



# An introduction to threat intelligence

# Contents

## Introduction

Threat intelligence is an elusive concept. Cyber-security vendors have developed numerous definitions for it based not only upon different procedural viewpoints, but also driven by competitive imperatives. As a result, the scope of this paper is limited to an introduction of the key concepts and principles of threat intelligence, explaining the role it plays within network defence, offering advice and best practice, and pointing out available community support. This will equip the reader with a basic understanding of the benefits of threat intelligence and the importance of investing effort and resources into developing it.

As elusive as a definition may be, this one offers a comprehensive description:

> [It is] *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]

## Key concepts and principles

Within the context of cyber-security, threat intelligence represents the synthesis of information detailing potential threats with a solid understanding of network structure, operations, and activities.[2] In order to generate this evidence-based knowledge with any value for network defenders, information on the mechanisms and indicators, often termed 'threat feeds', must then be contextualised by contrasting it with baseline knowledge of network activity. The collation and collection of threat feeds is the creation of threat intelligence, which then informs 'security analytics' to improve chances of detection. Security analytics in a network defence setting usually takes one of two forms:

1. 'Big data' platform crunching network data to ascertain trends
2. Security information and event management (SIEM) infrastructure with rules set up to automate the detection of anomalous activities; both of these are stand alone and do not require threat intelligence to function, however they are informed by it at a strategic and operational level

At the strategic level, threat intelligence enables the development of future cyber-security testing by:[3]

- Identifying and detailing emerging threats and possible mitigation
- Framing testing scenarios by confirming they are relevant to such threats
- Supporting business cases for network control settings to counter vulnerabilities
- Directing sensor enrichment network defence policy

[1] Definition: Threat Intelligence https://www.gartner.com/doc/2487216/definition-threat-intelligence
[2] INSA Cyber Intelligence Task Force White Paper http://www.insaonline.org/CMDownload.aspx?ContentKey=cfdfcf7c-02b4-4507-a054-2606d684ffb0&ContentItemKey=bc0f998f-85f7-4db6-9288-903f748e1de9
[3] CBEST Threat Intelligence Framework Qualities of a threat intelligence provider http://www.bankofengland.co.uk/financialstability/fsc/Documents/cbestthreatintelligenceframework.pdf

Understanding these factors will enable network defenders to determine their resilience to compromise, ability to detect threats, and speed of recovery. It will also inform operational level activity such as:[4]

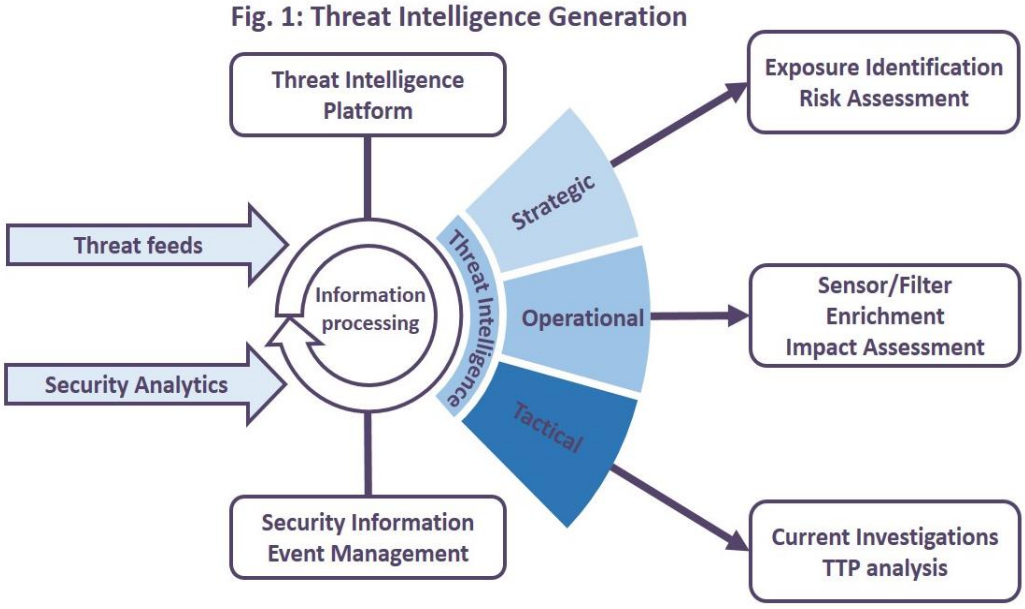
- Trend analysis determining the evolving capabilities of attackers
- Indicators that highlight current attack vectors being exploited
- Tracking changes in the capability of attacks
- Understanding of the operational cycle of attacks
- Identifying opportunities to exploit potential vulnerabilities of an attacker
- Establish a better picture of the environment/threat

At the tactical level, threat intelligence allows the network defender to monitor for threats in as close to real time as possible by:

- Exposing attack infrastructure and methodology
- Identifying an existing or emerging menace or hazard
- Comparing observed activity with known tactics, techniques and procedures (TTPs) and indicators of compromise (IOCs)
- Highlighting the implications of a compromise and actionable advice
- Informing defensive actions and mitigation of current threats

Depending on the accuracy and reliability of the threat feeds, effective threat intelligence also covers three temporal aspects, a past, present, and future: it identifies previously unidentified network vulnerabilities by exploiting threat details of historical incidents; it prioritizes current investigations according to alerts of active threats; and finally, it enables the monitoring of infrastructure for, and prevention of, repeat attacks.

**Fig. 1: Threat Intelligence Generation**




[4] INSA Cyber Intelligence Task Force White Paper http://www.insaonline.org/CMDownload.aspx?ContentKey=cfdfcf7c-02b4-4507-a054-2606d684ffb0&ContentItemKey=bc0f998f-85f7-4db6-9288-903f748e1de9

## Role within network defence

A primary consumer of threat intelligence products generated by this process is the security operations centre (SOC) in their mandate to triage and respond to security related incidents. Ideally, enterprise software termed a threat intelligence platform (TIP) is used to manage the information relevant to the SOC's function. At this stage, other security related information relevant to the organisation is often introduced. For this reason, the TIP is typically integrated with the SIEM feeds. This can be a powerful method of combining internal security analytics data with external threat intelligence data.[5]

The majority of security operations in organisations that cannot afford to build a SOC still have a threat intelligence function utilising a STIX/TAXII platform (explained below) to automatically create indicators of compromise (IOCs) to inform rules in their intrusion detection systems (IDS), intrusion protection systems (IPS) and firewall devices. From a management perspective however, the TIP must simultaneously provide near real-time tactical threat intelligence, inform operational concerns for handling such threats, and support strategic prioritisation of cyber-security issues across the organisation. Customisation is key to the success of a TIP, and so each SOC will require different processes and data customisation needs across processes for aggregation, analysis, and action.[6]

## Common languages and frameworks

In order to rationalise and standardise the transmission of threat feeds, there is a collaborative effort by numerous cyber-security vendors to establish common languages and standards. Some of the most widely adopted are listed below:

- **Common Attack Pattern Enumeration and Classification (CAPEC)** is a publicly available, community-developed list of common attack patterns that include comprehensive schemas and classification taxonomy. Each entry captures knowledge about how specific stages of an attack are designed and executed. It provides guidance on ways to mitigate the attack's effectiveness.[7]
- **Cyber Observables (CybOX™)** is a standardized schema for the specification, capture, characterisation, and communication of threat related events. It provides a standard format for addressing cyber observables improving consistency, efficiency, interoperability, and overall situational awareness. [8]
- **Microsoft Interflow™** is a security and threat information exchange platform for professionals working in cyber-security. It is part of the Microsoft Active Protections Program (MAPP), established in 2008 to help provide security software vendors with early access to software vulnerability information.[9]
- **Structured Threat Information (STIX™)** is a collaborative project to define and develop a standardized language to represent structured cyber threat information. The STIX

[5] Getting Ahead of Advanced Threats https://www.emc.com/collateral/industry-overview/ciso-rpt-2.pdf
[6] ThreatConnect: What is a Threat Intelligence Platform
http://www.threatconnect.com/why_threat_connect/what_is_threat_intelligence_platform
[7] Common Attack Pattern Enumeration and Classification http://capec.mitre.org/index.html
[8] Cyber Observable eXpression http://capec.mitre.org/index.html
[9] Microsoft Active Protections Program http://msdn.microsoft.com/en-us/library/dn750892.aspx

language intends to convey the full range of potential cyber threat information and in as expressive, flexible, extensible, automatable, and as human-readable way as possible.[10]

- **Trusted Automated eXchange of Indicator Information (TAXII™)** is a set of services and message exchanges that enable actionable cyber threat information to be shared across organization and product/service boundaries. It is the preferred mechanism of exchanging information represented using the Structured Threat Information Expression (STIX™) language, enabling organizations to share structured cyber threat information in a secure and automated manner.[11]

## Best practice and support

Traditionally the term 'intelligence' has been understood as meaning either a product or a process, however within the context of cyber-security, threat intelligence is also a service available for purchase. As the time available to react to a threat is compressed, threat intelligence has become a critical element to a successful security program.

A good threat intelligence service can provide immediate security information tailored to the client's network. These services prioritise vulnerabilities and predict threats, enabling security teams to rapidly take action. More advanced services also integrate vulnerability alerting with real-world threat intelligence covering geo-political and business intelligence.[12]

Regardless of an organisation's size, the following steps will guide organisations in improving their cyber-security:[13]

- Understand the target network, the incident response process, and the risk
- Identify and communicate the benefits to key stakeholders
- Build an effective team that can respond to the challenges and educate employees
- Refine sources of threat data and security analytics for better threat intelligence
- Define relevant processes, then test and review them regularly
- Automate these processes to reduce reaction time

There are a number of communities that offer the network defender support and advice. The Cyber-security Information Sharing Partnership (CiSP) is one. As part of this community, CiSP members receive enriched cyber threat and vulnerability information from the 'Fusion Cell', a joint industry and government analytical team who examine, analyse and feedback cyber information from a wide variety of data sources. The Fusion Cell also maintains the capability to conduct bespoke malware and phishing email analysis on behalf of CiSP members.

More information about CiSP, including how to join, can be found at www.cert.gov.uk/cisp.

[10] Structured Threat Information eXpression http://taxii.mitre.org/
[11] Trusted Automated eXchange of Indicator Information http://taxii.mitre.org/
[12] An Introduction to Threat Intelligence http://www.secureworks.com/resources/newsletter/2003-10/
[13] Getting Ahead of Advanced Threats https://www.emc.com/collateral/industry-overview/ciso-rpt-2.pdf

## Conclusion

Within this paper, the key concepts and principles of threat intelligence have been introduced. The role it plays within network defence, has been explained, and the best practice and supporting advice has been offered. The manipulation of security analytics to combine various threat feeds with a solid understanding of the target network is a complex challenge. However, by taking advantage of threat intelligence services, and refining existing systems, network defenders can help to mitigate their exposure to the vast array of threats.

The temptation might be to dismiss the importance of threat intelligence under the impression that competing cyber-security vendors have exaggerated and diluted the potential benefits. That is short sighted as it ignores the value of raw information for improved network defence. Intelligence is fundamentally information with capital, added through a systematic cycle of collection, collation, processing, and dissemination. The value of any intelligence is judged by the utility it offers in both reducing uncertainty and enabling decision makers to understand the merits and consequences of choices. Threat intelligence is a facet of cyber-security that network defenders simply cannot ignore, as the quote below stresses:

> *Make no mistake about it: computer network defence contains a strong element of intelligence and counterintelligence that analysts and managers alike must understand and leverage.*[14]

## Further reading

For further information on threat intelligence and more technical advice, CERT-UK and CPNI in partnership with MWR Security have produced 'Threat Intelligence – Collecting, Analysing and Evaluating' available here:
http://www.cpni.gov.uk/advice/cyber/Threat-Intelligence/

[14] SANS Cyber Threat Intelligence Summit http://www.sans.org/event/what-works-cyber-threat-2013


www.cert.gov.uk
@CERT_UK

A CERT-UK PUBLICATION


CERT-UK was formally launched on 31 March 2014 and is the UK National Computer Emergency Response Team. We work closely with industry, government and academia to enhance UK cyber resilience and are funded via the National Cyber Security Programme (NCSP).

CERT-UK has four main responsibilities that flow from the UK's Cyber Security Strategy:

- National cyber-security incident management
- Support to critical national infrastructure companies to handle cyber security incidents
- Promoting cyber security situational awareness across industry, academia, and the public sector

Providing the single international point of contact for co-ordination and collaboration between national CERTs