Advanced Cyber Situation Awareness for Fossil Fuel Power Plants by Machine Learning and Threat Behavior Analytics

Scott Brunza, Tim Ouellette, Bill Russ

NEED

Fossil fuel power generation plants risk interruptions of service caused by malicious attacks from insider threats and cybercriminals. These facilities need a comprehensive capability that will detect known and emergent cyberattacks in the short and long term, on their singly and combined ICS, IT, and physical assets, over the entire range of facility types.

SOLUTION

Sonalysts is developing MetaPhortress: a situational awareness tool that will incorporate Sonalysts’ patented, leading-edge cyber behavior modeling and temporal analysis platform, Occulex™, to capture, transmit, store, view, and analyze real-time data from all power plant assets to deliver a highly improved threat detection, and to increase system robustness and resiliency.

DEVELOPMENT

Sonalysts is developing MetaPhortress as a SBIR Phase I with the U.S. Department of Energy.

Milestones

Phase I: Work with power generation plant operators, owners, and OEMs to determine requirements, workflows, and integration strategies. Deliver design of MetaPhortress based on Occulex technology. This work completes in June 2019.

Phase II: Implement prototype MetaPhortress system and demonstrate feasibility.

Phase III: Produce beta system ready for field deployment and demonstration verification as part of the commercialization process.

FUTURE WORK

MetaPhortress will be applicable to a wide variety of government and industrial missions. Beyond its initial scope in fossil fuel power generation, MetaPhortress can extend to address more energy production modes, and additional environments characterized by critical reliance upon ICS.

Specific applications include:

- SIEM software
- SCADA for wastewater management
- Power Plant control systems
- Smart Grid cybersecurity

REFERENCES


ACKNOWLEDGEMENTS

Sonalysts gratefully acknowledges the support of the following during our Phase I development of MetaPhortress.