CUSTOMER STORY

Austria’s Largest Power Producer uses ExtraHop Reveal(x) as a building block for its Security Operations Center (SOC)

Real-time visibility and threat detection across all network traffic, including encrypted traffic

Seamless integration with core ITSM applications, streamlined threat detection, and response activities

Easy-to-use interface without the need for system training allowed rapid adoption across security and operational teams

Executive Summary

VERBUND is Austria’s leading utility and one of the largest producers of hydro power in Europe. Following a review of its cybersecurity processes, VERBUND selected ExtraHop Reveal(x) to help monitor network traffic in real time, detect anomalies, and feed the results into the central Security Operation Center. In day-to-day usage, Reveal(x) significantly improved the ability to track down security issues and respond more quickly with greater precision, giving what VERBUND’s InfoSec-team described as “unprecedented” visibility within a highly integrated workflow.

> “
>
> ExtraHop gives us a holistic view of any situation and the ability to understand how each event impacts all the connected systems. This is a major advantage for us.
>
> **Florian-Sebastian Prack,**
> **Project Manager SOC and OT**
> **Security Specialist at VERBUND**

THE BEGINNING

Providing Critical Utilities

VERBUND is Austria's largest electricity producer and operates critical infrastructure assets, covering approximately 40%of the country’s electricity generation. As such, the company takes cybersecurity extremely seriously and has invested significantly in technical training, systems, and expertise to protect its enterprise applications, IT-infrastructure, and its operational technology (OT).

Traditionally, VERBUND has relied on individual departments to design, implement, and manage security within their respective domains and operational roles. However, following a cybersecurity strategic review in 2018, senior management decided to consolidate security functions into a more centralised Security Operations Centre (SOC). As part of this process, VERBUND evaluated several network detection and response (NDR) platforms in search of the solution that would form one very relevant component of its new SOC.

THE TRANSFORMATION

Getting Fast, Actionable Insights

The Extrahop toolset is one component to help build up the new SOC. VERBUND evaluated Reveal(x) alongside other well-known NDR vendors as part of an eight-week proof of concept. "It really opened our eyes to what is possible and gave us a good understanding of how each solution worked," said Florian-Sebastian Prack.

ExtraHop proved itself superior in a number of areas, especially in terms of its core capabilities. "Some of the other systems rely just on metadata and extensive training, whereas ExtraHop is able to quickly give insights and then allow to easily drill down to find specific items that the other systems were simply unable to uncover. It also gives visibility into SSL/TLS 1.3-encrypted traffic without compromising data privacy—a major consideration of VERBUND.

VERBUND also found that Reveal(x) easily paired with its existing systems and workflows. The security team has integrated Reveal(x) with its SIEM and its Atlassian Jira ITSM to provide a process-driven method of analysing alerts and managing responses.

THE OUTCOME

Strong Tools Enable Confident Security Operations

Although the development and organisation of teams for the new SOC is ongoing, VERBUND already uses ExtraHop to more quickly detect and respond to security incidents.

In one example, ExtraHop automatically identified a development environment linked to an unsecured server outside its protected network.

Reveal(x) has also detected previously undiscovered anomalies within the network and application data flows. Many of these application-layer issues were hard to spot before.

This comprehensive visibility has dramatically improved the accuracy of threat detections and speed of response times.

Development of the SOC is progressing rapidly, and VERBUND is confident about the value ExtraHop Reveal(x) delivers. They are now in the process of getting more people trained and using ExtraHop on a daily basis. They are also looking at creating dashboards, additional scripts, and integration of ExtraHop as a core part of both security and IT support across the entire organisation.

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