fractal

The evolving role of AI in effectively combating cybercrime

Rohit Kewlani, Principal Consultant, Fractal Analytics

The vast proliferation of data, faster computing, digital detonation, and the need for continuous innovation to stay ahead of cyber criminals has put the cybersecurity industry at an interesting inflection point, needing a radical paradigm shift in the way we foresee cyber businesses operating in the near future. Cybercrime is increasingly becoming prominent in every boardroom's agenda, as it is costing businesses across industries nearly $118bn annually, and the role of cybersecurity experts is undoubtedly gaining more relevance in today's ever-evolving IT landscape. This paper discusses in detail how cyber security officers can respond more proactively and more effectively to cyber threats using AI & machine learning techniques.

Despite the sophistication in tools and technology and machine learning driven solutions available out there, cybersecurity officers have been barely successful in bringing down the time it takes to acknowledge an attack 'after it has happened', let alone stay ahead of the curve and predict the next breach or attack much before the attackers strike the first blow.

As per a recently published Verizon Data Breach Investigation Report, more than 50 percent of data breaches go undetected for several months. And most of the traditional approaches tend to focus on just aggregating data around malware, hacking attempts, identity thefts, data breaches, phishing campaigns, etc., translating these into threat signatures (digital fingerprint of the attack) and then analyzing streams of historical/real-time data for finding similar patterns/behaviors. Not so surprisingly, owing to our adversary's inventiveness, cybersecurity criminals have always been one step ahead in terms of constantly advancing and fine-tuning their attack strategy to circumvent existing systems and finding newer innovative ways to threaten organizations.

Cybersecurity officers today are looking to employ a more advanced, intelligent and less human-intensive system to proactively monitor cybersecurity threats and mitigate them in order to reduce cost, prevent fraudulent activities from happening in the first place or even improve the efficacy of their current cybersecurity implementations. And when the rules of the game are changing at such an unprecedented pace, agility and the right attitude to let go of the old rules and learn new ones is no longer a matter of choice but rather a necessity to avoid the extinction event.

Having said that, the critical questions that loom unanswered are:

- **How can** cybersecurity officers break this endless loop of playing a catchup game with cyber criminals and have an advantage in the game? How can they tackle evolving fraud?
- **How can** they properly channelize investments to handle the volume and complexity of today's cyber-attacks?
- **How can** they move beyond the current sub-optimal approaches of maintaining black-lists and adopt a more signature-free security approach?
- **How can** they truly differentiate between an actual/genuine human activity vs intentional misconduct and minimize false-positive alerts?
- **How can** they proactively detect out-of-normal behavior by analyzing real-time data streams from multiple network and infrastructure assets to uncover threats in real-time?
- **How can** they automate interventions based on severity/criticality/ complexity of the threat event as well as the risk appetite of the organization?

Growing Beyond a "Reactive" Signature-Based Methodology

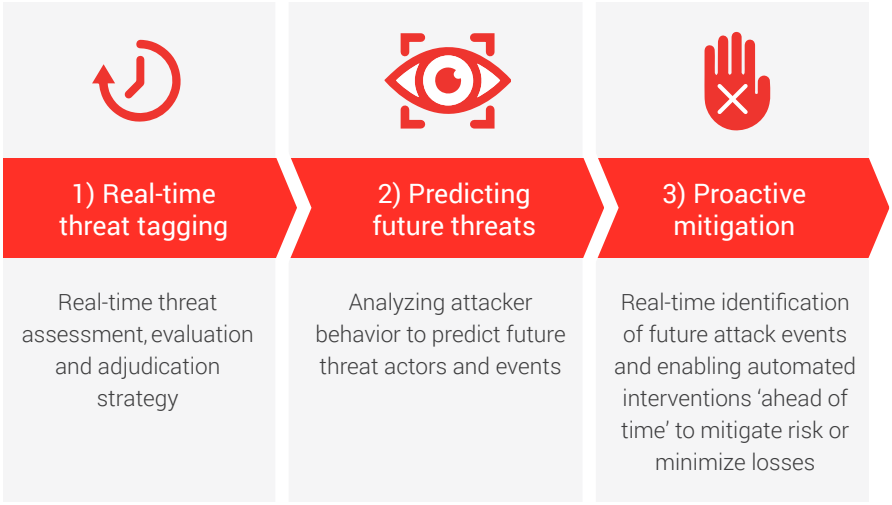
A cyber-attack, security breach, hacking attempt or security threat is not identified until after the event has occurred. Organizations today are looking for options to rapidly mitigate threats in order to avert ramifications associated with retrospective identification, rationalize spends and opportunity cost tied to the investment, and also implement a robust, scalable cybersecurity strategy which caters to their future needs.

Fraudulent behavior or misconduct in this context must be looked at through a different lens, a new perspective which most of the traditional approaches don't cater to today. Most current implementations out there look at historical evidences of attacks and potential breaches from 'known' sets of events. Instead of just gleaning over individual areas of anomalous behavior, we should mathematically define 'what is normal'; the reason being fraud is ever-evolving.

By following this approach, we should be able to understand and digest the nuances of what is "Not Normal". And by doing so, we have a higher likelihood of uncovering out-of-normal activity, improving overall detection, automating incident investigations, improving threat containment and implementing better threat aversion strategies.

An Innovative Approach to Combating Evolving Cyber Threats

Using the following three-phased approach, businesses can establish a System of Intelligence for end-to-end cyber threat prediction, detection, prevention and intervention in real-time, thereby improving the overall cyber threat remediation process.



1) Real-time threat tagging

Real-time threat assessment, evaluation and adjudication strategy

In this phase, historical cyberthreat activity and potential threat actor information will be used to determine what is 'normal' and what is 'not normal'. When normal is understood, a model will be developed to identify all non-normal activity which will flag incoming real-time activity from IR tools (incidence reporting) or logs/events from systems, applications, network, security devices and other sources. These events will then be bucketed into various 'known' threat categories (threat types defined based on historical incidences plus SME knowledge) and unknown/undefined events which could be newer forms of evolving threats (discovery of new trends and behavioral patterns).

In real-time, the potential threat events that are flagged 'At Risk' will be adjudicated through RPA systems (robotic processing automation) based on client's risk appetite or severity/criticality/complexity of the threat involved and associated downstream effects. For example, if you have a vendor or contractor, Edward Snowden, downloading copious amounts of data and has done the same thing "X" number of times over a certain period, he will be referred to for human investigation vs an email/text/pop-up message if it's just the first attempt. Similar anomalies in employee and/or vendor/contractor behavior can be brought to light ahead of time and adjudicated for early mitigation.

2) Predicting future threats

Analyzing attacker behavior to predict future threat actors and events

Build profiles of the top 5-10 percent of cyber criminals responsible for extreme threat events in the past by analyzing their longitudinal digital footprints over elongated periods of time, plus profiles of 'known' threat types and finally ideal profile(s) for a user who had a genuine digital/web activity.

Based on these profiles, build a mathematical model to predict WHO is a potential threat actor and WHEN will they indulge in a potential cyber threat activity.

When these events are predicted, a Robotic Processing Automation (RPA) system shall be implemented to contact the concerned party using the ideal outreach channel (email/text/pop-up window/phone call) based on the event's risk score, organization's risk appetite and/or employ a human investigator to intervene for a corrective action.

3) Proactive mitigation

Real-time identification of future attack events and enabling automated interventions 'ahead of time' to mitigate risk or minimize losses

This phase combines the results from phase 1 and 2 with unstructured tertiary inputs from cybersecurity SME's and/or external world events to make the system more intelligent and reduce false positives or negatives.

This phase will drive compliance and education (via training, behavioral coaching, etc.), decreasing the amount of non-compliance, avoiding mistakes from genuine users and/or averting actual intentional cyber threats. This phase will help detect and stop threats ahead of time, and shorten time to remediation when attacks occur (using next best action).

Conclusion

Cybercrimes are growing exponentially, faster than what most business could decipher and embrace the winds of change. Naysayers will perish, existing market incumbents will be toppled and early winners shall rewrite the underlying business fundamentals, disrupting the marketplace in ways unimagined. Cyber business across the globe should get attuned to this new operating model paradigm shift. The situation may seem insurmountable unless businesses are equipped with the right set of tools/technologies and knowledge partners to help. "AI-driven" cybersecurity implementations behold the future for businesses bracing up to flip the markets again.

It's the tip of the iceberg, or just scratching the surface—call it what you may! There's a new cybersecurity story waiting to be etched in history, and it's being driven by AI and powered by analytics.

fractal

Fractal Analytics is a strategic analytics partner to the most admired Fortune 500 companies globally and helps them power every human decision in the enterprise by bringing analytics & AI.

Fractal Analytics has presence across 12 global locations including the United States, UK and India and has been recently featured as a leader on Forrester Wave™: Customer Analytics Service Providers, 2017. Fractal has also been recognized as "Hot Artificial Intelligence (AI)" company by Forbes and a "Cool Vendor" and a "Vendor to watch" by Gartner.

©2018 Fractal Analytics, Inc., all rights reserved

Learn more at www.fractalanalytics.com

For more information, contact us at:
+1 201 469 0600
info@fractalanalytics.com

Follow us