Active learning in cybersecurity

SAND2017-7181PE

Cybersecurity is an adversarial environment with an evolving set of indicators and features.

Our tool: **Active Learning for Alert Triage (Candlestick)**.

- Work for DHS.
- Collects cybersecurity alerts, using SNL's SCOT tool (open/promoted/closed)
- Use standard machine learning (i.e., Random Forests) to classify alerts
- Use a budget to generate a list of low confidence open alerts
- Dramatically reduce classifier variance, using Query by Committee – Active Learning

Future Research Areas:

- **Model survivability and Concept Drift**
  - Length of model usefulness
  - Optimal retrain scheduling
- **Fast classification and clustering**