Building an effective threat intelligence platform that would make Einstein proud

Leon Ward

Leon Ward, ThreatQuotient

It seems as though everyone is talking about threat intelligence at the moment. Nearly every security vendor wants to get in on the action and the majority of security operations groups are either being told by their management to get on board with it, or they've attended various security conferences and realised they need to add threat intelligence into their security programme for the year.

That said, the questions most security operations groups always come back with are: What sort of threat intelligence should I get? How do I use it effectively? How is it going to help me? And perhaps the best one – what is threat intelligence? We'll get to the Einstein bit soon enough.

Evidence-based knowledge

Gartner has defined 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."[1] By all means, this is a good definition but what does it all mean? And, how can threat intelligence benefit organisations?

Defending a business and its customers against cyberthreats starts with understanding what you're up against. Now, that may sound pretty obvious; studying the adversary is a common practice in many situtations. In sports, for example, even in nature, it's done all the time. So why then, when it comes to cyber-security, instead of looking outward, have organisations become accustomed to traditional security approaches that start at the perimeter and focus inward? In today's increasingly connected and digital world it is important to expand this perspective, looking outside the walls of the enterprise, as well as in.

"Threat intelligence platforms (TIPs) allow security teams to become more proactive and anticipatory by profiling not only the attack, but attackers who rapidly change their tools, techniques and procedures to evade defensive technologies"

To establish a solid foundation for intelligence-driven enterprise security, what's needed is a way to bring all this global data together in one manageable location, translate it into a uniform format and correlate it with local data, events and context. With all the threat data in one place and usable for ingestion, analysis and exporting, organisations will be well on their way to expanding security perspectives and better defending against cyberthreats.

That's where the platform comes in. Threat intelligence platforms (TIPs) allow security teams to become more proactive and anticipatory by profiling not only the attack, but attackers who rapidly change their tools, techniques and procedures to evade defensive technologies.

Experience shows that a threat intelligence platform that's worth its salt has the potential to help organisations in three key areas: to communicate more effectively, to focus resources more efficiently and to manage risk more successfully. These are by no means the only areas of an organisation's security strategy that will feel the benefits, but here are some thoughts on why they are the top three.

Improve communication

At some stage in their career, every CISO or SOC manager will be asked by management, concerned about the latest reported hack: "What do you know about it? How does it affect us? What are we doing about it?". Though not explicitly stated, the underlying assumption here is that preventative measures have already been taken to ensure that such an attack will not occur on their organisation.

This is where a solid threat intelligence strategy is key, providing individuals with a means of being proactive and ensuring that they're on top of their cyber-security. As a result, security teams will then be in a position to answer these questions before they are even asked.

Leaders also want a way to answer these questions in business terms in order to let management know what is being done by the security operations group. Effective threat intelligence provides all of the information needed to change the conversation from 'a million events were blocked this month' to 'ransomware attacks were stopped that would have cost the company £2m'.

Focus resources

On a network, there are only three things security operators need to deal with – noise, nuisance and threats. The noise needs to be filtered out, blocking it at the perimeter or detecting it and automatically remediating. Threats need to be focused on – they are the real rascals that can negatively impact shareholder value. And nuisances need to be determined as simply noise or rather an actual threat that needs to be dealt with accordingly.

An effective threat intelligence platform helps organise the threats and provide the information needed to isolate what really matters. It provides security teams with a means of automatically filtering the noise while also enabling threat intelligence enrichment through an analyst workbench to understand and address the nuisances. In short, a good TIP lets an organiation operationalise its approach to cyber-security.

Manage risk

Once an organisation begins to use threat intelligence to improve communications and focus its resources, it can begin to dive into risk management. A threat intelligence platform lets organisations take a more strategic view of the business critical assets that it needs to protect, the threats that are targeting these assets and the ways in which security teams are going about it, plus the countermeasures that are in place. From there, the risk gap can be figured out and turned into a strategic discussion with the board about accepting, transferring or mitigating risk and the investments required.

Moving forward, it's clear that threat intelligence will be a deciding factor in the success of many cyber-security strategies and it is vital that organisations stay ahead of the curve by actively looking at how they improve communication, operationalise threat intelligence and manage risk.

For organisations that have already implemeted a TIP, the most frequently cited challenge is being inundated with threat data and not having a clue where to start. It is clear that the aggregation and sharing of threat data is simply not enough to succeed; TIPs need to do more to support the utility of threat intelligence as part of security operations. Without comprehensive context and priorities, it can be extremely difficult for security operators and threat analysts to identify a starting point for investigations.

With this in mind, let's examine how TIPs can respond to the industry's demand for more fine-tuned controls and streamlined threat operations, with just a little help from Albert Einstein and his three rules of work:

1. **Out of clutter find simplicity:** not all threat data will provide the same level of value or, indeed, hold that value over time. So a successful TIP should be built with the purpose of addressing the clutter of data overload with automated prioritisation of intelligence based on customer-defined parameters. The way this works is by prioritisation being calculated across many separate sources, both external and internal, into a single opinion which removes the noise.
2. **From discord find harmony**: a unified opinion with a single, transparent score helps alleviate operator confusion. This may have otherwise happened in a case where threat data was rated differently by various providers or if the data was lacking context behind how the rating was initially determined.
3. **In the middle of difficulty lies opportunity**: a self-tuning threat library is able to update priority and relevance based upon the customer-defined parameters as more data and context comes into the system. With validated context and a stronger understanding of what data is the most relevant to an organisation, operators can cut through the noise, focus their investigations on the highest risk threats first and improve their security posture – and that's the real opportunity with threat intelligence.

Empowered operators

Security operators and threat analysts can now become empowered to operationalise threat intelligence with the fine-tuned controls of a great TIP. Threat data can be operational, based on user definition, rather than vendor definition. Teams are able to maintain control over 'how', 'when' and 'where' intelligence is used. On top of this, tool over-subscription is prevented by deploying only the most important intelligence and stopping stale data from becoming active.

Out of chaos comes clarity. That's why threat intelligence platforms should be built to not only enable successful cyber-threat operations and management, but also to empower teams to collaborate on intelligence and manage defences across their infrastructure when responding to threats. By continuing to work with Einstein's three rules, the way will be paved for organisations that need faster, richer insights in order to make accurate decisions and improve their security posture.

About the author

Leon Ward is VP for product management at ThreatQuotient. Prior to joining ThreatQuotient, he led a team responsible for network security innovation at Cisco. Here he drove the development of specialist threat-focused protection targeted against advanced network attacks. His experience also includes working as director of PM for Sourcefire, where he focused on network threat detection, including vital components such as the Snort Intrusion Prevention engine. Ward is an active contributor to multiple open source security projects and frequently speaks at industry events.

Reference

1. 'Definition: Threat Intelligence'. Gartner. Accessed Mar 2017. www.gartner.com/doc/2487216?ref=clientFriendlyURL.