ExtraHop

CUSTOMER STORY

# Österreichs größter Stromerzeuger nutzt ExtraHop Reveal(x) als Baustein für sein Security Operations Center (SOC)

Echtzeit-Transparenz und Bedrohungserkennung über den gesamten Netzwerkverkehr, einschließlich verschlüsseltem Verkehr

Nahtlose Integration mit zentralen ITSM-Anwendungen, optimierte Bedrohungserkennung und Reaktionsaktivitäten

Einfach zu bedienende Oberfläche ohne die Notwendigkeit einer Systemschulung ermöglichte eine schnelle Akzeptanz in Sicherheits- und Betriebsteams


**Executive Summary**

VERBUND ist Österreichs führender Energieversorger und einer der größten Erzeuger von Wasserkraft in Europa. Nach einer Überprüfung seiner Cybersicherheitsprozesse entschied sich VERBUND für ExtraHop Reveal(x), um den Netzwerkverkehr in Echtzeit zu überwachen, Anomalien zu erkennen und die Ergebnisse an das zentrale Security Operation Center weiterzuleiten. Im täglichen Einsatz verbesserte Reveal(x) deutlich die Fähigkeit, Sicherheitsprobleme aufzuspüren und schneller und präziser zu reagieren, was das InfoSec-Team von VERBUND als "beispiellose" Transparenz innerhalb eines hochintegrierten Workflows beschreibt.


## THE BEGINNING

### Providing Critical Utilities

VERBUND ist Österreichs größter Stromerzeuger und betreibt kritische Infrastrukturanlagen, die rund 40 Prozent der Stromerzeugung des Landes abdecken. Als solches nimmt das Unternehmen Cybersecurity sehr ernst und hat erheblich in technische Schulungen, Systeme und Know-how investiert, um seine Unternehmensanwendungen und IT-Infrastruktur sowie seine Betriebstechnik (OT) zu schützen.

Traditionell hat sich VERBUND darauf verlassen, dass die einzelnen Abteilungen die Sicherheit in ihren jeweiligen Bereichen und operativen Rollen entwickeln, implementieren und verwalten. Nach einer strategischen Überprüfung der Cybersicherheit im Jahr 2018 beschloss die Geschäftsleitung jedoch, die Sicherheitsfunktionen in einem zentraleren Security Operations Centre (SOC) zu konsolidieren. Als Teil dieses Prozesses evaluierte VERBUND mehrere Network Detection and Response (NDR)-Plattformen auf der Suche nach der Lösung, die eine sehr relevante Komponente des neuen SOC bilden würde.

> “ExtraHop gibt uns eine ganzheitliche Sicht auf jede Situation und die Möglichkeit zu verstehen, wie sich jedes Ereignis auf alle angeschlossenen Systeme auswirkt. Das ist ein großer Vorteil für uns.

FLORIAN-SEBASTIAN PRACK, PROJEKTLEITER SOC UND OT SECURITY SPECIALIST BEI VERBUND

## THE TRANSFORMATION

### Getting Fast, Actionable Insights

Das Extrahop-Toolset ist eine Komponente für den Aufbau des neuen SOC. VERBUND evaluierte Reveal(x) neben anderen bekannten NDR-Anbietern im Rahmen eines achtwöchigen Proof of Concept. "Es hat uns wirklich die Augen geöffnet, was alles möglich ist, und uns ein gutes Verständnis für die Funktionsweise der einzelnen Lösungen vermittelt", sagt Florian-Sebastian Prack.

ExtraHop erwies sich in einer Reihe von Bereichen als überlegen, vor allem in Bezug auf seine Kernfunktionen. "Einige der anderen Systeme verlassen sich nur auf Metadaten und umfangreiche Schulungen, während ExtraHop in der Lage ist, schnell Einblicke zu geben und dann einen einfachen Drilldown zu ermöglichen, um spezifische Elemente zu finden, die die anderen Systeme einfach nicht aufdecken konnten. Es bietet auch Einblick in den SSL/TLS 1.3-verschlüsselten Datenverkehr, ohne den Datenschutz zu gefährden - ein wichtiges Anliegen von VERBUND.

VERBUND fand auch heraus, dass sich Reveal(x) leicht mit seinen bestehenden Systemen und Arbeitsabläufen kombinieren lässt. Das Sicherheitsteam hat Reveal(x) in sein SIEM und sein Atlassian Jira ITSM integriert, um eine prozessgesteuerte Methode für die Analyse von Warnmeldungen und die Verwaltung von Reaktionen bereitzustellen.

## THE OUTCOMES

### Strong Tools Enable Confident Security Operations

Obwohl die Entwicklung und Organisation der Teams für das neue SOC noch nicht abgeschlossen ist, nutzt VERBUND bereits ExtraHop, um Sicherheitsvorfälle schneller zu erkennen und darauf zu reagieren.

In einem Beispiel identifizierte ExtraHop automatisch eine Entwicklungsumgebung, die mit einem ungesicherten Server außerhalb des geschützten Netzwerks verbunden war.

Reveal(x) hat auch zuvor unentdeckte Anomalien innerhalb des Netzwerks und der Anwendungsdatenströme aufgedeckt. Viele dieser Probleme auf der Anwendungsebene waren vorher nur schwer zu erkennen.

Diese umfassende Transparenz hat die Genauigkeit der Erkennung von Bedrohungen und die Geschwindigkeit der Reaktionszeiten drastisch verbessert.

Die Entwicklung des SOC schreitet zügig voran, und VERBUND ist von dem Wert, den ExtraHop Reveal(x) liefert, überzeugt. Sie sind jetzt dabei, mehr Mitarbeiter zu schulen und ExtraHop täglich zu nutzen. Außerdem werden Dashboards, zusätzliche Skripte und die Integration von ExtraHop als Kernbestandteil des Sicherheits- und IT-Supports in der gesamten Organisation geprüft.

FIND MORE EXTRAHOP CUSTOMER STORIES AT **EXTRAHOP.COM/CUSTOMERS/STORIES**

### ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business. Learn more at www.extrahop.com.



ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101