MWR INFOSECURITY

CERT-UK

CPNI
Centre for the Protection of National Infrastructure

Being Intelligent about Threat Intelligence

The concept of threat intelligence is alluring – marketed as a powerful tool to help manage business risk at all levels of an organisation. Yet although threat intelligence is an increasingly popular "must-have" for organisations, there is little consensus on what it actually is, or how to use it.

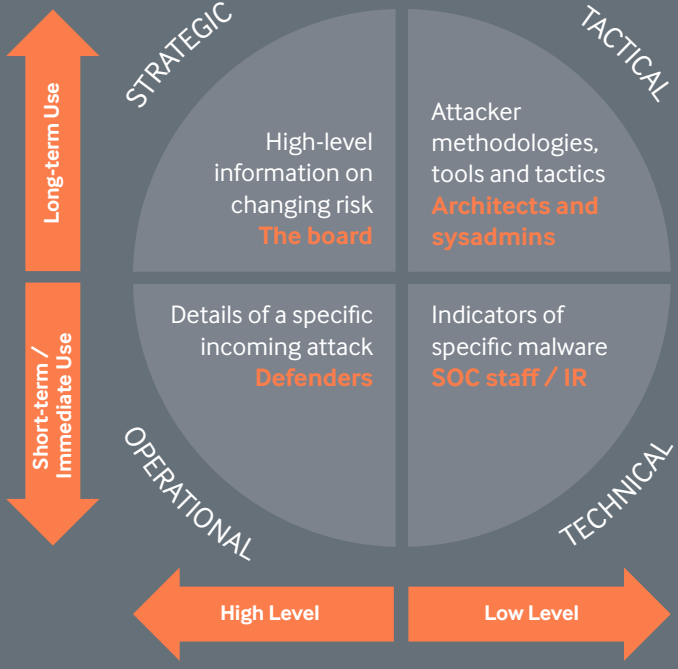
A wide array of threat intelligence products is now on offer in the market-place. However, without any real understanding of what they need or why, organisations risk investing large amounts of time and money with little positive effect on security.

To address this, MWR InfoSecurity studied the growing field of threat intelligence. From extensive literature review and interviews with experts across a wide range of industry sectors, it became clear that an effective threat intelligence strategy is best devised by applying the principles of traditional intelligence.

Effective threat intelligence focuses on the questions that an organisation wants answered, rather than simply attempting to collect, process, and act on vast quantities of data. This means rigorous planning, execution and evaluation.

It can be helpful to break down the enormous variety of products and services in the market place classed as "threat intelligence" into four distinct categories. Each category is relevant to a different internal customer, ranging from the board all the way to technical consumers such as firewall administrators.

Subtypes of threat intelligence



It soon emerges that the most useful sources of threat intelligence are not necessarily the most expensive. Significant value can be gained – for example – from simple activities such as sharing threat intelligence with other organisations. One-to-one human contacts can be one of the simplest, yet most effective, sources of actionable information.

In summary, 'doing' threat intelligence is important – but doing it intelligently is critical.

For the full, in-depth white paper, see http://mwr.to/threat-intel