CUSTOMER STORY

LEEDS FC, RENFORCER LA RÉSILIENCE CYBER DANS UN ENVIRONNEMENT À FORTS ENJEUX

“

Pour nous, la priorité était de trouver une solution apportant une réelle valeur. Tandis que certains clubs se tournaient vers des fournisseurs historiques, **nous avons vu en Gatewatcher un leader émergent aux capacités solides.**

Graham Peck
Responsable de la sécurité de l’information et DPO au Leeds United Football Club

#SPORT #NDR # ÉVÉNEMENT À FORTE VISIBILITÉ

01

QUELS SONT LES ENJEUX CYBERSÉCURITÉ SPÉCIFIQUES ET UNIQUES AUXQUELS EST CONFRONTÉ LEEDS FC, ET QUEL IMPACT ONT-ILS SUR LES OPÉRATIONS DU CLUB ?

La cybersécurité chez Leeds FC va bien au-delà des jours de match. En tant que club, nous gérons des **milliers de données personnelles, des transactions financières, et une infrastructure numérique complexe** couvrant tout, des **plateformes de billetterie aux systèmes de sécurité du stade.** Avec un écosystème aussi fragmenté, **sécuriser chaque point d'entrée est un défi majeur.**

La protection des **données des fans et des informations financières** est une priorité absolue. Nos plateformes de billetterie et de vente en ligne traitent d'importants volumes d'**informations personnelles et de paiements,** ce qui en fait une cible pour les cybercriminels. Une violation aurait non seulement des **conséquences financières,** mais entamerait sérieusement **la confiance et la réputation** du club.

Au-delà des risques numériques, notre infrastructure de stade, **les systèmes de contrôle d'accès et les prestataires tiers** ajoutent une couche de complexité. Qu'il s'agisse de **sécuriser les réseaux internes, d'empêcher les accès non autorisés ou de garantir la conformité aux réglementations cybersécurité de la Premier League et de l'UEFA,** nous devons **sans cesse nous adapter aux menaces émergentes** pour assurer la sécurité des opérations du club.

02

EN QUOI LES ÉVÉNEMENTS À FORTE VISIBILITÉ AUGMENTENT-ILS LES RISQUES CYBER ?

Les jours de match génèrent **une augmentation massive du trafic numérique et une hausse du risque d'attaques cyber.** Avec **plus de 37 000 spectateurs dans le stade — bientôt 55 000 — notre réseau doit garantir un accès sécurisé aux systèmes de contrôle, de paiement, et au Wi-Fi public,** tout en restant résilient face aux attaques potentielles. Imaginez une **défaillance de l'assistance vidéo (VAR)** lors d'un match décisif : décisions retardées, confusion sur le terrain, et résultat remis en question par des millions de spectateurs. Une cyberattaque sur **la transmission des données en temps réel** pourrait **perturber les décisions, influencer l'issue du match et nuire à la crédibilité de la compétition.**

La **portée mondiale des matchs à forte visibilité** fait de nous une cible encore plus attrayante. Des cybercriminels peuvent tenter de **perturber les retransmissions en direct,** de **surcharger notre infrastructure numérique** ou **d'exploiter les vulnérabilités des systèmes de billetterie et de sécurité.**

La **diversité des personnes et des appareils connectés** multiplie les risques d'**accès non autorisé ou de fuite de données.**

*Enjeux cybersécurité_*

Gérer
une infrastructure segmentée

Détecter
les menaces ciblées en temps réel

Contrôler
les pics d'exposition temporaires

Corréler
efficacement les signaux de sécurité

Garantir
la protection des données

Graham PECK_
Responsable de la sécurité de l'information et DPO au Leeds United Football Club

03

COMMENT L'ARCHITECTURE RÉSEAU DE LEEDS FC EST-ELLE STRUCTURÉE, ET COMMENT LA SOLUTION NDR A-T-ELLE ÉTÉ DÉPLOYÉE ?

Leeds FC exploite un **réseau segmenté,** garantissant que les **opérations les jours de match et les systèmes administratifs restent séparés.** Le réseau dédié aux jours de match prend en charge les opérations du stade, la billetterie, et la diffusion des matchs, tandis que le réseau du siège gère les transactions financières, les communications internes, et la gestion du club. Cette séparation est essentielle, car les environnements administratifs sont plus vulnérables aux menaces cyber du fait du facteur humain.

Lors du déploiement de la solution NDR, notre priorité était d'**assurer une visibilité sur les deux environnements sans ajouter de complexité.** Gatewatcher nous a permis de surveiller le trafic de manière centralisée, sans perturber les opérations quotidiennes.

Le déploiement a été simple, car nous utilisons une infrastructure virtualisée plutôt que de nous appuyer sur **des équipements physiques,** ce qui facilite la montée en charge, la configuration, et l'intégration dans notre dispositif de sécurité existant. Cette approche nous a offert **une surveillance en temps réel** sur les deux réseaux, garantissant que nous puissions **détecter et répondre rapidement aux menaces.**

04

QU'EST-CE QUI A MOTIVÉ LEEDS FC À METTRE EN PLACE UNE SOLUTION NDR, ET COMMENT CELLE-CI S'INTÈGRE-T-ELLE AUX OUTILS DE SÉCURITÉ EXISTANTS ?

En évaluant notre posture cybersécurité, nous avons réalisé que **le réseau était notre plus grande zone d'ombre.** Nous avions Crowdstrike pour la protection des endpoints (EDR) sur les **postes utilisateurs**, et un XDR pour sécuriser **les serveurs et applications,** mais **l'activité réseau restait largement invisible.** Sans outil de détection d'anomalies en temps réel, nous étions exposés à des **menaces furtives capables de circuler sans être repérées.**

Et pour être honnête, **le coût a aussi été un facteur important dans notre décision.** Beaucoup de solutions NDR sont associées à des tarifs élevés, **souvent liés à la notoriété de la marque plutôt qu'à la valeur fonctionnelle.**

En explorant plusieurs solutions NDR, ce qui nous a convaincus chez **Gatewatcher**, c'est leur **agilité et leur capacité d'adaptation.** Plutôt que de nous imposer un cadre rigide, ils ont su évoluer avec nous, en nous aidant à traiter des **vulnérabilités spécifiques** au fur et à mesure de leur apparition. Pour nous, la priorité était de trouver une solution apportant une réelle valeur ajoutée. Alors que certains clubs se sont tournés vers des fournisseurs historiques, nous avons vu en Gatewatcher un leader émergent avec de fortes capacités.

Pour un club de football, la sécurité doit être **rapide, transparente, et adaptée à notre environnement unique.** Le NDR de Gatewatcher **s'intègre de façon fluide** à notre stack de sécurité existant, **en renforçant la visibilité sans perturber nos opérations quotidiennes.**

> Lors du déploiement de la solution NDR, notre priorité était d'assurer une visibilité sur les deux environnements sans ajouter de complexité. Gatewatcher nous a permis de surveiller le trafic de manière centralisée, sans perturber les opérations quotidiennes.

SIÈGE
Leeds, Angleterre

SECTEUR D'ACTIVITÉ
Club de football professionnel

> 196,1 millions de dollars
Revenus

>37 000 *(extension prévue à 55 000)*
Capacité du stade

ENVIRONNEMENTS VARIÉS
Stade, centres d'entraînement, siège, plateformes en ligne

PROFILS UTILISATEURS DIVERS
Fans, joueurs, personnel, médias, partenaires, prestataires

VISIBILITÉ MONDIALE
Audience internationale, échanges de données transfrontaliers, points d'accès à distance

05

COMMENT LEEDS FC A-T-IL DÉFINI LE SUCCÈS LORS DE LA MISE EN ŒUVRE DU NDR, ET QUELLES ÉTAIENT LES PRIORITÉS CLÉS ?

Lors de l'adoption du NDR, notre objectif principal était la **visibilité.** Les outils de sécurité ne sont efficaces que s'ils fournissent d**es informations claires et exploitables** — sinon, ils génèrent **trop de bruit**, submergeant les équipes avec de faux positifs. La première étape consistait **à garantir que le système puisse apprendre précisément le comportement normal de notre réseau,** avant de passer à la **détection active des menaces.**

Un autre facteur clé était **l'intégration.** Nous ne voulions pas d'un outil isolé ; nous avions besoin d'une solution NDR **capable de transmettre les données de manière fluide et de fournir une vue unifiée aux côtés de notre XDR, EDR et d'autres outils de sécurité.** Gatewatcher a répondu à cette attente en nous permettant de visualiser **toute l'activité en un seul endroit,** sans avoir à naviguer entre plusieurs tableaux de bord.

Le succès, ce n'était pas seulement détecter les menaces — c'était le faire **efficacement, sans perturber les opérations quotidiennes**. En réduisant les alertes inutiles et en ajustant finement les capacités de détection, nous avons permis aux équipes sécurité de se concentrer uniquement sur les **risques réels,** tout en maintenant **un réseau sécurisé et réactif** pour le club.

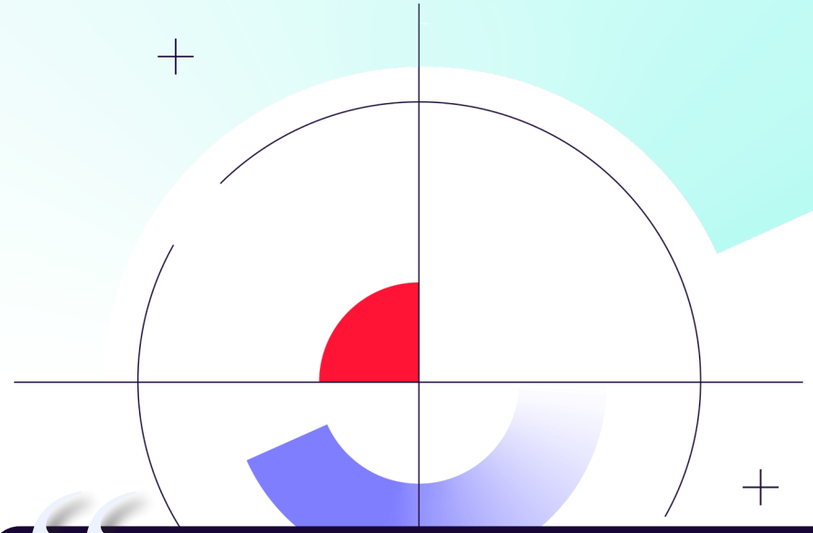
06

COMMENT LA SOLUTION NDR S'ALIGNE-T-ELLE AVEC LES POLITIQUES DE SÉCURITÉ ET LES OBJECTIFS STRATÉGIQUES DE LEEDS FC ?

La cybersécurité dans le football évolue, et **la visibilité réseau est aujourd'hui aussi critique que la protection des endpoints.** Les clubs ne peuvent plus se reposer uniquement sur des antivirus ou des pare-feux — sécuriser l'ensemble du réseau est devenu essentiel pour protéger les données sensibles et garantir la continuité des opérations. Chez Leeds FC, notre objectif était d'**aligner le choix de notre solution cybersécurité avec nos politiques de sécurité,** à savoir : **détection des menaces, réponse aux incidents, et surveillance proactive.**

La solution NDR de Gatewatcher nous a permis d'obtenir des **informations claires et exploitables.** Au lieu d'être submergés par les alertes, nous sommes désormais capables **d'identifier ce qui est un trafic normal et ce qui ne l'est pas**, ce qui nous permet de nous **concentrer uniquement sur les menaces réelles.** Qu'il s'agisse d'une véritable cyberattaque ou d'une requête d'accès inhabituelle mais légitime provenant d'un autre club ou d'un fournisseur externe, nous sommes désormais en mesure de l'**analyser et d'y répondre avec précision.**

Cette approche **soutient directement nos politiques de sécurité et s'aligne sur les meilleures pratiques du secteur sportif,** où **la protection des données sensibles, la continuité opérationnelle, et la conformité aux réglementations cybersécurité** sont des impératifs.



Le succès, ce n'était pas seulement détecter les menaces — c'était le faire **efficacement, sans perturber les opérations quotidiennes**. En réduisant les alertes inutiles et en ajustant finement les capacités de détection, nous avons permis aux équipes sécurité de se concentrer uniquement sur les risques réels, tout en maintenant un réseau sécurisé et réactif pour le club.

07

QUEL EST LE RÔLE DU NDR DANS LA STRATÉGIE XDR DE LEEDS FC ?

Chez Leeds FC, le **NDR est un composant essentiel de notre stratégie XDR,** garantissant **une approche unifiée et proactive de la cybersécurité.** Tandis que le XDR assure la détection et la réponse sur les endpoints et les environnements cloud, l'intégration du NDR nous permet d'**étendre cette visibilité à l'activité réseau,** en éliminant les zones d'ombre.

En intégrant le NDR à notre cadre XDR, nous pouvons **corréler les données issues des endpoints, du cloud, et du réseau,** créant ainsi **un écosystème de sécurité cohérent.** Cette intégration fluide nous permet de détecter et neutraliser les menaces plus rapidement, en garantissant la protection de l'ensemble de notre infrastructure, qu'il s'agisse des systèmes internes ou des opérations les jours de match.

AVANTAGES_

Sécuriser un écosystème segmenté
Fournit une surveillance en temps réel couvrant les stades, centres d'entraînement, sièges sociaux et plateformes en ligne.

Gérer les risques liés aux événements à forte visibilité
Détecte et neutralise les menaces visant les jours de match, les diffusions en direct et la connectivité massive des fans.

Contrôler les pics d'exposition temporaire
Suit et analyse chaque appareil connecté et interaction réseau pendant les événements.

Renforcer la visibilité sur les menaces ciblées
Identifie les attaques furtives exploitant les vulnérabilités dans les systèmes de billetterie, de paiement et de diffusion.

Corréler efficacement les signaux de sécurité
Unifie les alertes issues des systèmes IT, OT et opérationnels pour accélérer la détection des menaces.

Garantir la protection des données
S'adapte à des environnements à fort trafic et à forts enjeux sans impacter les performances.

*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

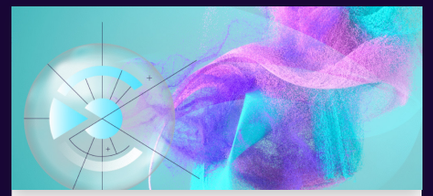
Plateforme **NDR_**
GATEWATCHER

- GEN AI_
- CTI_
- NDR_
- DEEP VISIBILITY_
- TAP_

La plateforme NDR de Gatewatcher offre une cartographie des cybermenaces et une analyse comportementale afin d'assurer la détection des attaques ciblées, même en cas de flux de données chiffrées. Elle combine notamment du machine learning avec des analyses statiques et dynamiques.

Envie d'en *savoir plus ?_*

[PODCAST]
DANS L'OEIL DE LA CYBER S03 EP03
Sports, Beyond the Pitch : Cyber Threats in Football



[CAS D'USAGE]
SURVEILLER UN ÉVÉNEMENT SPÉCIFIQUE ET À FORTE VISIBILITÉ

[VIDÉO]
DÉCOUVRIR NOS VIDÉOS EASY AS NDR