patternex

Detecting and Preventing Business Logic Abuse

A PatternEx Solution Guide

patternex

Problem

"Business Logic Abuse," is the collective expression for the fraud and breach that happens when a criminal uses the normal functionality of the site in an unauthorized manner. Examples include things like Account Takeovers, Sweepstakes Gaming, Inventory Freezing, Web Scraping, Click Fraud, DDoS, Gift Card Fraud, and Testing Stolen Credit Cards.

Business Logic Abuse is an extremely difficult—and constant—problem for organizations for three reasons: a) it occurs via legitimate functions of the web app; b) there is a significant gap between what is required to detect it and what is available in the market today; and c) the ownership of the issue is not clear.

Criminals take part in these activities both to make money and to damage brands. The Ponemon Institute surveyed over 600 firms globally and estimated that business logic attacks cost any given firm an average of $7m per year.

Current rule-based technology is no match for these attacks, which are virtually invisible to existing solutions like SIEMs or IDS/IPS.

Current rule-based technology is no match for these attacks, which are virtually invisible to existing solutions like SIEMs or IDS/IPS. These solutions are looking for known malicious signatures that a rule can block. However, the hallmark of a Business Logic attack is that the attacker is using your web application as it was designed.

Current Solutions Are Fundamentally Lacking In Key Areas

Currently, there are two kinds of InfoSec technology solutions: those that are 'analyst-driven' and those that are 'anomaly detection'-driven. Both have important shortcomings when faced with business logic abuse scenarios.

Analyst-Driven Solutions:

Analyst-driven solutions include such products as network firewalls, Fraud Detection/ Prevention systems, SIEM's, and Intrusion Detection and Prevention Systems (IDPS). Fundamentally, they are tools that allow analysts to create rules that allow or deny access to a user. And while these are a necessary component to your security posture, they are not sufficient.

Rules-based approaches have a high rate of undetected attacks. A rule, by definition, is something that reacts to a new attack; it prevents historical attacks from happening again. Rules-based solutions can not "see"—much less prevent—new and emerging attacks. Given that Business Logic Attacks use the site as intended, rules are particularly bad at stopping them.

A second problem is the delay inherent to analyst-driven solutions. Once the attack is discovered, a human must create, test, and validate the rules that prevent the attack from happening again—in the meantime your company remains exposed.

Finally, rules are detectable and solvable. While rules remain static, cyber-criminals are constantly adapting their behavior, testing the rule until they find a way to circumvent it and re-establish their fraud or breach.

Approach	UnSupervised Learning (No Labels)	Supervised Learning (Static labels)	Active Learning (Dynamic labels)
Real-time (learning continuously)	Anomaly Detection for UBA		$(AI)^2$: Active Learning + Analyst Intuition
Batch (Learn offline)	Anomaly Detectors	Offline Fraud models	

Anomaly Detection Solutions

The new class of emerging solutions based on machine learning hold promise, but fall short in critical areas. These "anomaly detection" products discard static rules in favor of statistical models that determine when certain events are outliers. While these solutions tend to do better in the detection of new attacks, they suffer from high levels of false positives while still containing some important vulnerabilities.

The major failing of these anomaly detection products is not in their capability but in their approach. While they can execute complex statistical analyses to identify anomalous events, the results they generate lack context. Not all anomalies are malicious, but generating alerts tied to anomalies means you generate many false positives.

The impact of too many false positives is severe: analysts become fatigued from seeing too many alerts; they then begin to distrust the system that generates false alarms, and eventually abandon the system.

Time to solution is also an issue. Anomaly detection (AD) products require a "baseline" of behavior upon which they can identify outliers. To do so, AD solutions require 90 days of data to form the baseline. Malicious behaviors in the baseline data may not appear as outliers to the machine learning solution, leading to blind spots in your defenses.

Behavior Patterns

The basic IT infrastructure generates terabytes of logs daily. Your firewalls, load balancers, and active directory all capture all the steps an attacker takes when they are defrauding or breaching you.

This information is called the "behavioral pattern" and is buried deep in your log data, and it holds the key to determining the difference between a legitimate user of your website or a criminal abusing your code.

Machines can process massive amounts of data and extract complex patterns, but without a human to guide them, they generate false alarms.

A Change In Perspective — And Approach

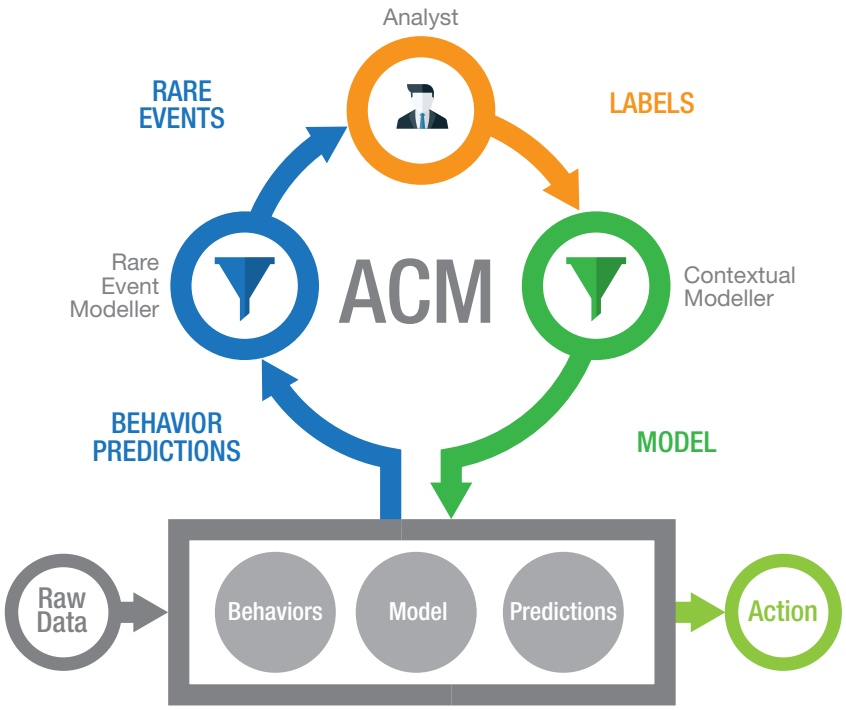
What is needed is a fundamental change in thinking and approach. Where analyst-driven or anomaly detection systems have important shortcomings, PatternEx combines the two into a powerful concept called $(AI)^2$.™

The heart of this concept is the notion that humans and computers each have different—and complementary— strengths. Machines can process massive amounts of data and extract complex patterns, but without a human to guide them, they generate false alarms. Humans excel at things like context, nuance and understanding implications. Combining these strengths yields a powerful solution. With a human training a machine, the machine will eventually be able to mimic the human's intuition to make value judgments about the implications of complex patterns at tremendous scale.

Patternex Threat Prediction Platform

The PatternEx platform combines big data infrastructure with human security expertise and artificial algorithms into a proprietary solution that can predict, in real-time, when you are being defrauded through business logic loopholes. The result is the industry's first Threat Prediction Platform.

The PatternEx Threat Prediction Platform is an end-to-end AI Platform for fraud and breach detection. For the first time, enterprises can now quickly and accurately detect malicious user intent. If malicious intent is confirmed, the system automatically engages your existing defenses, in real-time, to challenge/delay/block the user. Such an approach can detect both historical and emerging threats for both fraud and breach.



Active Contextual Modeling

If the vision is $(AI)^2$, then Active Contextual ModelingTM (ACM) is that vision at work. ACM is the patent-pending system that takes raw data and ultimately delivers highly actionable alerts for your Security teams.

The first step in the ACM process is to ingest all the relevant log data from your IT infrastructure. PatternEx then transforms those logs into quantifiable identities and behaviors. From there, the data are run through a combination of Artificial Intelligence models to produce a highly focused list of alerts for the analyst. The number of alerts addressed is determined by your analyst team based on their bandwidth and perceived importance of the alerts. The analysts review the alerts and can use the ACM-generated data to assess the alerts and label them as an attack or not. That analyst feedback updates the Artificial Intelligence models to be even more precise. The PatternEx Platform then can instruct your system to challenge, delay, or block the malicious user automatically via an API connection.

Benefits

By augmenting your InfoSec team with the PatternEx platform, you can:

- Gain visibility into previously invisible cyber attacks
- Receive real-time alerts enabling you to take immediate preventative action
- Reduce the risk of brand damage
- Reduce the risk of data exfiltration

With PatternEx, Business Logic Abuse problems are stopped as they unfold.

Conclusion

The key to detecting Business Logic Abuse is to monitor user behavior and ultimately predict user intent, ideally before the fraud occurs.

Malicious actors misusing your site behave differently than legitimate users and these behaviors are already being captured in your logs. What is required is a platform that can distinguish between these two. Combining machine learning models with Analyst Intuition is what enables the PatternEx platform to pinpoint these malicious behaviors. As the system is trained by your team, it becomes a virtual analyst for you, analyzing behavior patterns and assessing the implications of those patterns as massive scale.

With PatternEx, Business Logic Abuse problems are stopped as they unfold, and before the hacker can extract sensitive information or make an unauthorized purchase.

Deployment Options

We offer the PatternEx solution as a software package, available as a service, in your private cloud, or on premise. Your requirements are basic: stream log data to into PatternEx, review the real-time user behaviors, and provide feedback.

How To Contact Us

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

PatternEx is an Artificial Intelligence security company that has developed a Threat Prediction Platform to identify malicious user intent. The PatternEx solution enables security analysts to detect and prevent cyber attacks in real time, at scale.

patternex

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

www.patternex.com