With collaborations comes a program

Deloitte collaborated with a client, working deeply within its culture to build an Operational Technology (OT) Cybersecurity Program that met its needs.

The issue

A leading supplier of chemicals and other materials to semiconductor manufacturers had recently acquired a similar supplier making them the global leader in electronic materials. At the same time, the company was expanding its footprint around the globe with the construction of a new, massive manufacturing facility.

With the world still reeling from the pandemic's supply chain issues, public recognition of the semiconductor industry as a critical infrastructure sector was elevated given the impact it had on the pandemic-related supply chain issues. A bill passed by Congress in 2022 to boost the manufacturing of semiconductor chips in the United States meant a potential boom in US business if the client could get its security processes where they needed to be. The client was under pressure to assure its customers who had questions about the actions the company was taking to secure their manufacturing OT environment and the maturity of their OT cybersecurity program. The client acknowledged they had a lack of standardized policies and standards for OT cybersecurity to help guide and secure their many production sites. Additionally, the client was concerned about the potential impact from a cybersecurity incident to unplanned production downtime, impact to quality and its negative impact to reputation, and loss of competitive edge. It needed to build a strong foundation for its cybersecurity program by developing core policies and standards for the sites to follow while demonstrating the maturity of their cybersecurity program.

The client searched for a professional services organization with demonstrated knowledge of specific OT cybersecurity standards such as IEC 62443 and experience aiding global energy and chemical companies with the development of their OT cybersecurity programs. Deloitte was a match—and there was the added benefit that Deloitte hadassistedthe client on their recent merger and acquisition deal, IT security assessments, and policy development.

The solution

To get things started, the Deloitte team introduced its OT Governance Framework model and Top 20 OT Cybersecurity Practices—both solutions that are standard offerings for Deloitte's OT Cyber practice and accepted in the industry.

The team followed this by creating and facilitating a series of workshops with the client's stakeholders, collaborating with the client's leadership to create policies and standards aligned with engineering, maintenance, and operations practices at their production sites.

The technical workshops covered topics such as vulnerability and risk management, management of change, secure remote access, contractor access management, and supplier risk management. The live, facilitated workshops allowed the team to review real-time data, obtain quality feedback, pivot when necessary, and tailor the program to align with their business objectives.

With the teamwork and camaraderie that came from the completion of the workshops, the client was able to establish buy-in from its employees and the policies and standards have been embraced by key stakeholders. Establishing rapport with the client allowed Deloitte to become a trusted advisor.

The impact

The client has enhanced its knowledge and awareness of OT cybersecurity while revealing gaps within their infrastructure. They developed and implemented an approach using the newly produced policies and standards to apply and replicate through the organization to help with management of change functions. Finally, the client now feels confident about continuing to expand, knowing that they can scale and replicate their new OT architectural plans, protection technologies, policies, and standards.

Deloitte differentiators

The Deloitte team worked within the client's culture in intense workshops, collaborating with client stakeholders so they could develop the policies and standards that were right for them. That collaboration demonstrated that Deloitte was a reputable advisor, not just a vendor. Throughout the entire sales process, Deloitte demonstrated strong knowledge of OT cybersecurity. Deloitte was able to provide a standard solution and then tailor it to meet the client's needs.

Learn more from these additional resources

Cyber-physical security (CPS) solutions for Internet of Things (IoT) and Operational Technology (OT) products, systems, and ecosystems (deloitte.com)

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for suchprofessional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for anyloss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com /us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rulesand regulations of public accounting.