Intertec for Cybersecurity Solutions

Real-Time Attack Surface Management for a Major Energy & Utilities Provider

Industry: Energy & Utilities
Company Size: 10,000+ employees

Business Problem

The client faced growing cybersecurity risks due to insufficient visibility into external-facing assets. Manual identification and assessment of domains, IPs, applications, and databases were time-consuming and costly, leaving them exposed to vulnerabilities and unable to effectively manage security risks.

How Intertec Helped

Through a combination of **Automated Red Teaming** and **Continuous Attack Surface Management (ASM)**, we conducted a passive reconnaissance exercise on the client's primary domain and associated subdomains. This process mapped the organization's entire digital footprint as perceived by potential external attackers, identifying assets exposed to the public.

The goal was to provide a clear, comprehensive view of the attack surface and help pinpoint security vulnerabilities. The platform reliably delivered accurate, actionable insights, enabling the client's IT security team to quickly address these risks and strengthen their defensive posture.

Business Outcomes Delivered

- Continuous internet-wide monitoring now provides the client with real-time visibility into all digital assets exposed online—capabilities they previously did not have.
- Significant security risks, including previously unidentified domains and subdomains, have been discovered and added to the client's asset inventory, improving asset management.
- A unified dashboard enables streamlined management of vulnerabilities, hazardous open ports, and associated threats, centralizing oversight for the IT team.
- The IT team has been empowered to proactively minimize their attack surface, significantly strengthening their overall security posture.