LogRhythm®
The Security Intelligence Company

The rise of AI-enabled threat detection

How artificial intelligence adds crucial context to the pursuit of threats

LogRhythm
The Security Intelligence Company

The pace and complexity of cyber attacks mean organisations need to employ cutting-edge tools for effective threat detection

The modern threat landscape is evolving at an increasingly rapid pace. As a stream of news headlines will attest, corporate networks are at risk, and most are likely to be compromised. Indeed, 79 per cent of surveyed organisations said they were breached in 2016[1].

Today, organisations need to pay close attention to the six stages of the cyber attack kill chain to best protect themselves. These are reconnaissance, initial compromise, command and control, lateral movement, target attainment and, finally, exfiltration, corruption and disruption.

The further down the kill chain an attack goes, the more damage an organisation will experience and the higher the likelihood the brand will become headline news for all the wrong reasons.

Rapid detection of threats before they cause damage is therefore crucial for all organisations. But this capability is not always what it should be. In 2016, the average time it took for an organisation to realise it had been breached was 99 days[2] —more than enough time for significant damage to take place.

Hackers and malware now operate very quickly, making rapid threat detection an increasingly important capability. In addition, threats are becoming more complex, meaning traditional detection isn't always up to the job.

Threat detection needs to become more sophisticated if it is to pick up the kinds of threats that are increasingly affecting organisations.

In 2016, the average time it took for an organisation to realise it had been breached was 99 days

[1] CyberEdge 2017 Cyberthreat Defense Report http://www.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/Webroot_Q3_2017_CyberEdge_Cyberthreat_Defense_Report.pdf
[2] M-Trends 2017, Mandiant Consulting https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

LogRhythm
The Security Intelligence Company

Context is key

With a growing proportion of attacks conducted via compromised credentials, even apparently expected behaviours within the network can't be discounted. For example, what appears to be a user with privileged access uploading sensitive information to a cloud storage site could be the action of malware or compromised credentials.

To be effective, detection systems need to know the types of roles people in an organisation have, what systems they have access to, and what data should be transferred by individual employees. This is information only individual organisations will know, and so they need to ensure that it forms part of the dataset that security detection systems analyse.

In this way, security systems will understand the activity that individuals within an organisation generally undertake. If a member of staff wants to perform a task outside their normal routine, security systems should step in to verify whether it's a genuine request.

> Artificial intelligence can recognise significant changes in user behaviour that suggest a security risk

The need to add this contextual information is particularly important when you consider that many organisations are moving security operations to the cloud and employing managed service providers.

These providers won't know the relevant contextual information that will help fight modern cyberthreats, so organisations have a responsibility to provide this data to bolster the security services they receive. After all, if a major breach takes place, it will be the customer's name that makes the headlines, and rarely the service provider's.

How AI can help

Another area of development that can add the context needed to bolster threat detection—particularly for user-based threats—is artificial intelligence (AI).

The most dangerous threats are often the ones that are most difficult to discover. This is particularly the case as threats increase in number and complexity, while organisations grapple with staffing shortages, false alarms and inefficient manual workflows.

Analysts in the security operations centre need to be able to offload time-consuming tasks to focus on important problems that require their expertise, while better analytics are used to discover the threats that may otherwise go unnoticed. AI and machine learning can help deal with these challenges.

AI can be applied against environmental data to detect previously hidden threats and enable rapid qualification and investigation.

LogRhythm
The Security Intelligence Company

Used in this way, AI provides analysts with evidence-based starting points for threat hunting and powerful data visualisations for machine-assisted qualification and investigation. It is particularly useful for monitoring high-risk users, such as those in IT, finance and senior executive suites.

Artificial intelligence can recognise significant changes in user behaviour that suggest a security risk. Combined with field-proven threat models, it can support in-depth analytics to detect known and unknown threats and improve prioritisation of issues for further investigation.

The value of continuous learning

By applying models of user behaviour, artificial intelligence and machine learning, SOCs can pick up changes in how users interact with the IT environment, allowing them to pursue all manner of user-based threats.

AI can take into account the context needed for effective threat detection by mapping disparate user accounts (e.g. VPN, work email, personal cloud storage) and related identifiers (user name, email address) to individual user identities to create baselines of behaviour.

By associating highly-detailed models of user behaviour to an identity, all relevant user activity will be accounted for during analysis. These baselines can then be profiled against a historical baseline of that user's activity, as well as those of the user's peers.

The beauty of AI is that it learns from the environment to protect against current and future threats, and continuously evolves without manual intervention. It can also be trained by analysts during normal investigation activity to accelerate its learning process.

Tools like LogRhythm's CloudAI can detect insider threats, compromised accounts, administrator abuse (and misuse), and other user-based threats. LogRhythm's CloudAI provides the means to accelerate threat detection by adding the context needed to prioritise investigation efforts. To find out how you can power your SOC with AI, contact LogRhythm.

About LogRhythm

LogRhythm is the pioneer in Threat Lifecycle Management™ (TLM) technology, empowering organisations on six continents to rapidly detect, respond to and neutralise damaging cyberthreats. LogRhythm's TLM platform unifies leading-edge data lake technology, artificial intelligence, security analytics and security automation and orchestration in a single end-to-end solution. LogRhythm serves as the foundation for the AI-enabled security operations centre, helping customers secure their cloud, physical and virtual infrastructures for both IT and OT environments. Among other accolades, LogRhythm is positioned as a Leader in Gartner's SIEM Magic Quadrant.

www.logrhythm.com