CASE STUDY

Boliden, Sweden, chooses ABB for cyber support

ABB Ability™ Cyber Security Fingerprint makes risk manageable

Cyber threats to industrial control systems are on the rise. That is why the operations managers at Boliden, a Swedish maker of high-tech metals that operates mines and smelters, decided to harden their existing cyber security defenses using ABB Cyber Security Fingerprint, a non-invasive diagnostic and gap analysis service that generates recommendations that improve cybersecurity protections for industrial control systems (ICSs).

—
01 The mining industry is tackling cyber threats head on.

When Boliden's managers learned ABB offered a Cyber Security Fingerprint service customized for the ABB 800xA control system, they immediately asked ABB for help. Their objective was simple: to reduce the risks of malware and unauthorized access that could endanger their people, plants, production, or data by validating existing security policies and identifying areas for improvement.

Customer challenge

Supplement existing cyber security program by:

- Obtaining a qualified, third-party review of existing security strengths and weaknesses;
- Validating existing policies, procedures, and protections as up to date and in line with best practices;
- Identifying and prioritize areas of protection and improvement; and
- Increasing Boliden personnel's knowledge of cyber security best practices.

ABB solution

Fingerprint employs a multi-layer approach to improve security. The Fingerprint process not only collects data from over 100 critical points in the ICS but ABB engineers and cyber security experts conduct in-depth interviews with plant personnel to understand how policies and procedures are implemented and followed day-to-day. A proprietary software-based tool then analyzes the findings and compares them with industry standards and best practices.

Fingerprint not only identifies potential threat vectors outside attacks can use to infiltrate the ICS, it also identifies ways to protect against "insider threats" – security breaches caused by company personnel who carelessly or maliciously spread malware by downloading viruses or from using infected USB peripherals.

—
02 ABB trained Boliden employees on methods to mitigate risks.

Results

Like many of our customers, Boliden was on top of their game. The plant received confirmation that its ICS protection was effective. But ABB also identified areas where protection could be strengthened. ABB explained all the ways their defenses could be breached, including new tactics used by hackers such as zero-day and advanced persistent threats (APTs). This helped to advance Boliden personnel's knowledge of the true nature of the cyber threats they were facing. ABB also trained Boliden personnel on new methods to mitigate these threats.

The open and forthright conversations sparked by the Fingerprint audit between plant managers, staff, and ABB proved to be a significant bonus for plant managers, as well. Plant managers repeatedly emphasized how constructive and productive these interactions were to gaining insights into a highly-complex and ever-evolving challenge. But this knowledge transfer is just part of the ABB culture and Fingerprint service. Our experts routinely answer questions and freely share their experience and advice.

These results provided Boliden with greater confidence in its ability to prevent cyber security attacks. Boliden now plans to conduct Fingerprint audits at additional facilities.

Customer benefits

- Greater confidence in the plant's current program to minimize cyber security risks;
- Customized, detailed action plan that identified and prioritized additional threat mitigation actions;
- Improved understanding of cyber security threats landscape following in-depth dialog with ABB cyber security experts and engineers; and
- Increased knowledge of proactive ways to prevent future cyber security incidents.

—
02

—
ABB Ltd.
579 Executive Campus Drive
Westerville, OH 43082
Phone: +1 800 435 7365

abb.com/cybersecurity

9AKK106321