Indegy
Activate All Your Senses

Case Study

Nesher Cement Secures Complex SCADA Environment from Cyber Threats

At a Glance

Customer:
Nesher Israel Cement Enterprises

Challenges:

- Maintaining safety, reliability, and productivity
- Protection from sophisticated cyber threats
- Improving visibility of controllers and other devices
- Enabling SOC analysts to investigate and remediate alerts more efficiently

Results:

- Visibility and Control – 360-degree situational awareness across a complex SCADA environment
- Advanced Cybersecurity – Hybrid threat detection combining passive network monitoring and active device querying
- Ease of Use – Intuitive user interface and visualizations remove technical barriers and simplify the user experience
- Accurate Alerts – Custom security policies reduce number of alerts and eliminate false positives
- Safe and Transparent – Use of native protocols ensures zero impact on network operations

Background

Nesher Israel Cement Enterprises is the largest cement producer in Israel. With a 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 "connected" technologies, Nesher realized that its SCADA network could potentially 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.

Ensuring Safety, Reliability and Productivity in Nesher's SCADA Environment

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

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 to Nesher.

To avoid these scenarios, 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 was crucial for enabling early detection and mitigation of security risks before they impact productivity or endanger employee safety.

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 the training effort.

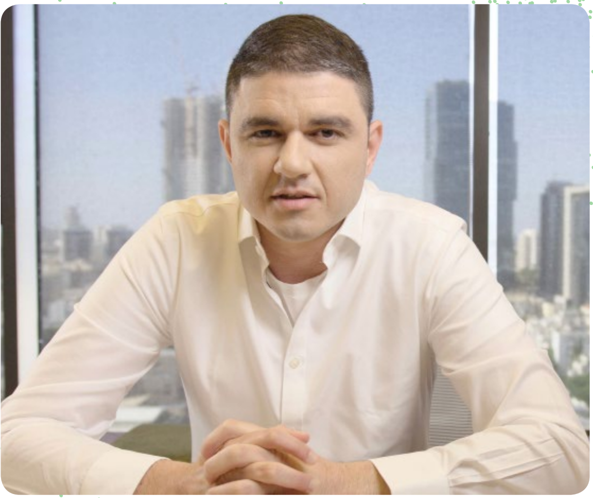
Why Nesher Chose Indegy

With these requirements in mind and following an in-depth evaluation by its technical team of a number of other providers, Nesher selected the Indegy Industrial Cybersecurity suite.

Nesher was particularly impressed by the comprehensive situational awareness provided by the Indegy solution.

> “Indegy increased our **SCADA network visibility**, and also gave us visibility which we didn't have before,” said Roy Shalev, CISO at Nesher.

Play Video



Unparalleled Visibility

Indegy enables Nesher to achieve maximum visibility using proprietary technology that actively queries devices in Nesher's industrial environment, ensuring that its SCADA engineers are aware of every change to every asset in the ICS environment. This Device Integrity component enables unmatched visibility and control over ICS assets without impacting the safety or reliability of Nesher's industrial operations. "We are using Indegy's device integrity capability with zero interference to our SCADA environment," said Shalev.

Ease of Use

One of the main drawbacks of competitors' systems was their complexity and cumbersome user interface. Indegy's UI design makes it easy for Nesher's engineers to control traffic and operations in the SCADA network. "What really stood out in the Indegy security suite 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."

Accurate Alerts

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

> Indegy's team was very flexible and resourceful in helping us expedite the system implementation, added Lukutin.

Solution: Indegy Industrial Cybersecurity Suite

Nesher deployed Indegy's solution at its cement factory and its power plant - both based in Ramla. Indegy's professional services team worked closely with Nesher's experts to devise the optimal implementation strategy.

Device Integrity

Indegy Device Integrity meets Nesher's requirement for 360-degree visibility of its complex SCADA environment, enabling its engineers to stay apprised of every detail for every ICS asset in a single pane of glass. Device Integrity 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, this active detection technology provides critical information about Nesher's ICS environment that cannot be gathered solely by listening to network traffic.

Automated Asset Discovery

The Device Integrity feature allows Nesher to automatically discover all assets within its large and complex SCADA environment, including dormant devices. Indegy 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, such as Windows user, hotfix lists, firmware version and PLC backplane configuration. This in-depth visibility into the state of each device enables Nesher to immediately detect misconfigurations, identify potential security breaches and remediate threats.

Policy-Based Detection

Nesher is using Indegy's policy-based detection feature to configure custom security rules that reflect its specific organizational requirements. Using a flexible, wizard-based interface, Nesher can fine-tune pre-defined 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, as well as improving alert accuracy.

Context-Rich, Real-Time Alerts

In addition to dashboard alerts, Indegy 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, quickly identifying the source of potential problems and instantly mitigating potential risks.

Like this case study?

Visit us at Indegy.com for more content like this.

Follow us:

Indegy