Switched-on security

Protecting networks through effective threat intelligence

1

USE YOUR RADAR

Threat intelligence can allow targeted defence

What is intelligence?

Information that can aid decisions with the aim of preventing an attack or decreasing the time taken to discover an attack.

What is threat intelligence?

A new field. Applies traditional intelligence to cyber threats. Targets defences, increases threat awareness and improves responses to potential attacks.

2

THE 4 TIER MODEL OF THREAT INTELLIGENCE

The four types of threat intelligence

Strategic threat intelligence

Consumed by: board and senior staff.

Form: often written or verbal, such as reports, briefings or conversations.

Example: reports on financial impact of cyber activity or attack trends that might impact on high-level business decisions.

Tactical threat intelligence

Consumed by: architects and sysadmins.

Gained by: reading white papers or the technical press, communication with peers in other organisaitons, purchasing from an intelligence provider.

Example: it is discovered that attackers are using tools to obtain cleartext credentials and then replaying those credentials through PsExec.

Operational threat intelligence

Consumed by: defenders, responders.

It will be difficult for a private company to legally acquire operational intelligence on many groups. However some public groups are easier.

Example: regular attacks in response to news coverage can be used to predict future attacks.

Technical threat intelligence

Consumed by: SOC staff / IR.

Form: data or information normally consumed through technical means. Often has a short lifetime.

Example: a feed of IP addresses suspected of being malicious or implicated as command and control servers.

3

TAILORED INTELLIGENCE

Focus on your organisation's specific threat intelligence requirements

Ask the right questions

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.

Don't just buy cool sounding products

Not all threat intelligence products are useful. The most useful sources of threat intelligence – for example personal contacts in other organisations – are **not necessarily the most expensive.**

4

START SMART

Threat intelligence first steps that work – even with minimal staff and budget

Organisational

Identify where threat intelligence processes might be taking place unofficially and assess how they could be better supported

Strategic

1. Identify whether current perceived cyber threats have been realised in the past.
2. Liaise with industry peers to determine whether there are other threats.
3. List all actors who would benefit from access to your sensitive data – or your inability to function effectively.

Tactical

1. Extract key tactical indicators from incident reports and white papers on threat groups.
2. Determine changes needed to make your organisation less susceptible.
3. Identify planned refreshes of technologies, or systems. Feed tactical intelligence into those refreshes to mitigate attacks.

Operational

1. List people to contact if your organisation receives notice of an impending attack.
2. Google your organisation's name for dates immediately before DDOS attacks to determine whether negative coverage is leading to them.
3. If not, attempt to identify other potential trigger factors.

Technical

1. Obtain access to the daily C2 list from CISP* or other free feeds and place the IP addresses in an 'alert' list on the primary firewall or IDS.
2. Review regularly to determine whether outbound connections are being made from within your organisation.
3. If so, initiate incident response.

5

TWO HEADS BETTER

One-to-one human contacts can be among the best information sources

Forums

Discuss threat intelligence in forums. The CISP* allow organisations to share information securely.

Organisations

Meet with appropriate peers in similar organisations to discuss your joint perception of existing threats.

Focus on relationships where there is already some trust and develop further trust.

* The Cyber-security Information Sharing Partnership (CISP) is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.

CPNI

Centre for the Protection of National Infrastructure

This Infographic presents one perspective on the topic of Threat Intelligence.

For more information on the topic:

www.cpni.gov.uk/advice/cyber/Threat-Intelligence

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu