APERIO

Aperio - A ‘last line of defense’ against cyber attacks on critical infrastructure

Presented by: Gilles Barnier

©2018 OSIsoft, LLC

Pat Kennedy – CEO of OSIsoft



APERIO

©2018 OSIsoft, LLC

Who We Are

- Our business is based on a revolutionary approach to strengthening security for Critical Infrastructures through assuming the ‘worst case scenario’.
- Our solution uses machine learning to detect of any attempt to ‘mask’ an attack through forged sensor data – a common feature of large-scale attacks on critical infrastructure.
- Aperio is backed by leading VCs, Corporate Investors and known cybersecurity entrepreneurs. Founding shareholders previously founded CyActive which PayPal acquired in 2015
- $4.5m raised since founded in 2016

Critical infrastructure cyber attacks in recent years



UKRAINE ELECTRIC GRID ATTACK, 2015



CHEMICAL PLANT ATTACK, SAUDI ARABIA, 2017



US WATER PURIFICATION PLANT BREACH, 2016



AND STUXNET OF COURSE

APERIO

©2018 OSIsoft, LLC

Our Projects

- Product installed globally at world's leading Power Generation, Transmission, Oil & Gas and Chemical players
- Both Data Forgery (Cyber security) and Data Quality (asset maintenance & shut downs)

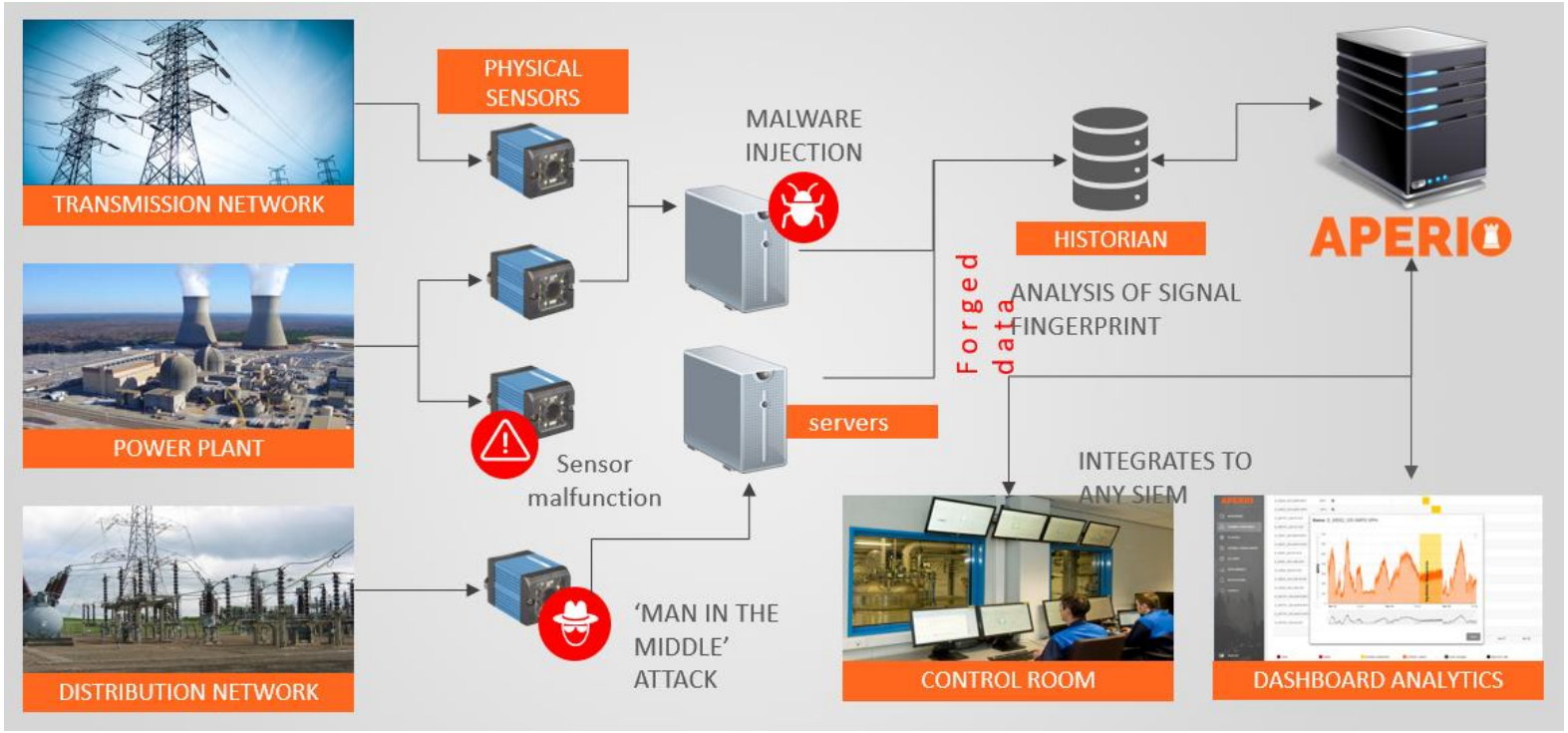
Our Team

- Multidisciplinary R&D team: Physicists, engineers, mathematicians, signal processing, dynamic systems and operational control
- Management team from Army Intelligence and leading global cyber companies

APERIO

©2018 OSIsoft, LLC

Thousands of sensors reflect reality in an unsecure environment



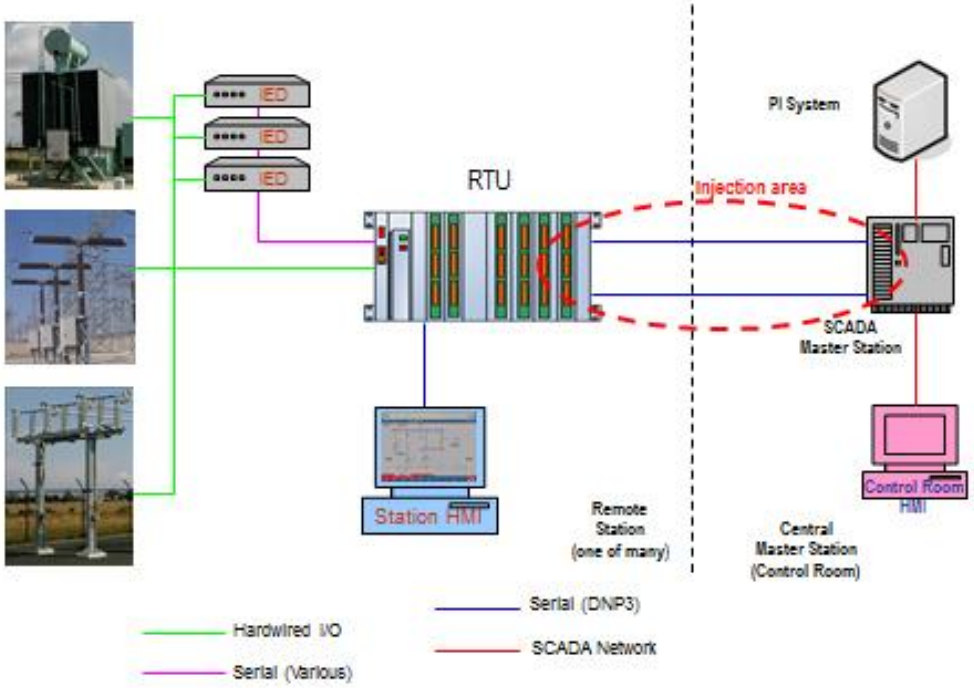
©2018 OSIsoft, LLC

Aperio Use Case – Client X

APERIO

©2018 OSIsoft, LLC

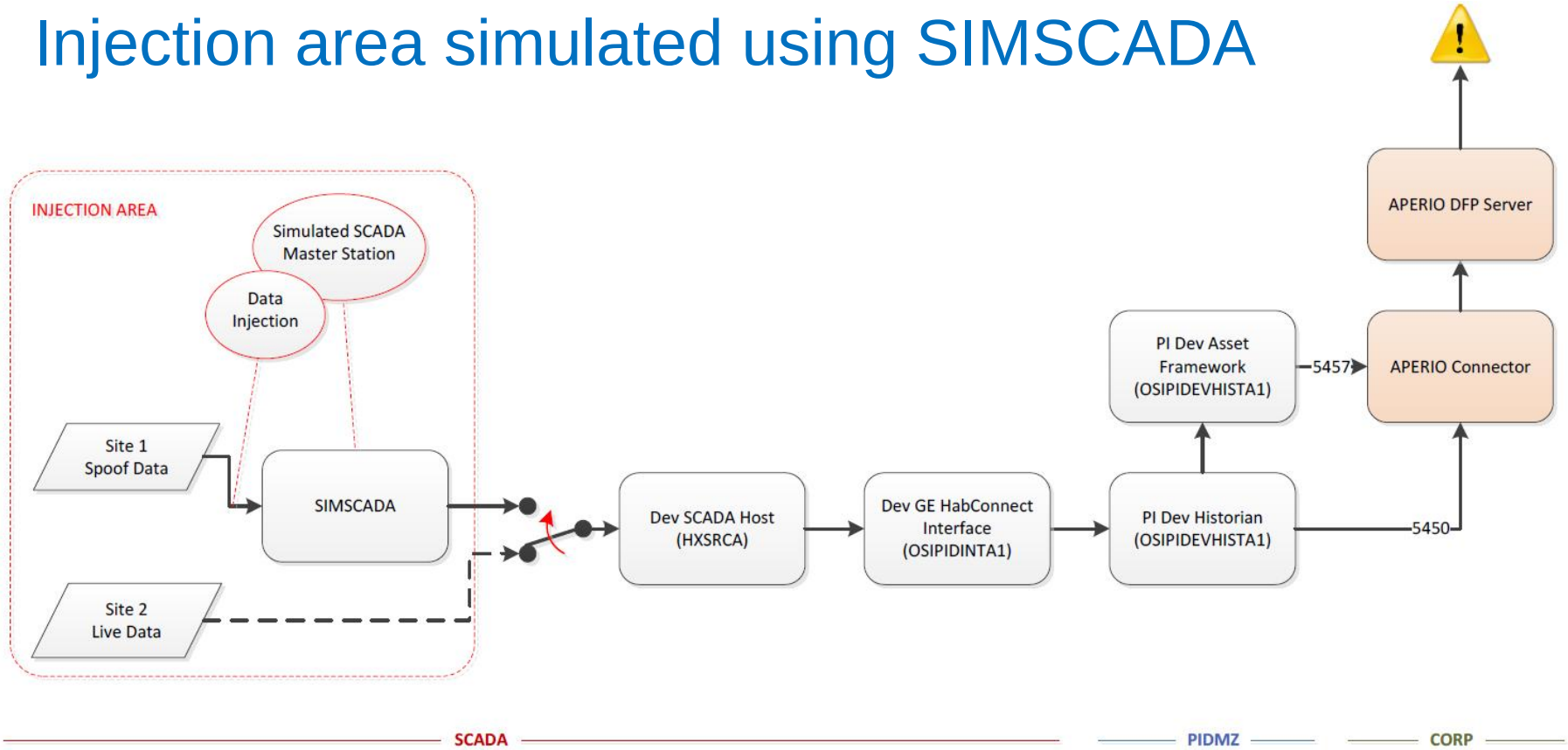
Typical Injection area for a Data Forgery Attack



APERIO

©2018 OSIsoft, LLC

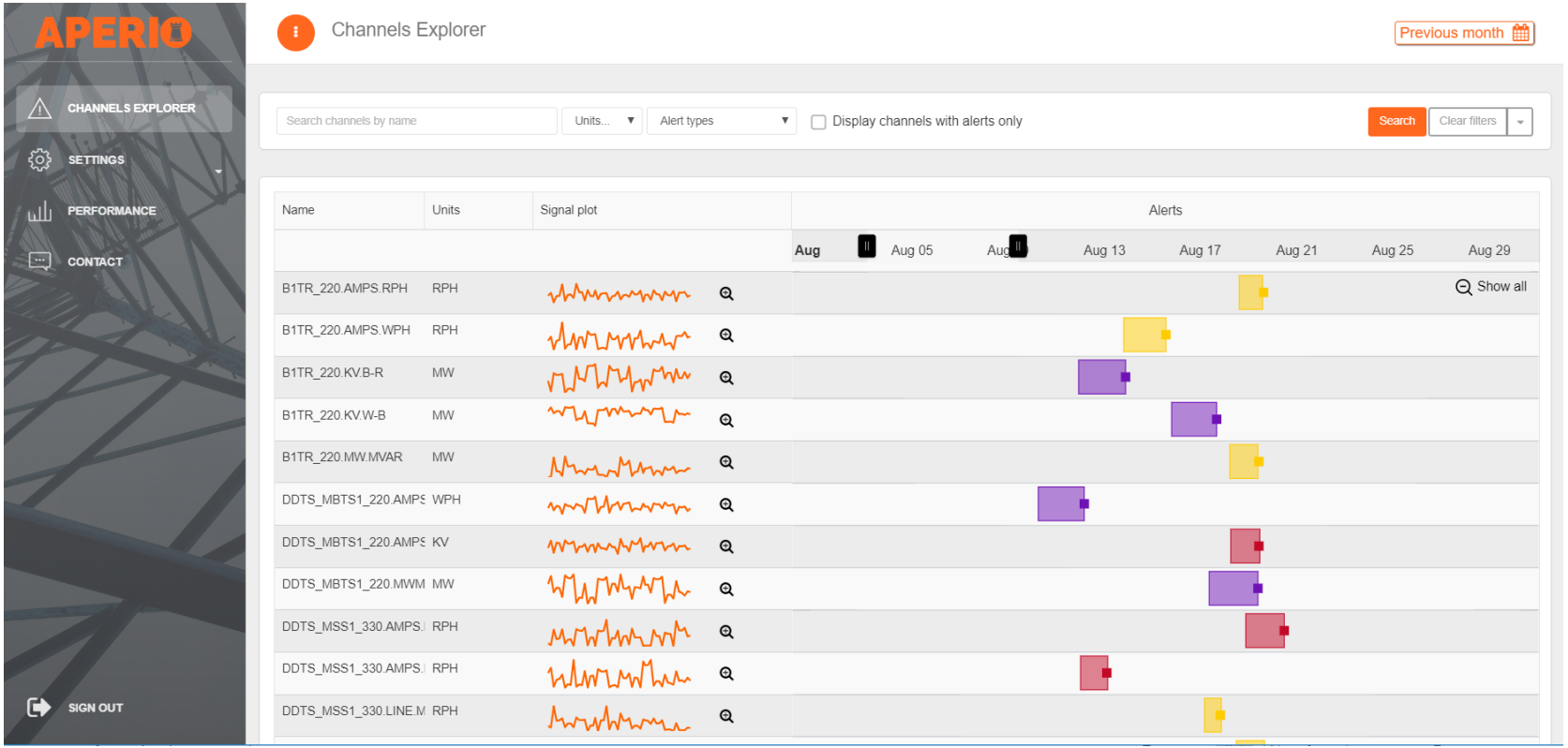
Injection area simulated using SIMSCADA



©2018 OSIsoft, LLC

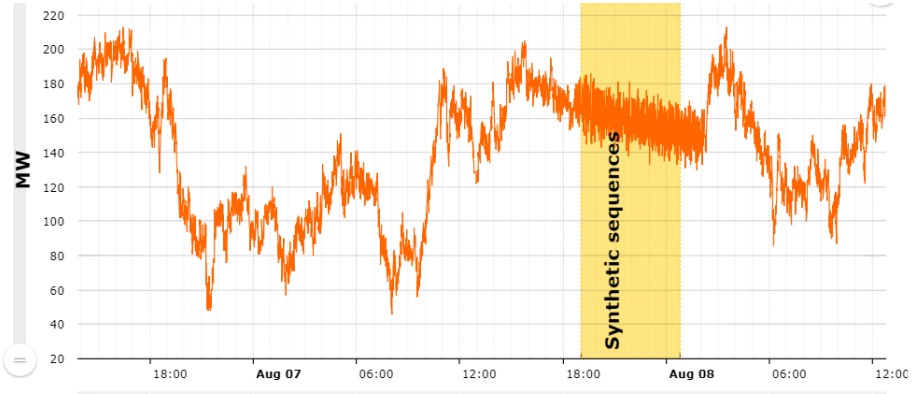
Aperio GUI during simulated attack

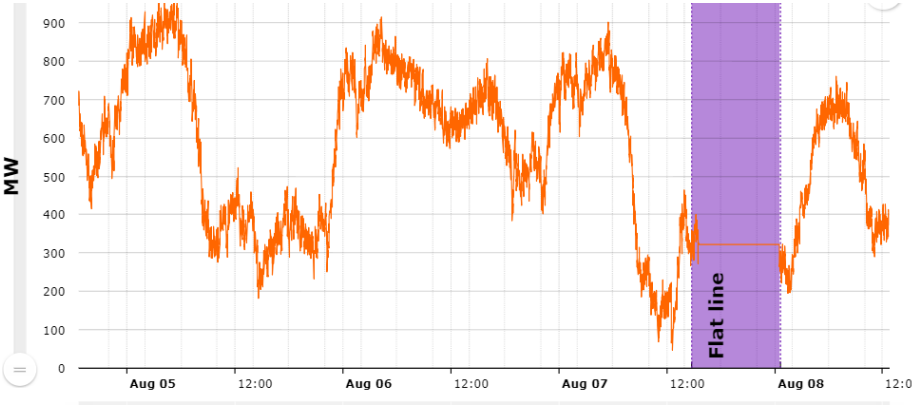
APERIO



©2018 OSIsoft, LLC

Examples of findings





©2018 OSIsoft, LLC

Any Questions?



©2018 OSIsoft, LLC



APERIO

©2018 OSIsoft, LLC