IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

Five Pointers for Choosing a Threat Intelligence Platform: What to Look for in a TIP

Anthony Perridge

Anthony Perridge
Vice President,
International
ThreatQuotient

Biography

Anthony Perridge is Vice President, International for ThreatQuotient (https://www.threatq.com), a company dedicated to revolutionizing cyber defence capabilities by building analyst-driven applications, helping organizations manage threat intelligence and therefore defending against sophisticated cyber attacks.

Prior to joining ThreatQuotient, Anthony served as the EMEA Sales and Channel Director and previously held senior leadership roles at AirDefense and McAfee.

Anthony blogs at https://www.threatq.com/resources/

Keywords Cyber security, Threat Intelligence, IT, Business, Software, Crime, Security operations, Cloud
Paper type Opinion

Abstract

As 2022 gets under way and the new financial year looms, many companies are starting to identify the key strategic focus areas for the year ahead and the technology investments needed to deliver them. In this article, the author gives five top pointers and discusses what to look for when choosing a Threat Intelligence Platform.

Introduction

Given the aggressive cyber threat environment experienced over the past 18 months, cybersecurity investment is high on the list for many. Increasingly, organizations are building out their own Security Operations Centre (SOC), incident response capabilities and threat intelligence teams, as they aim to meet risk management and compliance demands and proactively defend the business.

However, building a SOC unleashes a deluge of data from disparate sources which often overwhelms in-house teams and prevents the SOC from functioning effectively. The solution – one which is on many 2022 shopping lists right now – is a Threat Intelligence Platform.

A Threat Intelligence Platform (TIP) serves as a central repository for all threat data and intelligence from internal sources. Correctly configured, the TIP should be able to deliver essential context around threats that helps the team understand the who, what, when, how, and why of a threat. Crucially, it should also help prioritize threats, based on the parameters set by the organization, filtering out the noise so the resulting actions are clear.

A good TIP benefits a range of stakeholders, from the board aiming to understand strategic risk to CISOs focusing on improving defence while staying on budget, and from security analysts collaborating more effectively to incident response teams benefiting from automated prioritization of incidents.

Knowing what you need to invest in is the first step. The next is to understand the key features you need and why. There is a lot to consider, but in my view the following are five key areas that should be on your checklist as you evaluate TIPs:

1. **Ability to consume structured and unstructured data**
   A TIP must be able to import data from every possible source – internal and external, proprietary, and open source – and in every format, whether structured or unstructured. This includes data from the full ecosystem of

modern security tools such as endpoint detection and response (EDR), Network Detection and Response (NDR) and Cloud detection and response (CDR). Where unstructured data, such as blogs and social media posts is concerned, the platform must be able to parse and extract "de-fanged" or "neutered" data such as neutralizing potentially risky URLs while leaving them readable by analysts.

The threat environment changes constantly, so the facility to create new custom connectors to ingest intelligence around new threats as they emerge is also key. So, too, is the ability to define additional objects to fit specific use cases, allowing teams to tailor the platform to their preferred workflows.

2. **Context is king!**

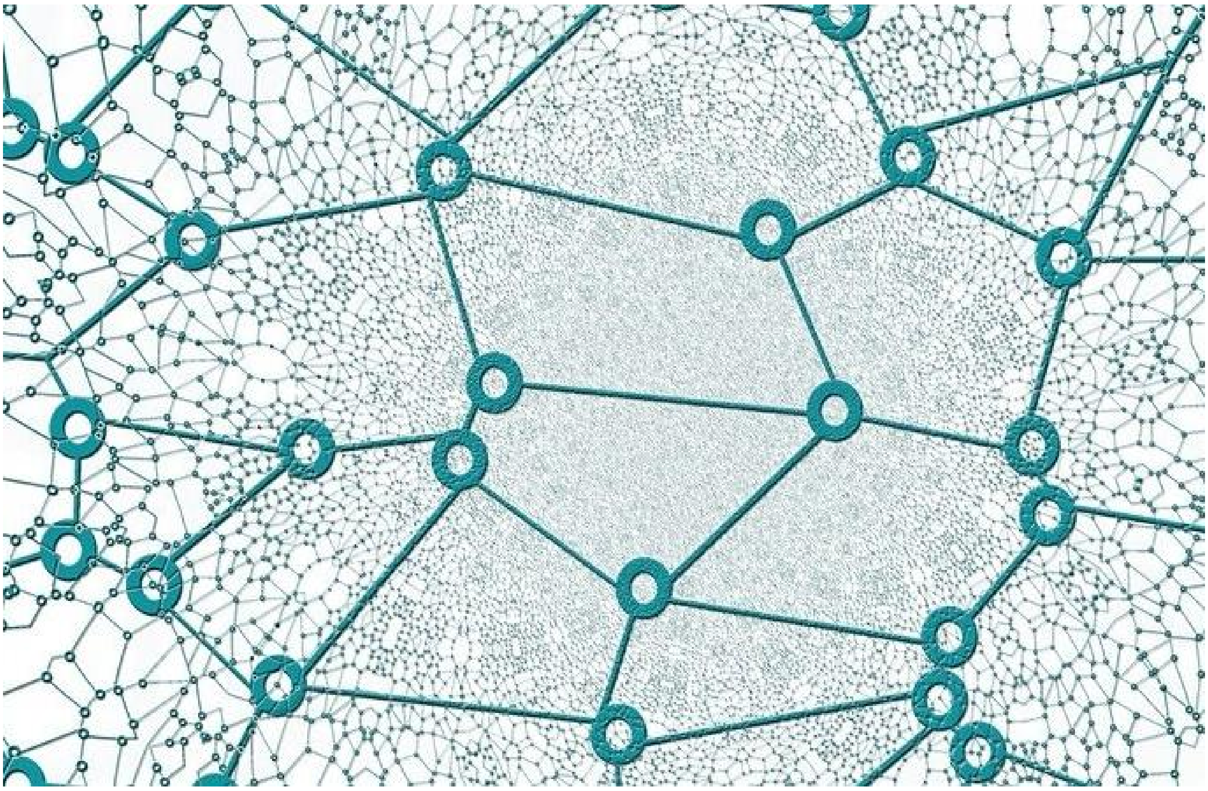
Context is the crucial piece of the jigsaw allowing teams to make sense of what the mass of indicators are telling them and respond appropriately. Due to the importance of the supporting context, it is important to determine if the TIP vendor imports all the data and/or if they modify any of the data.

Modification can be helpful as a layer of normalization is critical to de-duplication efforts. However, normalization and unification of data must be done while preserving context. For instance, if Feed X publishes https://www.badguy.com, Feed Y publishes http://www.badguy.com and Feed Z publishes www.badguy.com, all three should be reconciled into a single IOC entry. Those are all "technically" different indicators; however the goal is to efficiently maximize detection strategies with minimal duplication. Data feed normalization helps to consolidate analyst comments, better organize associated intelligence and effectively export one IOC in lieu of three IOCs, which makes for greater efficiency.

3. **Scoring and prioritization**

The sheer volume of indicators published today means it is impossible – and indeed undesirable – to monitor them all. This makes scoring and prioritization a key feature of an effective TIP. Teams need a mechanism to prioritize which indicators should be detected to investigate, blocked or disregarded as a non-threat.

Scoring is highly specific to the organization and the mission of the team and should not simply reflect vendor or community opinion. A progressive TIP will let you set your own scoring algorithm based on any piece of data in the system, making it a more tailored and accurate threat management solution.



4. **Multiple integration options**

Integration with the full ecosystem of security tools is central to the value proposition of a TIP. The tighter the integration, the less manual work is required of analysts and the greater the efficiency of operations teams.

Uni-direction integration – from the TIP into an endpoint solution for example – is a given. This is a purely defensive strategy and is the most common integration, moving the automatically scored highest threats from the intelligence platform into the trenches of the organization's sensor grid for detection and/or blocking.

The next wave of TIP integration is bi-directional, with data pushed out from and pulled back into the tool. Key use cases for bi-directional integration are SIEM or log repository, ticketing systems, vulnerability management solutions and SOAR solutions. These combine to drive efficiency, improve prioritization and reduce incident response times and vendors should offer software development kits (SDKs) and open APIs to facilitate powerful integrations.

5. **Data-driven automation and investigations**
For under-pressure security teams, the ability to automate repetitive, time-consuming, low-level tasks is essential. If a tool can combine this automation with the real-time data and context needed to empower analysts to investigate high impact, time-sensitive incidents, even better! Effectively, teams need a balance between automation and manual investigation and the threat intelligence platform should deliver that using a native, data-driven approach.

Business considerations when choosing a TIP

Beyond the technical considerations – of which the above provide a snapshot and are not exhaustive – organizations also need to evaluate business factors.

Pricing is usually on a subscription and per user licence basis, which is a straightforward initial calculation based on the number of tactical users you have. However, a successful implementation should see a broader set of stakeholders realizing the value of having access to the platform, so it is worth forecasting for access by teams such as risk management.

As discussed above, integration is central to the TIP value proposition, and vendors should provide an SDK and open APIs to facilitate this, but some charge a fee per integration. This can significantly increase the budget when you consider the number of different tools you want to integrate, so it is vital to know this upfront. Similarly, should the business undertake mergers or acquisitions, this will entail integrating the acquired company’s tools into the TIP, which will have a financial implication if a fee is payable each time.

Finally, understand the cost implications of hosting the TIP on-premise or in the cloud. If you are evaluating a cloud-based service but know you will need to deploy a private cloud instance for compliance or privacy requirements, be sure to understand if there are any additional costs and trade-offs in functionality/features. A TIP designed to run in the cloud often cannot offer full functionality on premises.

The right Threat Intelligence Platform has the potential to dramatically boost the performance of the SOC and selecting one should be a carefully researched and rigorous decision. As organizations aim to improve proactivity and embark on activities such as threat hunting, while effectively prioritizing response to incoming threats, a powerful TIP will allow them to get the most out of existing resources and maximize the return on historical investment in security tools.