Trellix

Multi-Utility Provider Defends Communities' Health and Safety

Corix enhances security posture with Trellix Security Suite

CORIX®

Corix is a multi-utility provider that harnesses economies of scale to ensure the communities it supports have reliable access to safe, affordable and sustainable services. The company is responsible for the public and environmental health of one million customers, a vote of public trust that Corix considers one of its most valuable assets. CIO Carol Vorster emphasized, "Everything we do is inspired by our purpose 'to help people enjoy a better life and enable their communities to thrive'. We differentiate ourselves from traditional utility service providers through our broad expertise in water, wastewater, and energy utilities, and our ability to use that expertise to structure tailored solutions for our customers."

Corix works to ensure its utility infrastructure solutions function harmoniously with the surrounding environment and that its communities have continuous access to basic life necessities such as clean drinking water and proper sanitation. The company also stewards significant volumes of customer data, including information about individual consumers as well as the data entrusted to it by municipalities and military installations.

The utility provider's IT and OT environments were previously safeguarded by multiple security products sourced through different vendors but the disparate tools impeded visibility across Corix's infrastructure. Investigating alerts became an arduous task of tracing these alerts across disparate system logs. When a cyber attack swept the globe in late 2016, Corix's IT team had to work through the weekend to coordinate security patches from each vendor to defend against the vulnerability.

Vorster recounted, "**It became very apparent how incredibly difficult it would be for our small team to respond to a major incident at Corix.** We have a profound commitment to the people and the communities we serve. Preventing an attacker from exploiting plant operations to instigate an environment-harming spill or contaminate drinking water is paramount."

Cost Savings Plus a Managed Service Bonus

To improve the security team's ability to quickly identify and remediate high-risk threats, Corix set out to reinvigorate its security posture. The goal was to improve visibility across the company's environment, augment the team's daily working capacity and reduce complexity in the security technology stack.

Vorster explained, "We wanted a strategic partnership with a single provider that offered an end-to-end solution and a managed detection and response (MDR) service. Our team needed a more efficient way to manage alerts and analyze threats and their potential movement through the environment quickly and efficiently."

Corix's search for a strategic cyber security partner ended with Trellix. Around-the-clock support from Mandiant Managed Defense, which ensures continuous monitoring of the company's network, offered a sustainable shared services model. Corix was able to replace all the functionality provided by the eight different security vendors in its environment with a cohesive suite of solutions from Trellix.

Vorster highlighted, "**Deploying Trellix was more cost-effective than paying for the eight separate, independent security products we had deployed at the time.** Plus, we added a managed service component on top of the technologies, further enriching the new capabilities and visibility established across the environment and providing for full 24x7 visibility. This was important as Corix's operations span five time zones."

Trellix Endpoint Security, Trellix Network Security and Trellix Email Security—Cloud Edition proactively exchange intelligence to fortify defenses along all threat vectors from the core to perimeter. Trellix Helix centralizes the collection of security data and management of the infrastructure, facilitating informed and efficient detection and analysis of threats. Corix also feeds firewall logs from its plants' SCADA systems through Helix to provide real-time visibility into its OT infrastructure.

An Operational Partnership and Extension of the Team

To improve the quality-of-service delivery to constituents, Corix has embarked on a company-wide transformation project to consolidate IT operations under a shared services model. The initiative will align core business processes across corporate offices and includes plans for an enterprise security program.

To build a rigorous program and assure the safety of the communities it serves, Corix conducted a Mandiant Security Program Assessment of its infrastructure. Mandiant experts delivered a comprehensive three-year plan to improve the maturity of the utility provider's overall security posture. Vorster and her team have progressed to the second year of initiatives but continue to collaborate with Mandiant Managed Defense analysts on an ongoing basis to implement the projects and additional capabilities and improve the maturity of their security program as needed.

Vorster enthused, "The Mandiant team meets regularly with our security group to discuss the most recent events in our environment, cyber security trends in the utility industry and ideas for fortifying our defenses. The operational partnership and extension of our team are really important to us."

She continued, "The support from highly trained security experts to scrutinize incidents and contextualize our security efforts with global trends is extremely valuable. Having frontline insights on major attackers and threats brings me great peace of mind."

112022-14