APERIO Systems Emerges from Stealth, Unveils Data Forgery Protection Technology to Defend Critical Industrial Control Systems from Cyber Threats

"Seeing is NOT always believing": Industrial cybersecurity startup protects SCADA systems by detecting and immediately correcting falsified readings for unprecedented operational resilience

HAIFA, Israel, Nov. 15, 2016 – APERIO Systems today emerged from stealth mode, launching the industry's first technology that detects artificial manipulations of industrial process data, enabling operators to take real-time corrective action without service disruption to industrial control systems (ICS). From the rate of gas flow at a petroleum refinery, to the temperature and spin rates of turbines in a power plant, or the chlorine level of water supply networks, APERIO Systems' proprietary Data Forgery Protection™ (DFP) technology delivers the last line of defense in protecting critical SCADA systems against insider and external threats.

APERIO Systems, already deployed at several sites across EMEA, secured seed funding from a consortium of private investors, including prominent cybersecurity veterans Doron Bergerbest-Eilon, Liran Tancman, and Shlomi Boutnaru. Bergerbest-Eilon is renowned for his role in establishing the agency charged with protecting all critical infrastructure in the State of Israel and is the former director of the security and protection division of the Israel Security Agency (ISA). He is currently the founder, president and CEO of ASERO Worldwide, a security consulting firm. Tancman and Boutnaru, who played key roles in building Israel's cybersecurity capabilities, founded predictive cybersecurity startup CyActive, which was acquired by PayPal in 2015.

"Current solutions focus on keeping hackers outside critical systems, but attacks like the one that took down the power grid in Ukraine clearly show that sophisticated attackers will eventually penetrate these systems," said Bergerbest-Eilon. "Once attackers breach a system, they must blind the operators and protection mechanisms by falsifying data in order to inflict severe and long-lasting damage. This entirely new category of Data Forgery Protection (DFP) is the key to keeping our critical infrastructure safe from attacks."

Industrial control systems (ICS) are generally outdated from a cybersecurity perspective, vulnerable and difficult to patch because mission critical systems cannot be taken offline. While the threat to ICS is growing, critical systems security products on the market today are intrusive, hard to maintain, costly to integrate, and often produce vague and unactionable alerts, which cannot be acted upon by critical utility control rooms.

"Think of APERIO Systems as a polygraph for process data — it detects when your system is lying to you," said Yevgeni Nogin, CEO of APERIO Systems. "With the unrelenting tenacity of cybercriminals, critical infrastructure breaches are inevitable. By guaranteeing the authenticity and integrity of operational data, APERIO Systems ensures that operators always know what's

really going on, enabling them to react quickly to a breach and take corrective action — making the critical systems resilient to the most dangerous of attacks."

APERIO Systems' advanced proprietary algorithms search for the data's unique fingerprints and validate its authenticity. Any mismatches generate an alert and APERIO Systems pinpoints the attacked equipment and forged process data. Using a sophisticated combination of physics and state-of-the-art machine learning techniques, APERIO Systems reconstructs the real values of the forged operational data and reverts it to its original state in real time — establishing unprecedented operational resilience.

How APERIO Systems Protects Critical Infrastructure Control Systems

Both internal and external attackers can penetrate the most critical infrastructures, causing severe and long lasting damage. In order to do so, they must hide their malicious activity and deceive plant operators by forging the reported values of critical devices — remaining undetected and preventing timely corrective action. APERIO Systems' Data Forgery Protection technology immediately exposes forged system readings to safeguard critical control systems and allow quick and effective remediation.

APERIO Systems provides:

- **Data Forgery Protection (DFP):**
  Validates integrity and authenticity of reported signals to provide operators with true state awareness, enabling them to take corrective action in real time.

- **Process Continuity:**
  Enables trust in the most critical data and provides resilience when attacked.

- **Operational Alerts:**
  Fast, actionable, specific and accurate alerts integrate cybersecurity into operational emergency procedures, allowing operators to mitigate permanent damage.

- **Accurate and Relevant:**
  Alerts operators only when the reported process state does not reflect the plant's real situation — providing an extremely low false alert rate.

- **Minimized Risk:**
  Passive and non-intrusive system minimizes operational risks, as well as installation and maintenance costs.

- **Counters Insider Threats:**
  Protects the plant's process continuity from both external and internal actors.

APERIO Systems is led by a veteran executive team with roots in the elite units of the Israel Defense Forces (IDF), as well as top cybersecurity and industrial companies:

- Yevgeni Nogin, CEO – a graduate of the elite "Talpiot" IDF military academy served over nine years in elite intelligence and R&D units of the IDF, and brings expertise in SCADA systems security.
- Michael Shalyt, VP Product – a graduate of the "Psagot" IDF academic program and served as leading researcher and team leader in the elite 8200 unit. Prior to joining APERIO Systems, he led the malware research team at Check Point.
- Itay Baruchi, Head of Algorithms – served as director of Industrial MRI, where he worked closely with several of the biggest oil and gas drilling companies. Before that, he founded and served as CTO of Pythagoras Solar.
- Charles Tresser, Chief Scientific Officer – a world renowned expert in dynamical systems. Tresser is one of the world's leading experts in chaos theory and formerly Director of Research at IBM and France's National Center for Scientific Research (CNRS).

About Aperio Systems

APERIO Systems secures critical control systems with a last line of defense against both internal and external cyber threats and malicious actors. APERIO Systems uses statistical physics and state-of-the-art machine learning techniques to detect operational data forgery attempts and reconstruct the true state of industrial control systems in real time. APERIO Systems enables unprecedented resilience and operational integrity for critical infrastructure such as power plants, water and waste control, manufacturing, oil and gas, energy, transportation, pharma, and food and beverage. More information at www.aperio-systems.com

Media Contact:
Leron Kornreich
Silicon Valley Communications
leron@siliconvpr.com
415.937.1724