciplinaires ou suivis psychopédagogiques, pièces d'identité numérisées pour les examens en ligne. Autant d'éléments qui attirent l'attention des cybercriminels. Une violation n'aurait **pas seulement des conséquences financières,** elle compromettrait gravement **la confiance des familles et la réputation de l'établissement.**

Au-delà des risques numériques, **nos systèmes de gestion des bibliothèques, réseaux de partenaires externes, et infrastructures distribuées** ajoutent une complexité supplémentaire. Que ce soit **sécuriser l'accès aux réseaux des campus ou prévenir les intrusions non autorisées,** nous devons constamment nous adapter aux menaces évolutives pour maintenir nos opérations sécurisées.

02

COMMENT LES CONTRAINTES BUDGÉTAIRES IMPACTENT-ELLES VOTRE CYBERSÉCURITÉ ?

Mon établissement fait face à un paradoxe cruel : des besoins de sécurité croissants avec un budget IT stagnant (ou trop peu croissant). Contrairement à certains grands groupes qui disposent d'équipes dédiées, dans l'éducation, on plafonne autour de 6,6 % du budget IT en cybersécurité, bien en deçà des 10% recommandés, une différence qui pèse quand les attaques ont augmenté de plus de 100%. **On doit donc faire des choix difficiles entre renouveler les équipements pédagogiques et renforcer la cybersécurité.**

Cette réalité budgétaire nous expose dangereusement. **Une contrainte qui nous a longtemps poussés à privilégier "des dépenses visibles et urgentes" au détriment du renforcement des réseaux,** moins perceptible mais vital. Les cybercriminels le savent: c'est ce qui a fait de l'éducation une cible facile. Une cyberattaque sur nos systèmes de gestion pédagogique pourrait paralyser les cours et compromettre les données d'examens, avec des coûts de remédiation pouvant atteindre **plusieurs mois de notre budget IT.**

*Enjeux cybersécurité_*

Protéger
la propriété intellectuelle contre l'espionnage industriel et étatique

Détecter
et gérer les menaces avancées (APT, ransomwares, attaques ciblées)

Maintenir
un haut niveau de cybersécurité avec des ressources limitées

Garantir
la souveraineté et le contrôle des données sensibles

Assurer
une posture de sécurité agile et évolutive

03

COMMENT VOTRE ARCHITECTURE RÉSEAU EST-ELLE STRUCTURÉE ?

Notre réseau est segmenté entre **un réseau pédagogique** (élèves, enseignants, plateformes d'apprentissage) et **un réseau administratif** (données sensibles, gestion interne). Cette séparation limite les risques, mais la multiplication des outils numériques, des connexions distantes et des usages croisés a complexifié notre sécurité.

Avant, nous utilisions plusieurs outils qui ne communiquaient pas entre eux, ce qui nous laissait **sans vue d'ensemble avec une détection qui nous semblait partielle**. Le déploiement de la plateforme NDR de Gatewatcher a changé la donne : nous avons désormais une visibilité complète et centralisée du trafic réseau, sans modifier notre infrastructure. De plus, nous savons que pour des établissements encore plus vastes ou multi-sites, ces défis deviennent encore plus critiques dans notre secteur.

Cela nous permet d'**identifier rapidement les comportements anormaux,** de **protéger l'ensemble de nos environnements** (campus, cloud, outils externes), et **de soulager notre équipe IT.** La solution s'est intégrée naturellement à notre système, **offrant une cybersécurité renforcée sans sacrifier la simplicité de gestion, ni perturber les opérations quotidiennes.**

04

POURQUOI AVEZ-VOUS DÉCIDÉ DE METTRE EN PLACE UNE SOLUTION NDR ?

En évaluant notre posture de cybersécurité, **nous avons identifié le réseau comme notre principal angle mort**. Nos solutions déjà existantes protégeaient efficacement les appareils des utilisateurs, et nos serveurs ainsi que nos applications bénéficiaient déjà de mesures de sécurité solides. Pourtant, l'activité réseau restait largement invisible. **Sans capacité de détection en temps réel des anomalies, nous demeurions vulnérables aux menaces furtives circulant à l'intérieur de notre infrastructure.**

Pour un établissement éducatif, il est crucial que la sécurité soit à la fois rapide, transparente et parfaitement intégrée à notre environnement. **L'implémentation d'une solution NDR répondait à cet impératif, en renforçant notre visibilité sans perturber nos opérations quotidiennes.**

05

POURQUOI AVOIR CHOISI GATEWATCHER COMME PARTENAIRE NDR ?

Ce qui nous a convaincus chez Gatewatcher, c'est **leur agilité et leur capacité à s'adapter à nos enjeux spécifiques.** Plutôt que d'imposer un cadre figé, ils ont proposé une solution modulable, capable de cibler nos vulnérabilités réelles et d'évoluer avec notre environnement. **L'approche est granulaire :** nous pouvons ajuster les fonctionnalités en fonction de nos priorités et de nos besoins opérationnels, ce qui maximise la valeur apportée.

En conséquence, le coût devient non pas une contrainte, mais un atout : il est mesuré et proportionnel à l'usage, ce qui rend la solution accessible tout en offrant un niveau de performance équivalent, voire supérieur, à celui de solutions NDR bien plus onéreuses.

> *Nous devons constamment nous adapter aux menaces évolutives pour maintenir nos opérations sécurisées.*

SECTEUR
Éducation

EFFECTIFS
> 4 000
salariés

> 25 000
étudiants

> 80
laboratoires de recherches

PROFILS UTILISATEURS VARIÉS
Élèves, étudiants, enseignants, personnel administratif, parents, intervenants externes, et partenaires pédagogiques

EXPOSITION NUMÉRIQUE
40 plateformes (ressources spécialisées, plateformes de gestion de cours, portails étudiants, etc.) et plus de 15 000 appareils connectés (ordinateurs fixes, tablettes, bornes Wi-Fi, équipements IoT pour la gestion des bâtiments, etc.)

06

COMMENT GATEWATCHER UTILISE L'INTELLIGENCE ARTIFICIELLE POUR MIEUX PROTÉGER VOTRE ÉTABLISSEMENT ?

GAIA, le cyber assistant de Gatewatcher, aide à tout simplifier et allège la charge des équipes IT. Il aide dans les analyses des informations issues de multiples sources, permettant aux équipes une compréhension claire et rapide des incidents détectés. Ça simplifie donc la prise de décision et clarifie les protocoles à suivre dans les actions de remédiation. Cette assistance intelligente transforme la complexité des alertes en actions concrètes en renforçant le reporting d'incidents, libérant les analystes SOC de cette charge fastidieuse. Il optimise la détection, la compréhension et les investigations des cybermenaces, tout en s'intégrant parfaitement aux outils déjà en place dans les établissements.

> *Ce qui nous a convaincus chez Gatewatcher, c'est leur agilité et leur capacité à s'adapter à nos enjeux spécifiques. Plutôt que d'imposer un cadre figé, ils ont proposé une solution modulable, capable de cibler nos vulnérabilités réelles et d'évoluer avec notre environnement.*

07

COMMENT DÉFINIR LE SUCCÈS AVEC LE NDR GATEWATCHER ?

Notre priorité était d'avoir une **visibilité claire et intelligente,** capable de distinguer les vraies menaces du simple bruit de fond, un vrai défi quand les équipes IT sont petites ou peu nombreuses.

La solution NDR de Gatewatcher est devenue essentielle, surtout **pour gérer le Shadow IT** très présent dans nos établissements : laboratoires avec systèmes autonomes, classes qui utilisent des outils pédagogiques spécifiques, ou services administratifs qui déploient parfois des plateformes non centralisées. Ces usages, même utiles, peuvent ouvrir des portes aux cyberattaques, souvent invisibles avec les protections classiques.

Avec la plateforme NDR de Gatewatcher, nous avons nettement amélioré notre temps de détection et réponse aux incidents. **Dès l'apparition du moindre signal faible, notre équipe reçoit des alertes enrichies de données contextuelles** (type d'attaque, terminal concerné, vecteur potentiel). **La CTI Gatewatcher** apporte un vrai plus en communiquant des informations précises sur les menaces propres à l'éducation, ce qui aide à réagir vite et efficacement. Cette intelligence contextuelle nous permet d'anticiper les campagnes d'attaques récurrentes dans notre domaine et d'adapter nos défenses en conséquence.

De plus, la solution **REFLEX** automatise les réponses aux incidents ce qui soulage nos équipes. Je dirai qu'on a économisé **30 à 50 % de temps sur la qualification des incidents,** car les analystes accèdent immédiatement aux informations clés. Finalement, Gatewatcher nous permet de sécuriser notre environnement éducatif de manière simple, transparente et adaptée à nos besoins réels.

Bénéfices clés_

Garantir
une surveillance continue et granulaire de l'ensemble des infrastructures pour anticiper et neutraliser les cybermenaces

Gérer
proactivement les périodes critiques (examens, inscriptions) pour maintenir la continuité pédagogique sans interruption

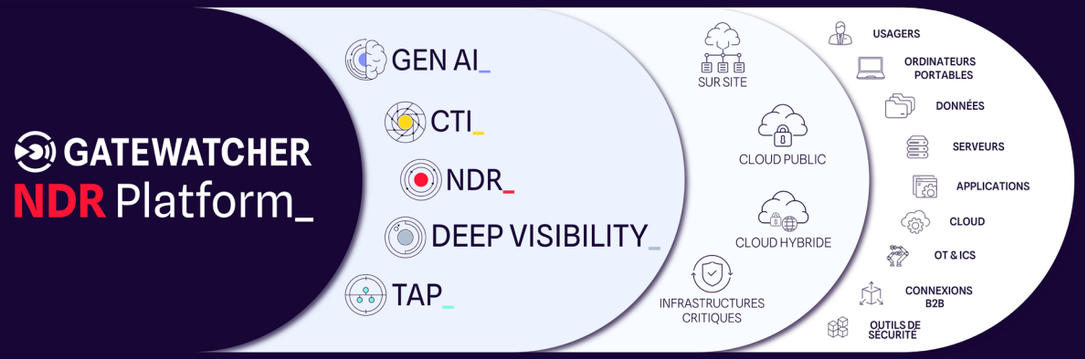
Cartographier
l'ensemble du trafic réseau pour une visibilité complète

Centraliser
intelligemment les alertes dans un tableau de bord unique pour une réponse accélérée et une priorisation efficace des menaces

*À propos_*

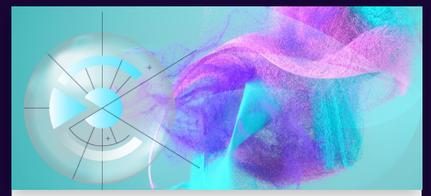
Leader de la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux des entreprises et des institutions publiques, y compris les plus critiques. La plateforme NDR Gatewatcher (Network Detection and Response), combine intelligence artificielle, techniques d'analyse dynamiques et comportementales et Cyber Threat Intelligence (CTI) contextualisée. Elle offre ainsi une visibilité unifiée et complète, une détection et une cartographie des systèmes en temps réel et une réponse globale, automatisée et priorisée face aux attaques. Déployée sur infrastructures cloud, on-premise ou sensibles, et compatible avec les environnements IT, OT et IoT, elle sécurise l'ensemble des actifs critiques et simplifie les opérations grâce à son assistant IA intégré. Gatewatcher allie puissance technologique et sérénité opérationnelle, afin d'aligner la cybersécurité sur vos objectifs business.

Contactez-nous

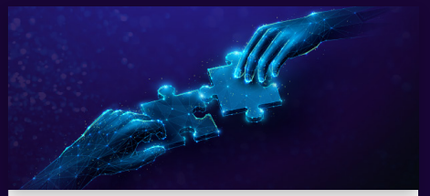


Envie d'en *savoir plus ?_*

[PODCAST]
S3 #E1 – Agnès Fabre, Génération connectée : l'Éducation au péril du tout numérique ?



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



[ARTICLE]
Cybersécurité : en quoi l'EDR et le NDR sont-ils complémentaires ?