IT SECURITY GURU

PRODUCT REVIEW

ANOMALI®

"Anomali weaponizes your cyber security teams by providing all the intelligence they need to detect, assess and mitigate threats"

Supplier: Anomali
Website: www.anomali.com
Price: Based on size of organisation

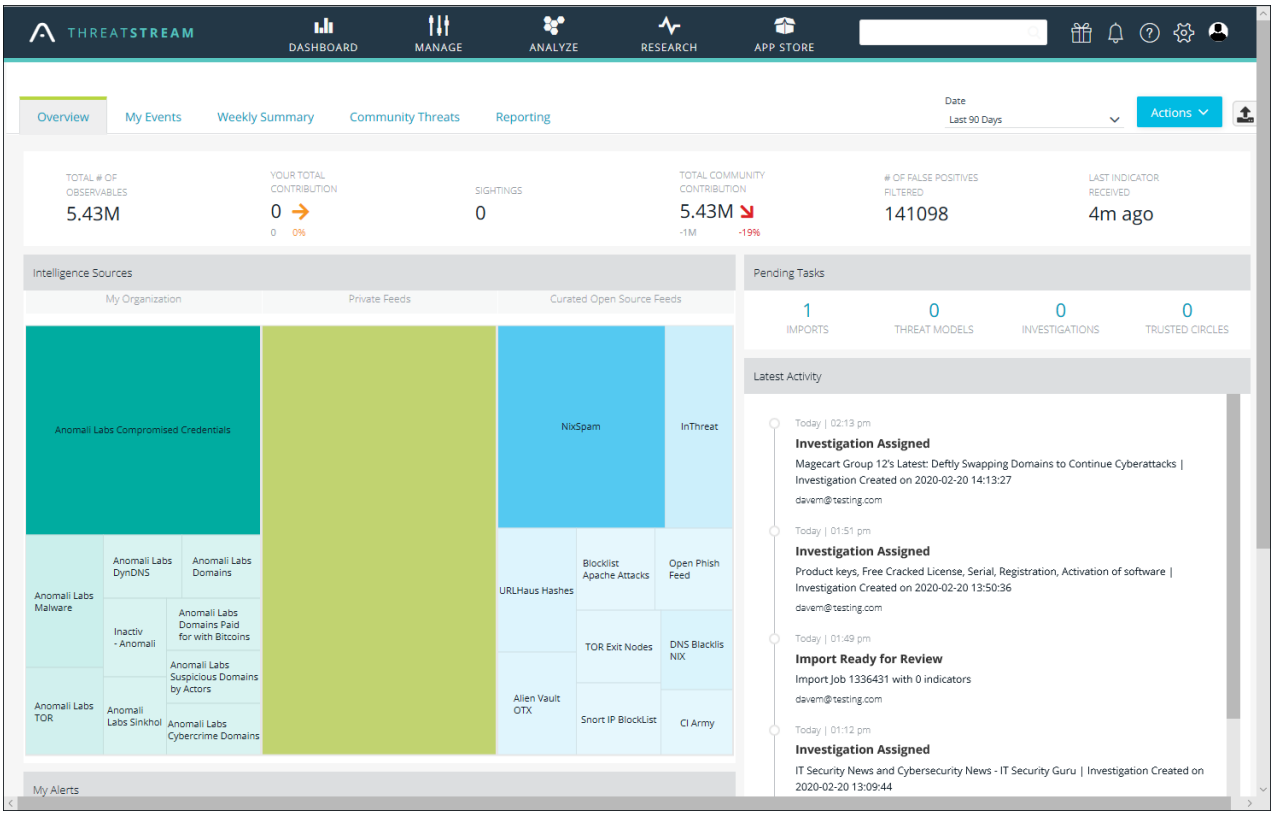
Scores:
Performance 5/5
Features 5/5
Value for Money 4.5/5
Ease of Use 4/5
Overall 5/5

Verdict: Anomali weaponizes your cyber security teams by providing all the intelligence they need to detect, assess and mitigate threats

Enterprises that rely on reactive responses to cyber threats are asking for trouble. Ever increasing numbers of businesses are only discovering data breaches often months after they have occurred so all they can do is own up, engage in damage limitation and brace themselves for a potentially punitive fine.

Cybersecurity analysts are on the front line but to be able to take a more proactive stance, they require knowledge. Threat intelligence can make all the difference as it arms them with the information they need to predict the next attack and strengthen their network defences accordingly.

Anomali's threat intelligence platform (TIP) is designed to provide the knowledge analysts and threat hunters demand to stay one step ahead of their adversaries. Comprising three core components – ThreatStream, Match and Lens – it aggregates threat intelligence from a vast array of sources and feeds, transforms it into understandable and actionable formats and integrates seamlessly with existing security tools.



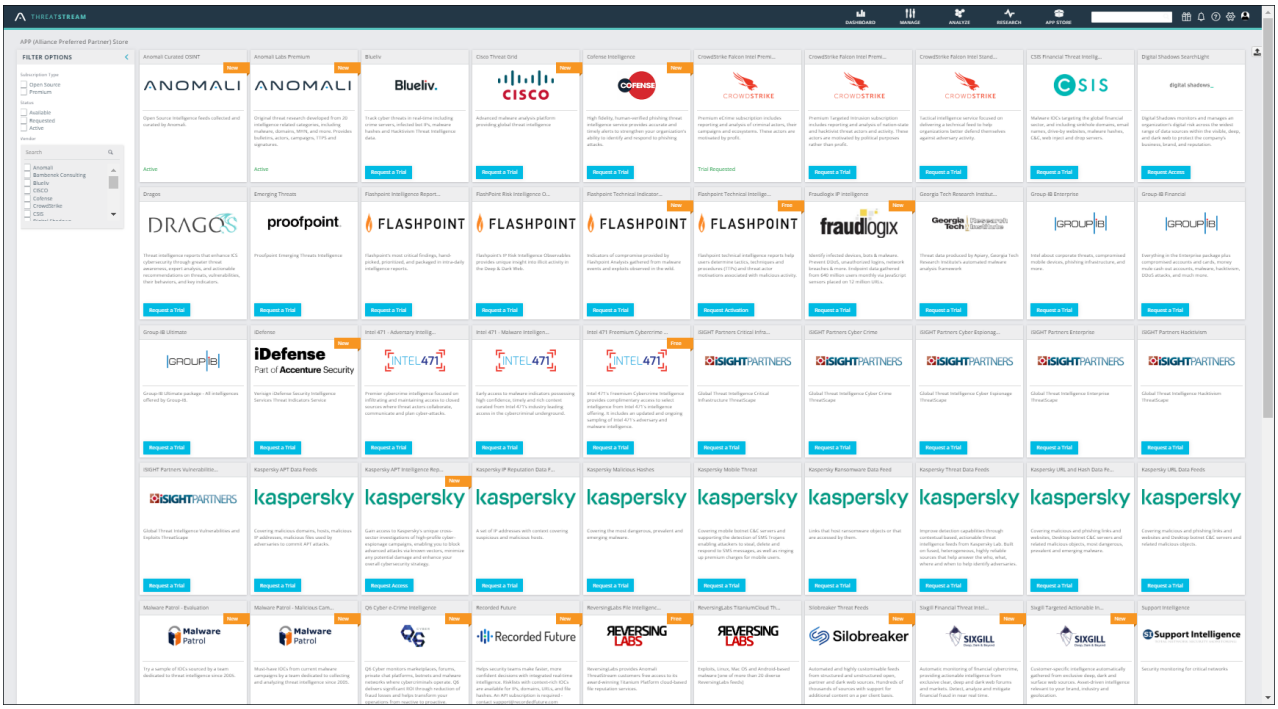
The ThreatStream dashboard provides a detailed summary of threat intelligence, the latest activities and alerts

Anomali ThreatStream

Anomali ThreatStream is available in three deployment options. You can choose from native cloud, hosted on-premises, or for environments where security requirements are particularly strict, you can choose an airgap solution.

We review the native cloud version of Anomali ThreatStream, where the portal dashboard opens with a widget-based overview of all intelligence sources, feeds, alerts, pending tasks and the latest activities. Even a quick glance shows how much intelligence it can provide and the portal's universal search bar allowed us to quickly pull up details on entities ranging from actors, campaigns and investigations to malware, observables, threat bulletins and vulnerabilities.

The smart MyEvents map shows the most recent intelligence on global threats and the countries they are emanating from plus specific details on observables that have triggered alerts on integrated security tools such as SIEMs. Along with weekly summaries, you can view all threats relevant to the Anomali communities you are a member of and create detailed reports on user activity
going back up to a year.



The APP (Alliance Premium Partner) Store is a threat intelligence marketplace that provides access to a wealth of Anomali partners for adding enhanced threat intelligence streams

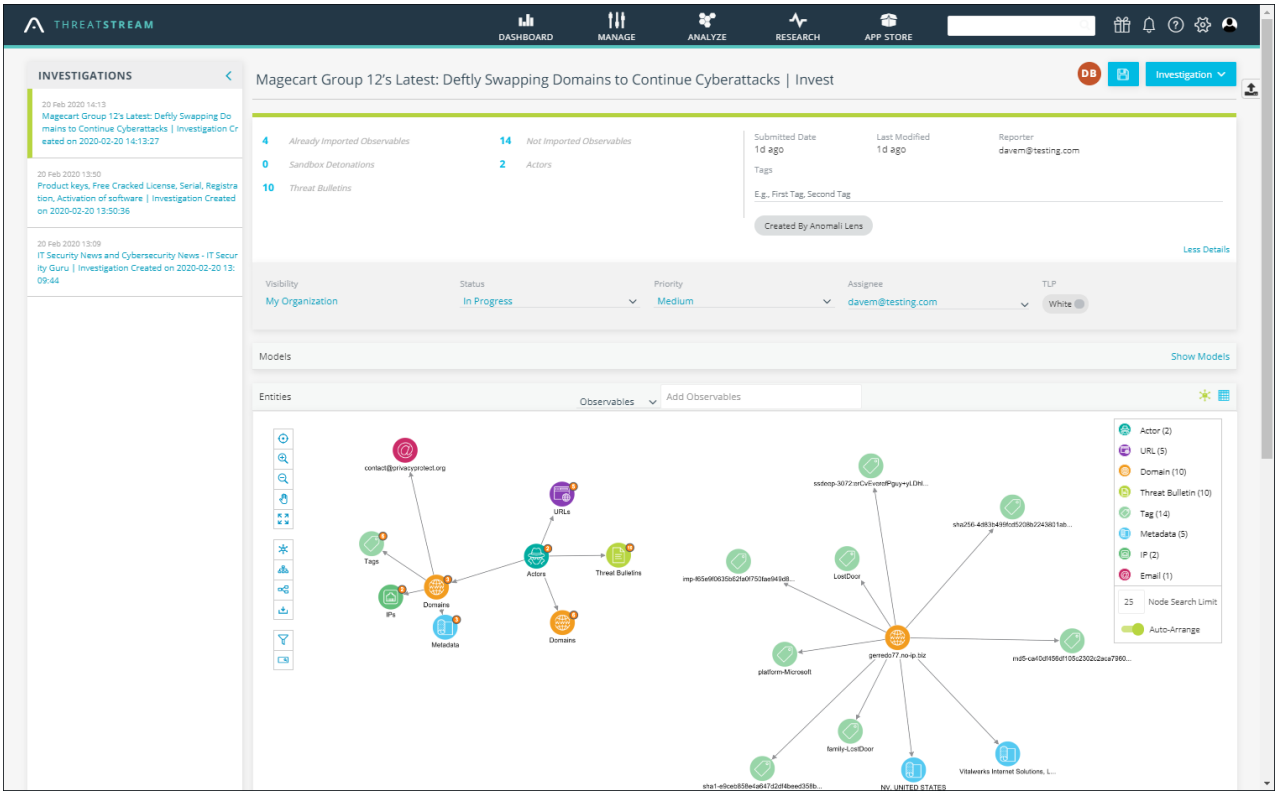
Using threat intelligence

A key feature of ThreatStream is its Investigations workbench, which is used to delve deeper into threats of interest. Investigations are simple to create as you add the desired observables, assign it to a user or workgroup and if required, use ThreatStream's integration with ServiceNow to assign a ticket.

From the Investigation workbench, users can view all associated entities, see links, make connections and add more entities by searching for observables and threat models already available in ThreatStream. Selecting an entity allows deep searches to be conducted to see what associations are already available about them such as actors, malware and vulnerabilities.

For email, you can search Whois threat intelligence while for URLs, you can look for intelligence on SSL certificates. The ThreatStream Explore tool also comes into play as you can use it to look for internal and external information that may be related to the investigation.

Any information not already available in ThreatStream can be imported as new observables to enhance available intelligence. Furthermore, entire investigations can be exported into ThreatStream as specific threat model entities.



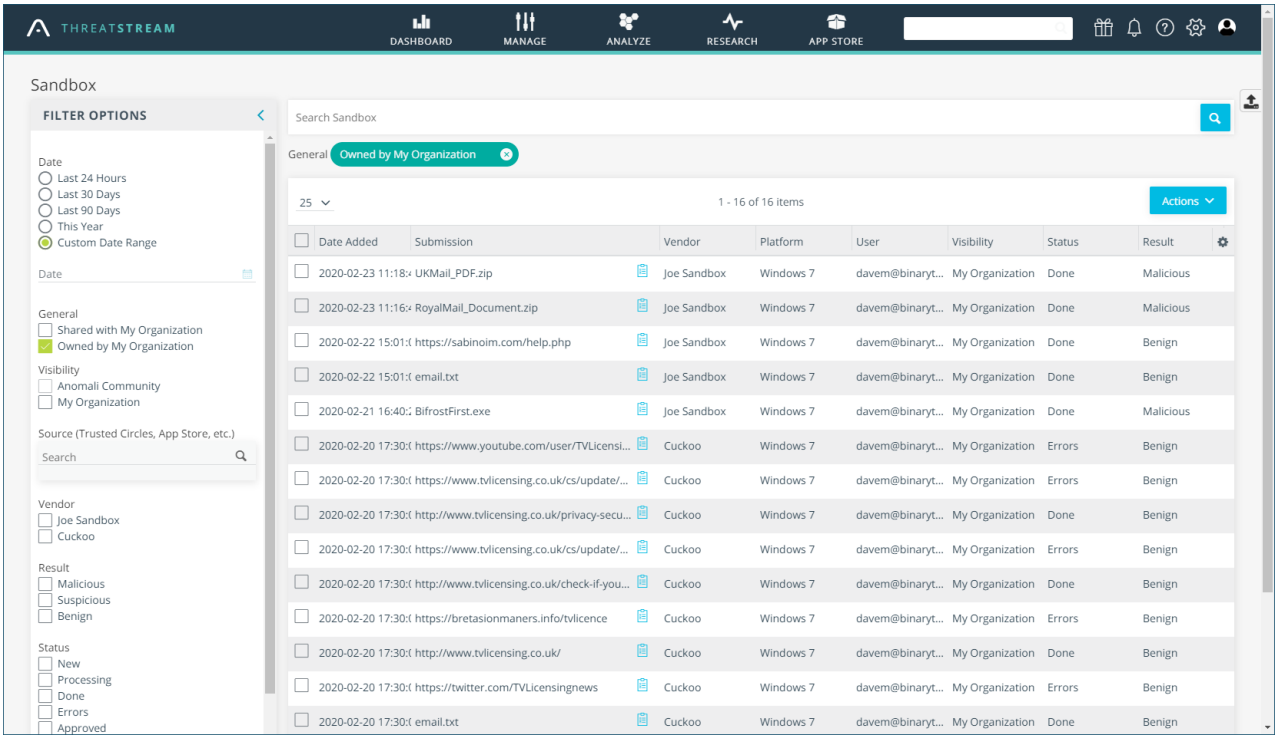
The Investigations page provides a collaborative workspace for deep threat analysis

Sandbox detonation

The ThreatStream Sandbox can be used to upload suspect files or content and safely detonate their payloads. Accessed from the console's Research tab, you paste a URL or upload a file, choose the Windows platform you want it tested on and decide on the visibility of the results.

We tested this by uploading files attached to genuine phishing emails and on average, had to wait around two hours while they were being processed by the default open-source Cuckoo sandbox. The wait was worthwhile though, as selecting an entry provided detailed descriptions of the payload and a behavioural analysis accompanied by sandbox screenshots showing the detonation processes.

Phishing emails can be ingested into ThreatStream by creating an import email entry in the Settings page and opting to automatically create an investigation or threat bulletin and detonate any URLs and attachments. At no extra cost, you can swap over to the Joe Sandbox from Joe Security which we think is a no-brainer as it provides a deeper analysis and is much faster than Cuckoo with our malware samples processed in around 15 minutes.



The ThreatStream sandbox can be used to safely detonate suspect payloads and create investigations

Match, Integrator and Lens

Threat intelligence isn't just about predicting the next attack but also about finding those that have already targeted and breached your network. Anomali Match leverages intelligence from existing security systems by taking log data from multiple sources such as Syslog, SIEMs, NetFlow and sFlow.

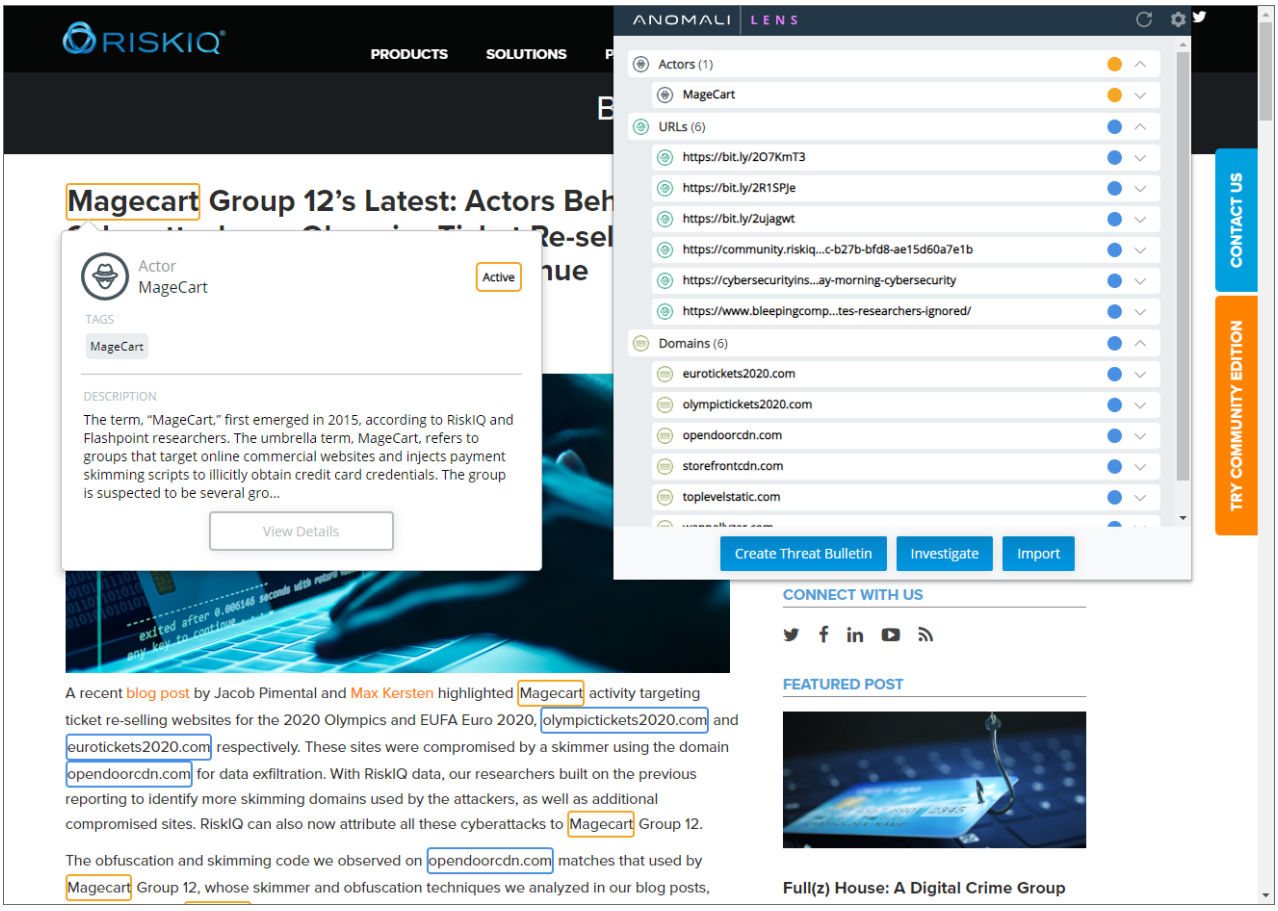
Using ThreatStream intelligence, Match compares millions of IOCs (indicators of compromise) with your internal network traffic logs going back up to a year. This allows it to identify active threats specific to your organisation and automatically feed alerts back to SIEMs.

Anomali Integrator is the next logical step as this component shares ThreatStream intelligence with your resident security systems to support blocking, alerting and remediation. Turnkey integrations exist for many different vendor systems including SIEMs, firewalls, DNS servers, proxies, and SOAR platforms. We found it easy to install where its browser-based management console provided wizards for linking up with our ThreatStream account, downloading intelligence feeds and selecting destinations for forwarding observables.

Hailed as the first natural processing language (NLP) based web content parser, the innovative Anomali Lens makes threat intelligence knowledge accessible to a much wider audience.

The Lens browser extension scans any web page content with a single click and uses different coloured highlights to identity detected threats such as actors, malware, URLs, CVE identifiers and IP addresses.

As the extension is logged into an Anomali account, the user can instantly create a threat bulletin and investigation, import the content and pivot directly to ThreatStream for further analysis. The analyst can use Match to see if their organisation is already impacted and bring Integrator into play to pass the intelligence on to their internal security systems.



Anomali Lens provides instant analysis of web pages and facilities for creating threat bulletins and investigations

Conclusion

Anomali is an undeniably powerful threat intelligence platform capable of delivering a vast amount of relevant information to security professionals. Everything is neatly integrated into a single console allowing analysts to focus on identifying and mitigating real threats to their organisation without being hampered by a smokescreen of false positives.