CASE STUDY

Boliden, Sweden, continues to implement ABB cyber security solutions

ABB Ability™ Cyber Security Fingerprint makes risk manageable

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

Increasing cyber threats to industrial control systems pursued the operations managers at Boliden, a Swedish maker of high-tech metals that operates miners and smelters, to continue using ABB Ability™ Cyber Security Fingerprint for the third consecutive year. It is a non-invasive diagnostic and gap analysis service that generates recommendations and improves cyber security protections for industrial control systems (ICSs).

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:
- Building on 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 since the time we started supporting them with our cyber security solutions. The plant received confirmation that its ICS protection was effective. Earlier, ABB identified areas where protection could be strengthened while making them aware of how their defenses could be breached, including new tactics used by hackers such as zero-day and advanced persistent threats (APTs). 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 us to advance Boliden personnel's knowledge of the true nature of the cyber threats they were facing.

As part of the annual ABB Ability^{TM} Cyber Security Fingerprint implementation process, all systems at the ABB installed base have been upgraded to 800xA 6.x. ABB's Cyber Security systematic activities for Boliden have been planned and documented for the OT environment for the whole year. This gives the customer significant leverage to build it's resilience against both external and internal threats.

—
02

Open and clear conversation between ABB, Boliden's plant managers and the staff led to the successful execution of the Cyber Security Fingerprint while gaining insights into a highly complex and ever-evolving security atmosphere. Knowledge transfer being an integral part of ABB's culture, 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;
- Plan for future cyber activities based on evidence and validate the result
- Improved understanding of cyber security threats following in-depth dialog with ABB cyber security experts.

—
ABB
Operating in more than 100 countries

abb.com/cybersecurity