patternex

Brochure

Introduction to PatternEx

Transforming cyber security analysts into super heroes with a Virtual Analyst Platform.

AN ARMY OF SECURITY ANALYSTS ON YOUR SIDE

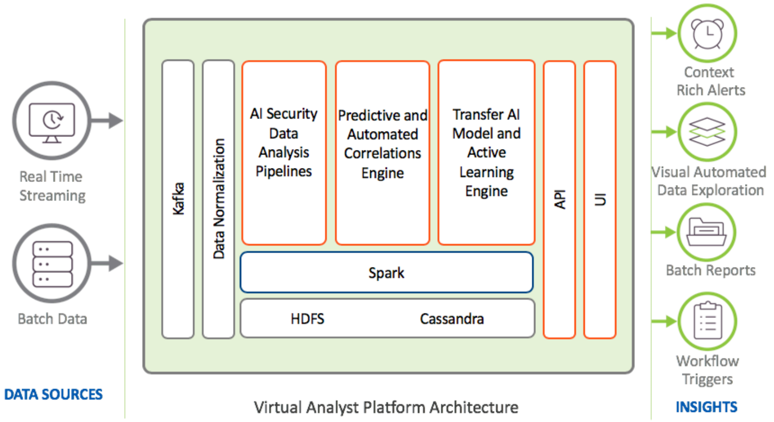
PatternEx turns cyber security analysts into super heroes – enabling detection of 10x more threats, at 1/5th cost with automated and crowd sourced based AI attack detection models. PatternEx's Virtual Analyst Platform automates threat detection with "out-of-the-box" AI that covers most threats; and provides hunting-based analyst models to capture unique or highly sophisticated threats. The technology leverages active learning for automated learning to detect threats earlier in the attack kill chain. Customers such as enterprise, MSSP, and MDR vendors all use PatternEx to decrease costs, increase security, and enhance value to their users.

> *What is needed is something built from the ground up to detect threats that traverse multiple tactics and entities over long time horizons. PatternEx's concept of 'virtual analysts' does exactly that, and has helped improve our SOC efficiency." – Thomas Whang, Impelix*

MORE COST-EFFECTIVE DETECTION

PatternEx provides re-usable and shareable AI models to find threats across multiple environments, users, and customers – all without having to write or tweak any rules. And your staff does not need to understand AI to use the platform. That is the power of AI.

By detecting more threats, earlier in the kill chain, the expensive process of analyst to analyst hand off gets shortened, saving your organization time and money. In addition, the advanced threat hunting capabilities in the platform mean you will have concrete answers, faster for your executives.


Real Time Streaming
Batch Data
DATA SOURCES
Kafka
Data Normalization
AI Security Data Analysis Pipelines
Predictive and Automated Correlations Engine
Transfer AI Model and Active Learning Engine
Spark
HDFS
Cassandra
API
UI
Context Rich Alerts
Visual Automated Data Exploration
Batch Reports
Workflow Triggers
INSIGHTS

Virtual Analyst Platform Architecture

FLEXIBLE, EASY TO DEPLOY AND SCALE

With various levels of operation, from "out of the box" ready to detect to more sophisticated analysis capability, PatternEx's Virtual Analyst Platform serves security analysts of all skill levels and technical leaders looking for reports and effectiveness of the enterprise security efforts and risk posture. No other vendor has the ability to provide self-detecting, out of the box models that will detect threats with no false positives AND provides analyst enhanced capability to train the AI models for more sophisticated threat detection. In addition, with advanced correlation capability, threat anticipation is made fast – so you can see an issue days before your threat intel feed .

Benefits

- Reduces security analyst time spent on false positives and false negatives without specialized skills
- Built-in hunting analysis platform with pre-defined attack stories and threat anticipation
- Validate effectiveness of current security tools and processes
- Works in historical, real-time, on-premises, and cloud modes for flexible deployments

Provable Results

Based on technology validation from MIT's AI CSAIL LAB (20x faster, 10x more threats detection, and 80% cheaper)

"System learns to defend against unseen attacks ... the detection rate shows ... improving by 3.41× with respect to a state-of-the-art unsupervised anomaly detector and reducing false positives by more than 5×." – MIT 2016

About PatternEx

PatternEx, based in San Jose, CA, was founded in 2013 by researchers from MIT's Artificial Intelligence Lab CSAIL. The company has backing from Silicon Valley legend Vinod Khosla (Khosla Ventures). Learn more at patternex.com or follow us on Twitter @patternex.