

## ABOUT US

As a female-owned, Indigenous-led company and certified member of the CCIB, our approach is rooted in understanding deep connections—to the land and the businesses we serve. We provide thoughtful, sustainable insight and guidance, cutting through vendor noise to design solutions that genuinely fit your needs and deliver long-term value. We focus on building the right solution for you, starting with your requirements, not a product.

## OUR MISSION

*To build trust in cybersecurity by serving as the independent consultant, connecting clients with the right partners and tailored solutions for their business*

**YOUR CYBER  
MATCHMAKER**

## Key Insight

SANS Institute - 2024 State of ICS/OT Cybersecurity:  
Only 56% of respondents had an ICS/OT-specific Incident Response plan.



## Overview

Operational Technology (OT) systems are the core hardware and software that monitor and control physical industrial processes, making them essential for the safety and reliability. While historically isolated, the convergence of OT with IT has exposed these critical systems to a complex, evolving cyber threat landscape. This exposure necessitates specialized security measures to prevent operational downtime and significant physical risks.

## OT Assessment

An Assessment is crucial for establishing and validating a truly defensible cyber posture. This involves a deep review of enhancement paths for the current OT network design and its integration with security controls. Compliance alone is insufficient, and security efforts must focus on the actual measurable performance testing of implemented controls. Our partners review architecture to ensure effective network zoning, segmentation, and alignment with critical standards like the Purdue Model, moving beyond paper compliance to achieve real-world security.

## Asset / Inventory

Understanding the current operational environment begins with a thorough, passive Visibility/Inventory Assessment. This process identifies all assets, including their types, roles, and the different industrial environments and equipment. Following inventory, a passive Vulnerability Assessment

and Insights review identifies anomalies, known vulnerabilities, misconfigurations, and best practices for assets and communications. The assessment also includes a passive Threat Assessment to identify possible threat actor activities and malware targeting the specific industrial environment.

## Byson-X by CyVault

BYSON X is a proprietary industrial security solution from Cyvault, designed to discover and protect assets within critical infrastructure environments. This proven technology has already been implemented by global leaders across the energy sector to secure their operational assets.

## Contact HillCyde

Ready to secure your Operational Technology environment with the industry's best expertise? The most critical step is partnering with a firm that understands your unique industrial needs and can deliver tailored, world-class solutions. HillCyde Cyber Matchmaker cuts through vendor noise to connect your organization-whether SMB or Enterprise -with the right partners to build a lasting, defensible security program. Reach out to us today to start the conversation.

Contact HillCyde at [sales@hillcyde.com](mailto:sales@hillcyde.com) to find your match.