CASE STUDY

HOW THE STADTWERKE KLAGENFURT GROUP REDUCES RISK TO CRITICAL INFRASTRUCTURE

OVERVIEW

The Stadtwerke Klagenfurt Group delivers essential municipal services, including electricity, gas, heat, and water, across Klagenfurt, Austria.

Challenge

Advanced threat actors are launching targeted attacks to disrupt critical infrastructure that delivers vital services to citizens around the world. These evolving cyber risks — coupled with increasing regulatory requirements — are driving many industrial companies to bolster cybersecurity programs. In fact, of those companies, 77% say improving security is a major organizational priority.

As the information security lead across the entire organization, The Stadtwerke Klagenfurt Group's CISO Rene Schmid is focused on meeting the EU NIS directive for operators of critical infrastructure. He is simultaneously preparing for ISO 27001 and NIS certification to demonstrate strong data protection practices.

Schmid's team relied on a mix of security systems, including domain name (DNS), intrusion prevention (IPS), firewalls, central logging, and a SIEM to track security events and threats targeting the organization. However, without a centralized way to view and understand all of the alerts coming from these disparate sources — plus a near-constant barrage of false positives — the team struggled to move quickly.

"We needed a way to correlate these data sources, prioritize events, and shorten our reaction time for detecting and fending off attacks — all while maximizing internal resources and meeting compliance requirements," says Schmid.

The team's greatest challenge was gathering intelligence on external threats targeting the organization in an efficient manner. For example, without the ability to rank specific IP addresses based on risk and understand known threats, manual internal investigations were laborious, taking the Schmid and his team members away from important tasks.

Solution

He recalls, "I was introduced to Recorded Future in 2019 and was very impressed by their unique thinking and approach."

Recorded Future's dark web monitoring and analysis capabilities and unprecedented real-time insights on leaked data and credentials across the internet sealed the deal for The Stadtwerke Klagenfurt Group. "There was no comparable service," Schmid says. "We knew Recorded Future would increase the security awareness of our colleagues enormously."

Leveraging Express — Recorded Future's browser extension — the team began integrating elite security intelligence with their internal security monitoring infrastructure. This enabled them to instantly prioritize alerts, incidents, and vulnerabilities based on real-time risk scores from the world's most advanced security intelligence platform.

> "Every six months, I present a risk report to the IT manager and our board of directors. Recorded Future is always mentioned as our main security intelligence system."
>
> *-Rene Schmid, CISO, The Stadtwerke Klagenfurt Group*

Says Schmid, "Recorded Future helps us to decide very quickly whether to take further action. Through the risk assessment of IP addresses and additional information about addresses in the same address range, we can rapidly decide whether to block a whole range of addresses or individual addresses — or not take action at all."

Additionally, Recorded Future's URL and file sandboxing capabilities empower the team to catch suspicious attachments before they're released to internal users, disrupting attacks before they begin.

Real-time, actionable context from the world's largest commercial collection platform was particularly welcome when the COVID-19 pandemic upended business as usual. As adversaries scaled their attacks, the team leaned heavily on Recorded Future's up-to-the-minute alerts based on aggregated data from the broadest range and variety of sources. Custom queries enabled them to actively monitor their tech stack and gain instant context around newly disclosed vulnerabilities and threats targeting their remote workforce.

Results

With elite security intelligence at their fingertips, The Stadtwerke Klagenfurt Group's security team has gained the context they need to accelerate IOC investigation and triage, reduce uncertainty, and make fast, confident decisions to protect the organization and meet compliance requirements.

This speed has translated to real cost savings. The CISO notes, "The time savings with Recorded Future is huge." He estimates that he personally saves two hours per day on manual security intelligence activities — approximately 540 hours per year — at a cost savings of roughly 40,000 EUR (about 47,000 USD).

Elite security intelligence also makes it easy to share insights with key stakeholders. Says the CISO, "Every six months, I present a risk report to the IT manager and our board of directors. Recorded Future is always mentioned as our main security intelligence system." By enriching each audience's cybersecurity knowledge, security intelligence has aligned everybody in the organization on the same page.

He concludes, "I am very satisfied with the performance and service of Recorded Future and its staff. All around I have a better feeling as CISO now."