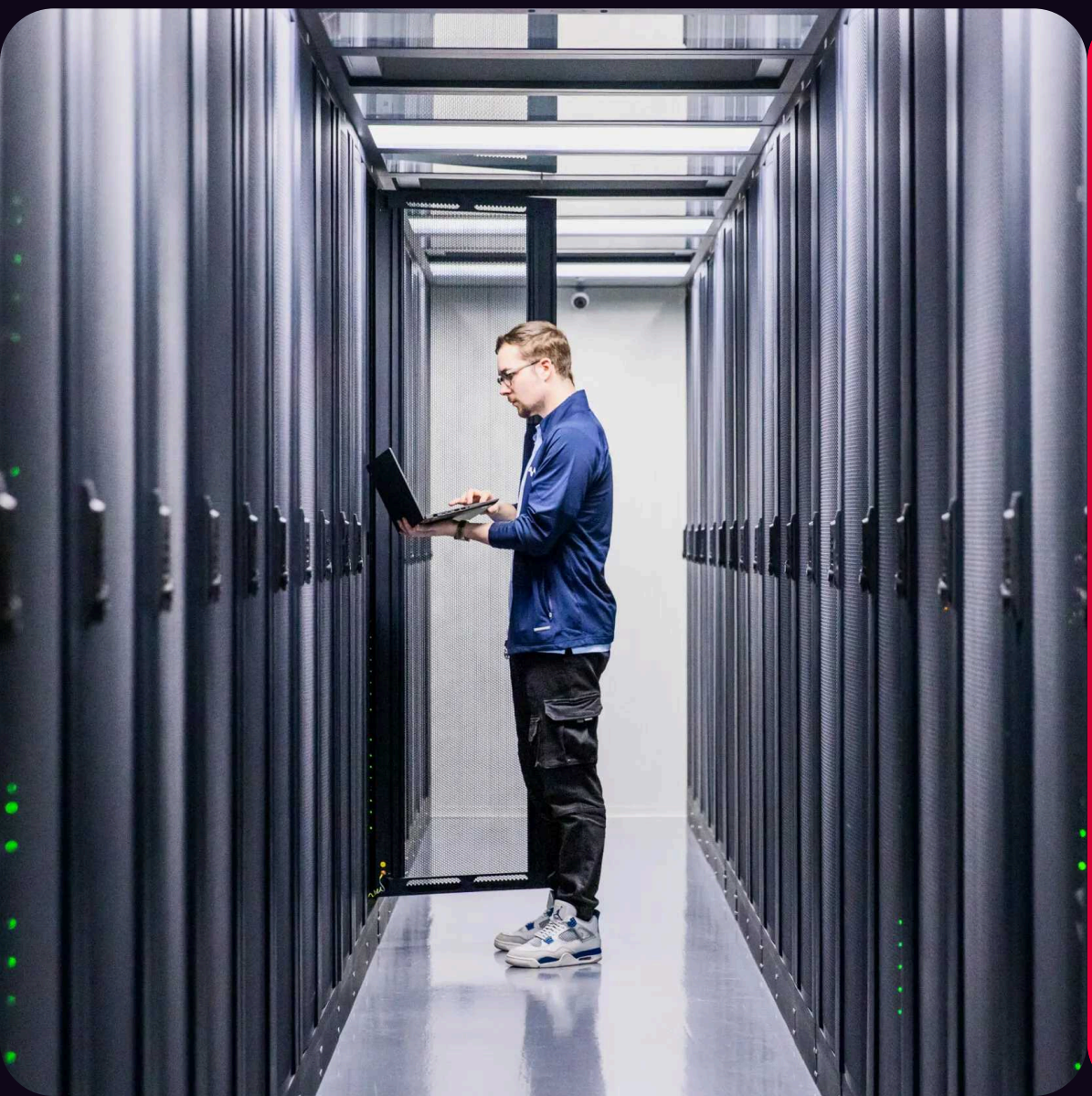
HADRIAN

WORLDSTREAM

FALLSTUDIE

Wie Worldstream das kontinuierliche Exposure-Management in einer kritischen Infrastrukturumgebung operationalisiert hat

IT-INFRASTRUKTUR, NIEDERLANDE

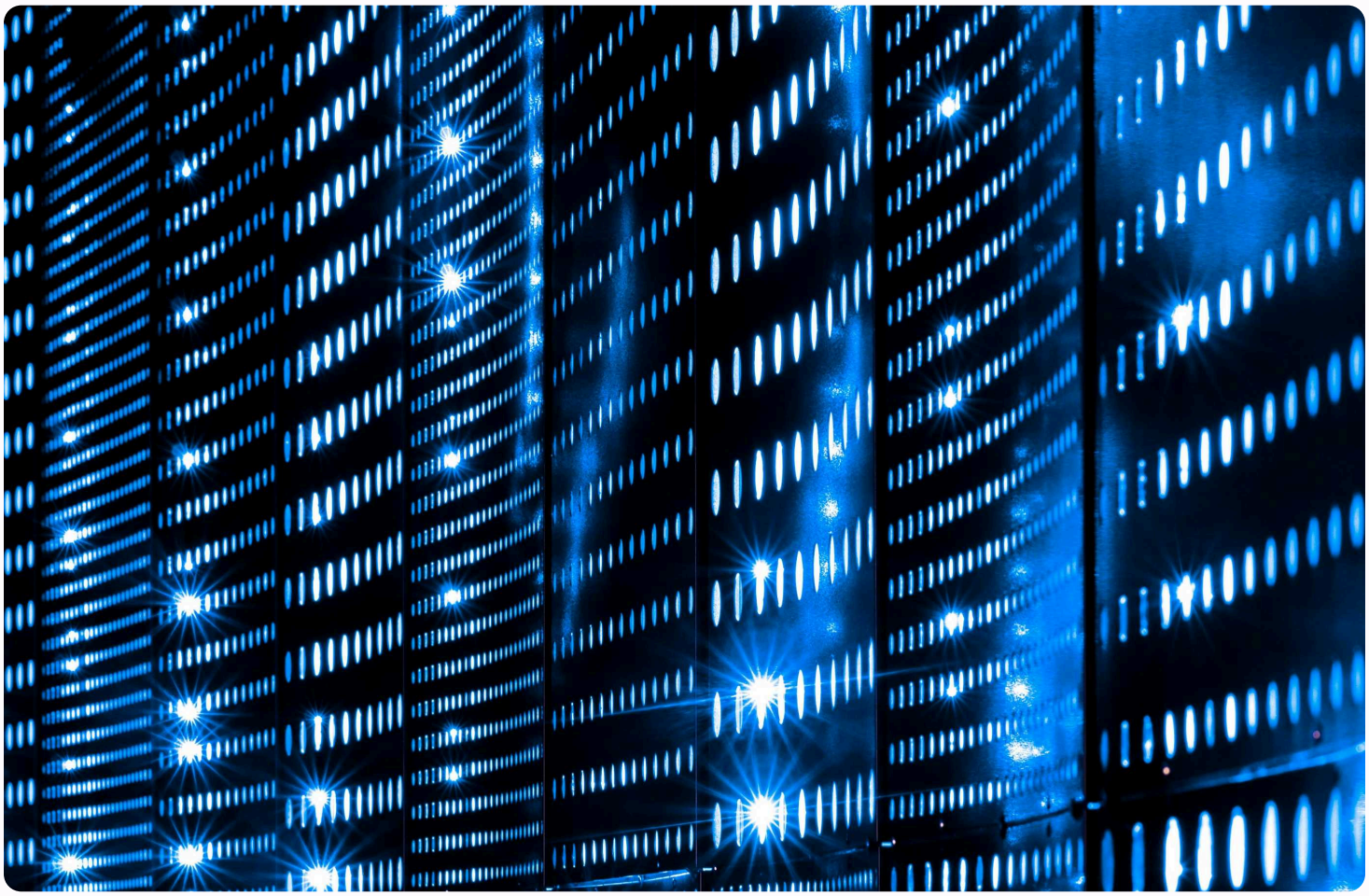


Über Worldstream

Worldstream ist ein niederländischer Cloud-Infrastrukturanbieter mit eigenen Rechenzentren und einem eigenen Netzwerk in Europa. Seit 2006 konzipieren, bauen und betreiben wir IT-Infrastruktur für Organisationen, die Kontrolle, Transparenz und Planbarkeit fordern.

Worldstream liefert dedizierte Server, Private Cloud und hybride Infrastrukturlösungen für geschäftskritische Workloads. Indem die gesamte Infrastrukturkette intern gehalten wird, von Rechenzentren und Netzwerk bis hin zu Hardware und 24/7-Support, bietet Worldstream Organisationen eine solide, transparente und planbare Grundlage für moderne IT-Umgebungen.

GEGRÜNDET	PHYSISCHE SERVER	KUNDEN
2006	15.000+	2.500+



Herausforderungen

01 **Kontinuierliche Kontrolle über eine sich verändernde Angriffsoberfläche**

Die Organisationen, die ihre Workloads bei Worldstream hosten, erwarten eine stabile und sichere Infrastruktur. Sicherheit ist ein zentraler Bestandteil des Mehrwerts, den das Unternehmen liefert, und die Aufrechterhaltung einer echtzeitfähigen, dauerhaften Sichtbarkeit über jeden extern exponierten Asset ist die Grundlage dieses Versprechens.

02 **Modernisierung vom Schwachstellenmanagement zur expositionsbasierten Priorisierung**

Das Team verwaltete einen großen, komplexen Bestand mit herkömmlichem Schwachstellenmanagement und priorisierte Findings nach CVSS-Scores.

03 **Sicherstellen, dass jede Eskalation gerechtfertigt ist**

Das Sicherheitsüberwachungsteam von Worldstream verfolgt die Angriffsoberfläche kontinuierlich, während ein interdisziplinäres Incident-Response-Team für kritische Findings bereitsteht. Das Ziel war es, sicherzustellen, dass nur bestätigte, tatsächlich ausnutzbare Findings eine Eskalation auslösen, damit Expertenkapazität genau dort eingesetzt wird, wo sie am meisten zählt.

Lösung

✓ **Kontinuierliche Außen-nach-innen-Sichtbarkeit über die Angriffsoberfläche**

Das Sicherheitsteam von Worldstream verfügt nun über eine Echtzeit- und kontinuierlich aktualisierte Ansicht seiner gesamten extern exponierten Infrastruktur, die mit Hadrian von außen nach innen kartiert wird. Neue Assets und Domains werden sofort erkannt, sobald sie auftauchen, sodass die Umgebung nie das übertrifft, was das Team sehen kann.

✓ **Expositionsbasierte Priorisierung ersetzt volumengetriebenes Schwachstellenmanagement**

Anstatt große Mengen von nach CVSS-Score eingestuften Findings zu bearbeiten, konzentriert sich das Sicherheitsteam von Worldstream nun auf eine kleinere Menge von Exposures, die als tatsächlich ausnutzbar in ihrer spezifischen Umgebung bestätigt wurden. Jedes Finding wird vor der Übergabe an das Team anhand realer Ausnutzbarkeit und Geschäftskontext geprüft, was eine lange Liste von Möglichkeiten in eine kurze Liste von Prioritäten verwandelt.

✓ **Validierte Findings, die jede Eskalation bedeutsam machen**

Bevor ein Finding das Sicherheitsüberwachungsteam erreicht, wird es als echtes, ausnutzbares Risiko bestätigt, nicht als theoretisches. Das gibt dem Team die Zuversicht, nur das zu eskalieren, was wirklich zählt, und dem Incident-Response-Team alles, was es benötigt, um sofort zu handeln, ohne von vorne recherchieren zu müssen. Jede Eskalation ist gerechtfertigt. Jede Reaktion ist präzise.

Ergebnis

Kontinuierliche Sichtbarkeit als Kundenversprechen

Für Worldstream ist die Sichtbarkeit der Angriffsoberfläche nicht nur ein internes Sicherheitsziel. Es ist Teil dessen, was Kunden kaufen, wenn sie sich entscheiden, ihre Workloads bei einem Anbieter kritischer Infrastruktur zu hosten. Organisationen, die Worldstream wählen, erwarten eine Infrastruktur, die kontinuierlich gesichert, überwacht und Herr ihrer eigenen Exposition ist. Das ist ein Versprechen, das regelmäßige Bewertungen und punktuelle Momentaufnahmen nicht halten können.

Das Sicherheitsteam von Worldstream erfasst nun jeden exponierten Asset in Echtzeit, während sich die Infrastruktur weiterentwickelt. Neue Domains, neue Dienste und Veränderungen in der Exposition werden im Moment ihres Auftretens erkannt, nicht bei der nächsten geplanten Überprüfung. Ob Wachstum durch neue Kundendeployments, erweiterte Dienste oder Netzwerkveränderungen entsteht, das Team sieht es sofort, und die Angriffsoberfläche driftet nie unbeobachtet. Diese Fähigkeit übersetzt sich direkt in die Sicherheit, die Worldstreams Kunden erwarten: dass die Infrastruktur, auf die sie sich verlassen, unter kontinuierlicher, aktiver Kontrolle steht und nicht nur planmäßig überprüft wird.

> **„ Mit Hadrian haben Sie einen wirklich starken Partner bei der Operationalisierung des kontinuierlichen Exposure-Managements in großem Maßstab. Der Aufwand für die Einrichtung ist gering, die Effizienz bei der Behebung von Findings und der Risikoreduktion verbessert sich, und das Tool ist wirklich einfach zu bedienen, skalierbar und wiederholbar."**
>
> Alan Lucas — CISO, Worldstream

Von der Bewertung zur validierten Ausnutzbarkeit

Das Sicherheitsteam von Worldstream arbeitet nun gegen eine kleinere, vertrauenswürdigere Menge bestätigter, ausnutzbarer Exposures, anstatt große Mengen von nach CVSS-Scores eingestuften Findings zu bearbeiten. Hadrian validiert jedes Finding gegen reale Ausnutzbarkeit und den spezifischen Kontext der Worldstream-Umgebung, bevor es angezeigt wird, sodass das Team auf das reagiert, was tatsächlich zählt, und nicht auf das, was ein Bewertungsmodell als möglicherweise relevant einstuft.

Ergebnis

Dieser Wandel verändert auch, wie das Sicherheitsprogramm gemessen und berichtet wird. Worldstream verfolgt seinen Sicherheits-Score über die gesamte externe Angriffsoberfläche, den Prozentsatz der Assets unter kontinuierlichem Scanning sowie die mittlere Zeit zur Identifizierung, Eindämmung, Beseitigung und Wiederherstellung, alles abgebildet auf das NIST Cybersecurity Framework. Diese Struktur läuft nun auf einer Live- und validierten Grundlage. Für einen Anbieter, der unter PCI DSS operiert, sich auf NIS2 vorbereitet und als IKT-Drittdienstleister unter DORA fungiert, ist dieser kontinuierliche Nachweis der Kontrolle sowohl operativ als auch kommerziell bedeutsam.

Ein Eskalationsmodell, dem das gesamte Team vertraut

Die operative Wirkung der Validierung geht über das Sicherheitsüberwachungsteam selbst hinaus. Die Incident-Response-Funktion von Worldstream besteht aus leitenden Experten aus der gesamten Organisation, die jeweils tiefes Fachwissen in ihrem Bereich einbringen und auf Abruf bereitstehen, um auf kritische Findings zu reagieren.

Dieses Modell funktioniert nur, wenn die Findings, die eine Eskalation auslösen, tatsächlich es wert sind, bearbeitet zu werden.

Da Hadrian die Ausnutzbarkeit bestätigt, bevor ein Finding das Überwachungsteam erreicht, trägt die Entscheidung zur Eskalation ein Vertrauensniveau, das dem Standard entspricht, den Worldstream an sich selbst anlegt. Das Überwachungsteam weiß, dass das Weitergegebene als echte, ausnutzbare Exposition getestet und bestätigt wurde, kein theoretisches Risiko. Das Incident-Response-Team erhält seinerseits validierte Findings mit dem vollständigen Kontext, der benötigt wird, um sofort zu handeln, ohne von vorne recherchieren zu müssen. Jede Eskalation ist gerechtfertigt, jede Reaktion ist präzise, und die Beziehung zwischen den beiden Teams basiert auf Signal statt auf Rauschen. Diese Dynamik ermöglicht es der Sicherheitsfunktion von Worldstream, mit der Geschwindigkeit und dem Maßstab zu operieren, die ihre Infrastruktur erfordert.