CASE STUDY

Stupp Corporation Reduces Cyber Risk With Full Visibility Into Its Industrial Control Network

> *Tenable.ot is far ahead of anybody that I reviewed in the control security space. The company understands controls... why did that change happen? Who made that change? We now have that power.*

JOHN ROOSA
Chief Information Officer

ORGANIZATION SNAPSHOT

ORGANIZATION
Stupp Corporation

YEAR JOHANN STUPP STARTED HIS IRONWORKS BUSINESS
1856

INDUSTRY
Manufacturing

CHALLENGES

- Protecting industrial control systems (ICS) from cyberattacks
- Gaining full visibility into any changes made to programmable logic controllers (PLCs) and other ICS devices
- Ensuring safety and preventing downtime due to unauthorized changes
- Streamlining asset management in a dynamic operational environment

SOLUTION
tenable.ot Powered by Indegy

IMPACT

- Improved network visibility that includes a complete picture of what's happening in the controls network, who made changes, and why
- Saved time through automated discovery and tracking of all ICS assets
- Accelerated response to security issues with real-time understanding of network traffic
- Ease of use makes it simple for the IT/OT teams to control system operations without technical training

STUPP CORPORATION

Stupp Corporation produces the pipelines that form the backbone of North America's energy infrastructure. Stupp's mission is to produce high-integrity pipes and services for the safe transportation of oil, gas and associated products.

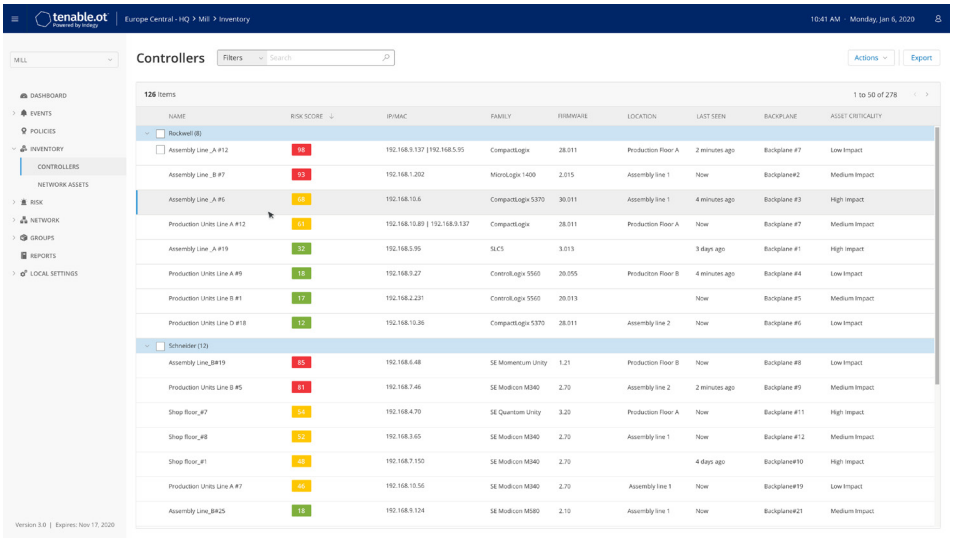
As the industrial threat landscape evolves, Stupp's chief information officer, John Roosa, believed it was only a matter of time before OT infrastructure could become vulnerable to cyberattacks. To protect its production environment from potential downtime and safety risks, Stupp decided to deploy an industrial-oriented cybersecurity solution.

CHALLENGES

Greater connectivity between IT and OT networks increased the chances that Stupp's ICS network could become compromised by a cyberattack. "You interface to the controls network through the same PCs that you use at your desk. Any threat that can be found in that PC-based environment can be projected down into the controls network very easily," said Rich Michael, operations data analytics manager at Stupp.

Like most mid-sized enterprises, Stupp did not have the internal resources for 24/7 monitoring and control of its operational technology (OT) network. Improving the company's cybersecurity posture meant being able to detect external attacks as well as insider threats and accidental or unauthorized changes to controllers.

Such changes to PLCs or other IT/OT devices can slow operations and in some cases result in a complete halt in productivity. According to Roosa, the cost of downtime can reach tens of thousands of dollars an hour. Real-time visibility and alerts to changes were essential for avoiding downtime scenarios.



Illustrative Data: Tenable.ot provides unified visibility, security and control of all controllers in OT infrastructures ensuring faster remediation of actual cyber risks.

SOLUTION

Following a successful proof of concept, Tenable.ot was deployed within Stupp's ICS network. "The deployment was extremely simple – within an hour or so the system was up and running," said Michael. "By the end of the day, I was comfortable with the user interface and was able to get value from it instantly."

- **Active Query Innovation**
  Stupp is using Tenable.ot's patented technology to actively query devices for configurations, code changes and state. Together with passive network monitoring, active queries provide Stupp with full visibility, security and control over every ICS asset in its mills. Using this technology, Stupp receives real-time alerts to any unauthorized or unintentional changes in the ICS environment. Tenable.ot safely queries Stupp's assets and devices in their native protocols, with zero impact on device configurations or network operations.

- **Packet-Level Monitoring**
  Unlike Stupp's previous solution that used agents on ICS devices, Tenable.ot monitors and analyzes all network traffic at the packet level. This allows Stupp to know exactly what's happening on the network, from intrusion detection to network configuration changes. If a new device pops up on the network, or somebody makes a change to a controller, Stupp's operations team knows immediately. "From a control standpoint, Tenable.ot is a great product because it basically monitors everything of interest to a controls engineer," said Michael.

- **Proactive Vulnerability Identification and Mitigation**
  Stupp's operations team does not have the time or resources to analyze and patch every published ICS vulnerability across its asset inventory. In addition to listing all the common vulnerabilities and exposures (CVEs) related to a particular asset, Tenable.ot gives Stupp the tools to analyze the surrounding network traffic around a vulnerable asset. By understanding the vulnerability and its impact on the network, Stupp can determine whether to remediate the risk or continue to monitor and run as usual.

IMPACT

- **Ability to Prevent Damage Before It's Done**
  Tenable.ot allows Stupp's operations team to understand what's happening inside the ICS environment. Previously, if an operator made a change to an asset, in many cases that change was never communicated to others within the organization. With Tenable.ot, designated personnel receive a real-time alert for any change to a device, disclosing who made the change and at what time. "We can then follow up with the relevant technician, find out why the change was made, and rectify it, if necessary, before any damage is done," said Roosa.

- **Speed of Response**
  Stupp gets insight into what's happening on each of its assets through Tenable.ot patented technology. One key advantage of this active querying technology is that it natively connects to Stupp's devices in a safe manner across control networks. "When you're connecting into different controls and environments, the speed of response on these networks is critical. You can't introduce a device that will cause any type of lag in the network," said Greg Canton, client executive at Brock Solutions, Stupp's automation and controls partner.

- **Reliable, Expert Service and Support**
  With the support of Tenable's engineers, Stupp smoothly deployed Tenable.ot within its OT environment. The initial system was up and running on the first day, providing local engineers with complete visibility, security and control over all industrial operations.

CONCLUSION

Familiar with the benefits of Tenable.ot, Brock Solutions set up a demo for Roosa and the Stupp team. "We reached out to several other vendors as part of our due diligence, but none of them showed me anything that was as forward-thinking as what Tenable.ot had in the controls security space," said Roosa.

Because safety is such a key requirement for Stupp, ensuring comprehensive security, visibility and control of the OT infrastructure that physically moves large pipelines and components is critical. If any compromise to the PLC device caused it to be modified in the wrong way, the error would have a serious impact on workers' safety

Learn more about Tenable.ot | Contact Us: **marketing@tenable.com**