CASE STUDY

tenable

Nesher Cement Secures Complex SCADA Environment from Cyber Threats

> "Tenable.ot gives us visibility in our complex SCADA network environment. We also have our eyes 24/7 on cybersecurity alerts and events in a way we have never seen before."
>
> **ROY SHALEV**
> Chief Information Security Officer

ORGANIZATION SNAPSHOT

ORGANIZATION

Nesher Israel Cement Enterprises

MARKET SHARE

60%

ANNUAL PRODUCTION OF CEMENT

6 million tons

INDUSTRY

Manufacturing

CHALLENGES

- Maintaining safety, reliability and productivity in a digitalized environment amid a growing number of sophisticated cyber threats
- Ensuring full visibility to industrial control systems (ICS) and other devices
- Providing security operations center (SOC) analysts with the data required to quickly and efficiently remediate alerts

SOLUTION

tenable.ot™
Powered by Indegy

IMPACT

- Employees work in a safe, always-on environment
- Security teams have complete visibility, security and control across a complex supervisory control and data acquisition (SCADA) environment
- Incident response is accelerated with simple-to-use, insightful visualizations and the patented Tenable.ot active query capability
- Peace of mind is achieved when security teams know they'll receive accurate alerts to any change in their OT network

NESHER ISRAEL CEMENT ENTERPRISES

Nesher Israel Cement Enterprises is the largest cement producer in Israel. With large-scale production sites in Ramla and Haifa, Nesher produces about 60% of the cement used by Israel's construction industry.

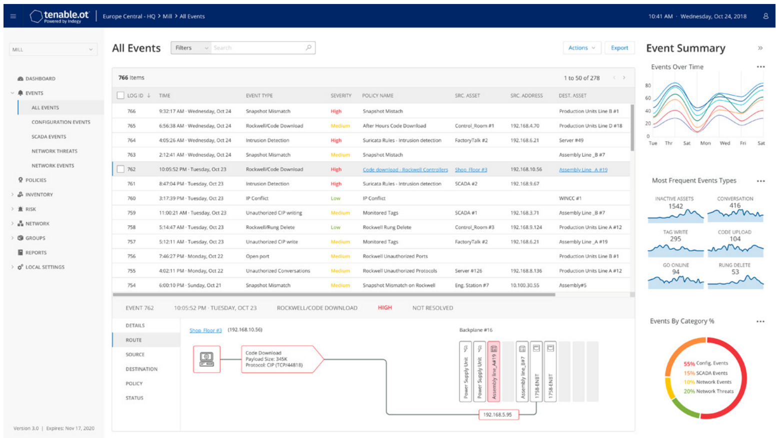
With the introduction of digital technologies, Nesher realized that its SCADA network could be exposed to cyber threats that jeopardize the safety and productivity of its factories. Determined to reduce risk and minimize production downtime, Nesher's management team made a strategic decision to invest in a dedicated industrial cybersecurity solution.

CHALLENGES

With cement furnaces operating around-the-clock at 1,200 degrees Celsius, Nesher's most important operational concern is safety. Nesher's furnaces and other critical equipment are managed by industrial controllers, which, if compromised by a cyberattack, could lead to a major explosion and even loss of life.

- **Maintaining safety, reliability and productivity in a digitalized environment amid a growing number of sophisticated cyber threats**
  From a business standpoint, a cybersecurity event in Nesher's SCADA environment could bring cement production to a halt. Such an incident could cause major shortages of cement in Israel's construction market as well as revenue losses of millions of dollars and reputational damage.

- **Lack of full visibility to industrial control systems (ICS) and other devices**
  Nesher required full visibility of its complex SCADA/ICS network together with real-time 24/7 alerts on any changes to its controllers. This level of visibility (see Figure 1) was crucial for enabling early detection and mitigation of security risks before they impact productivity or endanger employee safety.



LOG ID	TIME	EVENT TYPE	SEVERITY	POLICY NAME	SRC. ASSET	SRC. ADDRESS	DEST. ASSET
766	9:32:17 AM · Wednesday, Oct 24	Snapshot Mismatch	High	Snapshot Mistach			Production Units Line B #1
765	6:56:38 AM · Wednesday, Oct 24	Rockwell/Code Download	Medium	After Hours Code Download	Control_Room #1	192.168.4.70	Production Units Line D #18
764	4:05:26 AM · Wednesday, Oct 24	Intrusion Detection	High	Suricata Rules - Intrusion detection	FactoryTalk #2	192.168.6.21	Server #49
763	2:12:41 AM · Wednesday, Oct 24	Snapshot Mismatch	Medium	Snapshot Mistach			Assembly Line _B #7
762	10:05:52 PM · Tuesday, Oct 23	Rockwell/Code Download	High	Code download - Rockwell Controllers	Shop Floor #3	192.168.10.56	Assembly Line _A #19
761	8:47:04 PM · Tuesday, Oct 23	Intrusion Detection	High	Suricata Rules - Intrusion detection	SCADA #2	192.168.9.67	
760	3:17:39 PM · Tuesday, Oct 23	IP Conflict	Low	IP Conflict			WINCC #1
759	11:00:21 AM · Tuesday, Oct 23	Unauthorized CIP writing	Medium	Monitored Tags	SCADA #1	192.168.3.71	Assembly Line _B #7
758	5:14:47 AM · Tuesday, Oct 23	Rockwell/Rung Delete	Low	Rockwell Rung Delete	Control_Room #3	192.168.9.124	Production Units Line A #12
757	5:12:11 AM · Tuesday, Oct 23	Unauthorized CIP write	Medium	Monitored Tags	FactoryTalk #2	192.168.6.21	Assembly Line _A #19
756	7:46:27 PM · Monday, Oct 22	Open port	Medium	Rockwell Unauthorized Ports			Production Units Line B #1
755	4:02:11 PM · Monday, Oct 22	Unauthorized Conversations	Medium	Rockwell Unauthorized Protocols	Server #126	192.168.8.136	Production Units Line A #12
754	6:00:10 PM · Sunday, Oct 21	Snapshot Mismatch	Medium	Snapshot Mismatch on Rockwell	Eng. Station #7	10.100.30.55	Assembly#5

EVENT 762 10:05:52 PM · TUESDAY, OCT 23 ROCKWELL/CODE DOWNLOAD HIGH NOT RESOLVED

Figure 1. Tenable.ot provides the unified visibility of all assets and events in a simple interface that helps Nesher manage cyber risk.

- **SOC analysts lack the OT asset details required to quickly and efficiently remediate alerts**
  Simplicity of use and responsive vendor support were also important for allowing Nesher's operations and security teams to become proficient with the system in the shortest possible time. These attributes would enable Nesher to avoid hiring new cybersecurity and OT experts and reduce training efforts.

SOLUTION

Nesher deployed Tenable.ot at its cement factory and power plant – both based in Ramla. Tenable's professional services team worked closely with Nesher's experts to devise the optimal implementation strategy, which included the following capabilities:

- **Safely queries industrial control devices**
  Tenable.ot meets Nesher's requirement for 360-degree visibility of its SCADA environment, enabling its engineers to stay apprised of every detail for every ICS asset from a single pane of glass. Tenable.ot safely queries Nesher's assets and devices in their native protocols, with zero impact on device configurations or network operations. By working in conjunction with passive network monitoring, the Tenable.ot patented active querying technology provides critical information about Nesher's ICS environment that cannot be gathered solely by listening to network traffic.

- **Automates all asset inventory**
  Tenable.ot enables Nesher to automatically discover all assets within its large and complex SCADA environment, including dormant devices. Tenable.ot gathers and tracks all device-related activities, creating an up-to-date inventory of Nesher's ICS assets, including data stored within the devices themselves (e.g., Windows user, hotfix lists, firmware version, PLC backplane configuration). This in-depth visibility into the state of each device enables Nesher to immediately detect misconfigurations, vulnerabilities, potential security breaches and threats.

- **Produces context-rich, real-time alerts**
  In addition to dashboard alerts, Tenable.ot also provides Nesher with real-time alerts containing detailed contextual information gathered from devices. The data about suspicious activities and unauthorized changes enables Nesher's engineering and security teams to work together, helping them quickly identify the source of potential problems and mitigate potential risks.

- **Incorporates multi-tiered, policy-based detection**
  Nesher uses Tenable.ot policy-based detection to configure custom security rules that reflect specific organizational requirements. Using a flexible, wizard-based interface, Nesher can fine-tune predefined policies or create new ones as needed. Together with anomaly-based detection, these custom rules help Nesher effectively enforce its ICS network security policies against any type of threat and improve alert accuracy.

IMPACT

- **Employees work in a safe, always-on environment**
  The ability to detect any threat to Nesher's OT infrastructure enables Nesher to feel secure and confident their employees are in a safe environment. Tenable.ot greatly reduces their risk of any downtime while also enabling Nesher to keep all their assets current and document any change – malicious or not – that anyone has made.

- **Security teams have complete visibility and control across their SCADA environment**
  Tenable.ot uses proprietary technology that actively queries devices in Nesher's industrial environment, enabling its security teams to achieve maximum visibility and ensuring that its SCADA engineers are aware of every change to every ICS asset. This unique capability enables unmatched visibility and control over ICS assets without impacting the safety or reliability of Nesher's industrial operations. "We are using the Tenable.ot patented technology with zero interference to our SCADA environment," said Shalev.

- **Incident response is accelerated with simple-to-use, insightful visualizations and the patented Tenable.ot active query capability**
  One of the main drawbacks of the other systems we looked at in our RFP was their complexity and cumbersome user interface. The Tenable.ot interface makes it easy for Nesher's engineers to control traffic and operations in the SCADA network. "What really stood out in the Tenable.ot solution is the simplicity of usage," said Niki Lukutin, Nesher's technology development department manager. "After just one day of working with the system, I was familiar with the user interface," added Lukutin.

- **Peace of mind because of accurate alerts to any change in their OT network**
  Alert accuracy is another area in which Tenable.ot outperformed competitors. Unlike other vendors that had a high rate of false positives, Tenable.ot enables Nesher to define custom security policies which reduce the number of alerts and minimize false positives. Since security alerts and events are being sent 24/7 from Tenable.ot to Nesher's SOC, enhanced alert accuracy means Nesher SOC analysts can focus their efforts on investigating real threats.

CONCLUSION

After conducting an in-depth evaluation of several other OT security providers, Nesher's technical team selected Tenable.ot. They were particularly impressed by the comprehensive situational awareness it provided.

Thanks to Tenable.ot, Nesher now has a comprehensive view of their cyber risk across their OT network.

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