About the author

George Smyth joined Rocket Software in 2005 and leads the company's R&D Lab in the UK. He has more than 30 years' IT experience, both in management and development positions. He started his IT career at IBM UK before moving to IBM Silicon Valley Lab in California and is now senior director, R&D at Rocket.

References

1. Barlyn, Suzanne. 'Global cyber-attack could spur $53 billion in losses: Lloyd's of London'. Reuters, 17 Jul 2017. Accessed Jul 2017. www.reuters.com/article/us-cyber-lloyds-report-idUSKBN1A20AB.
2. Palmer, Danny. 'Security? What security? Four million data records are stolen or lost every day'. ZDNet, 28 Mar 2017. Accessed Jul 2017. www.zdnet.com/article/security-what-security-four-million-data-records-are-stolen-or-lost-every-day/.
3. 'Europe's Insider Threats: What CISOs Need to Know'. Forcepoint. Accessed Jul 2017. https://www.forcepoint.com/pt-br/node/10561.
4. '2015 Information Security Breaches Survey'. HM Government/PwC. Accessed Jul 2017. www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf.
5. 'Bupa data breach affects 500,000 insurance customers'. BBC News, 13 Jul 2017. Accessed Jul 2017. www.bbc.co.uk/news/technology-40595581.
6. 'Ponemon Institute Study: Reputation Impact of a Data Breach'. Data Breach Today, 27 Jan 2012. Accessed Jul 2017. www.databreachtoday.co.uk/whitepapers/ponemon-institute-study-reputation-impact-data-breach-w-540#dynamic-popup.
7. 'How long since you took a hard look at your cyber-security?'. Verizon. Accessed Jul 2017. www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.
8. Woodie, Alex. 'Forrester Sees Steady Growth for Big Data, Hadoop, and NoSQL'. Datanami, 16 Sep 2016. Accessed Jul 2017. www.datanami.com/2016/09/16/forrester-sees-steady-growth-big-data-hadoop-nosql/.

Can artificial intelligence help in the war on cybercrime?

Danny Maher

Danny Maher, HANDD Business Solutions

It is hard to avoid the buzz in the industry around artificial intelligence (AI) and associated technologies such as machine learning, deep learning, automated network monitoring and user and entity behaviour analytics (UEBA). Exciting as is it to hear these buzzwords, AI is in fact not a new concept. Yet suddenly we are starting to see it being applied more broadly and more enthusiastically by companies as tools in the fight in an increasingly challenging cyberwar.

But why now? Largely it's down to scale, with computing power, data and storage capabilities all increasing. Where there are large quantities of data, AI comes into its own, able to process and analyse huge volumes of data to predict trends and information far more quickly than ever before. In security terms, this means the ability to analyse new threats, vulnerabilities and attack vectors, which can help mitigate against future attacks. AI is being pitched as a key weapon in the armoury of organisations looking to increase their risk posture and stay one step ahead of the hackers.

AI certainly has a role to play – an important one. But it should not be seen as a panacea for curing all of security's ills. Like any application of artificial intelligence, AI within security is not a tool in its own right but needs a level of human interaction to enable it to constantly improve – for example, to learn to avoid false positives or understand new methods of attack devised by hackers. What it does do is to take on the more repetitive, time-consuming and potentially costly tasks of individuals sifting through large quantities of data, freeing them up to focus on more important tasks.

The reality is that AI alongside skilled individuals can be combined to create a very powerful and important aspect in an organisation's defence in the war on cybercrime. But how is it being used today and what is the potential for AI?

The role of UEBA

UEBA is a term coined by Gartner but the same concept is also defined by Forrester as security user behaviour analytics (SUBA) or more generally just as user behaviour analytics (UBA). Whatever term you use, UEBA is used for threat detection, using advanced analytics to baseline network activity to identify malicious

behaviour from external sources. More importantly, today it can also help in the fight against insider threats.

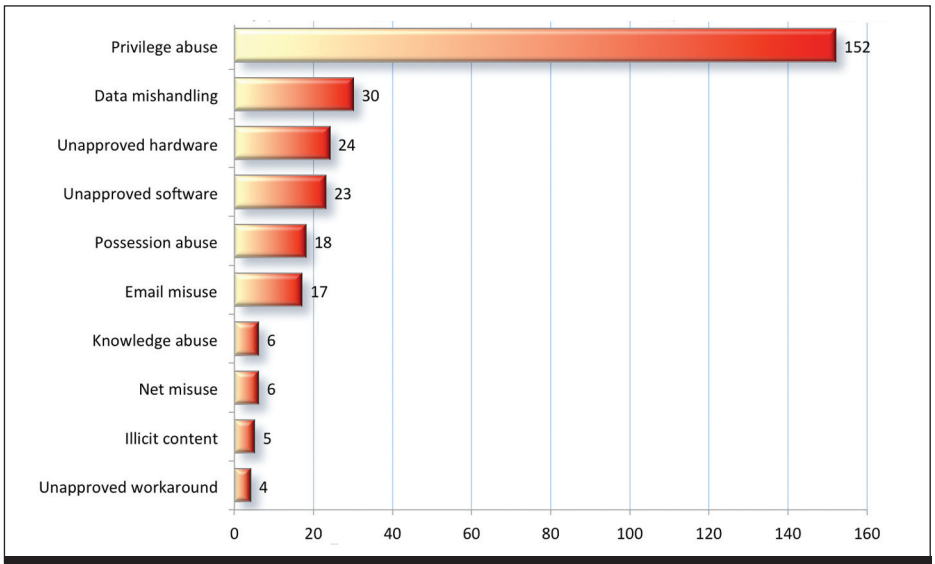
When it comes to insider threats the issue is rarely malicious behaviour on the part of an employee, but rather unintentional or negligent behaviour. According to Verizon's 2016 Data Breach Investigations Report, accidental insider threats accounted for 30% of security incidents in 2015.[1] More often than not, employees are just not educated enough about security best practice. Whether they open a phishing email or click on a malicious link, attackers are invariably waiting for one employee to slip up. In cases of negligence, employees will try to find ways around the security policies in place, so instead of abiding by strict controls on data sharing, for example, they decide to use a public cloud file-sharing application to make their job easier. Unfortunately this can expose them and their colleagues to attackers.

"SIEM only throws up what a security team tells it to. It assumes that the security team is always aware of everything in a constantly evolving threat landscape"

A recent survey seems to back this up, with nearly half (43%) of IT professionals saying that while employees are a company's greatest strength, they also pose the biggest challenge to data security.[2] More than a fifth say that the behaviour of individuals and their reaction to phishing attacks is a major risk to the business.

Malicious activity

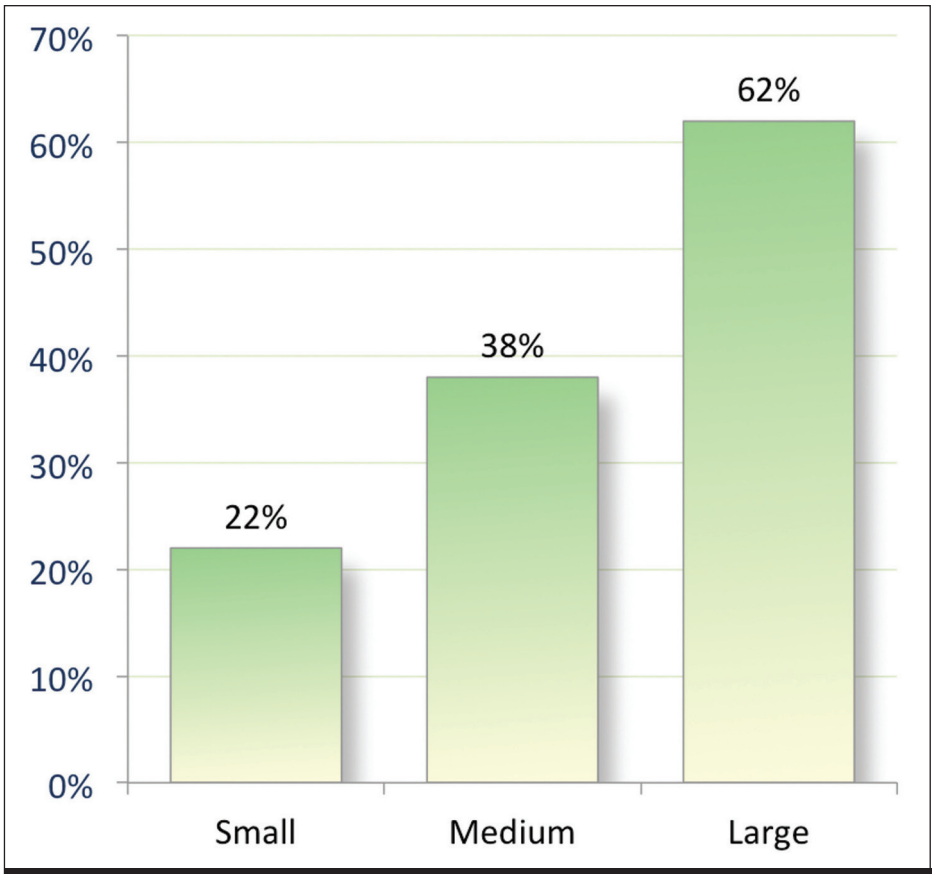
But we cannot dismiss malicious activity either, which is often overlooked as businesses focus on external threat agents. There are going to be times when someone within an organisation is motivated by financial gain or is disgruntled with their employer and may be tempted to steal data or pass it onto a competitor.



Types of misuse in insider and privilege abuse breaches. Source: Verizon '2016 Data Breach Investigations report'.

In this instance, UEBA automatically learns what is normal based on typical activity and then, using proprietary algorithms, assigns risk scores to potential malicious behaviour. Alerts provide close to 100% accuracy, thus helping to identify the risk and to protect an organisation before a threat becomes a major issue.

If an organisation is already using some form of security information and event management (SIEM), they might expect it to do this already. But there is a major difference between SIEM and UEBA. SIEM only throws up what a security team tells it to. It assumes that the security team is always aware of everything in a constantly evolving threat landscape and is able to configure



Businesses where staff have had cyber-security training in the past 12 months.