patternex

The PatternEx Virtual Analyst Platform

A PatternEx White Paper

Introduction

One of the most frustrating realities in the Information Security field is the knowledge that, even though attackers leave clear traces in our logs, our security systems often can't parse through all of the available data fast enough, or with enough intelligence, to accurately detect an attack in real time without returning mountains of false positives.

Meanwhile, human analysts can, using their skill and intuition, hunt through the data and find these attacks—but this analysis is slow, and almost always occurs after the fact.

Our challenge is how to achieve this insight when it matters: namely, when the attack is happening. Horizontally scaling by hiring more analysts is not a good solution. The best answer lies in vertically scaling existing teams, by making them more effective across the board.

PatternEx was founded on the idea that Artificial Intelligence, combined with high-performance distributed systems, can augment the skill and intuition of a human Information Security Analyst, at scale and in real time.

AI^2: Artificial Intelligence Driven by Analyst Intuition

The notion of identifying behavior patterns from data has driven many recent innovations within Information Security. Much of this innovation uses Machine Learning algorithms to search through massive volumes of entity data in our logs, and to identify anomalous behaviors that may indicate malicious activity. This technology is known as Machine Learning Anomaly Detection (MLAD).

If the definition of Artificial Intelligence is "the ability of a system to perform tasks commonly associated with intelligent beings[1]," then MLAD fails to meet the AI standard. MLAD alone does not achieve the goal of emulating the intuitive abilities of a human analyst, because it

[1] https://www.britannica.com/technology/artificial-intelligence

does not learn from humans. In order for the system to achieve something similar to real-time human intuition, it must interact with a human who can tell it which of the behaviors it intercepts are actually malicious, and which are benign. The system must then learn from these course corrections, and automatically improve future predictions based on the feedback given.

This combination of human and machine is the core of the PatternEx vision: Artificial Intelligence (AI) driven by Analyst Intuition (AI), or AI^2. In fact, the only way to make Artificial Intelligence useful in Information Security is to have a process that presents high fidelity alerts to analysts, receives feedback about those alerts from the analysts, and then uses that feedback to iteratively build or tune new models. As this process is repeated, the models increasingly approximate a human analyst's skill and intuition, and adapt to the unique threat landscape the analyst faces. MLAD solutions that work without human input are vastly less efficient— not all anomalies are malicious. These approaches invariably generate numerous false positives which must be manually filtered out, taking valuable time from analysts.

> This combination of human and machine is the core of the PatternEx vision, what we call AI^2: Artificial Intelligence driven by Analyst Intuition.

Information Security: A Thin Label Space

The premiere challenge facing anyone who attempts to build an Artificial Intelligence solution for use in Information Security is the lack of training data, or "labeled data." By comparison, computers that learn to correctly identify a picture of a cat must be fed hundreds of thousands of labeled pictures of cats before they achieve human-like levels of precision. While the InfoSec world has millions of attacks, these are not labeled as such. The Information Security industry is what data scientists call a "thin label space," which makes it a difficult domain for true AI to penetrate.

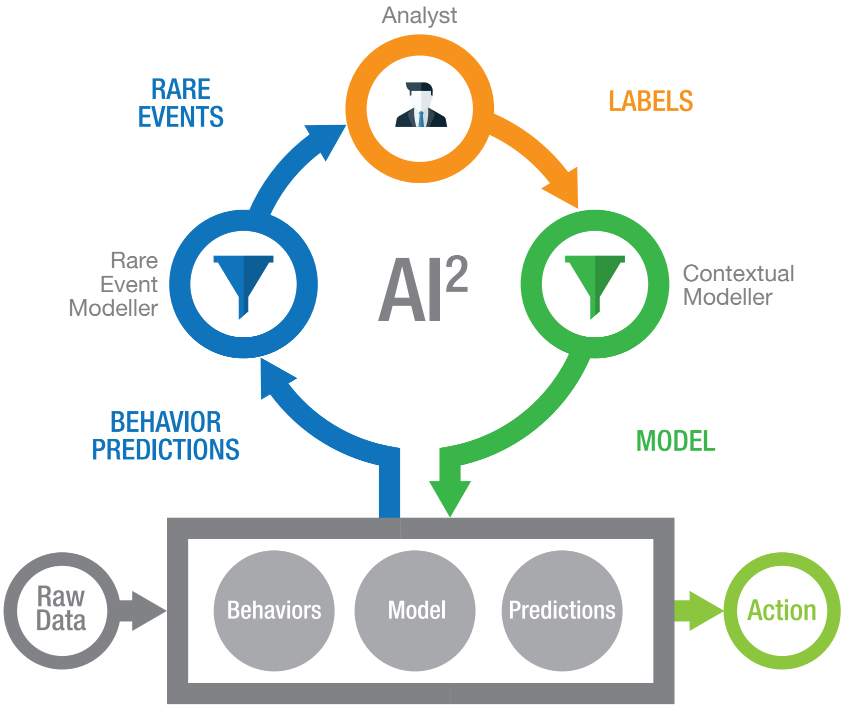
In Cyber Security, "labels" are the ground truth classification, by a human analyst, of a given behavioral pattern. The label is fundamentally either "malicious" or "normal"— although it is common to have more granular labels like "Insider Threat" or "Delivery." Labeling data is both time-consuming and expensive. Without labeled data, an AI system can't learn to distinguish between true attacks, and events that merely look like them.

Given today's environment of constantly morphing attacks, a learning system is necessary to defend our enterprise. The challenge, then, is figuring out how to generate labels inexpensively, and how to get the training data back into the system so that it can stay in tune with both the changing attack surface and changing attacks.

The good news: Information Security analysts are constantly judging whether the events they are monitoring and investigating are malicious or benign, they are generating labels all the time—but these labels are not directly available to the systems that need them. The first step toward solving this issue is a system that can absorb the analysts' judgments and turn them into labeled events for the AI. The next step is a set of algorithms that continuously look at labeled events in order to identify malicious patterns. This way, the moment a new malicious pattern is labeled, the system will automatically learn from it in real-time—and as the system accumulates labeled events, it will get better and better at emulating the analyst's' judgment.

Active Learning: The Key to AI^2

One AI-based approach to addressing thin label spaces involves a process known as "active learning." In active learning, an algorithm requests inputs from an external source in order to improve its own modeling capabilities. The goal here is to train our supervised learning models to separate data into semantically different categories—for example, "malicious behavior" or "benign behavior." Active learning is the most cost-effective way to take unlabeled data and organize it into labeled data that can be used for training.



PatternEx has developed an active learning technology that identifies new and evolving threats, gains context with the help of the analyst, and, once these threats are identified, develops new models that can directly predict attacks using behavioral descriptors. To achieve this, we designed a real-time, closed-loop Artificial Intelligence system in which the AI and the analyst continually feed information to each other.

There are four basic steps taken by this process, all of which must occur in real time:

- Automatically extract behaviors from raw data
- Model the data to find rare events
- Have a human analyst label the rare events
- Adjust the supervised models based on the analyst's labels

Over time, this process results in a supervised model that can accurately predict which label a human analyst would give any rare event. Below we take a look at each of these four steps.

Real-Time Behavioral Extraction

Attacks usually have a behavioral descriptor, or a "behavior," made up of the series of steps or events involved in committing that particular type of attack. The information used to quantify these behaviors is buried in the raw log data of one or more security devices. These items of data—known as "features" in the field of machine learning—are then extracted for a particular entity over a particular period of time. An entity may be any of a number of categories, including IP addresses, users, or sessions. PatternEx can scale easily to handling behaviors for all of the different entities across the whole body of inputs that it is examining.

The PatternEx platform is designed to horizontally scale so as to address billions of log lines per day.

- Process logs from a wide variety of data sources
- Extract entities and transform raw logs into behaviors
- Keep them up-to-date in real time on a rolling minute-by-minute basis

Rare Event Modeling

PatternEx combines three different outlier detection techniques, as attacks are rare and often exhibit distinctive behavioral profiles:

- Deep Auto-Encoders
- Matrix Decomposition
- Density Analysis

Combining these diverse techniques creates an superset model which is more robust overall, and can compensate for the individual biases of each separate model. We combine the outlier scores given by each individual method, and events must be given high scores by all methods in order to be shown to the analyst.

Analyst Feedback

To gain feedback from the analyst in the most efficient way, PatternEx sends over two items:

- Rare events with the highest score
- Predictions made by the platform based on the models currently running on real-time data

The analyst provides feedback to the AI by inputting labels into the PatternEx user interface in an offline mode, or through an API if there is already an automated system. Labels may also be accumulated through a process called Transfer Learning, which shares similar behaviors between different customers who have PatternEx deployed.

> Addressing today's threats requires real-time Artificial Intelligence to scale your team of Information Security Analysts across your entire enterprise.

Contextual Modeling

Next, the behaviors and their labels are fed into the Contextual Modeler. This is a collection of supervised learning algorithms that take the labeled data set and create a model that can predict attacks without the direct involvement of an analyst. This model is then put into use in the threat prediction platform.

Contextual modeling completes the loop: AI^2 leverages Analyst Intuition to create models, those models inform the analyst of newer attacks, and the analysts' feedback updates the models.This cycle captures the Active Learning effect of the human-machine interaction: the more attacks the predictive system detects, the more feedback it receives from the analysts, which, in turn, improves the accuracy of future predictions. As time progresses, and the system absorbs the analysts' feedback, there is a clear improvement in the detection rate.

Contextual Modeling has three phases:

- Training
- Deployment
- Feedback collection/updating

The algorithm cycles through these phases continuously. The set of behaviors and the labeled data serve as the algorithm's inputs. On an average day, the system trains a variety of predictive models. Next, it sends these models to the PatternEx Virtual Analyst Platform, applies them to incoming data, identifies a number of behaviors as events or attacks, and brings these to the attention of the analyst. The analyst then sorts through these events and picks out the ones that could truly be attacks, and the AI uses the analysts' deductions to build a new predictive model. The process then repeats.

Investigation Key Features

PatternEx Virtual Analyst Platform introduces two new key features that aid enterprises in protecting intellectual property, customer information, and confidential data: AutoCorrelate™ and Custom Analytics.

PatternEx AutoCorrelate automates the discovery of context between different types of data entities such as IP addresses, connection or session data. AutoCorrelate can learn what interactions between entities are malicious and which are benign. This provides far greater context for an analyst by presenting cluster visualizations rather than raw lists of data points. This additional context also reduces the number of false positive alerts that analysts need to chase while increasing the rate of accurate detection.

Currently, analysts write complex correlations by presupposing what an attack looks like. But as attacks morph, those correlations quickly become stale, generating massive amounts of false positives. PatternEx AutoCorrelate uses AI to map out all of the connections visually and requires no foreknowledge of a given attack. With this dynamic visualization, companies can speed up their investigations 20x by automatically discovering new and evolving correlations.

PatternEx Virtual Analyst Platform also includes Custom Analytics, which gives users the ability to do deeper analysis or extract deeper information from raw logs. Analysts can write SQL queries or use Python/Scala/Perl to visualize the data they are analyzing. These reports can be shared amongst analysts to enable collaboration and threat hunting. These new features improve investigation speed and enables analysts to share their knowledge across the company and PatternEx ecosystem.

Conclusion

Today's environments are both complex and constantly under attack from a wide variety of sources. Staying secure in the face of constantly changing attack surface and innovative attacks requires using all the tools at our disposal—both machine and human. The PatternEx platform combines analyst intuition with state-of-the-art machine learning and statistical modeling techniques to improve real-time attack detection, and to reduce the time between detection and prevention.

Results published in our latest paper, "The Research Behind Active Contextual Modeling": shows the PatternEx system achieving a 10x improvement in detection rates over state-of-the-art anomaly detection systems, along with a 5x reduction in false positives. Because the platform automatically learns and improves with each incident, and can learn from the experiences of other companies in the PatternEx network, it is the only system with the capability not only to detect, but also to predict—the threats of both today and tomorrow.

How To Contact Us

For more information or to request a demo, send your email to info@patternex.com or go to www.patternex.com/demo

Trademarked names appear throughout this paper. Rather than use a trademark symbol with every occurrence of a trademarked name, names are used in an editorial fashion, with no intention of infringement of the respective owner's trademark.

The information in this paper is distributed on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author nor the company shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this paper.

patternex

PatternEx
4620 Fortran Dr., Suite 202
San Jose, CA 95134

www.patternex.com