Industrial Control Systems (ICS) are cyber-physical systems that allow operators to monitor and control complex industrial processes. However, ICS and Critical Infrastructure are often targeted by malicious actors. At least 33% of ICS organizations are at high or critical risk of allowing attackers to gain control of target systems, potentially harm or compromise systems, or cause disruption of services (Kapellmann & Washburn, 2018).

ICS operators face numerous challenges, especially information overload, reliance on disparate information sources, and a lack of aggregated, consumable, and intuitive ways to gain insights on ICS vulnerabilities and risks to protect their assets.

In a recent study conducted by FireEye, ICS operators reported having to rely on a variety of different sources to stay current and 46% of them were dissatisfied with the data format, availability, and quality of information, citing these as barriers to effectively doing their jobs (Kapellmann & Washburn, 2018).

For his new client, Ryan can view all assets, help his client conduct vulnerability assessments, and prioritize risks.

Ryan can also alert all his clients in a timely fashion of a new vulnerability that might affect their operations.