Cyber & Operational Resiliency Solution for Data Centers

A paradigm shift for organizations with ZERO TOLERANCE for operational downtime, due to process disruption, in-efficiencies or failure of critical assets, regardless if triggered by Cyber Attacks, Malfunctions, Misconfigurations or Human Error.

While securing the data-network is crucial, the system remains vulnerable despite the layers of protection installed, and the operators wouldn't even know it – as demonstrated at the Stuxnet (2010), Irongate (2016) and Black Hat (2019) events, where PLCs were hacked and compromised without detection or operator awareness of such compromise.

This vulnerability can be solved by monitoring the most reliable source of information, the raw (un-hackable) electrical signals at level 0 - sensors and actuators, connected to the mission-critical assets (generators, UPS, air-conditioning systems, electrical rooms etc).

A data center's main function is to provide constant uptime for the mission-critical applications it houses.
Any downtime in a Data Center negatively affects your business.

- 1 minute of downtime costs a data center over **$8,000**
- Fortune 1000 lose $2.5 b a year due to application downtime (Business Insider, 2018)
- Average cost of data center outage in 2015 reached $740,357 (Ponemon Institute, 2018)

The top causes for Unplanned Downtime in Data-Centers: UPS failure, Cyber Attacks, Human Error, Electrical Deficiencies and HVAC Malfunctions.

SigaGuard safeguards data center assets by using an out-of-band network to monitor raw, untampered electrical signals. These signals are analyzed by SIGA's unsupervised machine learning software to provide operators real-time alerts on anomalies or operational failure indicators to maximize uptime.

Our Value Proposition