# Cybersecurity Analytics using Integrated Machine Learning and Attack Graph Framework

Sharif Ullah, Sachin Shetty, Amin Hassanzadeh, Kamrul Hasan

## PROACTIVE THREAT ANALYTICS

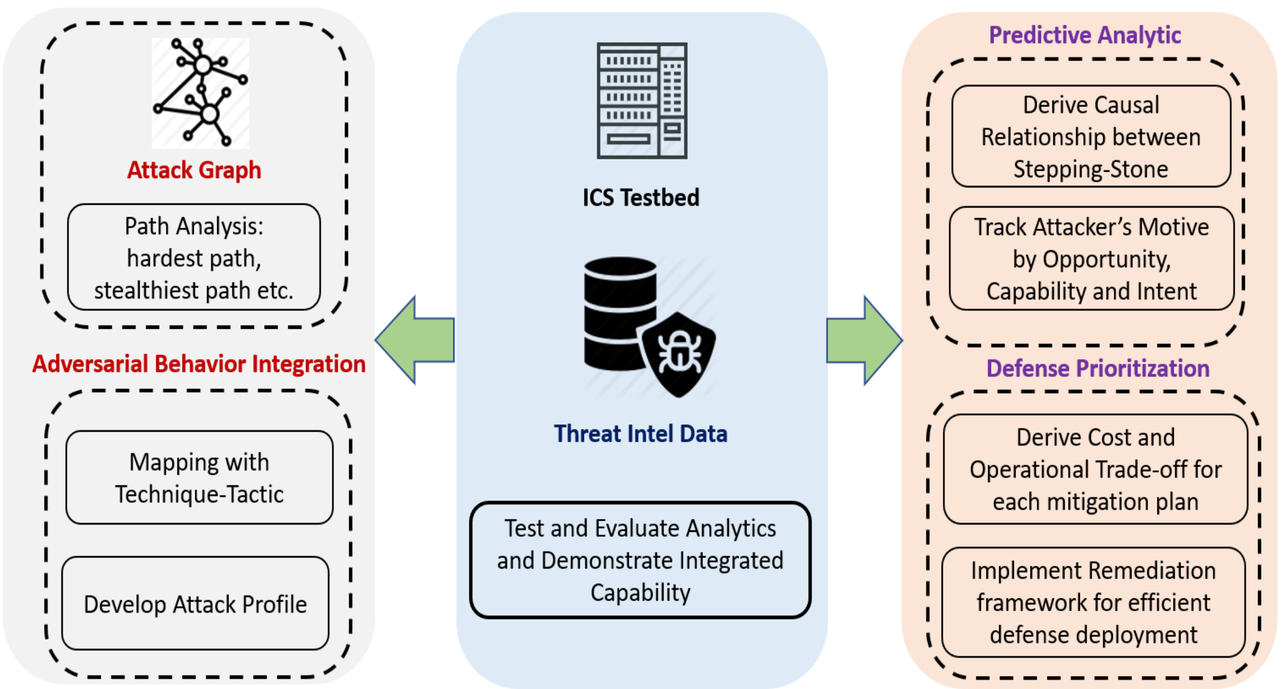
- Attacks are diverse in terms of techniques, progression and impacts; often follow a sequence of steps.
- In most cases, attack paths increase exponentially (state space explosion)
- There is a lack of detailed insight of each attack step.
- Security Operation Center (SoC) needs to act on prioritized response analytics.

## RESEARCH VISION

- Understand Adversary Strategy.
- Predict Attackers' movement into the system using TTP chain.
- Observe suspicious activity in the network and predict future action

**Integrate static network information with dynamic attack strategy**

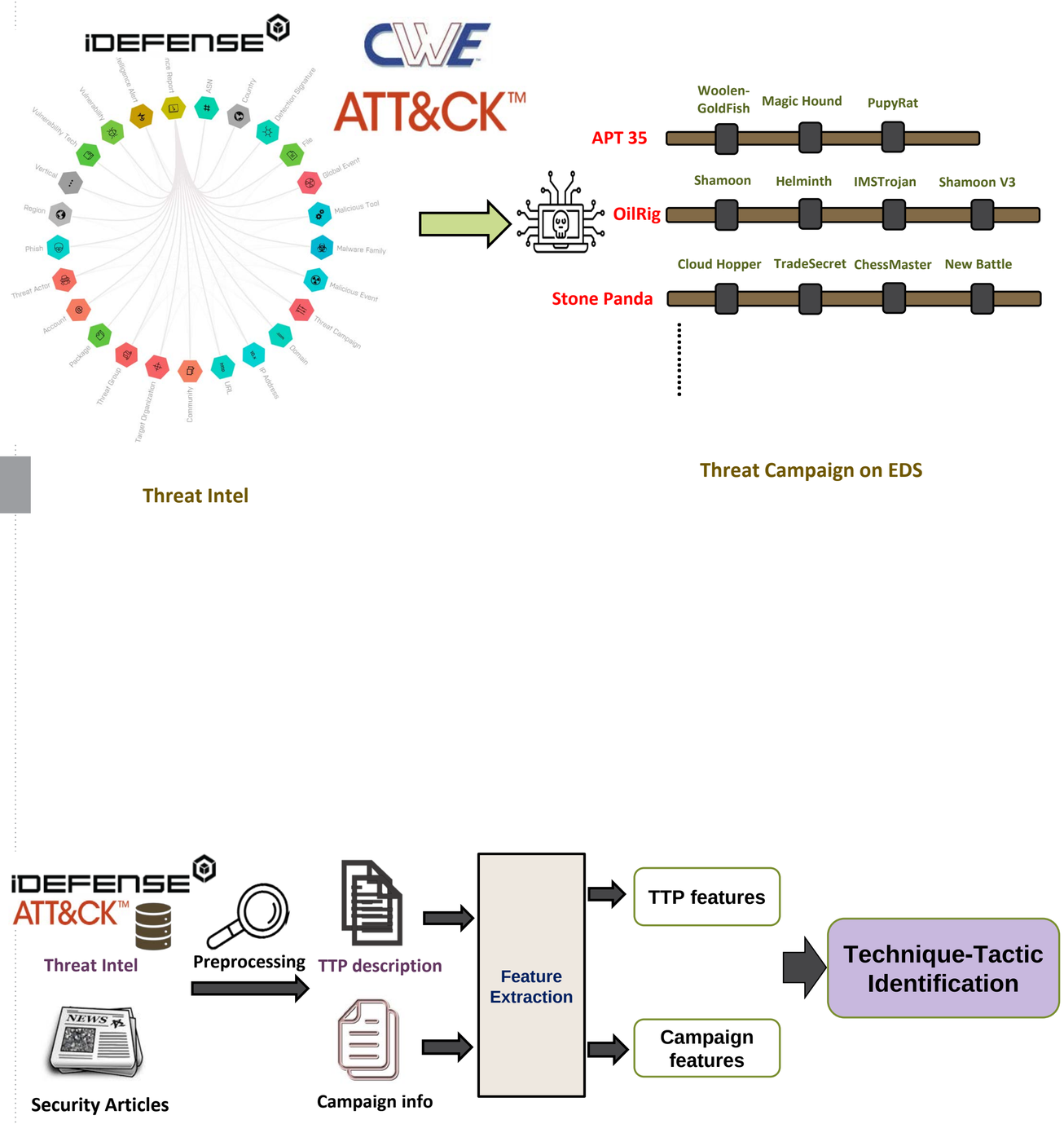
## APPROACH AND FRAMEWORK




Data driven cyber risk analytics framework.

- Map real network attribute to stepping-stones.
- Correlate adversary events to the attack surface.
- Characterize attack surface to potential cyber kill chain phases for different real-world threats.
- For a compromised set of stepping-stones, identify likely paths for responsible threats

## THREAT INTEL TO THREAT CAMPAIGN ON EDS




- Integrate threat intel to contextualize the threat campaign against EDS happened in the wild
- Use NLP techniques to extract semantic relationship between campaign and TTP features.
- Learn threat propagation sequence by our machine learning framework to identify attack pattern in attack graph (AG)

## BENEFITS

- Able to analyze attack progression from attacker's and defender's perspective.
- Uncover opportunity, capability and intent of a potential threat in the system.
- System security planner could efficiently incorporate our framework for proactive and reactive defense and mitigation plan in the system.

## COLLABORATION OPPORTUNITIES

Seeking collaborative opportunities from industry partners:

- EDS network infrastructure to investigate the risk of diverse adversarial exposure.
- Post compromise data of real attack on EDS.
- Evaluate the framework for assessing the risk and optimum remediation plan.

Contact: sshetty@odu.edu

Activity webpage:



FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY