MetaShield

MetaShield integrates Causal AI and Meta-Learning to transform threat detection for the critical infrastructure. By revealing cause-and-effect relationships in large datasets and dynamically orchestrating AI models in real time, MetaShield improves the accuracy, adaptability, and resilience of AI-driven detection.

MetaShield is an innovative cyber-physical security capability designed to enhance the resilience and protection of the critical infrastructure. By integrating Causal Artificial Intelligence (Causal AI) with Meta-Learning, MetaShield enables deeper understanding of cyber-physical data and how different AI models perform under varying conditions and attack scenarios. This approach supports real-time orchestration of AI models for threat detection, allowing the system to dynamically select the most appropriate model or combination of models for the data in a production system . The result is more accurate and adaptive anomaly detection, as well as improved explainability through causal insights. With is domain-agnostic and extensible design, MetaShield offers a transformative capability for securing the critical infrastructure against evolving cyber-physical threats.

Point of Contact/PI: Georgios Fragkos
Email: gfragko@sandia.gov

Key Capabilities

Causal AI & Meta-Learning Wrappers: Uncovers cause-and-effect relationships within cyber-physical data, enabling deeper understanding of threat mechanisms beyond correlation-based models.	**Real Time AI Orchestration:** Dynamically orchestrates and tunes AI models in real-time to adapt to new and unseen data, improving generalization and detection accuracy.
Enhanced Threat Detection: Reduces false positives and false negatives by combining causal insights with adaptive learning, resulting in more robust anomaly detection.	**Trustworthiness:** Offers insights into the decision-making processes of ML models, enhancing trust and transparency for operators and stakeholders.
Domain-Agnostic Framework: Designed to be applicable across various cyber-physical systems, not limited to	**Alignment with National Security Priorities:** Supports critical infrastructure protection goals by advancing state-of-the-art cyber-physical threat detection technologies.

specific grid configurations or technologies.	

Fig.: MetaShield-as-a-Service