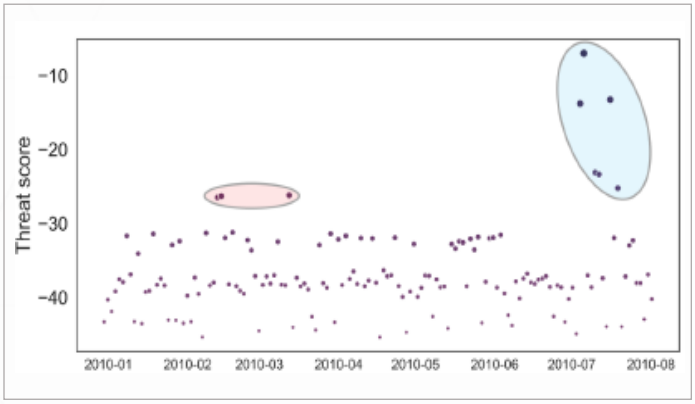
Advanced Cybersecurity Threat Detection Program

VTIP 20-090: "Probabilistic Programming-Based Insider Threat Reasoning and Detection"

THE CHALLENGE

In many cybersecurity settings there is a need to detect abnormal behavior patterns. These settings can include industrial espionage, insider threats due to disgruntled employees, or operational errors that result in data loss. Improved programs are needed to bolster cybersecurity efforts at large corporations to mitigate the risks involved with damaging online activities.



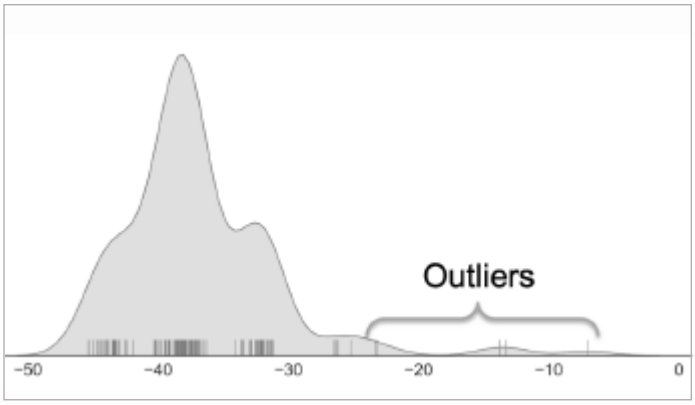
Threat score calculated from employee internet behavior data over the course of an 8-month period.

OUR SOLUTION

Researchers at Virginia Tech have developed a novel program for insider threat reasoning and detection. The system is an easy-to-use and easy-to-deploy solution for an organization to detect insider threat anomalies. The core of this system is the ability to sift through a huge amount of multi-attribute data and logs and recognize outlier user activities by modeling and capturing uncertainties associated with human behaviors.

Main benefits include:

- High accuracy
- Scalability
- Deployability



Normal distribution of threat scores.

CONTACT:

Grant Brewer
grantb76@vt.edu
540-231-6648