CTIPs
CREST Threat Intelligence Professionals

CREST

What is Cyber Threat Intelligence and how is it used?

Published by:

CREST

Tel: 0845 686-5542

Email: **admin@crest-approved.org**

Web: **http://www.crest-approved.org**

Contents

Introduction

About this guide

This guide provides an introduction to cyber threat intelligence. It provides practical advice on the practice and procurement of cyber threat intelligence services. It outlines the key concepts and principles that underpin cyber threat intelligence, along with the ways in which organisations use cyber threat intelligence to prevent, detect and respond to potential cyber security incidents. It also presents guidance and criteria to help you select a qualified supplier with the capabilities necessary to meet your requirements.

Audience

As organisations of all shapes and sizes globally increasingly adopt a Risk-based approach to managing cyber threats in line with best-practice, there has been a commensurate rise to prominence of cyber threat intelligence. This can occasionally mean that personnel without formal intelligence training, qualifications, and experience are required to procure intelligence services and oversee and develop intelligence products for their organisation. This guide is therefore intended to inform a broad information security audience – including those both with and without previous experience and understanding of cyber threat intelligence as a discipline. This guide is intended for organisations in both the public and private sectors.

Purpose

This guide is intended to help readers:

- **Understand the principles of cyber threat intelligence**, including the three levels of intelligence and different types of sources
- **Understand how cyber threat intelligence can be used**, including its various organisational and departmental applications
- **See the value in using specialist suppliers**, which includes expertise, responsiveness and insight
- **Identify criteria for selecting suppliers**, including questions to ask potential providers

What is cyber threat intelligence?

Cyber Threat Intelligence (CTI) can still be described as a nascent and fast-developing field. However, the practice of intelligence itself is historically and commercially a very well-established discipline.

There are a multitude of definitions of intelligence, and two of these are included below for illustration. Regardless of the precise role of the organisation and the plurality of opinions, however, it is clear that good definitions unanimously identify the product of intelligence as **understanding that can assist the decision-making process**.

"Intelligence is information that is received or collected to answer specific questions on who, what, where, when, how and why…"
UK National Crime Agency (NCA)

"Intelligence is knowledge and foreknowledge of the world aroud us – the prelude to decision and action…"
US Central Intelligence Agency (CIA)

The fact that cyber security is increasingly recognised as a priority business risk; the increasing variety in and maturity of products; and other factors, such as regulatory requirements, are all driving the demand for cyber threat intelligence services. This section therefore looks to introduce the key concepts that underpin cyber threat intelligence.

Intelligence-led security

Using an intelligence-led approach has long been accepted as best practice in the realm of conventional security. Without it, organisations will invariably defend against too little, because they don't understand the threats they face, or try to defend against all potential threats – an unsustainable approach that may also impair the organisation's ability to operate effectively. For example, a company looking to build a facility in a potentially hostile environment would first seek intelligence on the threat posed by malicious actors in the vicinity before trying to adopt appropriate security controls.

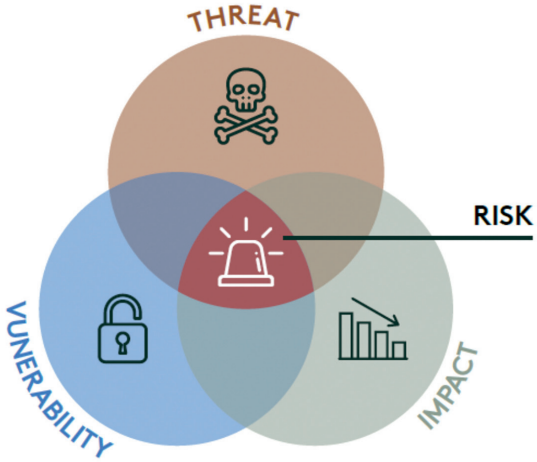


Figure 1: Frequently, risk is defined as a combination of threat, vulnerability and impact

This same principle applies to cyber security: you need to understand your threat before you can protect against it. This approach informs the uptake of the intelligence-led cyber security testing frameworks such as the Bank of England's CBEST programme. The cyber threat intelligence component of these frameworks ensures that organisations are tested on their ability to prevent, detect and respond to realistic, contemporary and accurate attacks. Although the Bank of England's CBEST was the first such scheme, the principle has since expanded, both internationally to other financial sectors, and to other regulated sectors in the UK. These new schemes include:

- TIBER-NL (Threat Intelligence Based Ethical Red-teaming Netherlands) for the Dutch financial sector
- TBEST for the UK telecoms sector
- TIBER-EU for the European financial sector
- iCAST (Intelligence-led Cyber Attack Simulation Testing) for Hong Kong's financial sector
- GBEST for UK government departments
- ATTEST for the UK aviation industry

Threat and risk

Frequently, risk is defined as a combination of threat, vulnerability and impact. In order to adopt a risk-based approach to cyber security, organisations therefore need to understand the threats they face. Threat is defined as the ***intent*** and ***capability*** of adversaries to target an asset – typically either information or a system, and it is intelligence about the threat that enables organisations to prepare for it and defend themselves. When an organisation knows how to answer key questions regarding the threats it faces – such as ***who*** is likely to target ***what*** assets, ***where, when, how*** and ***why*** then they stand a much better chance of defending themselves. This is particularly true in the field of cyber security, where the number and diversity of adversaries, and the pace of change of attack methods, makes defence a difficult task.

If organisations have a good understanding of the threats they face, then they are able to combine this understanding with an assessment of the maturity of their defences to understand the likelihood of an incident occurring. This likelihood can be combined with an assessment of the impact of such an incident to understand the risk. This allows organisations to deploy their usually limited security resources against the highest priority risks.

If organisations have a good understanding of the threats they face, then they are able to combine this understanding with an assessment of the maturity of their ***defences*** to understand the likelihood of an incident occurring. This ***likelihood*** can be combined with an assessment of the ***impact*** of such an incident to understand the ***risk***. This allows organisations to deploy their usually limited security resources against the highest priority risks.

Data vs information vs intelligence

The terms data, information and intelligence are often incorrectly used interchangeably.

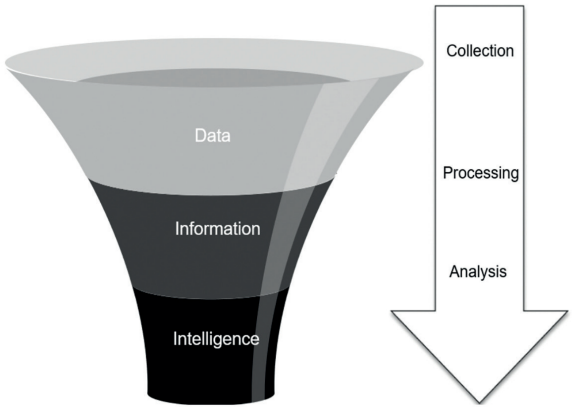


Figure 2: Producing intelligence from raw data

Data refers to simple facts that tend to be available in large volumes. In the context of cyber security, IP addresses or logs are typical examples. By itself, raw data is of limited utility.

Information is produced when this data is collated to provide a useful output – for example, a collated series of logs showing a spike in suspicious activity.

Intelligence comes from the processing and analysis of this information and can be used to inform decision making. For example, the collated log data is contextualised with prior incident reports regarding similar activity, which also allows for the development of a strategy to mitigate the incident.

The intelligence cycle is an effective model that shows this processing of raw data into finished intelligence products.

The intelligence cycle

The intelligence cycle is the process by which raw data and information is identified, collected and then developed into finished intelligence for use by decision makers. Adherence to the process will ensure that activities are directed and co-ordinated to efficiently satisfy the consumer's requirements.

Although the intelligence cycle typically features four main phases, the process is cyclical in nature. All phases should incorporate a review process to ensure that the required material is being processed and passed on correctly, and that the intelligence consumer's requirements are constantly at the heart of the process.

Planning and direction is the first phase of the intelligence cycle. It is used to coordinate intelligence activities to most efficiently serve the consumer's requirements, and should involve significant interaction between the consumer and producer. This phase should determine the exact requirements of the consumer - often called intelligence requirements (IRs) or priority intelligence requirements (PIRs). From these IRs and PIRs, one can establish what data and information is required and how it should be collected. This output is often codified in an intelligence collection plan (ICP).

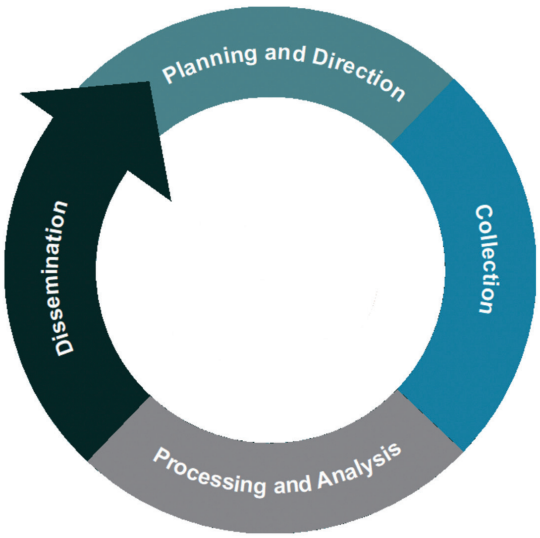


Figure 3: The four phases of intelligence cycle

The second phase, ***Collection***, involves gathering the data and information that is likely to meet the identified requirements. This will typically involve collecting from a wide array of sources (some of which are outlined in the section below). Understanding which sources are likely to produce the desired information, be reliable, and provide information that can be consumed in a timely manner, is a complicated process. It requires good planning and direction to help separate the signals from the noise.

Processing and analysis, in which raw data and information is collated, fused with other sources, and turned into intelligence, is the third phase in the cycle. Human and machine capabilities alike in this phase need to be geared towards answering the IRs for the engagement while adhering to the principles of intelligence (see below). Analysts will typically apply a variety of quantitative and qualitative analytical techniques to assess the importance and implications of processed information, integrate it by combining disparate pieces of information to identify patterns, and then interpret the significance of any newly developed knowledge. Analysts are likely to use a range of techniques in order to ensure accurate and unbiased assessments that should be predictive and actionable. Evaluation of the reliability of the source and the material collected is also applied during this phase.

Dissemination is the timely conveyance of completed intelligence products in an appropriate format to the intended consumers. The frequency of dissemination should match the time period on which the content is based – for example, operational material needs to be delivered frequently, whereas strategic content will be more intermittent. Via soliciting feedback and refining existing IRs – or developing new ones – the intelligence cycle can begin again.

The principles of intelligence

The infographic below summarises the principles that intelligence processes and products should adhere to. These principles are often known by the mnemonic CROSSCAT.

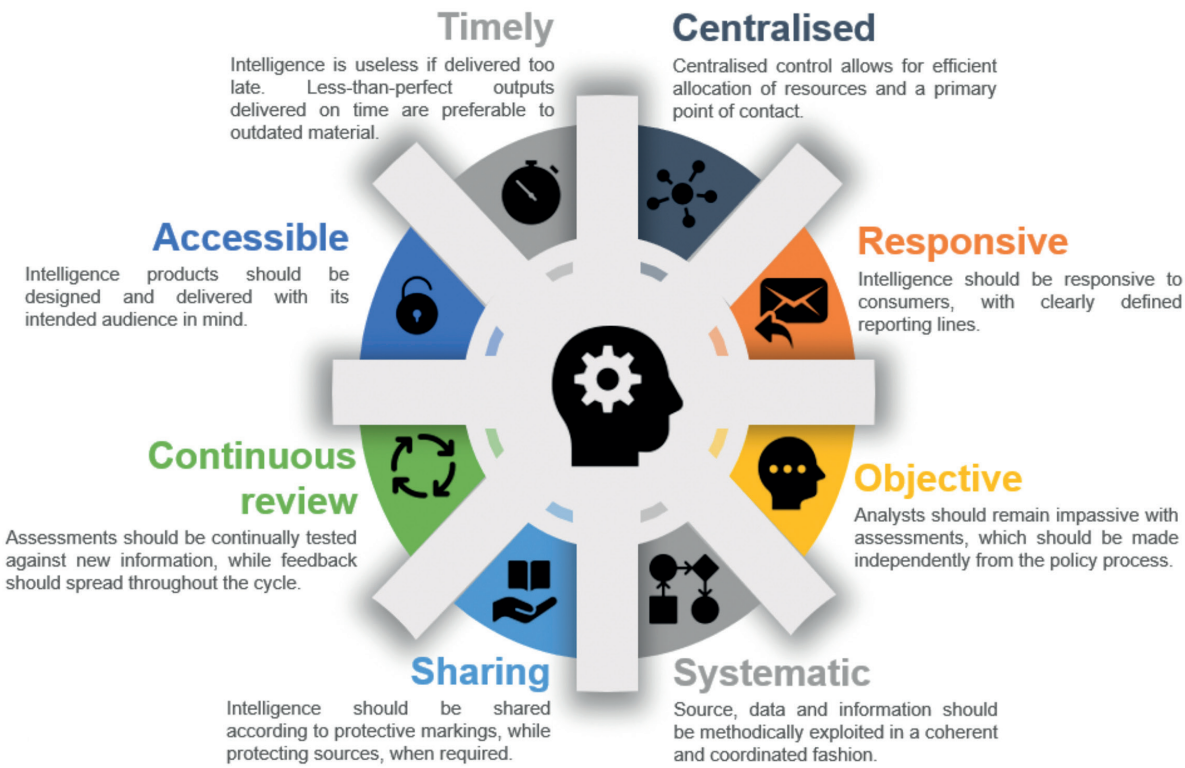


Figure 4: The CROSSCAT principles of intelligence

The different levels of cyber threat intelligence

As with conventional intelligence, there are different levels of cyber threat intelligence: operational, tactical, and strategic. Each level differs in the nature and format of the material conveyed, its intended audience and its application. These are summarised in the infographic below.

Operational threat intelligence often relates to details of potential impending operations against an organisation. Although it is not always easy to obtain, by using an all-source approach an intelligence provider will be able to detect, for example, chatter from cyber activists discussing potential targets for an upcoming campaign, or data leaked or sold on a dark web forum that could be used in an operation against the company. Cyber threat intelligence providers will generally supply operational threat intelligence in a combination of human and machine-readable formats.

Tactical threat intelligence consists of material relating to the techniques, tactics and procedures (TTP's) used by threat actors. Indicators of compromise (IOCs) are the main deliverable for tactical threat intelligence providers. These are particularly useful for updating signature-based defence systems to defend against known attack types, but can also prove useful for more proactive measures, such as threat hunting exercises. It is therefore particularly useful to network defenders such as Security Operations Centres (SOCs). CTI providers will generally supply IOCs in machine-readable formats, whereas intelligence on TTPs will be in human-readable formats, and will require human assimilation and action.

Figure 5: The three levels of cyber threat intelligence

Strategic threat intelligence exists to inform senior decision makers of broader changes in the threat landscape.

Because of this intended audience, strategic intelligence products are expressed in plain language and focus on issues of business risk rather than technical terminology. The reporting format of strategic cyber threat intelligence products will reflect this longer-term view – for example it will often be disseminated on a monthly or quarterly basis to assist the formulation of longer-term strategy.

Different sources of intelligence

Cyber threat intelligence suppliers should draw from a wide range of different sources to enable them to provide a rounded and holistic understanding of the threats that organisations face. This is particularly true because the range of cyber adversaries most organisations face are disparate, and relevant information sources about those threat actors need to match that challenge. Commonly used sources by cyber threat intelligence providers include:

Indicators of compromise (IoCs) associated with malicious activity. Hashes of malware samples, IP addresses and domain names can all be used to update firewalls and detection systems, as well as contribute to an understanding of threat actors' TTPs. IOCs are their own are more akin to data than processed intelligence, though are still included within the spectrum of cyber threat intelligence.

Client-derived data, such as that regarding its infrastructure or extracted from a security information and event management (SIEM) tool or other logs can be correlated with other sources, or for pro-active measures such as threat hunting.

Deep web, such as information from member-only hacking forums frequented by cybercriminals. These sources can provide valuable insight into the tools and services advertised and requested by cybercriminals, as well as identifying which exploits are being discussed to enable patch prioritisation.

Figure 6: A translated post from a Russian deep web forum illustrates intelligence regarding exploits

Dark web will include marketplaces and shops that are hosted on anonymity-focused networks such as Tor or I2P which criminals use to purchase goods and services. This will enable consumers to identify if their data – ranging from login credentials to valuable intellectual property – is available or being advertised for sale, or if infrastructure they use may be targeted.

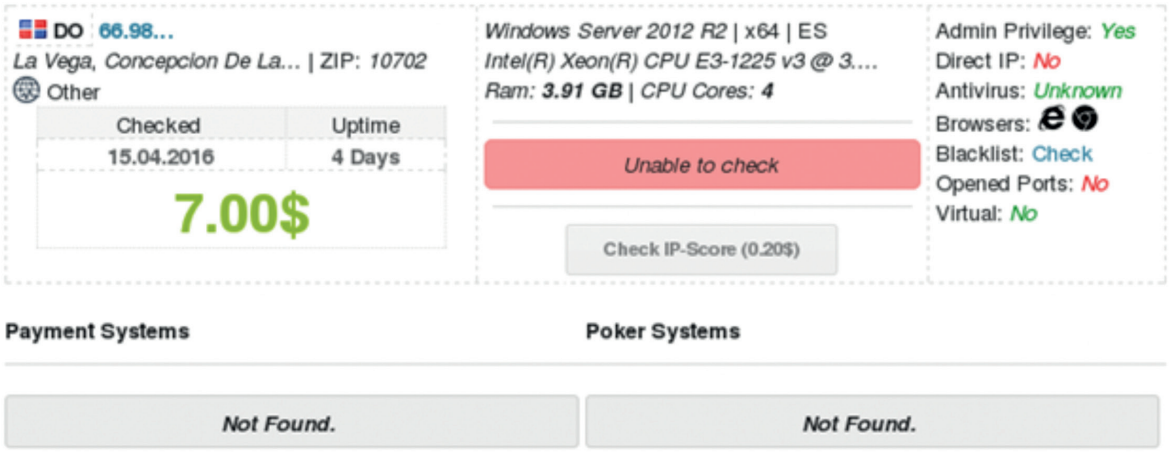


Figure 7: Dedicated dark web shops, such as this vendor of remote desktop protocol instances, can uncover indications that clients' infrastructure has been compromised

Messaging platforms are also used by threat actors to communicate, and can provide intelligence. Rather than relying on semi-public forums, some cybercriminals prefer more direct means of engaging each other to sell their goods and services. Similarly, cyber activists will often use a combination of outmoded Internet Relay Chat (IRC) channels and other messaging platforms to discuss impending operations, which can provide useful insight into potential tactics and targets.

Social media can be used by a variety of actors, typically those with low capabilities. Activists may signal their intent to pursue specific targets in advance via social media pages. Criminals may use popular networks as an alternative means of attracting potential customers, particularly in jurisdictions where law enforcement capability is limited and they do not run the risk of arrest. Social media collection may also include coverage of inadvertent data leaks by employees or potential threats from malicious insiders.

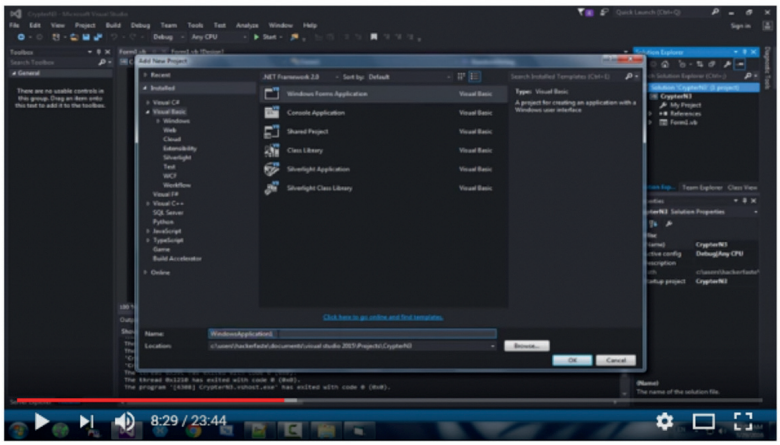


Figure 8: Social media, such as this YouTube video, can provide evidence of criminal TTPs

Human intelligence can be derived from engagement with individuals via several the above sources. However, threat intelligence providers should only engage in such activity under a strict and defined framework and in pursuit of specific intelligence requirements and in a legal and ethical way. Providers also need to ensure that collection efforts from social media and human sources are compliant with legislation such as the General Data Protection Regulation (GDPR).

Malware analysis, which allows analysts to extract information such as indicators of compromise from a sample, which can in turn be used to search the client estate. Analysis also allows providers to better understand the latest tactics, techniques and procedures that are being used by threat actors, with a view to informing network defenders how to better respond.

Figure 9: The tools within exploit databases are also available to malicious actors

Geopolitical developments can be used to derive an understanding of the intent of nation-state actors. For example, understanding how a state's strategic development objectives coincide with those of the client organisation, or how potential nation-state rivalries will affect the prospect of disruptive attacks in a region in which it operates, will help it understand the threats it faces.

Code repositories, such as exploit databases, can provide insight into which exploits are available for adoption by threat actors, and which vulnerabilities should be prioritised for patching as a result.

Paste sites can reveal a wide array of information, including leaked credentials, indications of impending activist operations, code snippets, and evidence of breaches. The example in the image to the right shows a message from a campaign by the Anonymous collective, which goes on to list a series of targets for DDoS attacks.

text 5.63 KB

```
1. World Banking Cartel Master Target List
2.
3. #OpIcarus #OpWhiteRose
4. #WhiteRoseSociety #WhiteRoseRevolt #WhiteRose
5. #DeleteTheElite #EndTheFed #AuditTheFed
```

Figure 10: Snippet of a Pastebin post from Anonymous' OpIcarus campaign against the global financial sector

Information sharing platforms can also provide additional context and insight to threat actors' current activity. These are typically divided along national or sectoral boundaries, and include:

- The UK National Cyber Security Centre's (NCSC) Cyber Security Information Sharing Partnership (CiSP)
- The Financial Services Information Sharing and Analysis Center (FS-ISAC)
- AlienVault's Open Threat Exchange (OTX), a crowd-sourced platform used by participants in 140 countries
- US-CERT's (United States Computer Emergency Response Team) Automated Indicator Sharing (AIS) platform
- The Asia Pacific (APAC) Intelligence Centre based in Singapore

Data from government partners is also available to some sectors and for specific projects. Rather than using these sources in isolation, effective cyber threat intelligence suppliers need to corroborate and fuse together material from different sources to better understand the nature of the threat that their clients face. Ideally, intelligence reports should be multi-sourced – potentially fusing information from at least two source types.

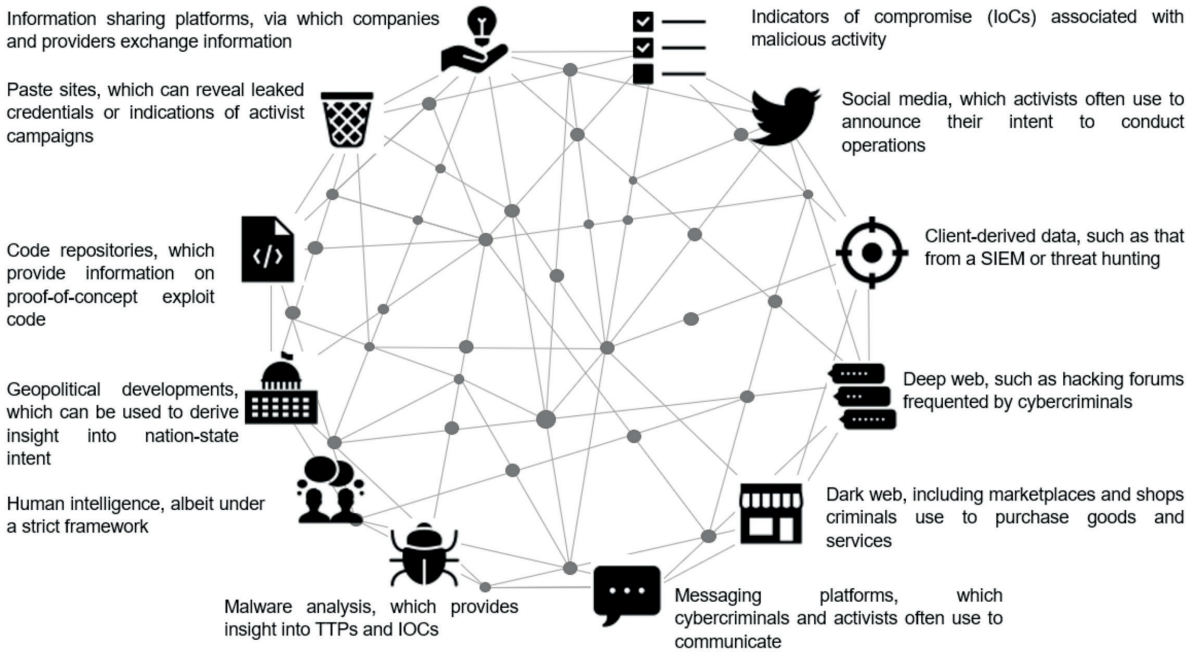


Figure 11: A summary of different sources typically used by threat intelligence providers

Different types of Cyber Threat Intelligence Services

The term cyber threat intelligence can refer to a number of different products and services. These can be split into two broad categories of standalone engagements and continued threat monitoring services.

Standalone engagements:

- ***"X"BEST project***s are regulator mandated intelligence-led security testing engagements. The schemes are typically named using the "BEST" acronym, such as CBEST in the financial sector, TBEST in the telecoms sector, TIBER-EU in the European financial sector and ATTEST in the UK aviation sector. Buyers use accredited threat intelligence providers to supply the threat assessment, targeting report and scenarios for testing that the penetration testing provider uses to develop a testing plan for the second phase of the engagement.
- ***CREST STAR*** assessments follow the "BEST" methodology for intelligence-led security testing, though can be conducted without the involvement of a regulator. This makes them appropriate for companies in sectors that have yet to establish such frameworks, or for companies that wish to conduct preparatory, repeat, or complementary intelligence-led security testing projects. In addition to providing the deliverables, CTI providers can provide useful scoping guidance in the absence of a regulator.
- ***Threat assessments*** are standalone deliverables that help buyers understand the intent and capability of threat actors to target their organisation. Threat assessments are increasingly used as the initial phase of intelligence-led security testing exercises.
- ***Investigations***, along with other smaller engagements, can be provided by cyber threat intelligence suppliers by leveraging their collection capabilities.
- ***Threat scenarios***, which have previously been delivered as part of intelligence-led security testing engagements, but can also be provided as a standalone deliverable to facilitate the development of a penetration-testing plan.
- ***Consultancy, training and capability building*** can also be delivered by providers as a means of improving buyers' abilities to consume threat intelligence, or produce their own.

Continued threat monitoring services:

- ***Subscriptions*** are typically provided via a dedicated portal and pushed reports. Suppliers will usually provide access to a steady stream of current and historic intelligence, along with the ability to interact with the intelligence, conduct investigations and integrate it into existing processes. Some providers will provide bespoke subscriptions which follow the intelligence cycle and deliver tailored intelligence reporting to meet an organisation's requirements, and this may be augmented by analyst access and in-person briefings.
- ***Threat Intelligence Platforms*** (TIPs) are used to aggregate and correlate different feeds and subscriptions, and allow consumers to pivot from various IOCs and conduct investigations.
- ***Data feeds*** consist of raw, uncontextualized or analysed data that will likely require some processing by the recipient organisation. These can include IOCs or dark web data that can be enriched by the consumer.

How do organisations use cyber threat intelligence?

In addition to the business functions outlined below, the application of cyber threat intelligence within an organisation can be summarised in four main categories:

- ***Predict:*** strategic threat intelligence can help organisations forecast evolving threats before they materialise, and plan accordingly to avoid them
- ***Prevent:*** threat intelligence that can stop incidents occurring in the first place, such as malware signatures that can be used to update signature-based detection mechanisms
- ***Detect: i***ntelligence that helps identify threats as they arise, or those that may already be present within a network, such as TTPs that can be used for threat hunting exercises
- ***Respond:*** material that can inform a response to an existing incident with a view to mitigating its extent or impact, such as TTPs used by a threat actor once its presence has been discovered on a network which will provide guidance on likely adversary next steps and how the victim should act

The degree to which an organisation can consume threat intelligence across multiple business functions will depend on the nature of the material provided and the maturity of the consumer organisation. A separate exercise to assess the maturity of an organisation to generate, consume and disseminate cyber threat intelligence is likely to be a useful way of understanding how to improve an organisations' capabilities in this regard.

Security Operations Centre (SOC)

The SOC will typically be responsible for processing threat intelligence and using it to add additional context to internal sources of data, such as logs of malicious activity. This is particularly valuable to SOC analysts that are responsible for working with and analysing big data sets. The SOC may have to prioritise incoming material using security information and event management (SIEM) tools and decide which to escalate. Intelligence has an important role in the SOC, and intelligence should be used both to aid the SOC operators in identifying malicious activity and as an output of the SOC to inform cyber security at the strategic and other levels. For example, a threat intelligence service that includes a moving threat level based upon specific operational and tactical intelligence can allow the SOC to activate a heightened state of readiness.

IT Security Management

Tactical threat intelligence can help IT security departments prioritise the adoption of appropriate controls throughout an organisation. For example, if a company understands that it faces a high threat from extortionists looking to use distributed denial of service (DDoS) attacks to take down its customer-facing portal, and it has tactical intelligence regarding the tactics, techniques and procedures (TTPs) typically used by the group – such as the specific protocols it exploits – and operational intelligence regarding the targeting of its peers, then it can adapt and improve its controls accordingly.

Vulnerability management

The sheer volume of vulnerabilities in a typical estate will mean prioritising vulnerabilities for patching remains a challenge, even for organisations with dedicated vulnerability management programmes. Threat intelligence regarding which specific vulnerabilities that are being and are likely to be exploited in the wild can help companies prioritise according to the likelihood and potential impact of exploitation.

Investigation and response

Intelligence is also critical for investigation and incident response processes. Understanding the TTPs used by threat actors enables proactive threat hunting for their presence on a network. Similarly, having an understanding of the intent and capability of threat actors allows responders to react appropriately in the event of a breach and mitigate its impact. Additionally, the best response will be to attacks that have been anticipated and trained for. Intelligence is vital in enabling security teams to understand which are the most likely and most dangerous attacks that they will experience so that they can prepare accordingly. Furthermore, threat intelligence can also provide a valuable explanation in the wake of an incident and assist remediation efforts.

Resilience exercises

Threat intelligence plays a critical role in resilience testing exercises. The intelligence on which threat actors are likely to target the client organisations' critical functions and the key systems that underpin them, along with why and how they are likely to do it, is used to develop threat scenarios. These not only provide technical narratives of a likely attack against critical functions and key systems, but provide the rationale behind the scenario and an assessment of its potential impact on the business. These scenarios also shape the penetration testing plan used in the second phase of the engagement.

This ensures that rather than taking a compliance-based approach to cyber security, organisations are tested on their ability to defend their critical assets against techniques employed in the real world. This more realistic approach can also assist business continuity planning for cyber attacks.

Strategy

Strategic intelligence is particularly valuable in helping an organisation shape its security strategy. By understanding broader trends and shifts in adversaries' behaviour – for example the increasing abuse of legitimate processes and use of fileless malware – then you can develop a strategy to counter it, such as by developing a threat hunting programme. A strategic approach to understanding your cyber threats will enable budget to be allocated and a long-term strategy developed – often at Board level.

Risk

Cyber threat intelligence can be used as the first phase of a broader risk assessment process. If an organisation is available to identify their key information and system assets – often referred to as critical functions in the context of regulator-mandated cyber resilience testing schemes – then threat intelligence can illustrate the intent and capability of actors to target these assets. Impact assessments can then be used to calculate the level of risk to these assets, from which appropriate remediation steps can follow.

Tabletop exercises

Threat intelligence can be used to develop scenarios regarding, for example, the most likely and most severe incidents that may affect a particular company. In addition to using scenarios to shape a penetration testing plan, scenarios can be used to shape tabletop exercises. These are particularly effective in engaging the board, and assessing preparedness for certain scenarios in a time- and cost-efficient manner.

Training and awareness

As threat actors continue to exploit human weaknesses as an alternative to technical weaknesses in security postures, intelligence regarding the latest techniques – be it social engineering or other developments – can prove vital for education and training programmes for staff.

Compliance

A threat intelligence capability will also help organisations comply with legal and regulatory requirements, such as the General Data Protection Regulation (GDPR) or the Directive of security of network and information systems (NIS Directive). For example, companies subject to the NIS Directive need to follow a risk-based approach to cyber security and those subject to GDPR are required to evaluate the security of their data processing capabilities. Threat intelligence can also allow consumers to proactively identify potential breaches.

Development

In some organisations, threat intelligence can provide insight used to refine operations. For example, software developers can use the understanding of malicious actors' behaviour to embed better security practices into their work.

Why use an external supplier for cyber threat intelligence?

Expertise

Cyber threat intelligence providers should be specialists in their field and are likely to have a combination of previous experience and academic training. In addition to bespoke collection, processing and analysis capabilities that most organisations will not have internally threat intelligence analysts will generally have a very different skill set to information security professionals working inside an organisation. This will mean they will be able to assess a broader range of potential threats more accurately.

Insight

Cyber threat intelligence providers will have collection capabilities and access to sources beyond the reach of most organisations. For example, access to deep and dark web forums and marketplaces can provide insight otherwise unobtainable by the consumer.

External view

External providers will also bring a fresh perspective to complement an organisation's existing understanding of the threats they face, and provide independent validation. Looking at key information assets and systems from this new standpoint can help identify potential areas of threat, re-prioritise existing ones, and mitigate the internal analytical bias of groupthink.

Responsiveness

In the case of operational threat intelligence, the speed with which specialist providers are able to detect and notify consumers of incidents can offer a benefit over internal capabilities. Many providers will also be able to offer a round-the-clock reporting capability. Specialist cyber threat intelligence providers will also typically be ready to supply intelligence in a considerably shorter timeframe than would be required to establish the requisite capability internally.

Regulatory requirements

In cases where regulators drive the requirement for cyber threat intelligence, the provider will often to have come from a list of accredited suppliers to show that they are capable of producing the necessary standard of product.

Reassurance

As some aspects of threat intelligence collection involve a degree of interaction with threat actors and potentially malicious content, using an external threat intelligence supplier will help to alleviate some of the risks that collection inevitably entails. These providers are also familiar with these challenges and will be able to navigate the risks and potential legal pitfalls which apply to cyber threat intelligence in the UK. Relevant regulation includes: Human Rights Act 1998 (Article 8), Regulation of Investigatory Powers Act 2000 (RIPA), Computer Misuse Act 1990, Data Protection Act 1998 (DPA), Criminal Procedure and Investigations Act 1996 (CPIA), Bribery Act 2010, and the Proceeds of Crime Act 2002 (POCA).

Value

Although threat intelligence products will require some investment, economies of scale mean that the quality of a product provided by specialists will likely exceed that which a company can produce internally for the same cost. Any organisation seeking to develop its own cyber threat intelligence capability will need to build and staff an intelligence cell with the appropriate sources of information to analyse, which is always going to be an expensive and time-consuming challenge outside the ordinary course of business. Working with specialist cyber threat intelligence companies is likely to provide a more cost efficient and higher quality resource.

Which criteria should you use to select a provider?

Accreditations

In the UK, there are several frameworks to which the top tier of cyber threat intelligence providers are accredited. These include:

- the Bank of England's CBEST programme for intelligence-led security testing in the financial sector;
- the CREST Simulated Targeted Attack and Response (STAR) framework;
- the Crown Commercial Service Supplier List, which enables providers to supply UK government departments; and
- the UK Financial Conduct Authority's Skilled Person Panel.

Companies should also look for suppliers with individually-accredited professionals. The CREST Registered Threat Intelligence Analyst (CCTIA) operates as an entry-level qualification, while the CREST Certified Threat Intelligence Manager (CCTIM) qualification is the highest-level qualification intended for those likely to manage complex cyber threat intelligence engagements.

Cyber threat intelligence providers will also typically have accreditations such as Cyber Essentials and ISO 270001, though these are not critical in verifying the quality of outputs.

Reputation

CTI providers will typically be eager to offer references to attest to the high standard of work they are able to provide. As CTI suppliers will often have experience working with your industry peers, informal guidance from them as to which suppliers they have used will also be useful. On top of the quality of the deliverables and service, this should also extend to the provider's project management skills, particularly for standalone threat intelligence engagements.

Value for money

Although it should not be the key differential, providers should be able to offer competitively-priced products, either for standalone products or subscription services.

Legal, ethical and reliable

Cyber threat intelligence invariably involves collecting large volumes of data, potentially interacting with threat actors, and gaining access to sensitive client data regarding potential vulnerabilities. Providers should be able to illustrate their ability to adhere to strict legal and ethical standards, and should be able to share policies that collectors and analysts are required to adhere to when working on intelligence products. CREST-accredited CTI providers and individuals are required to adhere to strict standards of conduct when conducting engagements.

Questions to ask suppliers of cyber threat intelligence

- ***How wide a range of sources do you use?***
  - Providers should collect from and fuse together a broad range of original sources to provide intelligence, as per the intelligence cycle

- ***How do you collect from these sources?***
  - Providers should be able to deliver sufficient detail to reassure regarding their collection capabilities, and ideally be able to collect the information on their own without having to rely on third parties

- ***What types of threat actors does the intelligence cover?***
  - Providers should cover all types of actors that you face a threat from, which will usually mean collecting from a diverse range of sources

- ***How timely is the intelligence you provide?***
  - This should be governed by the level of intelligence provided i.e. strategic, tactical or operational

- ***What format is in the intelligence provided in?***
  - This will vary according to the nature and level of the material, but analyst access, in-person briefings, bespoke reports and intelligence reports relevant to your organisation are likely to be more useful than generic threat data

- ***How can the product integrate with my existing capabilities?***
  - The ability to integrate will be important if a recipient has existing providers and infrastructure

- ***How bespoke is the product to my organisation?***
  - Tailored products will invariably be more useful than generic outputs, and data is invariably less useful than fused intelligence that has been assessed by skilled analysts for your organisation

- ***What evaluation process do you apply to the intelligence you produce?***
  - Mature providers will have established methodologies for assessing intelligence and making sure it is bespoke to your organisation

- ***How do you remove false positives?***
  - Human vetting of material will result in less inaccurate reporting

- ***What are your team's backgrounds and language capabilities?***
  - Diverse and experienced analytical teams will invariably be able to provide the highest quality products and certifications of individuals may well be a useful guide

- ***Is your analysis predictive as well as reactive?***
  - Mature providers should be able to provide forward-looking assessments for your organisation

- ***Are your team individually certified as Cyber Threat Intelligence professionals?***
  - Professional-level qualifications exist in the practice of cyber threat intelligence, such as those provided by CREST, and other organisations such as SANS

- ***Is your business accredited as a Cyber Threat Intelligence provider by recognised authorities?***
  - Accreditations, such as by CREST, the Financial Conduct Authority and the Bank of England, show that the provider has proved its capabilities in addition to high legal and ethical standards

- ***Do you regularly provide services for these regulated frameworks?***
  - Mature suppliers will regularly support engagements for these frameworks

- ***How can you demonstrate knowledge of our (the buyer's) sector?***
  - The supplier may have experience in conducting bespoke research and have dedicated subject matter experts within the team

- ***What security measures does your company employ to keep our threat intelligence secure?***
  - Due to the potential sensitivity of the intelligence produced, suppliers should be able to reassure clients as to its security, for example, by sharing client information security policies.

- ***How can you prove the quality of your products and service?***
  - Suppliers should be able to provide references following successful engagements

References

Bank of England, "CBEST Intelligence-Led Testing – Understanding Cyber Threat Intelligence Operations", http://www.bankofengland.co.uk/financialstability/fsc/Documents/cbestthreatintelligenceframework.pdf

CIA/Richards Heuer, "Psychology of Intelligence Analysis", https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

European Central Bank, "TIBER-EU Framework", https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

iSIGHT Partners, "The Definitive Guide to Cyber Threat Intelligence", https://informationsecurity.report/view-resource.aspx?id=4486

Hong Kong Monetary Authority, "Cybersecurity Fortification Initiative", https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160524e1.pdf

MWR InfoSecurity and the Centre for the Protection of Nation Infrastructure, "Threat Intelligence: Collecting, Analysing, Evaluating", https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf

National Cyber Security Centre (NCSC), "The cyber threat to UK business 2017-2018 report", https://www.ncsc.gov.uk/cyberthreat

NCSC, "The Fundamentals of Risk", https://www.ncsc.gov.uk/guidance/fundamentals-risk
TIBER-NL, "How to conduct the TIBER-NL Test", https://www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf

US Army, "FM 34-2 Collection Management and Synchronization Planning", https://fas.org/irp/doddir/army/fm34-2/toc.htm

Record Future, "The Buyer's Guide to Cyber Threat Intelligence", https://go.recordedfuture.com/buyers-guide

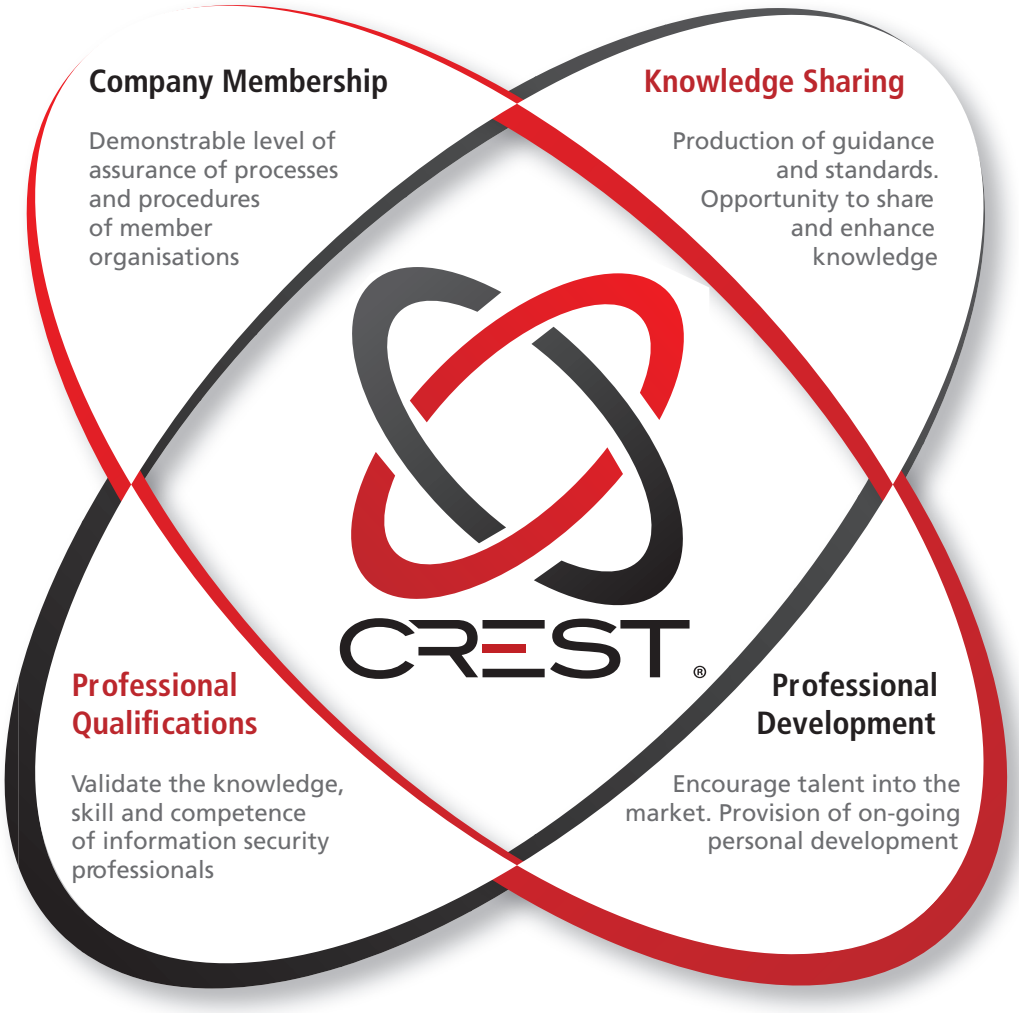
Resources

CREST, "What is CREST?", https://www.crest-approved.org/wp-content/uploads/CREST_UK.pdf

CREST BrightTALK Channel, https://www.brighttalk.com/channel/13519/crest

CREST Videos, https://www.youtube.com/channel/UCkfojeIzWdPTAmL4bLeewQw

CREST, "Cyber Security Incident Response Maturity Assessment", https://www.crest-approved.org/cyber-security-incident-response-maturity-assessment/index.html



For further information contact CREST at
http://www.crest-approved.org

Warning

This Guide has been produced with care and to the best of our ability. However, CREST accepts no responsibility for any problems or incidents arising from its use.