JUMPSEC

EVALUATING THE STATE OF CYBER THREAT INTELLIGENCE

Cyber threat intelligence (TI), defined as data that offers insight into a threat actor's motives, targets, and behaviours, has soared in popularity in recent years.

These factors have contributed to a TI boom where subscription data feeds proliferate.

However, organisations should not regard TI as a silver-bullet solution. This article explores the limitations of conventional TI data feeds and highlights the key characteristics of effective TI usage.

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

Why organisations should think twice before paying for a subscription to a threat intelligence platform, service, or data feed

Globalisation and modern geopolitics have contributed to increasing awareness of cyber threats, particularly outside of typical cyber security conscious teams and organisations.

These factors have contributed to a TI boom where subscription data feeds proliferate, and business executives base their investment decisions on the day's trending cyber threats.

The utilisation of TI in principle enables an organisation to move from reactive to proactive security, promising foresight to global threats posed by advanced cyber attackers. **However, organisations should not regard TI as a silver-bullet solution.**

This article explores the limitations of conventional TI data feeds and highlights the key characteristics of effective TI usage, making recommendations for organisations currently considering the purchase of a TI subscription.

In this article, we argue that:

- Investing in TI without possessing the foundational means to use it effectively will fail to deliver security advantages and can be actively detrimental to an organisation's cyber defences.
- Organisations mistakenly prioritise external TI, but TI gathered internally is the superior option for an organisation to find actionable and relevant data.
- TI is most useful when applied in support of an established security operations function (e.g. to aid a dedicated threat hunting team) contextualising external TI with business processes and deployed digital technologies to ensure TI-led operations produce the intended security benefits.

The state of threat intelligence today

TI has become increasingly generic and commoditised

TI has become a familiar concept thanks to the international spread of threat-led regulatory schemes (such as CBEST and TIBER in the UK and Europe), and the parallel rise of offensive security services designed to replicate real world threat actors.

In this environment, purchase of TI tooling and subscriptions to data feeds are more popular than ever, as more organisations seek to anticipate and defend against the latest offensive techniques and tooling, and react to the latest vulnerability disclosures.

Stakeholders outside of IT and security teams and external parties (customers, regulators) have become increasingly aware of the risks posed by cyber-attack. This has led to the definition of TI widening, and the best practices for effective use becoming blurred.

TI today has become a catch-all term, ranging from what has been defined as operational intelligence (technical details about specific attacks and campaigns) **to strategic intelligence**[1] (broader trends relating to the organisation's profile and its associated cyber risks). Some have advocated a change in terminology to acknowledge this shift in meaning, proposing the term 'security intelligence'[2] over TI to reflect its more comprehensive nature.

The limitations of generic TI

Ultimately, not all TI is good TI, and investing in a TI feed alone is not equivalent to developing a TI-led security operations function.

While most TI subscriptions rely on the sheer volume of data as an indication of value, an experienced operator knows that the amount of truly actionable TI is small, and that 'noisy' data feeds can impair operations. Most criticisms of the commodified TI available on the market focus on the merits of each category of TI, which are typically consumed by the different audiences – **strategic**, **tactical**, and **operational**.

Strategic

Intelligence relating to malicious cyber campaigns perpetrated by threat actor groups (often state-aligned)

Tactical

Intelligence relating to attacker techniques, tactics and procedures likely to be used against the organisation

Operational

Intelligence relating to specific vulnerabilities or threats, often focusing on specific indicators of compromise (IoCs)

[1] https://www.recordedfuture.com/threat-intelligence/

[2] https://go.recordedfuture.com/book

The reality is that all are typically executed in a flawed way. For example:

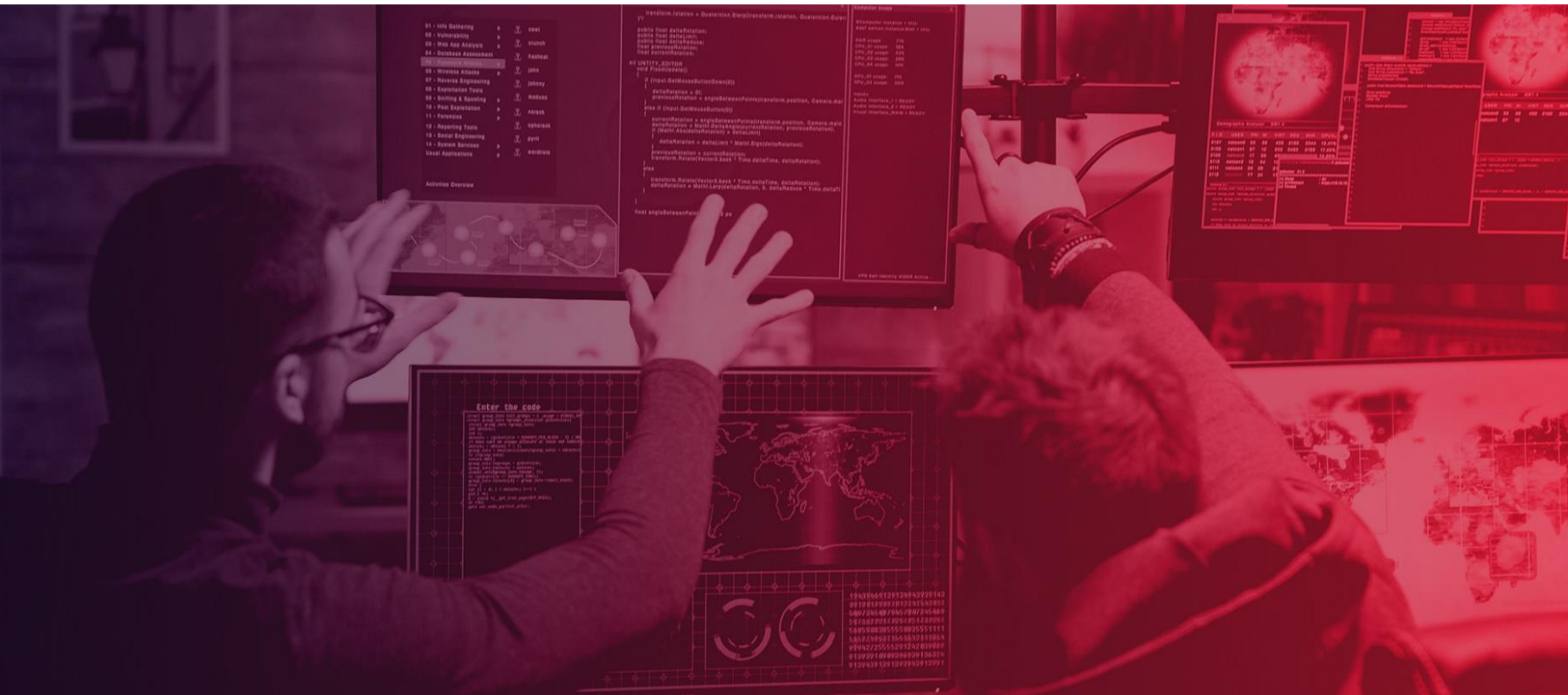
- **Strategic** TI is often indistinguishable from news and largely fails to be actionable or useful for security teams. This results in a disconnect between TI-led security strategy and operations.
- **Tactical** TI is often not targeted to an organisation's network or cannot be utilised effectively by the security team due to capability limitations, or a lack of visibility of network composition and topology.
- **Operational** TI is typically high-volume, low fidelity, often providing information that is either not relevant to the organisation's systems, or can only be used short-term before the attack techniques evolve and the IoCs are made redundant.

There are some key principles here which highlight where commodified TI fails to deliver security advantages:

- **Relevance** – Does the TI take into account the specific needs of the organisation? For example, is it relevant to the organisation's industry and threat profile, and the digital technologies they use?
- **Specificity** – Does the TI relate to the specific organisation? For example, considering focused offensive campaigns targeting the firm's assets, employees, customers, or supply chain.
- **Audience** – Is the information appropriate for the intended audience, with actionable outcomes? Also, is the intended audience able to use the information effectively, in tandem with other technologies (e.g. SIEM, EDR), to support security operations?

The primary audience of TI should always be the security team. TI that is designed for a senior business audience is likely to be of limited relevance to the organisation to inform security strategy. TI must first be processed and contextualised by the security analysts.

Basing security policy and investment on generic intelligence will inevitably result in security investment that is misaligned to the firm's actual security requirements. Security requirements should be contextualised with understanding of the network's 'attack surface'; the ways in which an attacker is most likely to target the organisation which would result in the greatest business impact.



Why organisations fail to use TI effectively

In short, TI fails where the consumer fails to understand their security requirements - the threats they face, the technologies they have deployed, and the most high-risk attack paths across their network.

The best TI doesn't relate to specific vulnerabilities, or generic news stories, but focuses on malicious activity specific to the business – such as campaigns in which similar organisations have been targeted, instances where credentials of your employees have been leaked (and where attackers have attempted to use them), ongoing targeting of your customers, impersonation of your brand, and typosquatting of your websites. All these sources, which can be actively investigated and monitored by a suitably skilled team, provide far more actionable intelligence than any generic data feed can.

Organisations can't expect their systems administrator to oversee TI-driven security operations. Generalist IT teams are thinly stretched in organisations without dedicated security staff, and in JUMPSEC's experience, many generalists lack the required capabilities, competencies, and capacity to use TI effectively. At best, TI is not applied due to capacity limitations. At worst, wider IT operations can be derailed by the business decision to focus on TI, leading to gaps in security operations as effort is misappropriated to TI. Organisations should always look to invest in the human resources and technology infrastructure to use TI effectively before investing in a paid-for TI feed itself.

All too often, subscription to a TI feed is driven by the promise of a silver bullet solution. However, like any other product purchase, failing to consider why it is needed and how it will be used (and by whom) will result in it failing to deliver the intended outcomes. These organisations typically lack the security foundation required to effectively use TI to their advantage.

The primary use case of TI is to drive security operations; prompting investigators to proactively search for the threats which are most relevant to their business, as opposed to reactively responding to security alerts. Without the necessary apparatus to support TI-led security operations, such as a sophisticated asset management system, robust vulnerability management process, security monitoring capabilities, and broader network visibility (e.g. EDR), consuming a TI feed will provide minimal security value.

In fact, analysing internal TI often enables more effective consumption and filtering of external TI. Internal data sources of value include network event logs, records of past incidents, IoCs found in firewall logs, and normalising user activity to better highlight abnormal behaviour.

> **For example, analysing how common base64 PowerShell encoded commands in your environment can be layered with your internal visibility of whether the action would blend into the noise of other encoded commands or stand out were an attacker to use this technique.**

Attackers will always look to traverse the 'path of least resistance' to their objective, the most optimal and direct path across the network. Organisations who lack foundational capabilities are likely to be exposed to common, pre-weaponised exploits which are trivial for an attacker to leverage. Investing in TI to identify a broader range of threats is redundant where obvious gaps in security posture exist. Put simply: TI won't help if there is an unpatched, legacy device exposed to the internet which is not appropriately secured.

The key principles of effective TI

- **TI must always be actionable.** There is no value in consuming a TI feed if it is not used in a constructive way - either because of the quality and relevance of the data, or the capability of the user.

- **TI is situational, not general.** Good TI should be relevant to a specific situation or context, enabling an organisation to focus in a specific risk area based on the threat posed. If an organisation's TI is generic, it belies the fact that deeper, root-cause security issues exist, indicating the need for broader security improvement and reducing the value of TI.

- **TI usage should be highly targeted.** Consuming too much TI is likely to pose a capacity issue. However, having large data sets is not harmful, so long as organisations are specific about the data they use. If an organisation is trying to use all the TI it ingests, it is likely not using it effectively.

- **TI does not always yield results.** TI does not always have a predictable outcome and ramping up TI-led operations does not necessarily equate to better value. Initial (good) TI adoption is likely to yield a number of wins which cannot be easily replicated. Equally, since TI operations do not always highlight issues, it can be challenging for TI teams to demonstrate the difference between finding nothing, and doing nothing.

- **TI gathering as a process is (arguably) more valuable than TI itself**. The process of gathering TI is synonymous with learning more about the organisation's digital workings and security requirements. The insights from gathering organisation-specific TI can often lead to deeper discoveries about how attackers are looking to abuse business operations.

> **The fact that the process of TI gathering is inherently valuable means that, while TI-led investigations (sometimes termed 'hunting') are not always fruitful, TI is always a useful and productive component of a security operating model when used effectively.**

Getting the most out of TI investment

TI-driven security operations are integral in driving effective security analysis and investigations. However, it is important to put the horse before the cart and invest in the proper apparatus before harnessing TI. **Organisations who do not have visibility of their network, an established security operations function with dedicated security analysts and threat hunters, and access to suitable tooling (SIEM, EDR) should not invest in a TI subscription.**

Organisations can find a wealth of open-source information over the internet providing threat intelligence without subscribing to a paid-for feed. Focusing on building a capability that will benefit from TI, and using open-source information to drive activities, will build the right behaviours and ensure that any future paid-for TI is certain to be of value.

If in-house capability is not an option, selecting a security partner who properly integrates with your organisation and leverages TI in a contextualised, specific manner will deliver the same positive outcomes.

Conclusion

Consuming a TI feed alone is not enough to realise the benefits.

As is ever the case in cyber security, there is no shortcut, and organisations need to be committed to putting in the hard yards to implement an effective TI-led security operating model. Before investing in an external TI feed, buyers should consider whether they have everything they need to make their TI programme a success.

If they don't, investing in capability development should precede a paid-for TI subscription, with a view to revisit the potential purchase at a later date. Then, if a feed is still seen to be beneficial, buyers can make the purchase with confidence. **However, they may well find that they no longer need to.**

Useful resources

Examples of useful (free) TI feeds include:

- https://cyware.com/community/ctix-feeds
- https://github.com/hslatman/awesome-threat-intelligence

JUMPSEC

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com