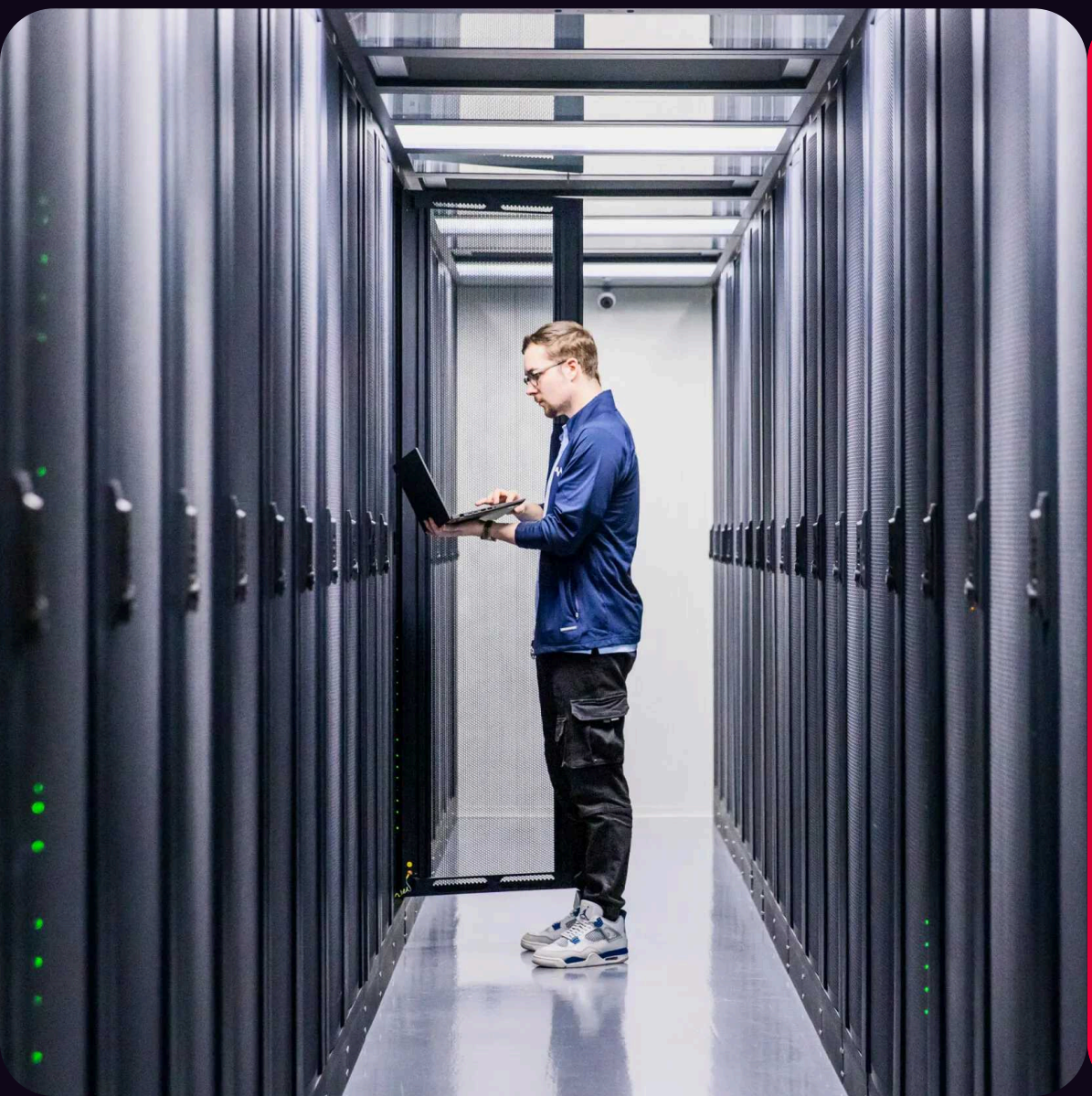
HADRIAN

WORLDSTREAM

ÉTUDE DE CAS

Comment Worldstream a opérationnalisé la gestion continue des expositions dans un environnement d'infrastructure critique

INFRASTRUCTURE IT, PAYS-BAS

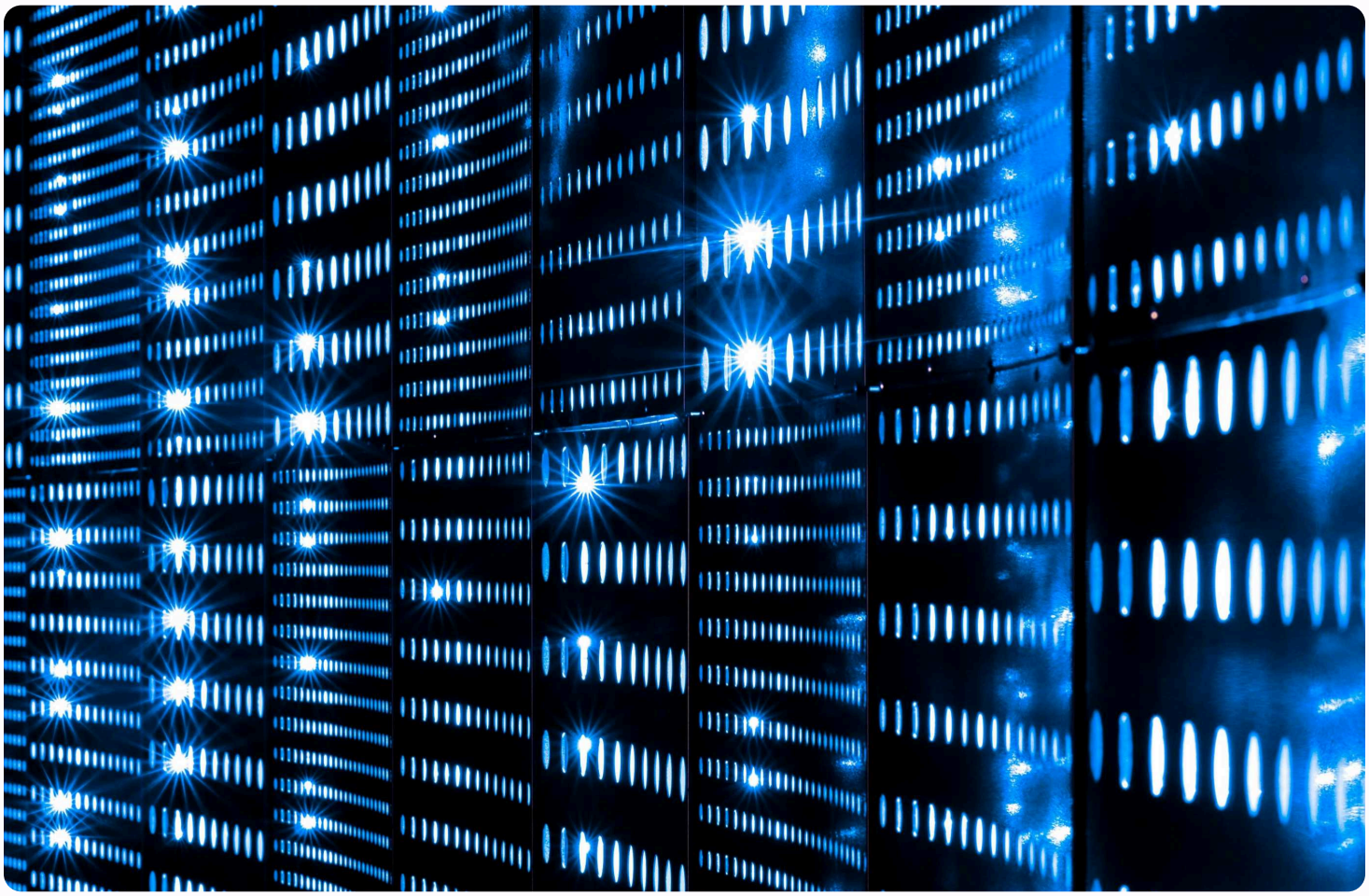


À propos de Worldstream

Worldstream est un fournisseur néerlandais d'infrastructure cloud disposant de ses propres centres de données et de son propre réseau en Europe. Depuis 2006, ils conçoivent, construisent et gèrent des infrastructures IT pour des organisations qui exigent contrôle, transparence et prévisibilité.

Worldstream fournit des serveurs dédiés, un cloud privé et des solutions d'infrastructure hybride pour les charges de travail critiques. En conservant la chaîne d'infrastructure en interne, des centres de données et du réseau jusqu'au matériel et au support 24h/24 et 7j/7, Worldstream offre aux organisations une base solide, transparente et prévisible pour les environnements IT modernes.

FONDÉE	SERVEURS PHYSIQUES	CLIENTS
2006	15.000+	2.500+



Défis

01 **Maintenir un contrôle continu sur une surface d'attaque en évolution**

Les organisations qui hébergent leurs charges de travail chez Worldstream s'attendent à ce que l'infrastructure soit stable et sécurisée. La sécurité est au cœur de la valeur que l'entreprise délivre, et maintenir une visibilité en temps réel et permanente sur chaque actif exposé externement est ce qu'exige cette promesse.

02 **Moderniser la gestion des vulnérabilités vers une priorisation basée sur l'exposition**

L'équipe gérait un parc large et complexe via une gestion traditionnelle des vulnérabilités, en priorisant les résultats par scores CVSS.

03 **S'assurer que chaque escalade est justifiée**

L'équipe de surveillance sécurité de Worldstream suit en permanence la surface d'attaque, tandis qu'une équipe de réponse aux incidents pluridisciplinaire est prête à intervenir sur les résultats critiques. L'objectif : garantir que seuls les résultats confirmés et réellement exploitables déclenchent une escalade, afin que la capacité d'expertise soit déployée exactement là où elle compte le plus.

Solution

✓ **Visibilité continue de l'extérieur vers l'intérieur sur la surface d'attaque**

L'équipe sécurité de Worldstream dispose désormais d'une vue en temps réel, continuellement mise à jour, de l'ensemble de son infrastructure exposée externement, cartographiée de l'extérieur vers l'intérieur avec Hadrian. Les nouveaux actifs et domaines sont détectés dès leur apparition, de sorte que l'environnement ne dépasse jamais ce que l'équipe peut voir.

✓ **Priorisation basée sur l'exposition remplaisant la gestion des vulnérabilités par volume**

Plutôt que de traiter de grands volumes de résultats classés par score CVSS, l'équipe sécurité de Worldstream se concentre désormais sur un ensemble réduit d'expositions confirmées comme réellement exploitables dans leur environnement spécifique. Chaque résultat est vérifié par rapport à l'exploitabilité réelle et au contexte métier avant d'atteindre l'équipe, transformant une longue liste de possibilités en une liste courte de priorités.

✓ **Des résultats validés qui donnent du sens à chaque escalade**

Avant qu'un résultat n'atteigne l'équipe de surveillance sécurité, il est confirmé comme un risque réel et exploitable, et non théorique. Cela donne à l'équipe la confiance nécessaire pour n'escalader que ce qui compte, et fournit à l'équipe de réponse aux incidents tout ce dont elle a besoin pour agir immédiatement, sans réenquêter depuis le début. Chaque escalade est justifiée. Chaque réponse est précise.

Il risultato

La visibilité continue comme promesse client

Pour Worldstream, la visibilité sur la surface d'attaque n'est pas qu'un objectif sécurité interne. C'est une partie de ce que les clients achètent lorsqu'ils choisissent d'héberger leurs charges de travail chez un fournisseur d'infrastructure critique. Les organisations qui choisissent Worldstream attendent une infrastructure continuellement sécurisée, surveillée et maîtresse de sa propre exposition. C'est une promesse que les évaluations périodiques et les instantanés ponctuels ne peuvent tenir.

L'équipe sécurité de Worldstream recense désormais chaque actif exposé en temps réel, au fil de l'évolution de l'infrastructure. Les nouveaux domaines, nouveaux services et changements d'exposition sont détectés dès qu'ils surviennent, et non à la prochaine revue programmée. Que la croissance vienne de nouveaux déploiements clients, de services étendus ou de changements réseau, l'équipe le voit immédiatement, et la surface d'attaque ne dérive jamais sans surveillance. Cette capacité se traduit directement par la garantie qu'attendent les clients de Worldstream : que l'infrastructure dont ils dépendent est sous contrôle continu et actif, et pas seulement révisée sur calendrier.

> **« Avec Hadrian, vous avez un partenaire vraiment solide pour opérationnaliser la gestion continue des expositions à l'échelle. La mise en place demande peu d'effort, améliore l'efficacité dans la mitigation des résultats et la réduction des risques, et l'outil est vraiment facile à utiliser, évolutif et reproductible. »**
>
> Alan Lucas — RSSI, Worldstream

Du scoring à l'exploitabilité validée

L'équipe sécurité de Worldstream opère désormais à partir d'un ensemble plus restreint et plus fiable d'expositions confirmées et exploitables, plutôt que de traiter de grands volumes de résultats classés par scores CVSS. Hadrian valide chaque résultat par rapport à l'exploitabilité réelle et au contexte spécifique de l'environnement de Worldstream avant de le remonter, de sorte que l'équipe agit sur ce qui compte réellement et non sur ce qu'un modèle de scoring suggère qui pourrait compter.

Résultats

Ce changement modifie également la façon dont le programme de sécurité est mesuré et rapporté. Worldstream suit son score de sécurité sur l'ensemble de la surface d'attaque externe, le pourcentage d'actifs sous scan continu, et le temps moyen pour identifier, contenir, éradiquer et récupérer, le tout mappé au NIST Cybersecurity Framework. Cette structure repose désormais sur une base live et validée. Pour un fournisseur opérant sous PCI DSS, se préparant à NIS2 et agissant comme prestataire tiers de services TIC sous DORA, cette preuve continue de contrôle est importante tant opérationnellement que commercialement.

Un modèle d'escalade en lequel toute l'équipe a confiance

L'impact opérationnel de la validation dépasse la seule équipe de surveillance sécurité. La fonction de réponse aux incidents de Worldstream est composée d'experts senior issus de toute l'organisation, chacun apportant une expertise approfondie dans son domaine, disponibles en astreinte pour répondre aux résultats critiques.

Ce modèle ne fonctionne que si les résultats qui déclenchent une escalade méritent génuinement d'être traités.

Hadrian confirmant l'exploitabilité avant qu'un résultat n'atteigne l'équipe de surveillance, la décision d'escalader porte un niveau de confiance à la hauteur du standard que Worldstream s'impose. L'équipe de surveillance sait que ce qu'elle transmet a été testé et confirmé comme une exposition réelle et exploitable, et non un risque théorique. L'équipe de réponse aux incidents reçoit à son tour des résultats validés avec tout le contexte nécessaire pour agir immédiatement, sans réenquêter depuis le début. Chaque escalade est justifiée, chaque réponse est précise, et la relation entre les deux équipes est fondée sur le signal plutôt que sur le bruit. C'est cette dynamique qui permet à la fonction sécurité de Worldstream d'opérer à la vitesse et à l'échelle qu'exige son infrastructure.