APERIO Systems Company Overview

Cyber Attacks on Critical Systems: Defenses Will Be Breached

A sophisticated attack on Ukraine's power grid leaves a quarter-million people in the dark and operators locked out of their SCADA system. Hackers with minimal knowledge and ability gain access to a water plant, hijacking PLCs controlling the flow of chemicals into the water supply. Recent incidents like these demonstrate the abilities of adversaries to penetrate systems controlling all areas of critical infrastructure, be they insiders, state-sponsored agents, cybercriminals, or hacktivists. A **persistent attacker will eventually breach critical SCADA systems**.

Both internal and external attackers can hide malicious activity and deceive the plant's operators by manipulating the reported values of critical devices. As long as operators in the control room know what's really going on, they can take action in time and prevent long term severe damage. However, once attackers take control of the SCADA system, they can effectively **blind operators** to the true state of the system and cause long term damage while operators have no chance to respond.

While increasingly sophisticated attackers pose an exponential threat, critical systems security products on the market today are intrusive, hard to maintain and costly to integrate. In addition, they often produce vague and unactionable alerts which are of little to no use to critical utility control room operators.

APERIO Systems: From Cyber Threat Detection to Process Resilience

APERIO Systems passively plugs into the existing monitoring systems. Using advanced proprietary algorithms, APERIO identifies unique fingerprints in reported signals, validating their integrity and authenticity. Based on those fingerprints, APERIO alerts and pinpoints the attacked equipment and forged process data. APERIO's unique capabilities are based on machine learning algorithms trained to detect artificial manipulations of process data. Its proprietary Data Forgery Protection (DFP) technology detects an injection of new synthetic data, a replay of past data, or an online transformation of process data (eg. multiplying the signal by a factor, in the simple case). APERIO Systems uses state-of-the-art algorithms to reconstruct the true state of the system in real time, enabling true state awareness and allowing the operator to take the relevant corrective action in time. By doing so, APERIO Systems provides unprecedented resilience against both internal and external malicious activity.

Resilient Control System:
"Maintains **state awareness** and an accepted level of **operational normalcy** in response to disturbances, including threats of an unexpected and malicious nature."
(U.S. Idaho National Laboratories)

APERIO Systems' Value Proposition and Key Differentiators:

- **Process Continuity**: APERIO Systems enables trust in the most critical data and provides resilience when attacked. Unlike traditional industrial Intrusion Detection/Prevention Systems (IDS/IPS), APERIO Systems **not only detects** that there's an attack, but also **pinpoints the manipulation** and **suggests a correction**.
- **Operational Alerts:** APERIO Systems provides fast, actionable, specific and accurate alerts - integrating cybersecurity into operational emergency procedures, allowing the operators to mitigate heavy permanent damage. APERIO doesn't just alert that "something is wrong", but actually **tells the operator what's wrong**.
- **Counters Insider Threats**: The majority of breaches begin from the inside. APERIO Systems protects the plant's process continuity from **both external and internal actors,** unlike traditional IDS/IPS that are irrelevant against internal actors.
- **Last Line of Defense:** APERIO Systems is the only solution focused on true state awareness of physical systems. As such, it provides the last line of defense once digital systems are penetrated by malicious actors.
- **Accurate and Relevant:** While classic anomaly detection products falsely alert when new legitimate operating modes are implemented, **APERIO** Systems **alerts only when the reported process state does not reflect the plant's real situation**. For example, when a turbine is operating at an unusually low power level, it can be due to special business requirements or as a consequence of an attack. **APERIO is able to separate the two cases** and provide the operator and the CISO with relevant alerts.
- **Minimized Risk**: APERIO Systems' solution is **passive** and **non-intrusive** – minimizing operational risks, as well as installation and maintenance costs. Unlike traditional industrial IDS/IPS, **APERIO Systems' solution doesn't require a painful deployment in the production network**.

Deployment and Integration:

APERIO Systems passively plugs into the plant's historians and PI servers and collects data from it. These systems are built for the purpose of allowing external analytic products to access the plant's production data and are deployed in the vast majority of critical utilities around the world.

The Team:

APERIO Systems' core team is led by multidisciplinary industrial and cybersecurity world-class experts in both computational and physical sciences:

- **CEO:** Yevgeni Nogin -— Former R&D Leader of national level cyber defense Projects; **Talpiot Israel Defense Forces (**IDF) elite-program graduate; BSc Physics + Computer Science, MSc Nanophotonics.
- **Head of Product:** Michael Shalyt — Former Research Leader – National Level Innovative Defense Projects; **Psagot** IDF elite-program graduate; Former head of malware research at Check Point Systems; BSc Physics + Electrical Engineering, MSc Quantum Computation.
- **Head of Algorithms:** Itay Baruchi — An experienced executive, entrepreneur and scientist with a proven track record in several industries including photovoltaic solar energy; prominent neuroscience & bio-medical researcher; BSc + MSc Physics, PhD Neurophysics.
- **Chief Scientific Officer:** Charles Tresser, world-renowned expert in Dynamical Systems and one of the world's leading experts in chaos theory. Former director of research at IBM and France's National Center for Scientific Research (CNRS).

Active Private Investors and Board Members:

- **Doron Bergerbest-Eilon** – Formerly Maj. General in Israeli Security Agency, founded NISA, founder & CEO of ASERO Worldwide, a global leader in HLS and national level cybersecurity.
- **Shlomi Boutnaru and Liran Tancman** — Played key roles in building Israel's cyber capabilities; Founders of CyActive Security (Acquired by PayPal in 2015).

For more information, please contact us at: info@aperio-systems.com