AbnorML

Advanced Insider Threat Detection Using Machine Learning

According to a 2018 study on insider threats in the federal government[1], 30 percent of respondents have experienced an insider breach or attack and over 60 percent indicate that insider threats are a priority for their agencies. Whether it is corporate espionage, sabotage, workplace violence, fraud, or an accident, insider threats are prevalent at federal agencies. The concern with the quantity of these threats is multiplied by the magnitude of the potential impact, especially involving sensitive systems and information. The destruction or theft of IT systems and data can lead to major financial and mission-critical impacts for any agency. SAIC developed AbnorML, a custom, adaptable, and extensible machine-learning (ML) algorithm to detect insider threats and further protect customers' mission-critical environments.

1 www.govloop.com/wp-content/uploads/2018/10/Insider-Threats-the-Danger-Within.pdf

SAIC®

INSIDER THREAT CAN MANIFEST IN A NUMBER OF WAYS, WITH A SUBTLETY AND COMPLEXITY THAT DEFIES RULES-BASED APPROACHES. AN INNOVATIVE ENSEMBLE ML/AI APPROACH CAN MAKE SIGNIFICANT IMPROVEMENT IN REAL-WORLD DETECTION IN ANY ENVIRONMENT.

Capability Highlights

MULTIPLE USE CASES

Use cases include behavioral analytics, MITRE ATT&CK techniques and tactics, and context-aware use cases that map a model of adversarial activity to user behavior, allowing identification of threats, data exfiltration, web proxy violations, unusual login behavior, and flight risk activity.

ADAPTS TO ENVIRONMENTS AUTOMATICALLY

AbnorML adapts automatically using a combination of unsupervised and supervised machine learning.

EASY TO USE FOR SOC ANALYSTS

Dashboards are very easy to read and provide immediate access to additional, enriching content for SOC analysts.

HIGH ACCURACY THREAT DETECTION

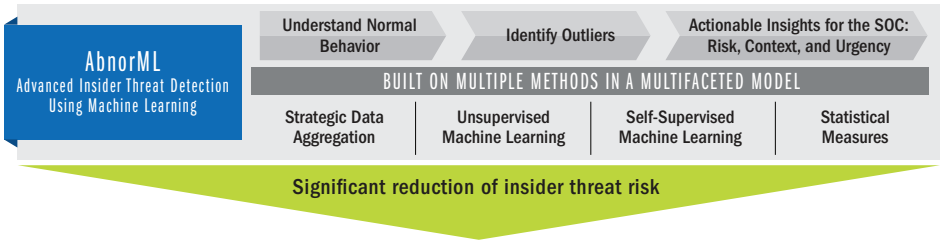
AbnorML was tested to ensure it identifies with accuracy insider threat use cases documented and categorized by the Carnegie Mellon CERT™ Insider.

AbnorML solves real problems for Security Operations Center analysts

Current user behavior analytic (UBA) solutions are expensive, hard-coded to specific data sources, and inaccurate. They are ineffective because they rely on the integrity of datasets, but perfect data does not exist in the real world, which has variable, complex environments. Based on scientific research and expertise and experience in cyber, SAIC created AbnorML to expand on existing solutions and address their shortcomings:

- Builds a baseline even in the presence of malicious activity
- Works with a flexible set of log files, including the ability to handle missing or messy data
- Maintains high true positives while reducing false positives
- Easily applied to any environment, no matter the maturity, breadth, or depth of customers' data repositories

AbnorML is built on a multifaceted model with multiple sub-models, each of which is built on one or more of the following methods: strategic data aggregation, unsupervised ML, and self-supervised ML. These models first understand normal behavior across available data in an arbitrary environment. Unlike other UBA solutions, during the training process to understand normal behavior, AbnorML does not make the baseless assumption that there is no current insider threat activity, resulting in a more-accurate normal environment understanding. AbnorML then identifies abnormalities and provides them to a Security Operations Center (SOC) team, giving context as to how risky an event or user behavior is, how urgent the related review or investigation needs to be, and what exactly the behavior is; for example, copying sensitive files to a USB drive. The models in AbnorML require minimal user intervention, tuning, and supervision after setup, which is only required when the environment has major changes.



SAIC, with AbnorML and other Cyber Situational Understanding (CSU) capabilities, provides a comprehensive advanced security threat identification solution with analytics, insights, and alerts. SAIC has customized over 50 rules native to the Splunk platform to align with the industry standard MITRE ATT&CK framework and has developed nearly 100 additional rules to more comprehensively cover the complete ATT&CK framework for known vectors. AbnorML allows SOC analysts to focus on what they do best by providing them actionable insights and freeing them from sifting through mountains of data to find a needle in a haystack. Customers realize significantly reduced risk of major financial loss, reputation damage, sensitive information exposure, and other harmful impacts caused by insider threats.

Contact

Russell Smith
703.676.4398
russell.j.smith@saic.com

Tyler Williams
703.350.6279
tyler.m.williams@saic.com

21-0421