What Is Cyber Threat Intelligence and How Is It Used?

CREST Guide

Published by:

CREST
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 — CTI. It provides accessible advice on the theory and practice of CTI products and services. It outlines the key concepts and principles that underpin cyber threat intelligence, along with the ways organisations use cyber threat intelligence to predict, prevent, detect and respond to potential cyber security threats and reduce the overall level of cyber risk faced.

Audience

Increasing desire to adopt an intelligence-led, risk-based approach to managing cyber threats, in line with established best-practice, has contributed to the increasing prominence of cyber threat intelligence.

This often means personnel without formal intelligence training, qualifications or experience are required to deliver and procure intelligence products and services for their organisation and oversee and develop an intelligence-led approach to cyber security. This guide is intended to inform a broad information security audience, including those with and without previous experience and understanding of cyber threat intelligence as a discipline. It is intended for organisations in the public and private sectors.

Purpose

This guide is intended to help readers:

- Understand the principles of CTI, including the three levels of intelligence and different types of intelligence sources
- Appreciate how cyber threat intelligence can be used, including organisational and departmental applications
- Understand changes in the practice of CTI since the initial iteration of the guide, and provide some insight into what is next for CTI

Updated version

Following its initial publication in April 2019, an updated version of this guide has been published in June 2022. While the core sections regarding the theory underpinning CTI remain largely unchanged, in addition to the cosmetic redesign, changes to the revised edition include:

- Refreshing the section on sources for CTI
- Updating the section on use cases for CTI
- Creating an additional resources section
- Removal of the sections on procuring CTI services, which have been addressed in a separate guide
- Adding sections on the development of the practice of CTI since the initial iteration, and an assessment of the future trajectory of the discipline

About CTIPs

CREST Threat Intelligence Professionals (CTIPs) is a CREST International Focus Group. It has been established to represent global CTI practitioners and providers, and has three main objectives:

1. Increase the capacity of the private sector to provide CTI services and products
2. Enhance and maintain the quality of these services and products
3. Communicate on behalf of its membership

CTIPS is led by a sub-committee, comprising established and recognised experts in the CTI field. Additional information on CTIPs is available in the resources section.

What is Cyber Threat Intelligence?

Cyber Threat Intelligence (CTI) is increasingly established as a field, though continues to develop at a fast pace. However, the practice of intelligence itself is historically and commercially a very well-established discipline.

There are many definitions of intelligence. Regardless of the specific context to which they apply, 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 around us — the prelude to decision and action…"
>
> US Central Intelligence Agency (CIA)

It follows from this that cyber threat intelligence is processed and analysed data and information regarding adversaries' intent and capability to target system and information assets that is designed to help mitigate that threat.

Adopting an intelligence-led approach to security requires understanding key concepts such as threat, and risk, which are introduced in the next section.

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 they may 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.

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 organisations are tested on the 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:

- STAR (Simulated Targeted Attack and Response) as a generic framework applicable in any sector
- STAR-FS (Simulated Targeted Attack and Response for Financial Services) specifically for smaller UK financial institutions (i.e. those that don't qualify for the CBEST framework)
- TIBER-EU (Threat Intelligence-based Ethical Red-Teaming) for the European financial sector, and its various national derivative schemes (TIBER-BE, TIBER-DE, TIBER-DK, TIBER-FI etc)
- iCAST (Intelligence-led Cyber Attack Simulation Testing) for Hong Kong's financial sector
- GBEST for UK government departments
- AASE (Adversarial Attack Simulation Exercises) for financial institutions in Singapore
- FEER (Financial Entities Ethical Red Teaming) in Saudi Arabia
- CORIE (Cyber Operational Resilience Intelligence-led Exercises) for financial institutions in Australia

Threat and risk

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

Frequently, risk is defined as a combination of threat, vulnerability and impact.

To adopt a risk-based approach to cyber security, organisations 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.

Intelligence about the threat 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, 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 potential adversaries, the extent of the potential attack surface, and the pace at which the threat landscape evolves all combine to complicate the challenge.

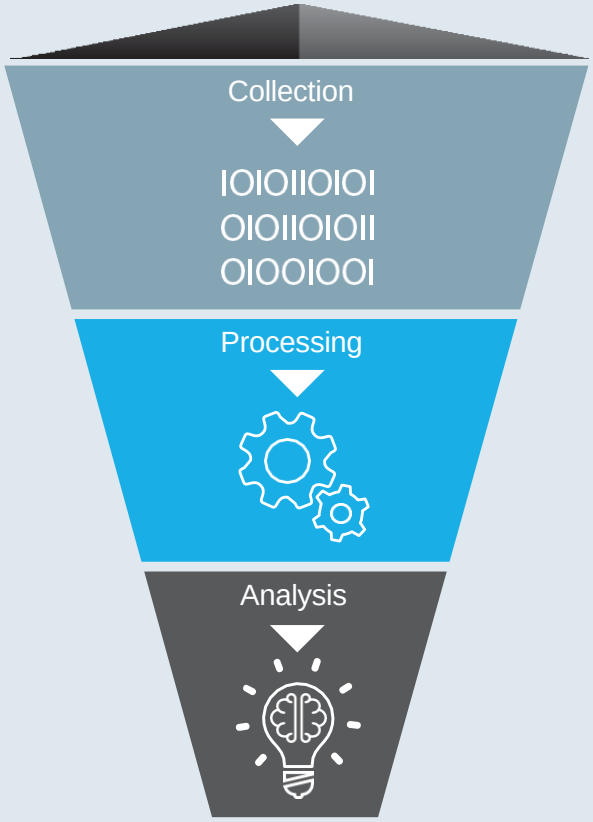
If organisations understand the threats they face, they can combine this with an assessment of the maturity of their defences — effectively their level of vulnerability — to ascertain the likelihood of an incident occurring.

Firms can also conduct impact assessments designed to place a monetary value on particular scenarios — for example, the loss of personally identifiable information (PII), or a 24-hour outage to a key system. The assessment likelihood and impact of a scenario can be combined to understand the risk. This allows organisations to prioritise cyber security resources against the most significant 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 development of incident mitigation strategies.

The Intelligence Cycle (see below) is an effective model that shows this processing of raw data into finished intelligence products.

The intelligence cycle

The intelligence cycle is a conceptual model that explains the process by which raw data and information is identified, collected, processed, analysed and disseminated as finished intelligence for use by decision makers. Adherence to the process and an understanding of what's needed at each stage helps ensure activities are directed and coordinated to efficiently satisfy consumer requirements

Figure 3: The four phases of the intelligence cycle

Planning and direction is the first phase of the intelligence cycle. It is used to coordinate intelligence activities to serve consumer 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).

Collection involves gathering the data and information likely to meet 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 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 intelligence cycle typically features four or five main stages, depending on whether processing and review are broken out from their respective parent phases of analysis and dissemination. Regardless of the specific model, the intelligence cycle is iterative in nature. All phases should incorporate a feedback and review process to ensure the required material is being processed and passed on correctly, and ensure consumer requirements are constantly at the heart of the process.

When applied practically, the intelligence cycle rarely operates with the strict demarcation between stages that the graphic suggests. Smaller, tighter cycles with their own feedback loops will typically operate throughout the delivery of a product or service to ensure its alignment with requirements.

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

Timely

Intelligence is useless if delivered too late. Less-than-perfect outputs delivered on time are preferable to outdated material.

Centralised

Centralised control allows for efficient allocation of resources and a primary point of contact.

Accessible

Intelligence products should be designed and delivered with their intended audience in mind.

Responsive

Intelligence should be responsive to consumers, with clearly defined reporting lines.

Continuous review

Assessments should be continually tested against new information, while feedback should spread throughout the cycle.

Objective

Analysts should remain impassive with assessments, which should be made independently from the policy process.

Sharing

Intelligence should be shared according lo protective markings, while protecting sources, when required

Systematic

Source, data and information should be methodically exploited in a coherent and coordinated fashion.

The different levels of cyber threat intelligence

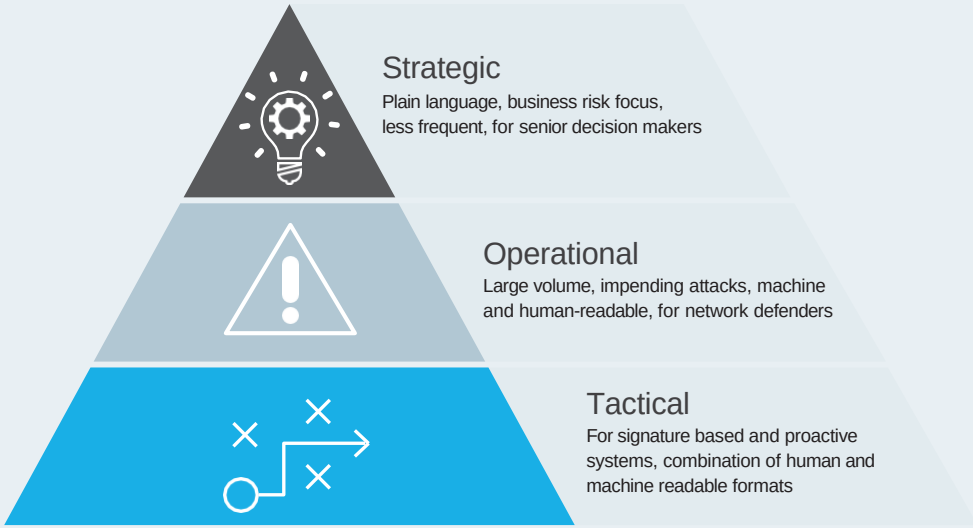
As with conventional intelligence, there are different levels of cyber threat intelligence: operational, tactical, and strategic. Each level differs in the nature and format of the material conveyed, its intended audience and its application. These are summarised in the infographic to the right.

Tactical threat intelligence is material regarding to the techniques, tactics and procedures (TTPs) used by threat actors. It is most effective in helping defenders understand how their organisation might be targeted, and what they can do to protect against it. This includes answering what tooling is used by adversaries, what infection vectors they are using to gain initial access, how they are avoiding detection after achieving a foothold, and what vulnerabilities they are looking to exploit.

Operational threat intelligence concerns details of impending or ongoing operations against an organisation. This will typically include large volumes of technical intelligence (which is occasionally tracked as a separate level) — such as atomic Indicators of Compromise (IOCs). Atomic IOCs are elements of data typically collected in the aftermath of an incident that can't be broken down any further — for example IP addresses, hashes, hostnames, filenames — which are consumed by automated security solutions.

Levels of intelligence

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 business risk rather than technical terminology. The reporting format of strategic cyber threat intelligence products will reflect this. For example, it will often be delivered on a monthly or quarterly basis to help shape longer-term security strategy.

Different sources of intelligence

Cyber threat intelligence suppliers should draw from a several different data sources to provide a rounded, holistic understanding of threats. As most organisations face a broad range of adversaries — including nation-states, cybercriminals and hacktivists, sources of data and information need to be equally broad to meet the challenge.

Most sources are technically open, in that the data they provide can be collected, processed and analysed by anyone with sufficient understanding and resources. In practice, however, although a one-person CTI function may be able to gather some form of data and information from several of these sources, systematic exploitation of many requires a level of capability and knowhow that tends to be concentrated in specialist CTI providers.

Sources commonly used by CTI providers and functions include:

Internal sources such as the output from a security information and event management (SIEM) tool, phishing filters, output from an endpoint detection and response (EDR) tool, and other logs covering system or network events provide a vital data and information source. Processing these requires careful configuration and will inevitably require dismissal of false positives. An understanding of the threats actually manifesting on a network, particularly when they can be corroborated with external sources, is of critical importance for understanding the overall threat a particular entity faces.

Atomic indicators of compromise (IoCs) are typically delivered in feeds consisting of malicious domain names, IP addresses (hosts) and hashes of malware samples associated with malicious campaigns. In recent years, EDR and firewall solutions increasingly automate bulk processing and ingestion of this data and alert when attempts to communicate with malicious infrastructure are detected. It is largely generated by reverse engineering malware variants. Previously, IoCs have been erroneously referred to synonymously with CTI, though require additional processing and analysis before they can be treated as an intelligence product in their own right.

Messaging platforms represent a crucial mode of communication for threat actors and can provide valuable insight into the goods and services cybercriminals are looking to provide to each other. The dynamic nature and rich functionality of platforms such as Telegram contribute to high levels of traffic, with dedicated channels or vendor shops facilitating the exchange of sensitive and illicit material. The more private the medium, the greater the collection resource required to gain and maintain access to the platform or conversation. In recent years, cybercriminal adversaries have increasingly engaged with their community via these dedicated platforms and via more direct, private means, rather than relying exclusively on forums and marketplaces on the deep and dark webs.

Deep web forums and other sites that sit behind login portals or paywalls, or are otherwise inaccessible via search engines, continue to represent a key mode of communication between cybercriminals, and therefore a potentially valuable source of information for threat intelligence services. These sources are particularly useful for understanding what data or information regarding your organisation has been exposed and is accessible to potential adversaries, such as leaked credentials, information, or even access for sale.

Dark web sources include marketplaces, shops and other sites hosted on anonymity-focused networks such as Tor or I2P. In recent years, the phenomenon of double extortion ransomware incidents has also seen the rise of sites operated by ransomware affiliates, which advertise their victims and publish stolen data. Although any CTI function can access these sources providing that they know where to look, operational security and logistical considerations mean more frequently, relevant sections of messaging platforms and the deep and dark webs are typically scraped in bulk by specialist threat intelligence providers, who provide access to the data as a service.

Social media represents a core part of the strategy of some threat actors, and this enables CTI providers to collect information directly from the source. Activists will often court publicity, encourage participation, and announce their intent to pursue particular targets. Criminals will use platforms to increase pressure on victims they are looking to extort or communicate with potential collaborators or purchasers of their goods and services. Threat intelligence services are also likely to use social media to collect information concerning the sentiment of the organisation and identify inadvertent or malicious data leakage. Finally, the cyber security community on platforms such as Twitter can also provide valuable and timely insight into developing issues.

Code repositories are an increasingly valuable source for CTI. Most threat actors have shifted away from developing their own malware, and instead rely on proof-of-concept exploits published by security researchers on sites such as GitHub, and on the capabilities of frameworks initially designed for legitimate penetration testers, such as Cobalt Strike. Understanding what tools and capabilities are accessible to threat actors via these sources is therefore crucial in understanding their capability. The publication of a proof-of-concept exploit on GitHub as part of the lifecycle of a vulnerability is often a key indicator for CTI analysts that broader exploitation is likely to ensue.

Vulnerability feeds and exploit databases have risen in prominence as sources of CTI as threat actors have become increasingly adept at the rapid exploitation of recently disclosed vulnerabilities. CTI programmes increasingly assess the implications of CVEs (common vulnerabilities and exposures) as they are released, to understand the potential implications for consumers.

Geopolitical developments are more important than ever as a source of information for holistic CTI services. Insight into a nation-state's strategic economic development plans can provide insight into the likely priority technologies and sectors its cyber espionage operations will target. In a geopolitical crisis, understanding how a state's objectives translate into the likelihood of disruptive cyberattacks helps inform which sectors should prepare.

Media coverage of technology and security-related developments will inevitably drive consumers' intelligence requirements. Where possible, CTI functions should remain focused on collecting via primary sources. However, an appreciation of what drives the public narrative around cyber security is also important, as this shapes mass perceptions of cyber security. Media sources are also typically the first to pick up company statements regarding breaches they have suffered, of particular importance in the era of big game hunting ransomware and securing supply chains.

Adversary tracking provides direct insight into the infrastructure, tooling and TTPs used by threat actor groups. Identifying patterns from past operations and exploiting lapses in operational security to proactively seek intelligence on adversary activity allows primary, timely and unparalleled insight into often sophisticated threat actors. However, the resources required mean this source is typically only exploited by CTI providers and organisations with an explicit requirement.

Incident response and breach investigations can provide deep insight into threat actor activity, particularly when the adversary has progressed through multiple phases of their operation. Specialist incident response firms can gather valuable insight into threat actor TTPs, though internal incident response capabilities can also reveal how an operation affecting the organisation itself unfurled.

CTI publications such as whitepapers and blog posts, largely based on the above two categories, represent a key source of potential intelligence. The threat landscape is so diverse and international, and different providers have different focuses, geographical presence, and expertise. Different approaches and techniques also mean providers identify overlapping clusters of activity and see different things, and increasingly reference each others' reporting. As a result, there is no single source of truth for this category, and lots of value to be derived from aggregating these different sources.

Human intelligence can be derived from engagement with individuals via several of the above sources — for example by engaging with an individual to gain insight unattainable via other sources. However, threat intelligence providers should only engage in such activity under a strict and defined framework and in pursuit of specific intelligence requirements — in a legal and ethical way. Providers must ensure collection efforts from human sources are compliant with legislation such as the Proceeds of Crime Act and the General Data Protection Regulation (GDPR).

Malware analysis allows CTI analysts to extract data such as IOCs from binary data, which can then be used to inform tools or investigate the intent and potentially attribute an operation. The accessibility of platforms such as VirusTotal and analysis sandboxes have helped democratise this capability, meaning you can derive actionable insight from a suspected malicious file without necessarily having extensive reverse engineering experience.

Government publications have developed in recent years as increasingly frequent and authoritative sources of CTI. The role of computer emergency response teams (CERTs), intelligence agencies and national cyber security bodies in responding to incidents and aggregating activity across multiple sectors provides unparalleled visibility into nation-state activity. Intelligence agencies can attribute operations to real-world adversaries and personnel. They are increasingly willing to do so via public statements and indictments, which provides additional insight into their operations.

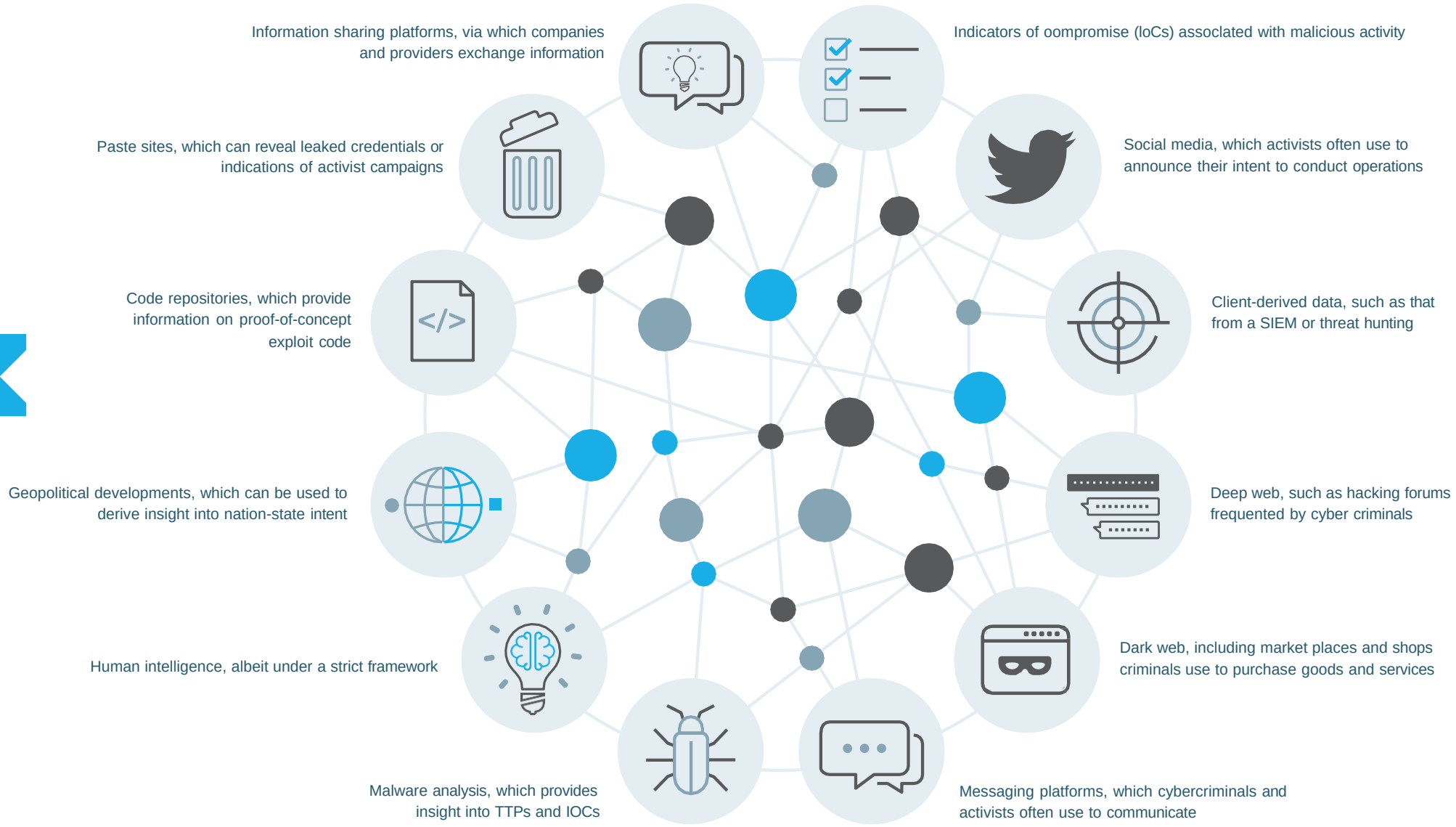
Digital risk protection typically encapsulates a variety of sub-sources, such as expired certificates, leaked credentials, phishing sites, paste sites and other potential sources of information leakage that can threaten an organisation's brand or operations.

Information sharing platforms provide context and insight into threat actors' current activity. These are typically divided along national or sectoral boundaries, such as:

- 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
- US-CERT's (United States Computer Emergency Response Team) Automated Indicator Sharing (AIS) platform

Rather than exploiting sources in isolation, effective CTI products and services should involve corroboration and fusing of material from multiple sources. It is possible for a CTI programme to have limited ability to exploit even just a handful of these sources and still satisfy the intelligence requirements of its consumers. However, this is a different challenge from establishing and maintaining a CTI programme with the capability to systematically exploit this full range of sources and satisfy consumers' intelligence requirements according to the principles of CROSSCAT.

Figure 6: A summary of different sources typically used by threat intelligence providers



Different types of cyber threat intelligence services

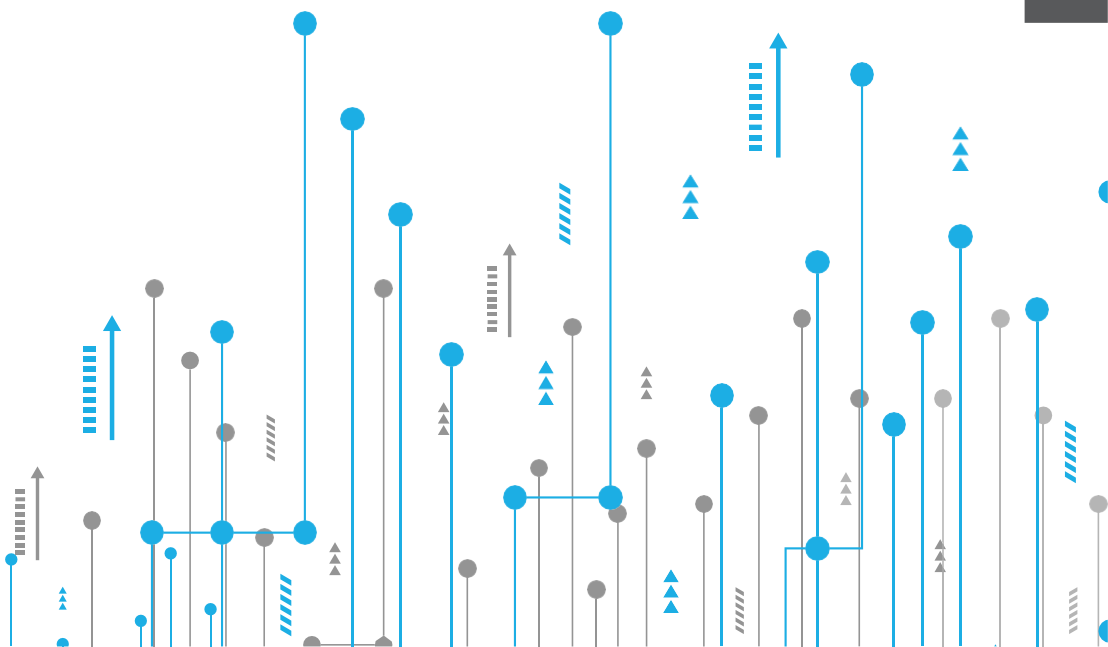
Cyber threat intelligence refers to a broad range of different products and services. These can be split into two broad categories: [a] standalone deliverables and [b] continued threat monitoring services.

A. Standalone deliverables include:

- Threat assessments that help consumers understand the intent and capability of threat actors to target their organisation, or a specific system or information asset. Threat assessments can be refreshed on a regular basis and consumed by a range of audiences and formats. These include the more strategic ones intended for consumption by senior leadership, to the more tactical assessments designed to inform controls and mitigation techniques.
- Targeting Reports, also known as digital footprinting assessments, look at the potential attack surface of an organisation, engaging reconnaissance techniques used by sophisticated threat actors to uncover and consolidate intelligence on the target entity. These increasingly include an assessment of the organisation's supply chain. They are designed to help consumers understand the extent of their exposure and how it could be exploited by an adversary.
- Threat scenarios detail potential attack paths against a particular system or asset within an organisation, often as a result of the output from a threat assessment and a targeting report. Such scenarios are used to shape penetration testing plans.
- "X" BEST projects, largely derived from the original CBEST framework for UK financial institutions, are regulator-mandated intelligence-led security testing engagements. These schemes require a combination of the above three deliverables, which help shape plans executed by penetration testing providers in the next project phase.
- Investigations, along with other smaller engagements, can be provided by cyber threat intelligence suppliers by leveraging their collection capabilities. Common use cases include trying to identify whether sensitive data has been exposed and is accessible on the deep and dark webs.
- Person-focused and protective open-source intelligence reporting, also known as Online Reconnaissance or VIP Exposure Reports, are intended to identify and mitigate potential threats to executives or VIPs. The CTI provider will imitate the reconnaissance processes used by adversaries attempting CEO fraud, or potentially more physical threat vectors, to present an overview of their potential exposure.
- Briefings into specific incidents, issues or areas of research, particularly suitable for senior personnel or those otherwise unfamiliar with cyber security.
- 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.

B. Continued threat monitoring services include:

- Subscriptions, provided via a dedicated portal and pushed reports, often integrated into the consumer's security architecture. Suppliers will usually provide access to a steady stream of current intelligence and timely reporting on relevant incidents, along with the ability to interact with the intelligence repository, 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 periodically by aspects of the above, standalone products.
- Threat Intelligence Platforms (TIPs) are used to aggregate and correlate different feeds and subscriptions, allowing consumers to pivot from various IOCs and conduct investigations.
- Data feeds consist of raw, uncontextualized or analysed data that will require some processing by the recipient organisation. These can include IOCs or data from messaging platforms and the deep and dark webs that can be enriched by the consumer.



How is cyber threat intelligence used?

In addition to the business functions outlined below, application of cyber threat intelligence in 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: intelligence that helps identify threats as they arise, or those that may already be present within a network, such as TTPs used for threat hunting exercises
- Respond: material that can inform a response to an existing incident to mitigate its extent or impact, such as TTPs used by a threat actor once discovered on a network which provide guidance on the cybercriminal's next steps and how the victim should act

The volume of threat intelligence an organisation can consume depends on the nature of material provided and maturity of the organisation. A separate exercise to assess the maturity of an organisation to generate, consume and disseminate cyber threat intelligence is a useful way of understanding how to improve an organisations' capabilities.

Security Operations Centre (SOC)

A SOC is responsible for processing and triaging large numbers of alerts from assets it monitors. CTI should help prioritise incoming material using security information and event management (SIEM) tools. CTI is also useful when deciding which incidents to escalate, and which are covered by existing controls or are less relevant considering the organisation's threat model.

IT security management

Tactical threat intelligence can help IT security departments prioritise adopting appropriate controls. For example, a company knows it faces a high threat from extortionists looking to use distributed denial of service (DDoS) attacks to take down its customer-facing portal. If the company has tactical intelligence regarding the tactics, techniques and procedures (TTPs) used by the extortionists — 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 means prioritising vulnerabilities for patching remains a challenge, even for organisations with dedicated vulnerability management programmes. Using a variety of sources, as discussed above, CTI services can provide crucial context regarding the potential threat to, and impact of, a CVE being exploited. This allows consumers to go beyond the standard Common Vulnerability Scoring System (CVSS) rating when deciding which CVEs to prioritise.

Threat hunting

For more mature consumers, CTI outputs can be used to proactively search for any evidence of malicious activity or potential compromise on the network or assets. Hunting can be driven by hypotheses around individual TTPs, using known IoCs, or more behavioural-based approaches.

Incident response

Intelligence is also critical for incident response processes. Understanding which TTPs and types of attacks used by threat actors most likely to target the organisation enables development of 'playbooks' to help guide response to a breach, train relevant individuals, and ultimately mitigate impact. CTI also helps dismiss false positives, provides valuable context in the wake of an incident and assists in remediation efforts.

Supply chain cyber risk

The increasing threat to supply chains has driven the use of CTI in third-party risk management (TPRM) programmes. Consumers that share relevant intelligence with key suppliers and partners will reduce the level of risk they face themselves.

Intelligence-led security testing

Threat intelligence plays a critical and increasing role in informing the penetration testing component of cyber resilience exercises (such as CBEST). Threat assessments, targeting reports and threat scenarios mean critical assets are tested using real-world techniques, as opposed to taking a compliance-based approach to security.

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 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 management

Cyber threat intelligence can be used as phase one 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. In addition to using scenarios to shape a penetration testing plan, they can also 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.

Situational awareness

Although broader in nature, improving situational awareness across the organisation on the latest developments in the threat landscape also represents a common use case for CTI. Although all intelligence products and services should be geared around actionability, contributing to a broader understanding of what cyber threats pertain to the organisation and its people is also important.

Training and education

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). Companies subject to the NIS Directive need to follow a risk-based approach to cyber security. 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.

Security engineering

In some settings, threat intelligence can inform controls and security mechanisms that can be built in to products during initial development cycles. 'Secure by design' approaches needs to factor in intelligence regarding threat actors and vectors most likely to target the technology.

Brand monitoring

Intelligence related to digital risk protection may be consumed by departments with a focus on brand and reputational monitoring — for example if adversaries are looking to imitate the organisation's brand or otherwise mislead potential customers.

Cyber threat intelligence past, present and future

How has cyber threat intelligence developed since the initial edition of this guide?

The first development that has ultimately driven all others is the increasing demand for CTI products and services. This demand has been largely driven by companies outside the most mature consumers of threat intelligence — for example large financial institutions and other well-resourced companies that face a disproportionately high threat — as these already had established programmes in 2019. Appreciation of the value of an intelligence-led approach to cyber security has increasingly encouraged the uptake of CTI.

This increasing demand has contributed to the growth of the commercial market for CTI products and services. Studies indicate the value of the CTI market has effectively doubled from US$5.5bn in 2019 to $11.6bn in 2021, with estimates for 2027 as high as $20.2bn.[1]

However, the way demand for quality CTI products, services, and practitioners continues to outstrip supply is also shaping the practice of CTI. As time has been at a premium for the resource available, there has been greater emphasis on automation.

New classes of products have emerged — such as Endpoint Detection and Response (EDR) and Security Orchestration, Automation and Response (SOAR) — designed to take an automated feed of threat data and respond accordingly. This has allowed analysts to move away from an exclusive focus on data and towards the true practice of CTI — analysing information regarding threats and informing decisions.

The growing adoption of these and similar technologies also means organisations consuming CTI have increased the capability to exploit native sources of data and information when trying to understand the threats that they face. For example, companies are now more likely to monitor logs via functionality on their cloud-based security platforms to identify and investigate suspicious activity than they were previously.

This shift has been facilitated by the growth and accessibility of open-source platforms and tools that help organisations establish their own CTI function and processes, where they would otherwise lack the resources to engage with a dedicated provider. The growing adoption of MISP and the OpenCTI platform are indicative of this trend, which, along with the exploitation of native datasets, has effectively helped democratise CTI capabilities.

As these changes have focused analytical capability, CTI functions and processes are seeing increasing integration within the broader cyber security architecture of the organisation. This represents a positive shift away from a standalone function and towards a model in which CTI can inform and direct a variety of different consumers within the company. Removing these silos and moving towards tighter integration of CTI within the organisation has also increased the typical numbers of stakeholders within organisations, each with their own requirements, feedback loops and processes of refinement.

A key contributing factor to integration of CTI has been the mass adoption of the MITRE ATT&CK framework. ATT&CK provides a common language to identify and track threat actors' activity and facilitates translation of CTI products and services into multiple different domains and use cases — such as security testing and evaluations of controls.

Another key development has been the rise of government bodies as providers of intelligence. Public reporting of CTI content remains dominated by the private sector. However, numerous national computer emergency response teams (CERTs), national security and intelligence agencies, and bodies such as the US Cybersecurity and Infrastructure Security Agency (CISA) have taken an increasingly active role in pushing out intelligence and enforcing associated standards.

These developments and increasing emphasis on transparency and sharing of intelligence have contributed to the notion of CTI as a public good. This has been driven by the increasing threat to supply chains and the interconnectedness of technology stacks — as illustrated by the 'Log4Shell' vulnerabilities. These shifts are increasingly resulting in better sharing of intelligence and capabilities from more to less mature entities, on the basis that rising security standards are a net benefit.

[1] 2021 SANS Cyber Threat Intelligence Survey

What next for cyber threat intelligence?

CTI products and services are likely to see deeper integration with other cyber security and broader business functions. Although we have outlined a broad range of use cases, it is important for CTI products and services to fully engage with other stakeholders to elicit and satisfy their requirements, as well as exploring how the principles and methodology of CTI can contribute to the broader organisation. Platforms are likely to move towards a 'single pane of glass' approach to provide a holistic threat-led perspective of the organisation.

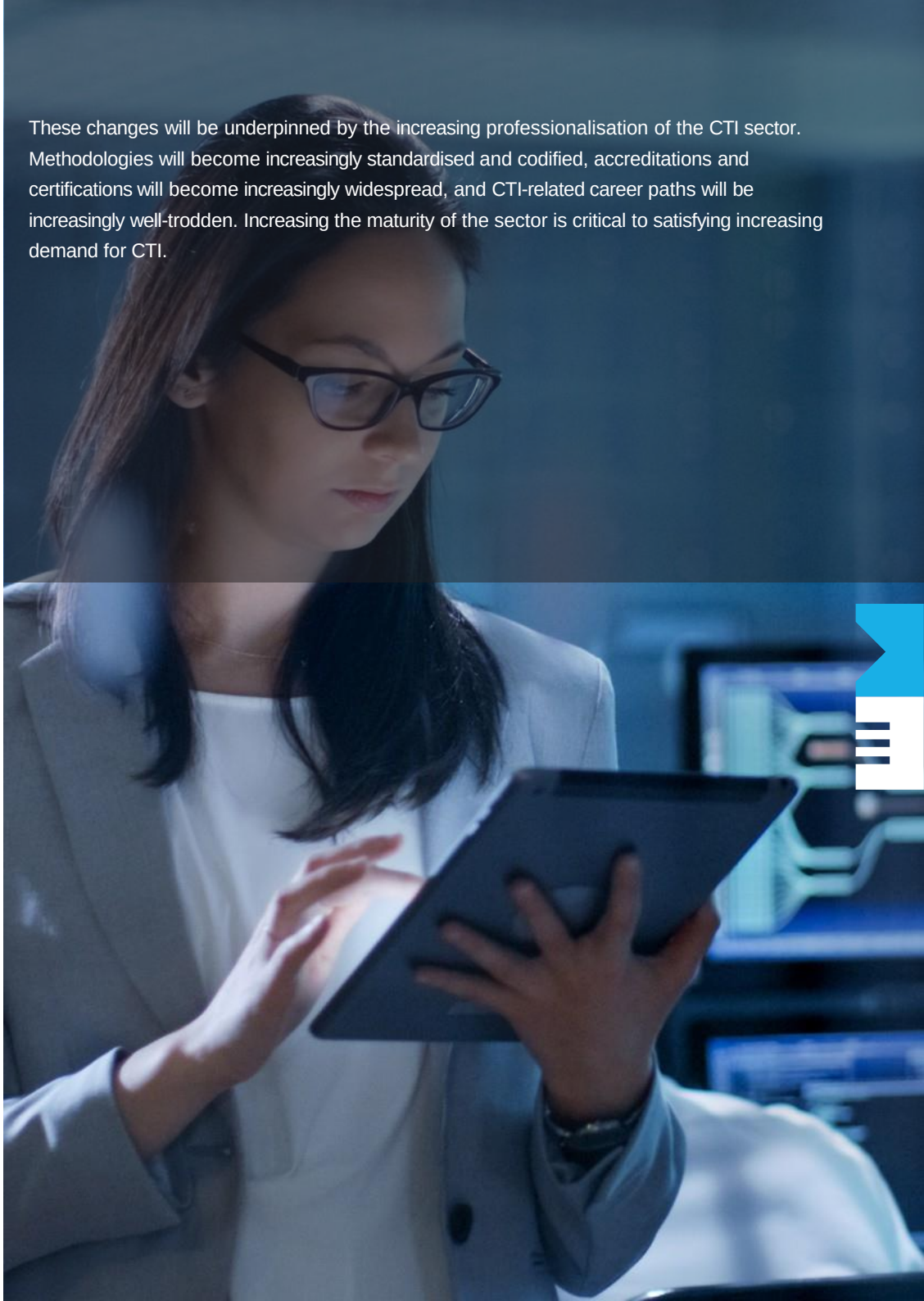
This trend should also be bolstered by the increasing sophistication and adoption levels of automated consumption and actioning of operational CTI outputs, which should mean more efficient human-machine interaction. For example, increasing adoption of machine learning in platforms to process and triage alerts should streamline and simplify the involvement of human analysts. Similarly, generative artificial intelligence and large language models will increasingly be used for repetitive tasks, like summary and report generation. This could mean more scope for more proactive CTI use cases within an organisation, and greater focus on what human analysts can do that machines can't.

The number of accessible data sources for an organisation to monitor and potentially exploit will also have significant implications for CTI. Solutions to monitor and establish a richer baseline of user activity — so anomalous activity can be detected — will be increasingly common. These solutions will attempt to address the continuing shift adversaries have taken towards fileless malware and 'living off the land.'

CTI products previously considered standalone engagements will increasingly be folded into business-as-usual practices for cyber security departments. Intelligence-led security testing will continue to develop as the gold standard for improving an organisation's cyber resilience. This approach is becoming more accessible to more firms in more sectors, with greater frequency.

Government bodies are likely to have increasing influence on domestic consumption of CTI. They will do this by declassifying and publishing CTI. They will offer a broader array of commoditised tools and services — particularly to organisations that would otherwise lack the resources to adopt an intelligence-led approach.

Public-private engagement will also be important in facilitating increased sharing of CTI products and services within relevant industry verticals and interest groups. The increasing emphasis of collective defence and appreciation of how threats to embedded technologies can result in systemic risks will also drive this development.



These changes will be underpinned by the increasing professionalisation of the CTI sector. Methodologies will become increasingly standardised and codified, accreditations and certifications will become increasingly widespread, and CTI-related career paths will be increasingly well-trodden. Increasing the maturity of the sector is critical to satisfying increasing demand for CTI.

Resources and References

CREST

What is CREST — https://www.crest-approved.org/about-us/who-are-crest/

CREST CTI Exams — https://www.crest-approved.org/certification-careers/about-crest-exams/

CREST YouTube Channel — https://www.youtube.com/channel/UCkfojeIzWdPTAmL4bLeewQw

CTIPS papers and guides

Cyber Threat Intelligence in a business context: A guide to finding the right cyber threat intelligence partner — https://www.crest-approved.org/wp-content/uploads/2022/04/CTI-in-Business-Context_2021.pdf

Assessment of Global Intelligence Led Penetration Test Frameworks: A report into how Global Intelligence-Led Penetration Testing Frameworks are perceived and might be improved — https://www.crest-approved.org/wp-content/uploads/2022/04/Assessment-of-Global-Intelligence-Led-Penetration-Test-Frameworks.pdf

Cyber Threat Intelligence Maturity Tools — https://www.crest-approved.org/cyber-threat-intelligence-maturity-assessment-tools/

Quantitative Risk Assessment: A guide to the practice of data-driven cyber risk assessment — https://www.crest-approved.org/wp-content/uploads/2023/05/How-to-Deliver-Quantitative-Analysis.pdf

Development of CTI

2021 SANS Cyber Threat Intelligence Survey — https://www.sans.org/white-papers/40080/

Rapid7 Evolution of Cyber Threat Intelligence — https://www.rapid7.com/blog/post/2021/08/25/r-evolution-of-the-cyber-threat-intelligence-practice/

Cyware: Evolution of Threat Intelligence — https://cyware.com/educational-guides/cyber-threat-intelligence/the-evolution-of-threat-intelligence-fdba

Threat Quotient: Evolution of Threat Intelligence Platofrms — https://www.threatq.com/evolution-threat-intelligence-platforms/

Intelligence led-security testing schemes

Association of Banks in Singapore: Red Team Adversarial Attack Simulation Exercises — https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf

Bank of England: CBEST Threat Intelligence-Led Assessments — https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide

European Central Bank: TIBER-EU Framework — https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

Hong Kong Monetary Authority: Cybersecurity Fortification Initiative 2.0 — https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/cybersecurity-fortification-initiative-cfi/

Other

Cyber Security Information Sharing Partnership (CiSP) — https://www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp-

NCSC: Weekly Threat Reports — https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc

NCSC: The Fundamentals of Risk — https://www.ncsc.gov.uk/guidance/fundamentals-risk

NCSC Annual Review — https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat

Richards Heuer: Psychology of Intelligence Analysis — https://www.ialeia.org/docs/Psychology_of_Intelligence_Analysis.pdf

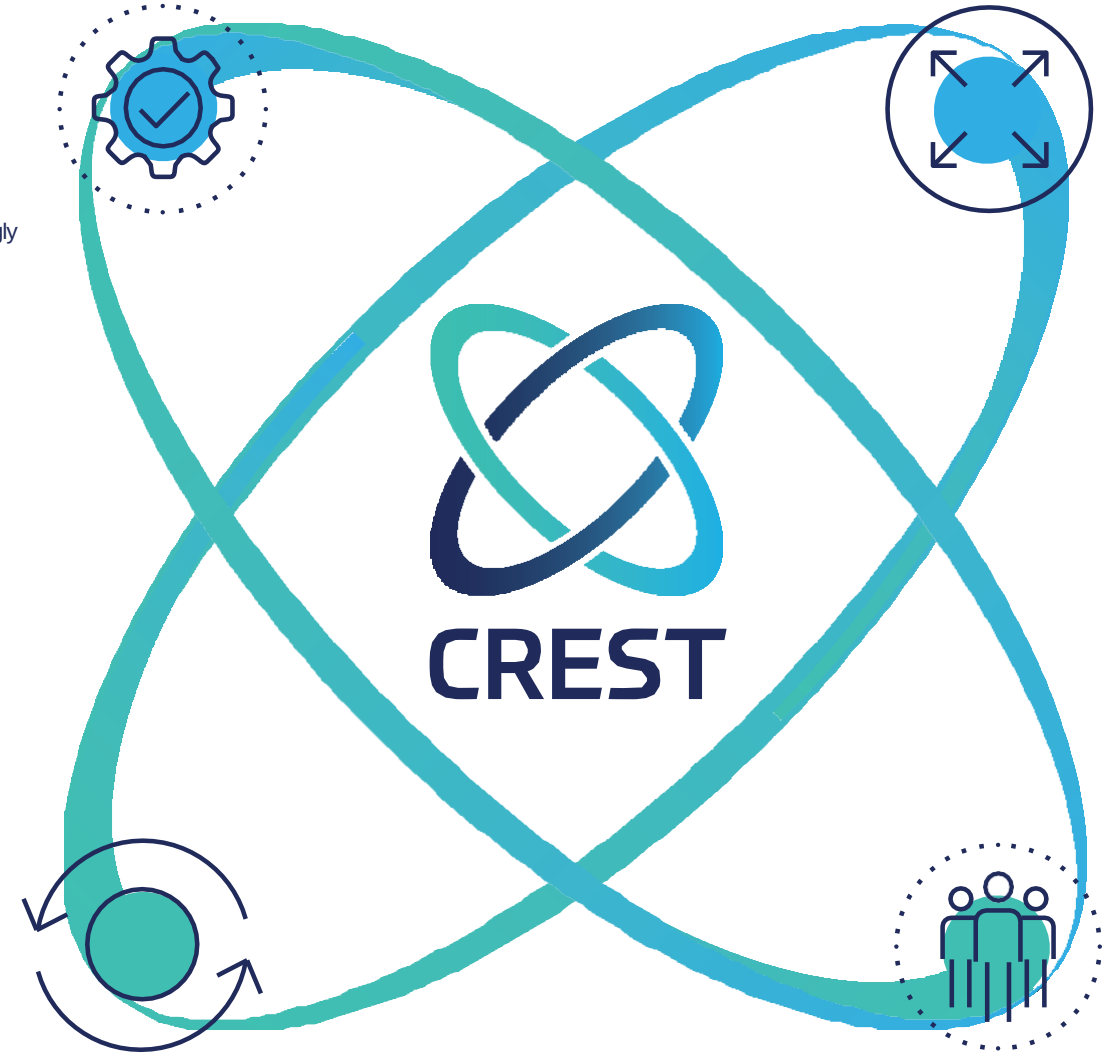
US Army: FM 34-2 Collection Management and Synchronization Planning — https://fas.org/irp/doddir/army/fm34-2/toc.htm

Capability

We develop and measure the capability of cyber security organisations and help individuals become increasingly skilled and competent

Capacity

We work across the industry to grow the pipeline of cyber security expertise



Consistency

We set global standards for cyber security organisations to deliver a high quality of service

Collaboration

We develop and engage with the global cyber security community to leverage our shared knowledge and capabilities for the benefit of all

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.