METAPHORTRESS

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

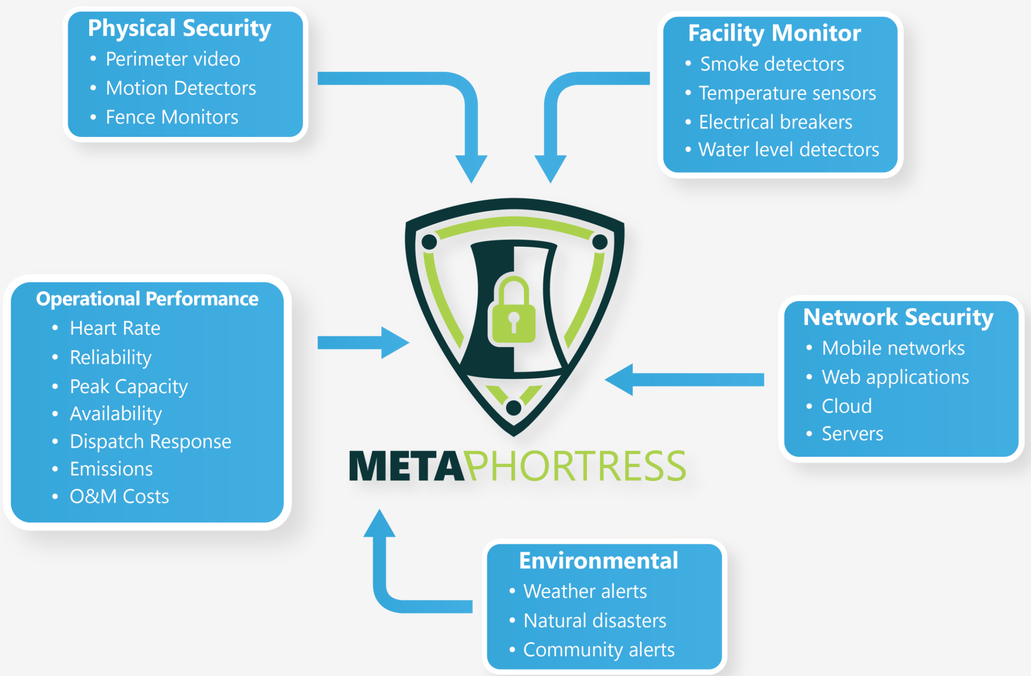
Scott Brunza, Tim Ouellette, Bill Russ

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 vastly 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 performance 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, MetaPhortresswill 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

Scott Brunza and Owen McCusker. "System and method for privacy-enhanced cyber data fusion using temporal-behavioral aggregation and analysis," US Patent 8,468,599

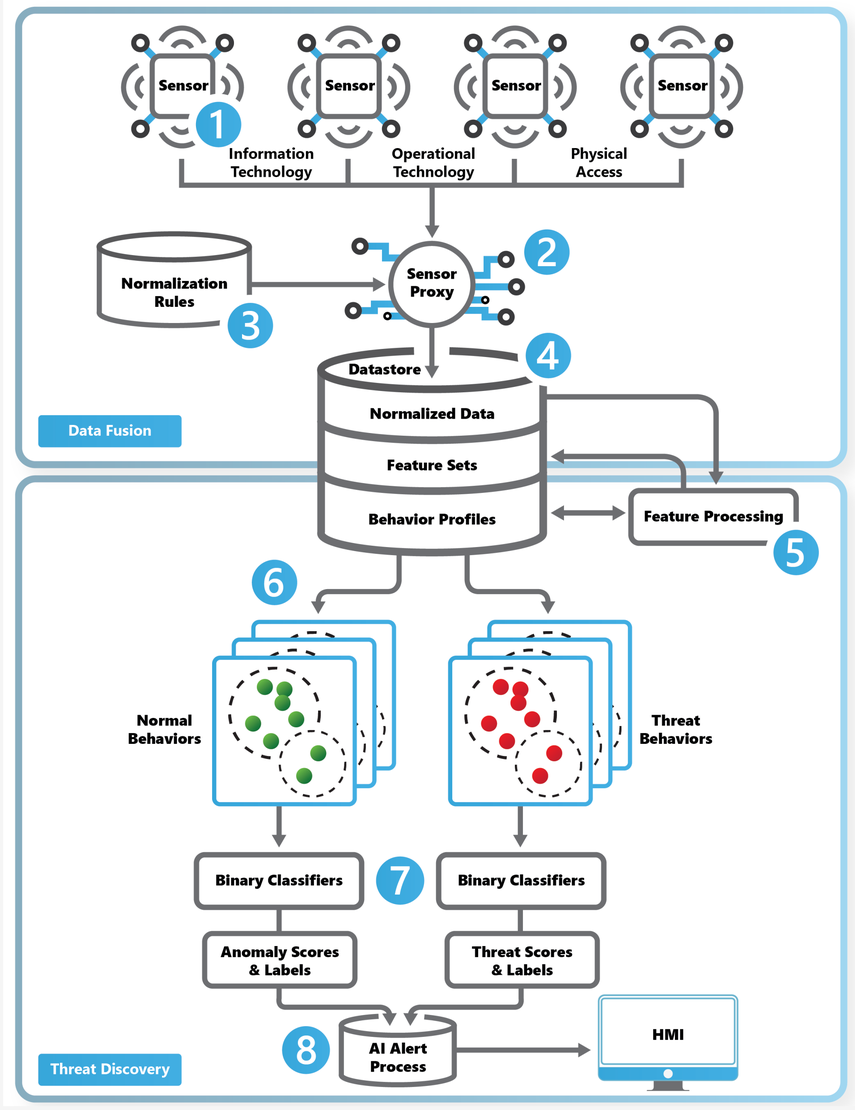
Scott Brunza et al., "Deriving Behavior Primitives from Aggregate Network Features Using Support Vector Machines," in Cyber Conflict (CyCon), 2013 5th International Conference on, pp. 1-18, 4-7 June 2013.

Jim McCarthy et al., "NIST Special Publication 1800-7, Situational Awareness for Electric Utilities," https://nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf, accessed Feb., 2018.

APPROACH

MetaPhortress will provide the required capability by leveraging Occulex to analyze, in real-time, the composite behaviors of cyber threats, in order to understand current data traffic and discover emergent threats. Capabilities include:

- Utilization of data fusion and data mining to discover emergent threats and resolve them against the time and system domains.
- Detection of attacks in different time frames.
- Scalable attack detection algorithms that apply across multiple databases.
- Rapid, clear, actionable presentation of threat alerts to power plant operators
- Improved resilience and robustness of critical energy infrastructure



1	Sensors	Raw data and events coming from combination of IT, OT and PA
2	Sensor Proxy	Converts all sensor inputs with normalization rules to standard formats and ranges, providing for consistent processing
3	Normalization	Aligns data using available calibrations, enumerations, units, mins and maxs for consistent formats and ranges
4	Datastore	Buffers normalized data, feature sets and behavior profiles
5	Features	Features are constructed from normalized data using behavior profiles. The profiles are stored templates of prescribed feature sets.
6	Behaviors	Behaviors (sets of features over some time period) are constructed from either expert knowledge of threat signature components or components from accumulated non-threat normal data. Normal behaviors are derived by Principal Component Analysis (PCA) or grouping by machine learning (SVM, cluster analysis).
7	Classifiers	Normal behaviors will be scored to reflect the degree of anomaly determined with a machine learning binary classifier and threat behaviors will be scored to reflect the likelihood of a threat with a machine learning binary classifier. ML algorithms might include random forest or recursive neural network.
8	Awareness	The outputs of the behavior classifiers (scores and labels) will be processed via fuzzy logic to provide human-interpretable input to the system human-machine interface (HMI).

ACKNOWLEDGEMENTS

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

EthosEnergy
tdi technologies
SIEMENS

NATIONAL ENERGY TECHNOLOGY LABORATORY
U.S. DEPARTMENT OF ENERGY