The great threat intelligence debate

Darren Anstee

Darren Anstee, Arbor Networks

Cyberthreats continue to evolve, with ever-more complex attacks being used and with a wider spectrum of motivations behind them. Cyber-attacks can be launched for extortion, vandalism, ideological hacktivism, data theft and financial fraud with all kinds of attacks being regularly featured in the news. For example, ransomware has seen huge growth in the past year or so, highlighted most recently with the global WannaCry/NonPetya cyber-attacks.

On the technical side of things, toolkits and weaponised attack capabilities are readily and cheaply available within the cyber-criminal community, where a whole sub-economy exists. And, of course, we have state-associated threat actors who have significant resources behind them to develop, utilise and release (to the broader community, for obfuscation purposes) new tools and exploits.

"Threat intelligence can be anything from statistical data on the kinds of threats being detected around the world by a specific vendor's solutions, through to specific indicators of compromise and the tools, techniques and procedures used by a cyber-criminal"

To best protect our organisations from these threats, businesses need to leverage the capability and expertise available across the industry, sharing intelligence to multiply their organisation's capabilities. This is something at which the cyber-criminal community has become increasingly adept.

What is threat intelligence?

If you search for 'threat intelligence' on Google, nearly 11 million results pop up. It has become an industry buzzphrase, but it describes a broad range of data types that can be used in different ways to (sometimes) solve different security problems. However, threat intelligence isn't a 'cure-all' that will magically protect us from the threats we face. The value we can get from threat intelligence is very dependent on how we apply it.

The first thing to address is the 'what'; threat intelligence can be anything from statistical data on the kinds of threats being detected around the world by a specific vendor's solutions, through to specific indicators of compromise (IOCs) and the tools, techniques and procedures used by a cyber-criminal. All of this information can be useful, whether it is to help organisations plan and prepare for attacks or more directly during threat detection, investigation and containment.

"Simply pushing all the threat intelligence we can acquire into a security information and event management (SIEM) system or detection stack is not a recipe for success"

Getting hold of threat intelligence is easy, as there are so many sources available. However, getting the right intelligence and integrating it into our security technologies and processes so that it effectively reduces our business risk, is much more difficult. If we get it right, it can make a big difference, but as with many areas of security the challenge is to turn another source (or set of sources) of data into real visibility and value.

In the security industry we have had a tendency to accumulate data without visibility and value. We all know that it is much easier to understand a trend by looking at a graph rather than a column of numbers. And in many cases, we have worked to build out many, many columns of numbers and very few graphs (metaphorically speaking). We have to be careful that we use threat intelligence in a way that enhances our abilities, without simply adding complexity to our existing processes.

Judging intelligence

Good threat intelligence is timely and relevant to the organisation using it and the data and processes being protected. Simply pushing all the threat intelligence we can acquire into a security information and event management (SIEM) system or detection stack is not a recipe for success – for example, using threat intelligence designed to identify a specific threat to an industrial control system (ICS) environment within a financial organisation. This could generate (more) false positives for our security teams to wade through – reducing our effectiveness.

Machine consumable threat intelligence can be used to provide both initial threat detection and context around detections. The latter is potentially more important in a world where we all have way too many events to process and where we need to quickly establish what represents a real threat as quickly as possible.

Turning threat data into intelligence is all about linking elements together and establishing context – in effect, collation and analysis. In most organisations, people still make the decisions in security and intelligence that improve a responder's ability to understand the risks behind a given detection. But building in context and what other elements to look for can be hugely powerful.

"People make decisions in security – and detections of suspicious behaviour using complex mathematical models that cannot be explained to the analyst are not actionable"

Similarly, human consumable threat intelligence is also hugely helpful as it can allow analysts to better understand their adversaries. Knowing our enemies and their likely tactics is important, as it can allow us to find things that may otherwise have been missed. Intelligence can help organisations to link together disparate behaviours and detections into an overall threat or campaign so that we understand the true risk. And it allows responders to better focus their time and resources on what matters the most.

Common ground

The one thing that most threat intelligence has in common is that it describes a known threat or behaviour. This means that someone else, such as a research team or a patient zero, has already spent the time and effort to research (or experience) a threat. In other words, most threat intelligence can only be addressed as a subset of the problems that we face today. However it is valuable, because dealing with known threats as quickly and automatically as possible can free up time for our analysts to focus on the unknown and harder-to-find threats. Attackers are increasingly using more stealthy techniques that can't be readily described by a signature or piece of reputational data (eg, stolen usernames and passwords) in order to gain access to our networks.

Dealing with these kinds of threats requires broader visibility and behavioural or policy-based mechanisms of threat detection. Traditional threat intelligence isn't useful (per se) in detecting these kinds of incursions, but some vendors are now providing mathematical models and behavioural fingerprints within their feeds to help their solutions detect more stealthy and sophisticated threats. This can work well, but avoiding false positives can be a challenge and we have to be wary of detections that cannot be understood or explained by our analysts. As mentioned earlier, people make decisions in security – and detections of suspicious behaviour using complex mathematical models that cannot be explained to the analyst are not actionable. For instance, no-one will quarantine his CEO's laptop if he can't understand why or if an event represents a real problem.

"What matters is stopping the attacks that represent real business risk before they come to fruition. Anything we can do to improve our chances is a positive, especially if it speeds up our processes and reduces the burden on our security resources"

Threat intelligence is a valuable part of our security toolkit and it can help to improve the efficiency of our security teams when applied in the right way. As with most tools, though, it is the skill of the users and their processes that determine the overall effectiveness. Having the right human skills in security is the most important thing, as people are very good at identifying unusual behaviours and activities and intelligence has a part to play here as well.

Hunting for threats

Threat 'hunting' is a more proactive approach to identifying and containing threats. Hunting is all about following a breadcrumb trail of unusual or suspicious events and activities, and the right intelligence can help join the dots here. Hunting can help us to unearth high-risk threats that would otherwise have remained hidden so that they can be investigated and contained before attackers achieve their goals.

To start hunting, businesses need to define what and how attackers are likely to target. Hunting requires a different mindset on the part of the analyst and a different toolset that allows data to be visualised so that unusual behaviours become apparent, so that data can be quickly explored. Hunting is all about following hunches and tools that support this activity provide a more interactive view of threat and traffic data than is traditionally available from forensic tools.

Hunting is an example of a more proactive approach to security, but in many cases budgets are still heavily skewed toward preventative and reactive technologies and processes. Preventative controls are still important, but we all know that we can't stop everything from getting in. What matters is stopping the attacks that represent real business risk before they come to fruition. Anything we can do to improve our chances is a positive, especially if it speeds up our processes and reduces the burden on our (usually scarce) security resources. Intelligence can help us here.

Act now

Intelligence is something that will continue to grow in importance and is a key part of the security toolkit that can help organisations protect themselves. The way we think about intelligence will evolve though, away from IOCs and purely reputational data, as more organisations and solutions start to utilise more complex forms of intelligence. This will allow organisations to identify bad actor behaviours and techniques using shared mathematical models, behavioural fingerprints and hunting.