SECURE:DATA

THE SCIENCE OF CYBERSECURITY

WHAT IS THREAT INTELLIGENCE *AND WHY DO YOU NEED IT?*

Investing in threat intelligence delivered as a managed detection and assessment service enables organisations to make better use of the technology they have already deployed and understand where key risks lie. **SecureData answers seven of the most common questions** we're asked about intelligence-led cybersecurity.

1 WHAT DOES THE TERM 'THREAT INTELLIGENCE' MEAN?

In the context of cybersecurity, threat intelligence means both understanding your adversary, and understanding the tools and techniques they might use, and also understanding your vulnerabilities as a business so that you can correlate these three elements and ascertain ways to reduce your risk of being subject to an attack.

2 WHAT BENEFITS DOES THREAT INTELLIGENCE PROVIDE?

Threat intelligence provides you with the ability to ensure your defences are sufficiently weighted towards the threats you are likely to face. It enables you to make that effective decision about where you should place your defences and where you should invest in defences.

3 HOW SHOULD ORGANISATIONS GATHER AND USE THREAT INTELLIGENCE?

Organisations can't buy threat intelligence, only threat information, which they need to transform before they can use it as threat intelligence. They should use a third-party service provider who is experienced in the cyber arena to help them apply threat intelligence to their business. They should also receive remediation actions and consulting advice from their chosen provider.

WHAT TYPES OF THREAT DETECTION TECHNOLOGIES SHOULD ORGANISATIONS HAVE IN PLACE?

All organisations should have intrusion detection systems (IDS) and intrusion prevention systems (IPS) in place. These appliances enable protection and blocking at the boundary of an organisation and can then feed information and intelligence back to a managed security provider for monitoring purposes.

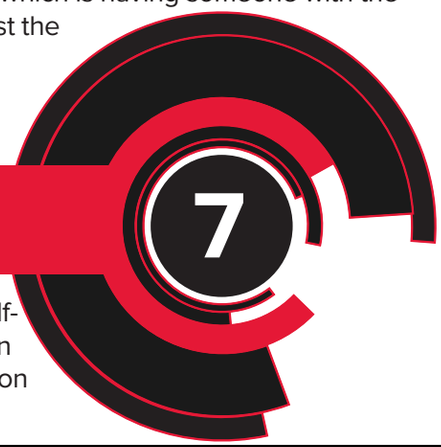
WHAT DATA SHOULD A THREAT INTELLIGENCE PLATFORM CORRELATE?

A threat intelligence platform should correlate all outputs from the major security devices producing logs across a customer's estate. It should also take in open source and paid for threat feeds, indicators of compromise, and human intelligence. The latter includes risk information from IT staff, which helps to identify the devices and assets that are the most important or valuable, and HR records – e.g. leavers and joiners records.

WHAT ARE THE BIGGEST CHALLENGES IN UTILISING THREAT INTELLIGENCE TODAY?

There are two key challenges. The first is contextualising intelligence – i.e. understanding whether that intelligence is relevant to my business and not just another indicator of compromise that will never effect me. The second challenge is the sheer volume of indicators of compromise, which are sent to subscribers in their millions per week.

There is also a people challenge, which is having someone with the expertise and experience to digest the information, 'humanise' it and understand what it means to your business.



WHERE SHOULD ORGANISATIONS FOCUS THREAT INTELLIGENCE INVESTMENT?

Threat intelligence is not something you should attempt to buy-in and self-manage. If you are making a threat intelligence investment, it should be in a provider that offers an extensive cloud-based service that is managed on your behalf, and which you can consume on a pay-as-you-grow basis.