ExtraHop

CUSTOMER STORY

Major European Power Producer Builds Its Security Operations Centre Around ExtraHop Reveal(x)

Complete, real-time visibility and threat detection, including encrypted traffic

Seamless integration with core ITSM applications

Easy-to-use interface allows for rapid adoption across teams

Executive Summary

Following a review of its cybersecurity processes, one of Europe's largest electric providers selected ExtraHop Reveal(x) to help consolidate disparate security controls around a new centralised Security Operations Centre. In day-to-day usage, Reveal(x) significantly improved their ability to track down security issues and respond more quickly with greater precision, giving what the InfoSec team described as "unprecedented" visibility within a highly integrated workflow.

THE BEGINNING

Providing Critical Utilities

As a major provider of electricity in Central Europe, this large power producer takes cybersecurity extremely seriously. In recent years, it has invested significantly in technical training, systems, and expertise to protect its operational technology (OT), as well as its enterprise applications and infrastructure.

The power company traditionally relied on individual departments to design, implement, and manage security within their respective operational roles. However, following a penetration testing exercise and cybersecurity strategic review in 2018, senior management realised they needed to consolidate security functions into a more centralised Security Operations Centre (SOC). As part of this process, the power company evaluated several network detection and response (NDR) platforms in search of the solution that would form the heart of its new SOC strategy.

> "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.

OT SECURITY SPECIALIST FOR CENTRAL EUROPE'S LEADING ELECTRICITY COMPANY

THE TRANSFORMATION

Getting Fast, Actionable Insights

To help them build out their new SOC, the power company evaluated Reveal(x) alongside three other well-known NDR vendors, including a provider based in Europe, as part of an eight-week proof of concept.
"It really opened our eyes to what was possible and gave us a good understanding of how each solution worked," said, an OT security specialist for the power company.

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

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

THE OUTCOMES

Strong Tools Enable Confident Security Operations

Although the development and reorganisation of teams into the new SOC is ongoing, the power company 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 of its protected network. "This is the type of security issue that is very difficult to detect without knowing what you're looking for and, without Reveal(x), would have required many time-consuming manual processes," he said.

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 and the level of visibility we have now gained is unprecedented," he said.

This comprehensive visibility has dramatically improved the accuracy of threat detections and speed of response times. "Instead of having to pour over logs, 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," he explained.

Development of the SOC is progressing rapidly, but even at this stage he is confident about the value ExtraHop Reveal(x) delivers. "We are now in the process of getting more people trained and using ExtraHop on a daily basis," he said, "We 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**

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101