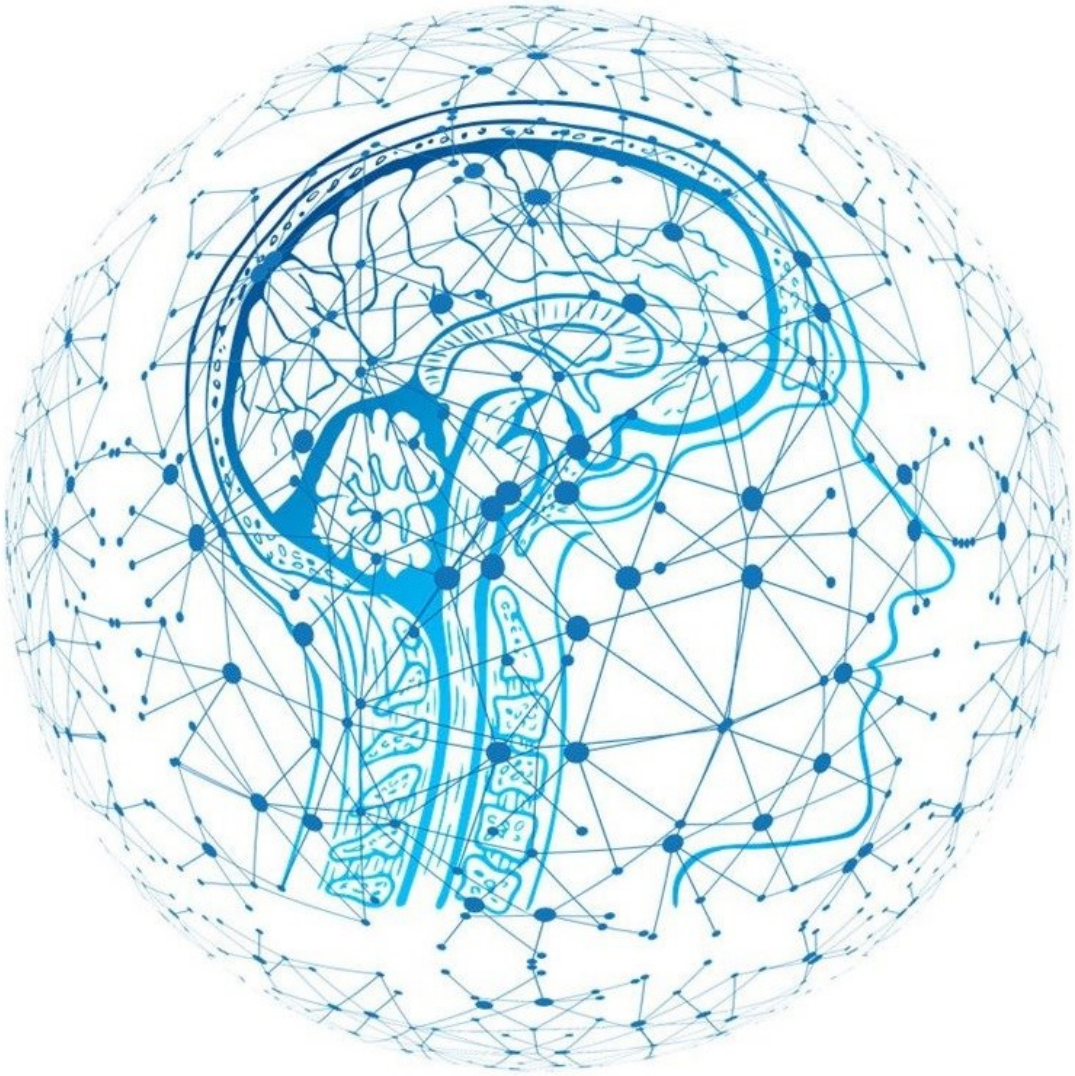
BIZCOMMUNITY

Adding threat intelligence to the security mix

By Simon Campbell-Young

26 Nov 2018

Today's threat landscape is so complex and fast-paced, it is impossible to prevent every threat or attack. The criminal organisations behind cybercrime are well-funded and have the technical skills to stay ahead of mitigation tools and techniques. They target technologies and the human weakness to find their way into corporate networks.



Source: pixabay.com

This is compounded by the fact that companies rely heavily on technology and connectivity, putting their data and systems at risk.

And these risks are not just about money - over and above financial losses, there is catastrophic damage to reputation to consider, as well as steep regulatory fines which can see a business close its doors, permanently.

One thing is certain, and that is that no organisation, either in the public or private sector, can hope to match the resources of today’s cybercriminals.

No sooner has a business got a handle on one type of threat, another raises its ugly head. Cybercriminals are constantly changing their tactics, widening the attack surface, and developing new tools and techniques to bypass even the most sophisticated security solutions.

Evidence-based knowledge

This is where threat intelligence comes in. Gartner describes threat intelligence as “Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.”

Threat intelligence can have a significant impact on a company’s ability to anticipate security incidents before they happen, which in turn, enables them to react more quickly to mitigate any potential damage, as well as put defence tools in place before the attack, and proactively fight a breach when it occurs.”

Know how to handle threats

Having insight into who might be behind the attack will enable an organisation to act decisively and appropriately, knowing how to handle a specific advanced persistent threat (APT), as they will already know how it works, and can block the avenues it uses to infiltrate the network.

For example, a certain cybercriminal group will be known to target specific types of information or systems, and a business can allocate defence resources accordingly.

Businesses today simply must find a way to add threat intelligence into their security strategies and integrate it into every aspect of security operations. Threat intelligence will provide the necessary information that could indicate the business is in danger of a breach.

It looks for specific indicators, and known cyber criminal activity, offering situational awareness and a deep understanding of the threat landscape. It gives insight into who might see your business as an attractive target, and what they might be after.

Predict what could happen

However, it goes beyond simply gathering this type of information.

Threat intelligence must be fully integrated, and tailored to offer actionable, accurate, relevant and timely reporting on any potential dangers. It isn’t a silver bullet by any means - it’s about the best guess. By understanding the past, it can help to predict the future, and highlight any probably targets for hackers. Essentially, it’s keeping an outward eye on the global threat landscape, to help a business prepare the strongest defences possible.

Threat intelligence is about predicting what is likely to happen, based on several different factors, which gives the security team the ability to be proactive in defence and on the look-out.

Adding threat intelligence into the security mix guarantees that all possible bases are covered, and the organisation is in the best place to not only prevent breaches, but identify a breach that is taking place in enough time to mitigate and manage the situation, so that no valuable data is compromised, and with it, the organisation's reputation.

ABOUT SIMON CAMPBELL-YOUNG

Having started his career as a startup partner for FSA Distribution in 1990, Simon Campbell-Young went on to start his own company called Memtek Distribution in 1995. This was sold to a public company called Siltek Holdings between 1998 to 2000. Shortly thereafter, he took his experience in the technology sector, garnered over more than 23 years, to form specialist distribution company Phoenix Distribution in 2000.

- Adding threat intelligence to the security mix - 26 Nov 2018
- Digital forensics is crucial to the security chain - 6 Nov 2018
- App permissions can be used to exploit your data - 26 Oct 2018
- 57 million riders, drivers affected by Uber breach - 13 Dec 2017
- Prevention through awareness - 12 May 2014

View my profile and articles...