ZoneFox

WHITEPAPER

ZoneFox
Augmented Intelligence (A.I.)

Empowering the Super-Human Element in Your Security Team

Introduction

In 1997 Gary Kasperov, the chess Grandmaster, was beaten by a computer. Deep Blue, designed by IBM, had played Kasperov before in 1996 and beaten him in the first game of a six-game match eventually losing to Kasperov 4-2. After a year's worth of tweaking and heavy upgrades Deep Blue finally defeated Kasperov in a re-match.

Although Deep Blue derived most of its power from brute-force analysis - it was, afterall, able to analyse 200 million potential moves per second. The story shocked the world because for the first time, human intelligence had been challenged - and surpassed - by a machine. "The Brain's Last Stand", read the Newsweek headline.

But in the years after his defeat to Deep Blue, Kasperov started experimenting with AI so he could study its impact on chess, and it was during this time that he formulated the 'Advanced Chess' League, allowing humans to play with the assistance of machines. This later evolved into a 'freestyle' chess event where it was found that the best results were obtained with a combination of both humans and computer assistance.

This realisation that a combination of AI and human characteristics delivers the best insights is what drives the ongoing development of ZoneFox. The information security industry has been party to many a silver-bullet, but in recent years, with the growth of well-funded adversaries as well as the chronic and continuing data-breach issue, attitudes have changed in relation to being better prepared to identify and respond to an incident rather than simply defending against it.

In this whitepaper we will provide you with an insight into how the latest developments in Machine Learning, combined with the ZoneFox Augmented Intelligence (A.I.) design philosophy can provide you with the insights you need to quickly and easily identify threats to your organisation - and empower your security team to act quickly and confidently.

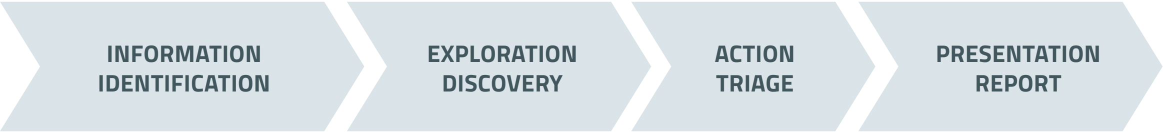
A Changing Information Security Landscape

When it comes to Information Security, historically we've been good at stopping people from doing things, for example with access control, firewalls and so on - at least when they work, or have been configured properly! We've also been OK at detecting commonly known attacks such as malware, certainly once they've been around for a while. But we've been really bad when it comes to providing insights into human behaviour or advanced malware. Why? Because of our traditional reliance on static rules. They're easy to subvert, and hard to update dynamically. SIEM came to the rescue to try and provide us with a greater insight into patterns of behaviour, but that too isn't as effective as we first thought.

The class of solution that implements something called User Entity Behaviour Analytics (UEBA) has started to become particularly useful. User behaviour has been a hard problem due to the fact that human behaviour is erratic and hard to predict. People can be very sneaky about removing data from your organisation. Where UEBA becomes really useful is its ability to provide a level of flexible pattern recognition which rules are unsuitable for, and which humans simply can't achieve due to the excruciatingly large amount of data involved. And that's where ZoneFox steps up to the plate.

ZoneFox Augmented Intelligence

Organizations use ZoneFox to assess and mitigate risk to their businesses, and in doing so, they follow the threat investigation pipeline:



INFORMATION IDENTIFICATION

EXPLORATION DISCOVERY

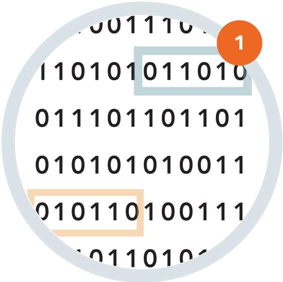
ACTION TRIAGE

PRESENTATION REPORT

ZoneFox supports this pipeline through rule maintenance and alert monitoring, to case management and investigation, and finally reporting.

At the moment, within an organization these activities are mostly manual, with rules having to be created and maintained, and the necessity to find related events not directly associated with an alert - something which can prove really difficult. Overall, this puts constraint on more detailed investigations and impacts breach detection and response time. Our solution is ZoneFox Augmented Intelligence.

AI is the next generation in UEBA threat detection and investigation built using UBA on top of the existing ZoneFox platform. AI optimises each stage of the threat investigation pipeline and results in automated detection and blazingly fast investigation of anomalous behaviour. It's built on four pillars; Machine Learning, User Driven Data Mining Visualisation and Augmented Intelligence..



Machine Learning

People don't normally steal information, so AI performs UBA using machine learning to spot when a user's behaviour changes. It's really that simple.

More specifically? AI analyses data across multiple dimensions and applies Bayesian probability metrics to produce complex mathematical models of user behaviour. These baselines allow AI to flag deviations from the norm in real time - allowing you to discover previously unknown anomalous behaviour.

To build these user profiles, AI observes historical and real time user data, until it has enough to accurately encompass normal behaviour. This is the 'training' stage - which is fully automated, meaning no hand holding required. It also has a rapid turnaround time, allowing it to start detecting anomalous behaviour in just a few hours.

However, turning people into mathematical models loses some information. With only this approach, AI could detect someone behaving abnormally - but not know why, or what exactly led up to it. We have to be able to take into account that a user could be behaving differently because, say, they've switched roles in an organisation, or because they're taking data in advance of their resignation.

But machine learning is a means to detect abnormal behaviour, not a path to complete autonomy. With just machine learning, you run the risk of drowning in a sea of un-actionable alerts.

User Driven Data Mining

Our brains are wired to pick out patterns and seek explanations for everything we encounter. By supporting human judgement and empowering our thought processes over artificial correlations, ZoneFox lets you prioritise what's important and relevant.

AI scales with your organisation, allowing comprehensive investigation at every level of detail and encouraging exploration through simple, obvious interfaces and inherent discoverability.

ZoneFox AI works on behalf of you, learning from the anomalies you find most valuable, and feeding this information back into its user behaviour models to screen out irrelevant detections - so as you learn from the system, the system learns from you. Coupled with machine learning, ZoneFox enables users to drill down and actively explore data complex relationships connecting multiple anomalous events - intuitively and fast.

Visualisation

ZoneFox AI displays data so that you can rapidly prioritise high risk anomalies. Each visualisation clearly expresses the shape of the data, accentuating high risk anomalies while giving you a bird's eye view of user behaviour.

And separate visualisations which share attributes are grouped together to allow fast correlation of disparate anomalies. We want our users to draw accurate conclusions faster through simple visual similarity and intuition. After all, this is where humans excel.

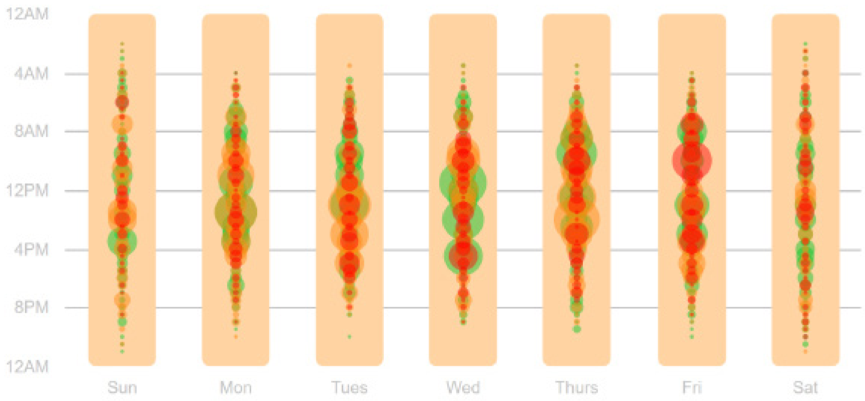


Fig. 1 Risk intensity - weekly view

Augmented Intelligence

Computers have always worked on behalf of users - and for the foreseeable future that's unlikely to change. They were made for algorithmic examination of data at scale. Humans have intuition: the ability to zero in on abstract conclusions. We can investigate while piecing together the reason behind a user's action.

Teaching a computer how to decode someone's intentions is difficult, since our thought processes are non-algorithmic and differ wildly from person to person. No-one can understand human behaviour better than a human. AI is more than an artificial human substitute. We don't want to replace users, we want to empower them. We believe that the solution to detecting anomalous behaviour is a fusion of human and machine: Augmented intelligence.

About Zonefox

ZoneFox is a market leader in User Behaviour Analytics that help secure your business-critical data - and backs it all up with a proven track record of protecting reputation, sales revenue, and competitive advantage. Bottom line? Really great Insider Threat protection that works the way your business needs it to, and not the other way round.

Like to Learn More?

www.zonefox.com/ai

youtube.com/zonefoxvideo

@zonefox

alerts@zonefox.com

Argyle House,
Edinburgh,
EH3 9DR

☎ 0845 388 4999

ZoneFox