CYJAX

Digital Intelligence
Securing the Future

Threat Intelligence Providers: An Overview

CLIENT CONFIDENTIAL

Businesses and organisations are faced with an ever-increasing number of cybersecurity events, including account take over, ransomware combined with blackmail, and Business Email Compromise (BEC) scams. The perpetrators range from state-sponsored actors launching cyber-espionage operations to entrepreneurial cybercriminals armed with commodity malware available from darknet markets through malware-as-a-service offerings.

2020 has been dominated by COVID-19: this has given threat actors the opportunity to launch pandemic-themed phishing campaigns to lure victims into providing them with corporate access or revealing credentials to email and other business systems.

In addition to these social engineering attacks, cybercriminals and nation-state threat actors have weaponised proof-of-concept (POC) exploits and have conducted a series of global cyber-attacks on vulnerable systems.

Meanwhile, threat intelligence (TI) providers are struggling to keep up with the demand for their services, particularly from small and medium-sized businesses. These organisations are faced with a confusing range of options to choose from and need to make decisions on effective cybersecurity aligned to their unique threat models. Complicating this decision are key outcomes such as protecting their organisation from attack; meeting compliance requirements and demonstrating a return on investment by mitigating business interruption; or catastrophic downtime associated with a cyber event.

This guide is intended to help companies and organisations looking for a TI solution to meet their unique requirements. It is focused on advising businesses how best to review and optimise their use of a TI provider. This decision is not to be taken lightly: what suits a company operating in the energy sector, for example, may not be relevant to a healthcare provider.

Choosing your TI solution

TI providers help organisations understand the cyber-threats they are currently facing, or with which they may be confronted in the future. Helping your company to build an effective TI capability involves collecting and analysing data from a wide variety of open and closed sources, and delivering it in a timely manner.

The goal of TI is to detect and prevent intrusions, and to offer mitigation strategies where appropriate. The range of TI solutions, however, has grown rapidly, leading to scepticism about their effectiveness, particularly with regard to the quality of analysis that is provided to customers.

What should you be looking for when making this important decision?

The most useful TI service is one that is tailored to fit the exact threat models of your organisation. Most providers will offer very similar services, typically with a focus on obtaining and analysing information from common TI sources. These should include darknet forums and marketplaces, as well as information from open-source websites and services. You can expect to receive advice on a broad range of issues relating to the protection of your critical assets. This will include information on:

- System vulnerabilities
- Software patches
- Indicators of Compromise (IOCs)
- Phishing campaigns
- BEC scams
- Malware variants

- Ransomware and blackmail campaigns
- Fraud and theft

Vendors may also monitor:

- Social media
- Instant messenger forums
- Mainstream media
- Data leaks
- Blogs and reports published by a range of researchers

While there will, of course, be common demands from all types of enterprises, the challenge lies in identifying the TI offering that best provides proactive, accurate, timely and actionable intelligence specific to the organisation's threat models.

One of the most useful things a TI provider can give to an organisation is intelligence that is specifically aligned to them. In the financial services industry, for example, banks will be particularly interested in receiving intelligence regarding banking Trojans [1] and ATM malware [2], as these threats are targeting the unsuspecting consumer who may be duped into downloading an app or visiting a malicious website that appears genuine but is actually a clever fake.

Companies operating in the retail and hospitality sectors will want intelligence on the latest attacks on Point of Sale (PoS) systems, particularly developments concerning the "Magecart" [3] techniques used to compromise payment portals.

Pharmaceutical companies and healthcare facilities are frequently targeted, as the personal and financial data held by them are extremely valuable on the criminal market. 2020 has been an interesting year in this regard: as well as threat actors launching phishing campaigns, the US and UK governments both claimed that pharmaceutical organisations and university laboratories had been targeted by Russian, Chinese, Iranian and North Korean threat actors intent on stealing COVID-19-related research as the race to find a vaccine continues. [4]

Businesses operating in other economic sectors will have their own unique requirements: those involved in energy, telecommunications or other vital critical national infrastructure (CNI) will need to know about attacks or campaigns aimed at their counterparts around the world, as this intelligence will allow them to prepare for the attacks that are likely to target their own networks.

It should be clear, then, that a 'one-size-fits-all' TI solution is not the optimum approach for companies of any size.

In addition, employees in your own IT departments simply do not have the time to wade through irrelevant data and general 'noise'. Ultimately, it is the responsibility of your TI provider to capture and highlight the information that is most pertinent to your organisation and turn it into accurate, timely and actionable intelligence.

Build TI capability in-house or outsource to a vendor?

It is worth mentioning here the financial issues to consider when making the decision on whether to outsource your cyber intelligence requirements to a third-party provider. Developing an in-house TI capability is expensive. You would need to hire and train analysts and purchase all the tools they need. In comparison, buying the service from a vendor could cost you around £50,000 - £100,000 or more per year. One major issue to consider is that an in-house team will be working alone and may lack the vigilance and responsiveness of a larger dedicated team. The cyber threat landscape is dynamic and broad: it is hard to keep abreast of all the developments.

Focusing on intelligence: the dashboard

A TI portal should be designed to allow your staff to access the intelligence they need to guide the organisation's cyber defence activities as quickly and efficiently as possible.

Many TI providers will offer dashboards to highlight key information and implement metrics for basic trend and pattern analysis. The issue with this approach is that determining what constitutes 'key' intelligence to a large multi-national bank, for example, might be vastly different to that of any other industry. Security teams working in IT departments do not want to be inundated with anything and everything that 'might' impact their networks: they need to focus on imminent threats.

Your organisation must concentrate on the protection of all its assets against both physical and cyber threats. The ability to have a dynamic TI solution that scales to global levels will allow you to separate these different cybersecurity and brand protection requirements across independent dashboards and visualise filtered information in multiple formats including metrics, data tables and maps.

A custom-built dashboard enables you to monitor all sources efficiently to visualise the risks to your critical assets in real-time and in one place. A brand monitoring dashboard, for example, can be created to pull information from a variety of mainstream and social media and filtered against keywords, providing visibility of what is trending and potential negative sentiments.

The service should be scalable so that various business units within an organisation can make use of it in their own way. Each member of your security or IT teams can have their own dashboards built to focus on their specific areas of responsibility. The marketing or PR team can monitor the organisation's brand, while a purchasing team can track third-party suppliers, and executives can get the latest news about your industry sector. Physical security teams can even stay informed about street protests that might be taking place close to your key company locations.

The ability to visualise your sources in multiple different presentation formats, especially using metrics alongside the filtered data, can be a powerful tool. The insights from pattern analysis can function as a precursor to looking into deeper trends leading to actionable intelligence. For instance, you could create a dashboard for an investigation into your threat landscape: this could start with a graph showing the number of incident reports linked to specific malware types over time; or you could focus more closely on monitoring vulnerabilities. You could then dig deeper by filtering the results to show those incidents and exploits which are affecting organisations in your sector. Your team will then be able to visualise relevant data and information in varied formats, and to identify trends and links, turning the intelligence into an effective recommendation for security action.

There is little point in subscribing to a service that provides real-time feeds if the information is not tailored to your industry sector, geography or unique organisational threat models. A customisable dashboard, therefore, boosts efficiency by enabling the creation of actionable intelligence which enhances the overall security of your business, reducing risks associated with attacks and exploits against your customers, employees and operations.

The analysts

While much of the dashboard technology means that the specific threat information your organisation needs will be accessed by your team with a simple click, support in the form of a team of organised, competent analysts is vital for effective TI. The role of the analyst is to harness information and data from a wide variety of sources - both open and closed - and turn it into actionable intelligence. This might involve something as simple as looking into an IP address with no context given: the job of the analyst, in this case, is to find the context, apply the intelligence process and provide a recommendation to protect your organisation. A more complex inquiry, on the other hand, might require some highly specialised and time-consuming research using technical or historical data.

Building up a personal relationship between a TI provider and your IT team can make all the difference. Having quick and direct access to an expert analyst who understands your organisation and its specific threat models is a significant yet often overlooked factor when making decisions about outsourcing TI to a third-party vendor. This is especially important at the start of any new TI programme.

Geopolitical events and cyber threats

Serious cyber-espionage and organised cybercriminal activity often stem from state-sponsored threat groups who have adopted Advanced Persistent Threat (APT) actor techniques, especially with the emergence of ransomware and blackmail tactics. The effective monitoring of geopolitical events, tensions and rhetoric – particularly those involving China, Russia, Iran and North Korea's relationships with nations of the West – offers a vital insight into emerging cyber threats and attack trends.

These state-sponsored threat actors have grown in sophistication over recent years. China, for example, has long been accused by the USA of engaging in cyber-espionage for the specific purpose of stealing corporate or government-classified information. Most recently, President Trump issued executive orders preventing Chinese companies such as Huawei from participating in business activities in the US; the UK, Australia and a range of other western countries have followed suit. [5]

Russian threat actors, on the other hand, are believed to place significant emphasis on interfering in elections around the world, in particular the US presidential election of 2016 and the EU referendum in the UK the same year. Operating from St Petersburg, they focus on disinformation and destabilising political systems globally. In addition, Russian APTs have targeted critical infrastructure in various post-Soviet states since 2007. Recent tensions in Belarus and the region of Nagorno-Karabakh need to be monitored for the emergence of threats that could spread in a similar way to the NotPetya attacks on Ukraine in 2017. [6]

The activities of Iranian APTs have also become more sophisticated in the last couple of years, particularly in response to President Trump's attempts to impose sanctions against the country. Some researchers believe the Islamic Revolutionary Guard Corps (IRCG) has developed arguably the widest range of offensive operational cyber capability seen thus far. The Iranian threat actors conduct operations focused on surveillance of dissidents, election interference, espionage and Bitcoin currency heists, as well as destructive cyberattacks including ransomware campaigns. The 2011 capture of an American Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle (UAV) by Iranian forces near the city of Kashmar in northeastern Iran elevated Iran to a near-peer adversary having developed capabilities potentially rivalling even the United States. It appears that due to Middle East geopolitical constraints, Iran has been forced to use cyber-operations as its primary foreign policy tool [7]; interestingly, it is also thought to outsource these attacks to intermediaries loyal to the regime.

North Korean threat actors are particularly interesting; they were believed to have been responsible for the hugely damaging attack on Sony in 2014, while in 2017 they were deemed by many researchers to have carried out the WannaCry ransomware campaign that affected as many as 300,000 computers worldwide. [8] In 2017, successful cryptocurrency heists were attributed to them. Then, in 2019 they were reported to have attempted five major cyber-thefts worldwide, including stealing $49 million from an institution in Kuwait. Some researchers have claimed that the North Korean government uses these cyber-operations to obtain funds for their nuclear arms programme. [9]

It is clear that these state-sponsored groups are responding to political events and perceived acts of aggression from the West and regional western allies. Given that their operations and successful attacks have been increasing, a TI provider offering analysis and effective monitoring of both cyber and 'real-life' events around the world will be of great use to organisations, especially if supply chain partners and/or regional offices are targeted. By effectively evaluating the potential fallout from emerging geopolitical events, analysts can predict possible physical or cyber threats and attacks.

Mapping risk

Some TI vendors produce a cyber risk map. We have all seen graphics featuring DDoS attacks currently taking place all over the world. They look nice but offer little else. A useful risk map will detail recent attacks and threats taking place in a country or region and may also include information about legal developments: this can be particularly beneficial for companies engaged globally. In China, for example, while the government continues to enhance its social monitoring programme for citizens, it has also been enacting laws that have an impact on foreign businesses operating there. By keeping track of these developments, TI can ensure the right parties are informed of any potential disruption to customers, team members or operations in the country or region.

An organisation doing business in India, for example, can rely on a TI provider to keep them up to date with news and analysis on unusual or concerning events taking place in the region. In December 2019, for instance, increased hostilities between India and Pakistan led to state-sponsored APTs from both nations targeting each other, something that may well have had an impact on organisations operating in both countries. Individual cybercriminal groups may also have taken the opportunity during a time of uncertainty to launch their own attacks. In these unstable situations, patriots and criminals will seek out opportunities, elevating both physical- and cyber-threats.

Activism has increased due to various global events and concerns such as climate change. As a result, a wide variety of government and corporate organisations have been targeted. These activities tend to reflect well-publicised political events involving large numbers of demonstrators. Government corruption, poverty, inequality and environmental concerns are particularly popular issues that mobilise people both on and offline. Spain, Chile and Nicaragua have all featured heavily in hacktivist activities, and support for street protesters has resulted in online activists directing sustained and often damaging cyberattacks against government and company websites.

The most recent example of the relationship between real-life protests and hacktivism was seen in August and September this year when thousands of people marched in the capital of Belarus every weekend to protest against the 'rigged' presidential election. Along with the demonstrations, unnamed threat actors leaked the personal data of more than 2,000 police officers. [10]

Tracking global political events and malicious cyber activity is a challenge for any organisation. The key to effective 'Geocyber' protection is the level of research and knowledge required to write an intelligence report that can mitigate or even bypass a disruptive physical or cyberattack. Knowing the tactics, techniques and procedures (TTPs) a malicious actor may use can ensure defensive measures are in place before the attack manifests.

SOCMINT and social media research

Social media and instant message monitoring is another important service which many TI vendors offer. While a team of analysts can carry out research on platforms such as Twitter and Facebook or instant messaging channels (Telegram, WhatsApp etc.), far more efficient results can be obtained by using a combination of manual and automated scraping techniques to filter information.

Like the requirements for "Geocyber" monitoring briefly outlined above, a dedicated team of analysts should be on hand to deal with any OSINT and SOCMINT-related requests and investigations required by your organisation. The more advanced providers have a search capability, allowing data on a variety of keywords or trends of interest to be gathered and analysed; security threats can then be forwarded to your organisation.

Darknet monitoring

Stolen credentials, compromised accounts, malware and ransomware, potential conspiracies, protests and petitions, drugs, firearms sales, terrorism, extremism and child exploitation material are all found on the darknet.

Some TI providers will claim to offer automated monitoring of these underground forums and channels: this can never compensate for having a dedicated team of analysts who focus exclusively on these. Ransomware operators also now have their own dedicated leaks sites to advertise their claimed attacks; while it may not be possible to see the data that is being listed for sale, the knowledge that it has been offered can provide useful insight.

If an analyst sees that 'insider access' is being offered to a bank's systems, for example, the financial institution can be alerted. Steps can then be taken to mitigate this issue, whether by choosing to track the threat actor or by using the information provided to make an attempt to identify the person responsible for the post. One recent example involved a threat actor posting a request for details of accounts so that his insider contact could check the balances and fraud markers – at a cost. When presented with an image of the forum post, the affected bank was able to identify the person responsible; legal action followed. This sort of intelligence will never be replaced by automation: much of it depends on an analyst building up a reputation on the darknet or relationships with threat actors using the forums and channels.

This cybercriminal underground has its own feuds and drama which lead to cyberattacks among these threat actors. In September 2020, 179 suspects were arrested in a massive global darkweb takedown called Operation Disruptor. [11] This was an unprecedented international law enforcement effort stemming from last year's seizure of a popular underground bazaar called Wall Street Market whose database of users was "doxed" by a rival criminal group.

Indicators of Compromise (IOC) validation and false positives

IOC validation is an essential feature of TI. A great deal of time can be wasted by providers sending over 'false positives' to a client: these can cause all sorts of issues for your organisation, including blocking business access to legitimate services or installed applications.

A TI vendor must have their own processes and tools which can identify and remove those false positive IOCs before they are sent to a client. With rapid digital transformation and organisational silos, it is important to ensure that a newly discovered website is legitimately malicious and not a newly created and owned business service. Looking at the details such as geo-location, hosting and IP reputation, and communicating the findings in an intelligence report can mitigate the chance of a false positive IOC from turning into a blacklist entry which will disrupt a smooth rollout of the organisation's newly launched service.

Tactics, Techniques and Procedures (TTPs)

Careful assessment of TTPs will provide you with the ability to focus on the activities of specific threat actors and create ‘heatmaps’ relevant to the sector your organisation is operating in, thereby helping you to gain the knowledge needed to detect possible attacks and strengthen your defences.

Security Tool Integration

To make use of security intelligence, you must be able to operationalise it in an efficient manner. You will most likely use a set of tools capable of ingesting API feeds to aid in your day-to-day security operations. One feed that may be particularly useful is contextualised and validated IOCs. It is recommended that you select a partner that has support for integrations with a range of security tools like SIEMs, SOARs and TIPs. The last thing you want to do is buy a TI capability that cannot integrate with your existing technology and may in fact prove to be an additional cost if the provider cannot accommodate your solution.

Conclusions

There are many benefits – both technical and financial - to using a TI provider for your intelligence information needs. It is important to understand the rules and regulations your organisation is subject to as fines and penalties for unauthorised disclosure of sensitive data can be significant, especially in light of the EU’s General Data Protection Regulation (GDPR). In October 2020 British Airways was fined £20 million for the 2018 data breach that affected 400,000 of its customers. All organisations that collect and process the data of EU citizens are subject to this regulation, not simply those based in the EU. [12]

In an ever-changing cyber-threat landscape, all organisations are advised to consider the use of TI and to research vendors carefully. Do not be afraid to ask questions; insist on detailed demonstrations; and above all, work towards building up a trusting relationship with your chosen provider.

“If the Intelligence you are receiving is not proactive, accurate, timely, actionable and specific to the organisation’s threat models, you are wasting your money.” – Ian Thornton-Trump (@PhatHobbit)

October 2020

Published by Cyjax Ltd., London

[1] https://www.zdnet.com/article/this-new-trickbot-malware-update-makes-it-even-harder-to-detect/

[2] https://www.wired.com/story/atm-hackers-jackpotting-remote-malware/

[3] https://www.csoonline.com/article/3400381/what-is-magecart-how-this-hacker-group-steals-payment-card-data.html

[4] https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development

[5] https://www.androidauthority.com/huawei-google-android-ban-988382/

[6] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[7] https://www.timesofisrael.com/how-irans-military-outsources-its-cyberthreat-forces/

[8] https://searchsecurity.techtarget.com/news/252448325/Lazarus-Group-hacker-charged-in-Wannacry-Sony-attacks

[9] https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf

[10] https://www.reuters.com/article/us-belarus-election/hackers-leak-personal-data-of-1000-belarusian-police-on-weekend-of-protests-idUSKCN26B09X?rpc=401&

[11] https://www.wired.com/story/operation-disruptor-179-arrested-global-dark-web-takedown/

[12] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

STATEMENT OF CONFIDENTIALITY

This document contains confidential trade secrets and proprietary information of Cyjax Limited. The recipient is expected to treat this document as they would their own confidential internal material. Neither this document, nor any diagrams contained in this document, may be disclosed to any person outside of the recipient's organisation without express written permission from Cyjax Limited. By accepting this document, the recipient affirms that they will comply with these expectations.

Cyjax Limited, Registered in England and Wales no 08302026.
Registered Office Suite 53 Peek House, 20 Eastcheap, London EC3M 1EB.
United Kingdom.