Ovum
TMT intelligence | informa

Ovum Market Radar: Threat Intelligence Platforms

Taming the mass of threat data and turning it into actionable security intelligence

Publication Date: 04 Dec 2018 | Product code: INT003-000291

Rik Turner

Summary

Catalyst

All organizations are facing increasing levels of threat as a result of being part of a hyperconnected world. The flipside of mass mobility of access and global connectivity to the plethora of available online services is the huge increase in opportunity for malicious actions and actors. Protecting against and reacting rapidly to cyberthreats is now a topic high on agendas in boardrooms as well as with security professionals. This has led to a demand for more dynamic and widespread information and intelligence about the threats being faced. Threat intelligence platforms (TIPs) should offer a coherent way to analyze threat data effectively to build better security intelligence and take proactive measures to mitigate the risks.

Ovum view

For those tasked with addressing security, there are many sources of data. Networks can be probed, devices inspected, anomalous actions detected, and log files analyzed. Reacting quickly is important to ensure that breaches are rapidly detected and responded to.

However, reacting is no longer sufficient. Potential threats need to be analyzed and understood before they hit the organization so that pre-emptive action can be taken. This means gaining further threat data, often from outside sources with varying degrees of trust and validity. It might also incorporate human as well as system-derived data. This information needs to be normalized, corroborated, aggregated, and refined to produce threat intelligence that can be readily analyzed and acted on.

This is what TIPs are designed to do and why they have come into being. Ovum's view is that a TIP does not replace other security tools, but instead will augment them by combining many different varieties of threat data. It also builds on the skills of threat analysts, allowing them to focus on adding forensic value to the security process rather than mundane investigative tasks. This vital addition to security capabilities provides a consistent model for gathering and understanding threat intelligence, as well as for being able to share it in a way that can be of use both externally and internally and taking action to mitigate risks.

This model is well structured for being delivered in some way as an outsourced service as well as in-house, meaning it should work for organizations both large and small. Some organizations will have dedicated threat intelligence teams in security or network operations centers (SOCs or NOCs), while others will rely on a managed security services provider (MSSP). A TIP could fit well in either case, serving in-house security experts or those delivering threat intelligence as a service.

To augment threat analysis, a TIP must deliver a significant element of automation and orchestration, both in the gathering of data and in the output and actions taken. There may also be significant application of artificial intelligence in aiding the understanding and interpretation of potential threats. There is already some use of machine learning and discernment and this is expected to grow as the market evolves. How much this might undermine the role of the threat analyst is open to question. Some vendors might try to fully automate the process with the ultimate aim of replacing the human

role. While this might eventually be possible for a significant number of threats, Ovum believes that there will be a role for highly skilled human intervention for the foreseeable future.

Ovum's view of the vendors assessed in this Market Radar is summarized in Figure 1.

Figure 1: Ovum Market Radar for Threat Intelligence Platforms

Key capabilities	Product vendor			
	Anomali	EclecticIQ	ThreatConnect	ThreatQuotient
Ingestion	◕	◕	◑	◑
Enrichment	◑	◑	◕	◕
Automation & correlation	◕	◑	●	◑
Visualization	◑	◑	◕	●
Analysis	◕	◕	◕	◕
Sharing	◕	◑	◑	◕
Integration	◕	◑	◕	◕

Key to assessments of functional areas:

○: Lacks capability ◔: Minimum capability ◑: Partial capability ◕: Broad capability ●: Advanced capability

Source:

Source: Ovum

Key messages

- Internal systems are often heavily monitored for security risks, but there is a vast amount of threat information available beyond the organization.
- External information varies in quality, form, and structure. Gathering and refining it for use is a significant undertaking.
- This will be worthwhile if it delivers intelligence that can be used proactively for both awareness and prevention.
- Threat intelligence platforms put structure and workflow in place to take best advantage of all available data and augment the capabilities of security experts so that pre-emptive action can be taken.

Recommendations

Recommendations for enterprises

Whether they have in-house capabilities or not, all organizations need to be taking preventive action against the cyberthreats they face. Many have adopted a defensive posture, reacting as quickly as they can and dealing with threats as they occur. This is no longer sufficient. Organizations need to collaborate with their peers and build a more proactive security stance. This will involve being able to model the threats they face, better understand the impact, and take action before an event occurs. This is where a TIP is designed to help. However, investing in a TIP is only part of what is required. A TIP will provide a framework and structure for the threat intelligence process and automation where possible. Embedding this into the organization's security strategy will take additional effort to ensure the required skills and expertise are in place to take full advantage of a proactive security stance.

Recommendations for vendors

The appetite for achieving the results that a TIP can deliver is broad, but not all organizations have the right capabilities. They need not only a TIP, but also help in how to build the best security posture and how to grow their own capabilities (and staff) to help deliver it. Where there are skilled security experts and analysts in place, the primary aim of the TIP should be to make them more productive. Tools should amplify their strengths and automate or minimize mundane work. Vendors also need to extend the software and services on offer beyond the platform itself. Integration with other security elements is vital, but so too is the building of a wider ecosystem of partners that are able to offer complementary or supporting services.

Defining and exploring threat intelligence platforms

Definition and characteristics

There is already much security information available inside an organization from either IT systems or from user activity. Security incident and event management platforms (SIEMs) provide real-time analysis of security alerts based on the logs generated by network hardware and applications. Other systems look into anomalous user activity, a technique referred to as user behavior analytics (UBA) or user and entity behavior analytics (UEBA) because their remit extends beyond end users to systems. This is useful for detection and investigation, but does not necessarily look further into potential risks, threats, and unknowns. However, there are many streams of external information available that could be intelligently applied to gain greater understanding of threats being faced. This is where Ovum believes that TIPs have a crucial role to play as part of the security architecture.

The capability exhibited by TIPs is sometimes referred to as "post-SIEM" functionality. They are designed to inform security analysts about threats and exploits happening outside their environment, enabling them to look for activity on their company's infrastructure that has not yet triggered any alerts but might nonetheless be malicious.

In combination with internal data as well as user behavior, there is a large volume and variety of potentially real-time data that has to be processed and understood to achieve worthwhile outcomes. TIPs do this by offering a framework based on three key elements: gather, understand, and act.

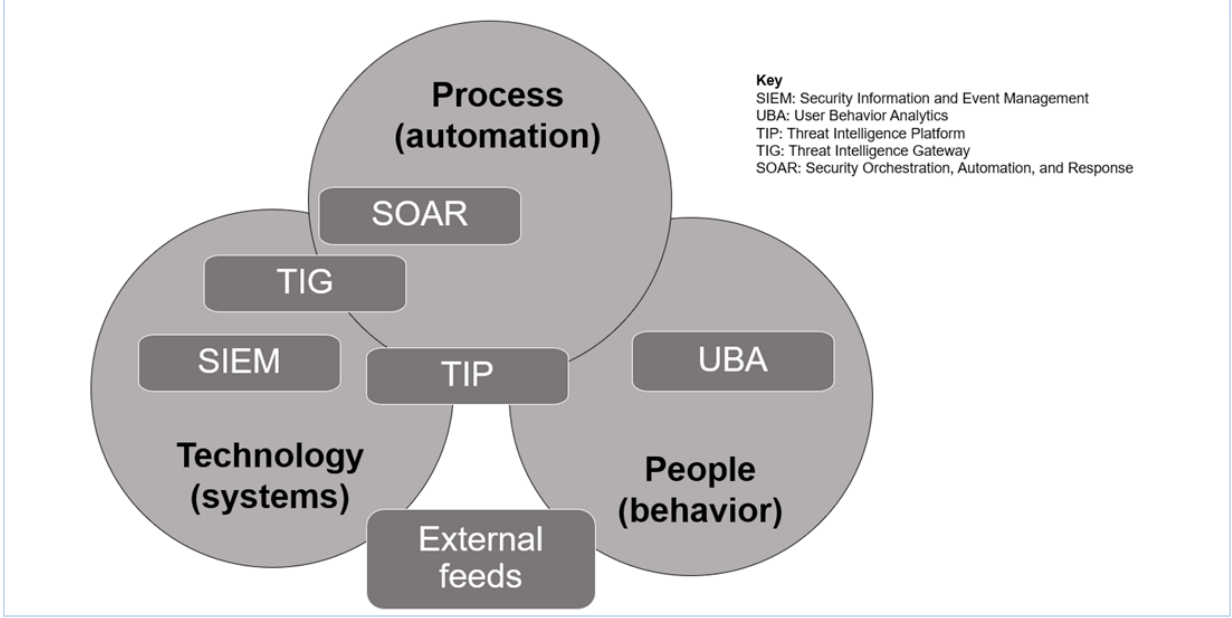
- Gather: Take data from multiple sources and aggregate and enrich it to put it in some form of context.
- Understand: Provide tools for threat analysts to rapidly investigate and make sense of the information.
- Act: Have the communication and collaboration mechanisms so that appropriate action can be taken.

Automation and artificial intelligence can and should be applied at every stage, but the breadth and depth varies. Some believe the goal of a TIP is to replace the need for human involvement, while others believe that a TIP massively augments the activities of threat analysts. Either way, the short-term goal is to reduce the need for security experts to spend their time on mundane activities and to allow them to grow and focus their skills on the aspects that will have the most positive business impact.

The number of TIP vendors is still relatively small, but the need for threat intelligence and analysis is not diminishing. Some suppliers will look to fill the gap by offering threat intelligence services (already a recognized channel for TIP vendors themselves), whereas other elements of the market will try to extend existing products and services to add threat intelligence capabilities. This will either be by time-consuming product development, the acquisition of an existing player, or by incremental shifts in both product marketing and development. All of these add to the potential for confusion in the minds of customers that are already concerned about security vulnerabilities and the vast array of tools available but lack specialists with the right skills.

Where TIPs fit along with the other security platforms is a moot point, but there is clearly an opportunity for aggregation and consolidation (see Figure 2). With an increasingly overwhelming amount of information from a diversity of sources, and a need for already stretched security analysts to collaborate more, there is considerable potential for automation and orchestration to be applied. Doing so with intelligence to improve outcomes for organizations is key and will increasingly become a differentiator for product vendors.

Figure 2: Different aspects of the security platform landscape



Source: Ovum

Solving the complex strategic riddle of how the different elements will evolve, converge, or merge over the coming years will be interesting, but there are pragmatic and tactical steps that can be taken immediately to improve understanding of security threats. For this reason, Ovum believes it is important to look at the capabilities that make up the range of functionality that can provide the important elements of a TIP.

Key capabilities

Like many other aspects of IT, the threat intelligence platform itself needs to support and enable processes that can be refined and repeated. Processes that are too long, linear, or cumbersome usually fail to deliver and adapt to changing circumstances. Agile and collaborative working with open attitudes and interfaces tends to provide more valuable business impact from its deliverables and outcomes.

The primary aspect of a TIP is that it needs to provide active threat awareness and intelligence in advance of the actual threat, rather than simply the tools to detect, mitigate, or react afterwards. This means it must be built from a range of capabilities, from information gathering to taking pre-emptive action, each with a level of pre-applied intelligence and automation to support the security analyst.

Platforms and services from different vendors will vary, but Ovum believes there are a number of areas of capability that TIP buyers should always consider and compare as part of their purchasing process.

Ingestion

Data gathering is a vital part of any approach to security, but what differentiates a TIP is the range and variety of sources of threat data. These will be external from sources trusted at differing levels, as well as internal from systems such as SIEM. Data gathering may also include human intelligence sources and collaboration with external agencies. The scale and speed of operation required will be a consideration, as will the applicability of alternative and customized sources for different vertical

markets or sectors. The value of specific threat data can vary or degrade over time and automated management of this is essential.

Enrichment

Raw data needs to be processed because otherwise threat analysts will be swamped with the sheer volume available. It needs de-duplicating and normalization so that a triage process can be used to prioritize the most significant threats. At this stage, further adjacent but relevant data can be drawn in and aggregated to enrich the quality of the intelligence and place the raw data in context for the analyst.

Automation and correlation

Intelligence can be applied to reduce the mundane chores that an analyst might otherwise have to undertake, and further levels of automation could be used to multiply the effort, skills, and experience of an analyst. Depending on the level of artificial intelligence applied, this could in some cases remove or reduce the need for expensive, highly skilled analysts in the more routine aspects of the process.

Visualization

Where the TIP augments the work of the analyst, its information will need to be presented with clarity yet still permit straightforward in-depth investigation by subject matter experts. It will also need to be collated, combined, and condensed for ease of interaction to give a seamless user experience. With a spectrum of threats at hand, some form of ranking might be useful to differentiate between threats and their relevance to a particular customer or user.

Analysis

Adding further automation and artificial intelligence to the analysis and investigation is also possible, but how far should this extend? Is the aim to augment and amplify the skills of threat analysts, or is the ultimate goal to replace them? Threat analysts are scarce and hard to recruit and retain, so the breadth and scale of tools available is important. However, analysis is not a goal in itself, and the aim should be to create operational intelligence that can be actioned and deployed to guard against threats.

Sharing

Intelligence needs to be applied, and there are multiple potential output routes, each with its own specific requirements. Documents will often be required for internal publishing to raise awareness for reporting and audit purposes. Documents must be clear and present the analysis in the context of the reader, not a security expert. Systems will need to be adapted and protected with changes to mitigate any new threats. There must be processes to update IT systems that can be enacted and then validated. Also, in the spirit of collaboration within the security community, platforms should support the ability for intelligence to be shared externally. Adherence to industry-wide standards is therefore critical here.

Integration

A TIP has to coexist but should ideally integrate with the wider security landscape. The greater the degree of automated and systemic integration, the greater the resilience and responsiveness of the entire security operation to respond to threats. Some vendors believe they can provide a closed end-to-end solution, and while this can often simplify processes, it is hard for any single vendor to be able

to deliver the best of breed in all elements. Open ecosystems of like-minded partners that have made efforts to integrate their products are usually more beneficial and offer greater flexibility.

Business value and applications

Despite some "breach fatigue" in the reporting of security incidents in the media, the business impact on any organization is significant. In addition to any reputational damage, there might be regulatory pain that affects individuals as well as the organization. There is also the time and effort that needs to be applied to fix the problem. Adopting a more proactive approach means that protective actions can be taken before a problem arises, rather than simply responding after the event and having to deal with the consequences. The primary purpose of a TIP is to build a better understanding of the specific threats being faced and to take action to avoid them.

Market landscape and participants

Market origin and dynamics

TIPs came into existence to deliver what is sometimes referred to as "post-SIEM" functionality. Whereas security incident and event management platforms (SIEMs) provide real-time analysis of security alerts based on the logs generated by network hardware and applications, TIPs are designed to inform security analysts about threats and exploitations happening outside their environment, enabling them to look for activity on their company's infrastructure that has not triggered any alerts but might nonetheless be malicious.

They do this by aggregating information feeds about current threats, supplied by threat intelligence services such as CrowdStrike, iSIGHT Partners (now part of FireEye), Flashpoint, and Digital Shadows. Because these come in different formats, a TIP normalizes the data, enriches and dedupes it, and correlates it into clusters of related information to facilitate the analytical process.

Future market development

Although a TIP might seem like a significant investment in technology, people, and processes, are there other ways to consider its implementation? What elements does the organization need to own and what can it outsource? Could threat intelligence be delivered to it as a service? Does it need to be relevant and specific to a specific industry sector or is generic threat intelligence more useful? The approach to and choice of TIP will depend not only on capabilities but also on what and how threat intelligence is actioned for each organization.

The TIP market is relatively new, but Ovum believes it occupies a significant space in the security sector, which is undergoing an evolution toward more integration between tools and more collaboration between stakeholders both within and beyond the organization.

Today, getting the best return from threat intelligence requires high-level security skills and expertise. Early TIP customers include security services and particularly vulnerable or valuable market sectors such as financial services. Larger organizations may have some of the capabilities required in house or will be willing to invest in growing threat analysis skills. However, as TIPs evolve, there will be with increasing levels of automation applied. For those with existing threat analyst teams, Ovum believes this is unlikely to remove the need for analysts, but they will be relieved of some of their more

mundane activities to enable greater focus on threat investigation. A more significant opportunity is that more automation will enable the deployment of TIPs, perhaps with some element of "threat analyst as a service" to a broader category of organizations. This is an opportunity not only for TIP vendors but also for MSSPs to add value.

Looking further into the future, it is likely that with further automation and integration there will be increasing levels of orchestration of threat mitigation and response directly based on incoming threat intelligence from multiple internal and external sources. Whether this is called post-SIEM, TIP, SOAR, or something else will not matter. The most important thing for CISOs and their organizations is that high volumes of varied security data are being intelligently assessed and acted on in a timely manner.

Vendor landscape

The TIP market is still in its early days with several pure-play startups, many with similar names, such as ThreatConnect, ThreatQuotient, and ThreatGRID, the last of which was acquired by Cisco in May 2014, as well as others such as Anomali (formerly ThreatStream), TruStar, and EclecticIQ.

Market participants estimate a total addressable size of about $400m in 2018. However, given the perceived need for this technology among their enterprise customers, other more established security vendors such as IBM, FireEye, and Palo Alto are also looking to play in this market with either their own products or by acquisition.

Vendors on the Ovum Market Radar: Threat Intelligence Platforms

On the Radar: Anomali

Ovum view

As the amount of threat data available to organizations from internal and third-party sources continues to mushroom, there is a growing need for TIP technology to help order and interpret it. Ovum sees platforms such as the Anomali Threat Platform gaining in importance, particularly among mid-to-large enterprises with the resources to benefit from them.

Key messages

- Anomali provides a TIP called Anomali Threat Platform made up from two primary components: ThreatStream (its core TIP solution) and Anomali Enterprise (threat detection and hunting engine).
- ThreatStream supports threat intelligence collection from Open Source, commercial third-party vendors, information-sharing organizations, and any STIX/TAXII compatible sources. ThreatStream provides third-party integrations covering SIEM, IPS, firewall, endpoint management, and other systems.
- It also has a threat hunting engine called Anomali Enterprise, which identifies active threats bycomparing millions of threat indicators against internal customer traffic. It can search retrospectively over a year or longer to uncover existing threats.

- There are a range of integration partners in the Anomali Preferred Partner Store (APP Store) and Anomali has a number of software development kits (SDKs) available to aid partner product integration.
- Anomali has formal partnerships with a large number of information security and analysis centers (ISACs) and frequently publishes security research from the Anomali Labs team.

Why put Anomali on your radar?

Anomali leadership team and founders are from ArcSight, explaining the firm's expertise in SIEM and security integrations, placing it in a good position in the emerging TIP market. The availability of the Anomali Enterprise add-on for threat hunting is of particular interest to customers looking to gain more complete visibility into active threats. The launch of STAXX, a Soltra Edge replacement, meanwhile, was a canny play for customers in the financial sector that are already betting on the emerging Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) standards.

Highlights

Anomali positions its solutions as helping organizations to "know your adversaries" and claims to deliver this promise by operationalizing threat intelligence. The company differentiates itself by offering not only a threat intelligence platform but also by incorporating a proactive threat detection and hunting solution.

Anomali's TIP is called ThreatStream (the original name for the company), an element of the Anomali Threat Platform. ThreatStream aggregates threat intelligence and normalizes, enriches, and dedupes it. It also removes false positives and builds clusters of relating information. The data can then be fed into a SIEM platform, monitoring system, firewall, or endpoint protection platform (EPP).

The company offers an APP Store, a marketplace for threat intelligence offerings that integrate with Anomali, including open source and paid commercial threat feeds, security integrations, and enrichments. ThreatStream is offered in a SaaS model, making use of the cloud to collect intelligence and apply the company's machine learning to optimize the data. Anomali also offers an on-premises deployment model that communicates with the Anomali cloud to download intelligence locally, as well as an Air Gap model for fully isolated deployments.

Because of the cloud model, Anomali is able to offer "Trusted Circles", which are customizable communities for trusted threat sharing. Administrators can control membership in Trusted Circles and whether the circle is visible to Anomali users or available by invitation only. These features have made Anomali a popular choice for information sharing and analysis centers (ISACs) globally.

In addition to its core TIP product, in February 2016, Anomali launched Anomali Enterprise, which it characterizes as a threat hunting engine that compares IOCs against a customer's internal traffic to identify active threats, scaling to analyze millions of IOCs against billions of events a day over 365 days. It is not a SIEM replacement, but instead extracts data directly from the network or from a customer's SIEM to perform the comparison on a year's back data.

In September 2018, the company launched a suite of SDKs to address three aspects of third-party integration: threat intelligence feeds, threat analysis, and data enrichment and integration of the Anomali Threat Platform into other products. This builds on the Anomali Preferred Partner Store approach to having an ecosystem of partners that extends the capabilities of the TIP with their own integrated products and services.

Background

Anomali was founded as ThreatStream in 2013 by its chief strategy officer Colby DeRodeff and strategic advisor Greg Martin. DeRodeff previously held senior leadership positions with SIEM vendor ArcSight and antifraud vendor Silver Tail Systems. He played an instrumental role in ArcSight's initial public offering and in its subsequent acquisition by HP, as well as in the acquisition of Silver Tail by EMC.

The company's CEO is Hugh Njemanze, who co-founded ArcSight in May 2000 and served as CTO as well as executive vice president of R&D. He led product development, information technology deployment, and product research at ArcSight, and then expanded his role to lead engineering and R&D efforts for HP's Enterprise Security Products group, the organization that ArcSight became part of post-acquisition. In a further ArcSight link, that company's former CEO Tom Reilly (now CEO of Cloudera) is also a board member of Anomali.

The company, which rebranded as Anomali in February 2016, has raised $96m in four rounds of funding. The Series C round was for $30m in April 2016, led by Institutional Venture Partners (IVP), with significant investments from General Catalyst Partners, GV (formerly Google Ventures), and Paladin Capital Group. In January 2018, a further Series D round for $40m was led by Lumia Capital and supported by Deutsche Telekom Capital Partners (DTCP), Telstra, Sozo Ventures, and returning investors GV, General Catalyst, IVP, and Paladin Capital Group.

Anomali has expanded globally with offices in the US, UK, Germany, France, Netherlands, UAE, Australia, Singapore, and Japan. The most recent funding added global investors including Deutsche Telekom Capital Partners in Germany, Sozo Ventures in Japan, and Telstra Ventures in Australia.

Current position

Anomali was created by a series of SIEM industry veterans to develop what might be termed "post-SIEM" functionality. Whereas SIEMs provide real-time analysis of security alerts based on the logs generated by network hardware and applications, TIPs are designed to inform security analysts about the threats and exploitations happening outside their environment, enabling them to look for activity on their company's infrastructure that has not triggered any alerts but might nonetheless be malicious. They do this by aggregating information feeds about current threats, supplied by threat intelligence services such as CrowdStrike, iSight Partners (now part of FireEye), Flashpoint, and Digital Shadows. Because these come in different formats, a TIP then normalizes the data, enriches and dedupes it, removes false positives, and correlates it into clusters of related information to facilitate the analytical process.

With its latest update of integration SDKs, Anomali continues to focus on its ecosystem of partners. Its Anomali Preferred Partner Store has more than 20 threat intelligence feed partners, more than 30 security integration partners, and five threat analysis and enrichment partners.

While it declines to reveal exact customer numbers, Anomali says it has about a quarter of the Fortune 100 paying it six-figure sums for its technology, which is delivered in a software-as-a-service (SaaS) mode.

The TIP market is still in its early days, with a number of pure-play startups, many of which have similar names, such as ThreatConnect, ThreatQuotient, and ThreatGRID, the last of which was acquired by Cisco in May 2014, as well as others such as EclecticIQ, and, of course, Anomali.

However, given the perceived need for this technology among their enterprise customers, other more established security vendors such as IBM, FireEye, and Palo Alto are also looking to play in this market, either with their own products or by acquisition.

Data sheet

Table 1: Data sheet: Anomali

Product name	Anomali Threat Platform	**Product classification**	Threat Intelligence Platform (TIP)
Version number	n/a (SaaS-based)	**Release date**	Launched in February 2014, latest platform update September 2018
Industries covered	All	**Geographies covered**	North America, EMEA, Asia-Pacific
Relevant company sizes	All	**Licensing options**	Subscription
URL	www.anomali.com	**Routes to market**	Direct, channel, MSSP
Company headquarters	Redwood City, CA, US	**Number of employees**	290

Source: Ovum

On the Radar: EclecticIQ

Ovum view

EclecticIQ's expertise in the TIP market is demonstrated by some of the intelligence agencies that use EclecticIQ Platform. While the EclecticIQ Fusion Center service is targeted at a wider audience in the midmarket segment, it can also appeal as a supplementary service to users of the EclecticIQ Platform.

Key messages

- EclecticIQ's flagship product is EclecticIQ Platform, which is an analyst-centric TIP.
- It also offers a feed aggregation service, EclecticIQ Fusion Center, where it enriches and provides only the feeds relevant to the customer's vertical market.
- EclecticIQ Platform is primarily sold directly, while EclecticIQ Fusion Center is a cloud service with which the company targets the midmarket.
- Managed security service providers (MSSPs) have opportunities to manage EclecticIQ Platform for enterprise customers and to offer EclecticIQ Fusion Center to midmarket customers.

Why put EclecticIQ on your radar?

If you have a sophisticated security team that knows what it needs in terms of threat intelligence, EclecticIQ Platform is a definite contender for a platform to help ingest, organize, and disseminate this information. If, on the other hand, you are a smaller outfit that wants an already ingested and merged subset of feeds, EclecticIQ Fusion Center is a compelling way of doing this without having to license from multiple providers or maintain a dedicated team of analysts for enrichment and vertical triage.

Highlights

As cyberthreats continue to proliferate and diversify, the volume of information on them is mushrooming. This increases the need for technology to help companies to ingest all this data and make sense of it to prioritize defensive activities. This is the promise of TIPs and the market in which EclecticIQ is a player with its flagship EclecticIQ Platform product.

TIPs came into existence to deliver what is sometimes referred to as post-SIEM functionality. Whereas security incident and event management platforms (SIEMs) provide real-time analysis of security alerts based on the logs generated by network hardware and applications, TIPs are designed to inform security analysts about threats and exploits happening outside their environment, enabling them to look for activity on their company's infrastructure that has not triggered any alerts but might nonetheless be malicious.

They do this by aggregating information feeds about current threats, supplied by threat intelligence services such as CrowdStrike, iSIGHT Partners (now part of FireEye), Flashpoint, and Digital Shadows. Because these come in different formats, a TIP then normalizes the data, enriches and dedupes it, and correlates it into clusters of related information to facilitate the analytical process.

The TIP market is still in its early days with several pure-play startups, many with similar names, such as ThreatConnect and ThreatQuotient, as well as others such as Anomali (formerly ThreatStream), TruStar, and, of course, EclecticIQ.

Market participants estimate its total addressable size at about $400m this year. However, given the perceived need for this technology among their enterprise customers, other more established security vendors such as IBM, FireEye, and Palo Alto are also looking to play in this market, either with their own products or by acquisition.

EclecticIQ Platform is a classic TIP in that it enables companies to ingest multiple threat intelligence feeds and perform data management on them, or as the company itself describes it, “analyst-centric technology to consolidate, analyze, manage, action, and disseminate intelligence and reports”.

The technology is well suited to institutions with a large, dedicated security team with the sophistication and resources to take in all the intelligence feeds they need and sift through them for relevant information. The burgeoning success of this market is evidenced by the proliferation of new feeds (from about 25 when EclecticIQ started out to about 60 now) as well as a slight trend toward commercial feeds replacing some open source ones.

In short supply, however, particularly among midmarket organizations, are the skilled staffers required to pore over multiple feeds and derive the appropriate insights. This is the rationale behind the EclecticIQ Fusion Center first launched in 2017. This is a feed aggregation, analysis, and enrichment service where for an annual fee, EclecticIQ is the licensee for multiple feeds and selects those that are relevant to a specific customer, such as, for example, a healthcare organization in the US or a retailer in Europe. It bundles only the feeds the customer needs into a single feed and enriches this with further investigations and strategic analyses. Customers remain able to change the mix of feed providers if they discover new ones that are more relevant to them. Interestingly, since its launch, customers have also included those that have already purchased the EclecticIQ Platform. While the aggregation service performed by EclecticIQ Fusion Center is a necessity for those lacking the inhouse skills, it is also clearly useful to a dedicated security team. It should reduce time and effort spent on mundane tasks, enabling it to be devoted to more complex threat analysis.

EclecticIQ has taken its analyst-centric approach a stage further with the launch of two new offerings: Academy and Advisory.

- Academy is a straightforward training package for customers that want to train new people to become threat analysts or to improve the skills of existing threat analysts.
- Advisory is a service where EclecticIQ consultants help customers to set up their own cyberthreat intelligence practice. It is not a traditional professional services offering to overlay a product sale, but instead an open advisory service for organizations that have the budget and understanding of the need, but lack the processes and people to put a practice in place.

Background

EclecticIQ was founded in 2014 by CEO Joep Gommers and its VP of products, Raymond van der Velde. Both men previously held executive positions at iSIGHT Partners, a threat intelligence vendor acquired by FireEye in January 2016.

They focused on the development of a TIP based on the OASIS STIX/TAXII standards for the gathering and operationalization of intelligence from multiple sources. More recently, the company has developed a cloud-based service for the aggregation of threat intelligence feeds that are specific to individual customers that should enable it to go down market to companies with smaller security teams and less time to manage multiple feeds.

The company has raised over €20m ($22.8m) in several funding rounds. There was a €5.5m ($6.3m) Series-A round, led by INKEF Capital, with participation from KPN Ventures. In November 2017, it raised a further €14m ($16.5m) Series-B round led by Keen Venture Partners, with current shareholders at the time also participating.

Current position

The EclecticIQ Platform was formally launched in December 2015 after working with beta customers that included Nato's Communications and Information Agency (NCIA).

EclecticIQ Platform is available for deployment on a company's premises or as hosted software. The on-premises option is favored by customers in the intelligence community, particularly because they themselves might use it to distribute information to other agencies. The second alternative is preferred by managed security service providers (MSSPs) that already offer EclecticIQ, including Dutch communications operator KPN which is also a shareholder.

EclecticIQ has three types of customer on EclecticIQ Platform: governmental agencies in the intelligence community, MSSPs such as KPN, and financial service institutions. Overall, this is split roughly 50/50 between government and non-government business. Its go-to-market on this product is direct and through value-added partners in countries including Australia, Belgium, Israel, and Singapore.

In May 2017, the company launched EclecticIQ Fusion Center, a cloud-based service that aggregates, analyzes, and enriches feeds from over 50 threat intelligence sources that are relevant to individual customers. EclecticIQ carries out all the legal and technical activities necessary for delivering the feeds and is the licensee. Customers are therefore able to receive a relevant bundle of feeds for a single, annual fee, with a consolidated feed into their security tools such as firewalls SIEM platforms.

For EclecticIQ Fusion Center, EclecticIQ envisages a mixture of direct sales to end customers and indirect ones through MSSPs and tech partners, such as companies that offer a platform to manage incident response. The service is sold for an annual subscription fee in the range of between $25,000 and $500,000, with access to the service for as many users as a subscriber wishes.

In terms of its competitive environment, there are many players in the TIP market, but EclecticIQ feels it has more of a lead with its new aggregation service. Against TIP vendors such as Anomali, it sees differentiation in the fact that it has more intelligence community customers, whereas other vendors might be stronger in the enterprise market for now. It is one of few European companies in this market and established its North American Headquarters in March 2018.

Its model of being analyst-centric means it is not looking to automate the threat analyst role away, but instead to augment and amplify it using supportive services and technology. The introduction of the Academy and Advisory services further highlights its analyst-centric strategy.

Data sheet

Table 1: Data sheet: EclecticIQ

Product name	EclecticIQ Platform; EclecticIQ Fusion Center	**Product classification**	Threat intelligence platform; threat intelligence aggregation, analysis, and enrichment service
Version number	EclecticIQ Platform: v2.3; EclecticIQ Fusion Center is a service so not applicable	**Release date**	EclecticIQ Platform: December 2015; EclecticIQ Fusion Center: June 2017
Industries covered	Finance, government, insurance, energy, critical infrastructure	**Geographies covered**	EMEA, North America, Asia-Pacific
Relevant company sizes	Enterprise and central/federal governments; midsize	**Licensing options**	EclecticIQ Platform: on-premises and hosted; EclecticIQ Fusion Center: service
URL	https://www.eclecticiq.com/	**Routes to market**	Direct and value-added partners, MSSPs
Company headquarters	Amsterdam, Netherlands	**Number of employees**	95

Source: Ovum

On the Radar: ThreatConnect

Ovum view

The complexity of the current threat landscape and the speed of its evolution as well as the volumes of threat data available are driving demand for TIPs. ThreatConnect has built up a significant customer base with the potential to widen its appeal through MSSP partnerships.

Key messages

- ThreatConnect offers a progression from basic threat feed management to complete threat intelligence analysis and security orchestration.

- The company offers four levels of its platform product that are designed to meet the needs of security teams of all sizes and maturity levels.
- The platform has a security automation and orchestration capability that can use existing playbooks or custom ones created by the customer.
- The products can be deployed in public or private cloud as well as on the customer's premises.
- A repository, TC Exchange, for the threat ecosystem has been established to be a community/hub for feeds, playbooks, apps, and services.
- Additional context about threats and indicators is provided through anonymized, crowdsourced intel via the Collective Analytics Layer (CAL), with insights coming from the analysts around the world who use ThreatConnect.

Why put ThreatConnect on your radar?

ThreatConnect offers a TIP, but with more advanced analytical capabilities and extensibility, as well as a built-in orchestration feature that sets it apart from the competition. This makes it a compelling candidate for any project an enterprise has for handling threat intelligence in a systematic way and dovetailing it into the actions taken based on the analysis of threat data.

Highlights

ThreatConnect offers a series of products designed to address the threat intelligence aggregation, analysis, and automation needs of security teams at different size and maturity levels, and with varying budgets. The individual products are:TC Identify, TC Manage, TC Analyze, and TC Complete.

- **TC Identify**provides vetted threat intelligence compiled from more than 100 source feeds, including crowdsourced information from multiple communities and ThreatConnect's own research team. There is also the option of adding data and intelligence from third-party vendors such as Attivo, FireEye, Lastline, McAfee, and Palo Alto. TC Identify uses the ThreatConnect data model and adds automated enrichments for analyst-curated context, delivering intelligence on malicious activity and how it is connected to other events.
- **TC Manage**, for which the company's tagline is "intelligence-driven orchestration," provides the ability to orchestrate security functions based on intelligence that customers have vetted and confirmed to be relevant to them. It can automate part or all of their processes for managing threat data, which includes sending indicators to defensive tools for alerting and blocking, as well as looping in members of the customer's security team for appropriate action. The vendor says that having aggregated and enriched threat data in the same place as orchestration enables customers to be more focused in their response activities without the need to expand their security team or buy additional tools.
- **TC Analyze**can be considered ThreatConnect's true TIP product in that it enables customers to enrich their threat data and create intelligence to provide insights and prioritize their security actions. It provides a central location from which to see a team's tasks, analyze data, and push vetted threat intelligence to their security tools.
- **TC Complete** includes all the features ThreatConnect has to offer, enabling customers to analyze their data, orchestrate security processes, and proactively hunt for threats.

In addition, ThreatConnect offers a free version called TC Open, which is designed for absolute beginners to gain an understanding of threat intelligence handling with its technology before signing any contract.

There is a "land and expand" strategy here. The idea is for customers to start with TC Identify then expand into a TC Complete license as their experience with the TIP grows and they become more confident in handling threat data and automating responses. The superset nature of the products can be seen from the fact, for instance, that TC Identify offers open source feeds, premium (paid) feeds, information from the Collective Analytics Layer (CAL) that the company puts together from anonymized data from multiple instances of its platform and other sources, and a Trusted Automated eXchange of Indicator Information (TAXII) feed.

Both TC Manage and TC Analyze also offer all the above, but whereas TC Identify only offers the ThreatConnect Intelligence feed, TC Manage and TC Analyze offer an à la carte menu and have customer dashboards. TC Identify offers three default dashboard versions only.

Similarly, TC Identify has none of the orchestration or incident and task management features of TC Manage, while TC Analyze enables customers to create customer intelligence and private communities for sharing threat data but lacks the orchestration capability of TC Manage. TC Complete, meanwhile, combines all the features of the individual products.

Background

ThreatConnect was founded in 2011 as CyberSquared by CEO Adam Vincent, CFO Leigh Reichel, VP of products Andy Pendergast, director of services Keith Gologorsky, and Rich Barger, who is now director of security research at Splunk. Vincent was previously CTO at Layer 7, an API management developer subsequently acquired by CA Technologies.

The company's founders were intelligence analysts who had perceived a need in the market for TIP technology. The platform went on general availability in 2013 with the name ThreatConnect, and a year later in November 2014, Cyber Squared changed its name, becoming eponymous with its product and thereby simplifying brand recognition.

ThreatConnect has so far raised just over $20m in funding, initially with $4.25m round led by Grotech Ventures, and most recently announcing a $16m Series B round in December 2015 led by SAP Security Services and also involving Grotech Ventures.

Current position

ThreatConnect is focused primarily on the enterprise market, with several Fortune 500 companies in its customer base. It also targets midsize customers through its MSSP relationships. It has some 19,000 individual users working at 1,600 organizations.

Broadly speaking, the ThreatConnect Platform enables companies to aggregate and analyze threat data then take action based on the analysis. These functions are available in its licensed products.

ThreatConnect has offered APIs for integration with third-party systems upstream and downstream of its platform from the outset. In early 2017, however, it went a step further, launching the capability to use pre-existing or custom playbooks to automate virtually any cybersecurity task, including incident response. Playbooks represent a further level of integration with third-party systems and processes, triggering changes in an organization's security posture by instructing a firewall to block something it might previously have let through, for instance. They are available in TC Manage, TC Complete, and in limited quantities in TC Analyze (in dedicated cloud and on-premises deployments).

The company can deploy its technology in public or private cloud environments, as well as on the customer's premises. Its customer base is divided, with roughly one-third in each of these situations. TC Manage and TC Complete are not available in public cloud environments.

Interestingly, it says customers in the early stages of processing threat intelligence to inform their incident response activities tend to start with the ThreatConnect Platform or a product or two in the public cloud, and as their expertise matures, move it in the direction of an on-premises deployment.

All ThreatConnect's products are licensed on a per-user basis, with no extra charge for the number of playbooks or dashboards an organization uses. Customers buy a license for a certain number of users and get a base set of API keys on top of which they can acquire additional ones as required.

The creation of ThreatConnect’s repository, TC Exchange, represents an attempt to foster and encourage an open community hub for all types of security tools and capabilities. This includes feeds, playbooks, apps, and services. While most of those provided are built and supplied by ThreatConnect, the company’s ambition is for this to be a repository open to all in the threat ecosystem.

Data sheet

Table 1: Data sheet: ThreatConnect

Product name	ThreatConnect Platform: TC Complete; TC Analyze; TC Identify; TC Manage	**Product classification**	Threat intelligence platform (TIP)
Version number	5.7	**Release date**	Launched in 2013, selling from 2014
Industries covered	All	**Geographies covered**	Worldwide
Relevant company sizes	Enterprise and midsize	**Licensing options**	Per user license, based on functionality
URL	www.threatconnect.com	**Routes to market**	Direct to large enterprise and through MSSPs for midsize customers
Company headquarters	Arlington, VA, US	**Number of employees**	125

Source: Ovum

On the Radar: ThreatQuotient

Ovum view

With threats mushrooming, companies need technology to help sort through, understand, and act on a mountain of data. Ovum sees potential for ThreatQuotient because it provides visibility into threats and customer controls to prioritize workloads using threat intelligence, and can be deployed by managed security service providers (MSSPs) to reach smaller customers.

Key messages

- ThreatQ is a threat intelligence platform that enables security teams to aggregate, correlate, and analyze internal and external threat data and turn it into actionable threat intelligence.

- It goes beyond conventional TIPs by offering the ThreatQ Threat Library, which prioritizes threat intelligence, provides context and enrichment, and automatically identifies the highest priority threats facing an organization.
- ThreatQuotient has a growing partner ecosystem that makes it easy to integrate ThreatQ with the existing infrastructure and tools an organization relies on.
- It has a strong channel focus, working flexibly with MSPs and MSSPs to deliver threat intelligence as a service.
- ThreatQuotient offers ThreatQ Investigations, a cybersecurity situation room built on top of ThreatQ to enable security professionals to investigate, collaborate, and operationalize the results of their analysis.

Why put ThreatQuotient on your radar?

If your security team is facing challenges in dealing with the growing amount of incoming threat data it needs to triage, a TIP can help them address this. ThreatQ is of particular interest because of its prioritization and noise-reduction capability, plus its collaboration and coordination functionality, and the way it can be integrated into a broader infrastructure to streamline incident response.

Highlights

All TIPs are designed to help organizations aggregate, correlate, and analyze threat data from multiple sources in real time to support defensive actions. They do for threat data from external sources what a SIEM platform does for internally generated data.

ThreatQuotient differentiates its product by going beyond these phases of data treatment into the operationalization of the analysis and the ability to use threat intelligence effectively. ThreatQ is designed to integrate with the rest of a customer's infrastructure, including any existing SIEM, to serve as a “single source of truth” for all systems and teams.

For this reason, the platform was created with an open architecture rather than a black-box approach, giving customers the control to define which information is most relevant, what should be prioritized, and how they want to use the data across their environment. A threat ops team might therefore want to send the intelligence it has gleaned from ThreatQ into the sensor grid, or use it for threat hunting or incident response, supplementing it with a query sent to the ThreatQ Threat Library.

An example of how this can work is the way ThreatQ provides the ability to automatically parse email content. This enables users to accelerate analysis and decrease response times to malicious phishing events. Once spear phishing-related indicators are stored in the Threat Library, they can be distributed to the network and can host controls automatically if desired. Using the Exports section of ThreatQ, analysts can make data available to the team or tool that needs to consume the critical threat data, for instance, via an integration with Carbon Black’s endpoint security platform.

To accommodate this degree of integration, ThreatQuotient provides its own threat analyst console, the Adaptive Workbench, but also lets its customers use third-party interfaces with which they are already familiar and access the ThreatQ Threat Library from there. The company has about 70 API-based integrations with other technology platforms for this purpose, and stresses that integrations are bidirectional (ThreatQ can provide and receive data from the other products). A threat analyst can therefore place a query from within environments such as Splunk or IBM’s Resilient incident response platform to the Threat Library, which can then automatically populate the systems with the resulting intelligence, context, and related information.

To bring some order to the complexity or “chaos” of incident response and threat investigations, ThreatQuotient has introduced ThreatQ Investigations. This is a cybersecurity situation room using a common visual representation that can be shared across dispersed teams and different roles to improve understanding and tasking to help teams coordinate responses. Its aim is to help incident handlers, researchers, and threat analysts to gain an understanding of the situation to enable them to take appropriate action faster.

Background

ThreatQuotient was founded in 2013 by its chief architect Wayne Chiang and CTO Ryan Trost. Chiang previously worked at IBM Global Business Services on a US Air Force contract, as well as designing strategies to enhance network security at General Dynamics’ Security Operations Center. Trost previously managed US government and commercial-sector SOCs, including General Dynamics, where he and Chiang had the idea for ThreatQ, and he was senior director of security and privacy officer for a healthcare company. He also developed geospatial intrusion-detection technology to identify geolocation attack patterns.

ThreatQuotient’s CEO, appointed in 2015, is John Czupak. His prior roles include GM of Cisco’s Advanced Malware Protection portfolio following its acquisition of Sourcefire, and various executive roles over 12 years at Sourcefire. ThreatQuotient’s SVP of strategy is Jonathan Couch, who previously co-founded threat intelligence vendor iSIGHT (subsequently acquired by FireEye) and served in the US Air Force at the NSA.

ThreatQuotient has raised $54m in funding rounds. In August 2016 it announced a $12m Series B round led by New Enterprise Associates (NEA), with participation from existing investors Blu Venture Investors and the Center for Innovative Technology (CIT), plus a $3m growth capital facility from Silicon Valley Bank. Most recently, in November 2017, it announced a Series C round, securing $30m in new financing led by Adams Street Partners. Strategic partners Cisco Investments and NTT DOCOMO Ventures also joined the existing investors.

Current position

The ThreatQ platform also addresses other security operations use cases. ThreatQuotient seeks to differentiate its offering in two ways. First, it maintains that most of its competitors, such as ThreatConnect and Anomali, focus on data sharing, whereas the ThreatQ platform is more for security operations and management, prioritizing, operationalizing, and automating the actual handling of threats.

Second, the ThreatQ platform was built from the outset with scalability in mind, which means that while it can scale up for high-end customers, it can also scale down for smaller customers. This makes the product suited to the MSSPs with which ThreatQuotient has a partnership and agreed revenue-share arrangement rather than simply a subscription. This model aims to offer MSSPs a flexible but standard and centralized way to deliver threat intelligence.

ThreatQ can be deployed on an enterprise customer’s premises (in their data center or private cloud) or in cloud environments. For smaller customers, ThreatQuotient recommends the MSSP route. The company declines to reveal details of its customer base but does say it has “dozens” of deployments in Fortune 2000 enterprises across industries, and is working with MSSPs including Thales and SopraSteria.

In April 2018, the company launched ThreatQ Investigations. This is a cybersecurity situation room designed to reduce mean time to detect (MTTD) and mean time to respond (MTTR). It provides a single shared visual representation of evidence gathered, a timeline and actions to be taken to foster better collaboration in threat analysis and investigation, and the delivery of a coordinated response. It is built on top of the ThreatQ platform.

Data sheet

Table 1: Data sheet: ThreatQuotient

Product names	ThreatQ; ThreatQ Investigations	**Product classification**	Threat intelligence platform and threat operations and management platform
Version number	ThreatQ 4.10; ThreatQ Investigations 4.10	**Release date**	ThreatQ and ThreatQ Investigations 4.10 released September 2018; ThreatQ Investigations first released April 2018
Industries covered	All	**Geographies covered**	All
Relevant company sizes	Enterprise and central/federal governments; midsize	**Licensing options**	Subscription
URL	www.threatq.com	**Routes to market**	Channel, MSSPs
Company headquarters	Reston, VA, US	**Number of employees**	94

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Authors

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Rob Bamforth, Associate Analyst

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo