SC Product Reviews:
Threat and Intelligence Analysis Tools

Threat intelligence has never been more valuable than it currently is. Having quality threat intelligence is a critical component of any organization's security posture. Threat intelligence solutions gather information on internal and external threats to provide a general picture of vulnerabilities and highlight risks of varying severity so analysts can concentrate their efforts on the most critical and vulnerable assets. The goal of these solutions is to unburden security teams while simultaneously giving them the tools necessary to proactively fortify their organization defenses instead of relying exclusively on reactive practices like responses and mitigations.

We live in a connected world and this is constantly expanding. Every connection presents another potential risk that can be exploited. These products embrace this interconnectedness and have built-in collaboration tools to facilitate internal communication and intelligence sharing as well as external, community forums where security professionals may either share or research public-facing intelligence to stay aware and ahead of new and re-emerging threats.

Everything about these solutions is designed to aggregate intelligence from multiple sources and present it in a way that makes it as easily digestible and actionable as possible. We probably saw the most improvement in the third-party integration capabilities. It seems these solutions are now designed for the logical integration with other products such as SIEM, SOAR and firewall solutions. We saw both pre-built integrations and API integrations, maximizing the value of these solutions for them to be leveraged for both consumption and production needs.

A careful balance needs to be met between having enough information, but not so much information that security teams are overwhelmed. The industrywide skill gaps and lack of resources make this exceptionally tricky. However, the robust automation capabilities of these solutions are minimizing the impact of any imbalance and effectively optimizing existing resources. We consider these staple products for any security toolset. Your security teams will be empowered with the targeted threat intelligence necessary to effectively make decisions and prioritize according to most critical need.

Threat intelligence

These products embrace interconnectedness and have built-in collaboration tools to facilitate internal communitcation and intelligence sharing, says Katelyn Dunn.

These products analyze internal and external threats and offer risk assessments of the vulnerabilities within an environment. The continuous growth of the threat landscape has not slowed down. On the contrary, the COVID-19 pandemic has helped identify and emphasize the many shortcomings the cybersecurity industry faces – analyst burnout, tool fatigue, and skill shortages.

Organizations are desperate for a way to bolster security posture and keep pace with threats. Therefore, these products are more important than ever with their automation capabilities and collaboration tools that arm analysts with the actionable information necessary for effective threat detection and response. In some cases, organizations can prevent threats with the strategic advantage of threat intelligence products, shifting security from purely reactive to proactive. The industry needs such a shift in momentum to effectively combat the advanced threats of the modern era and keep up with the never-ceasing workload.

Threat intelligence products are trending away from only

Specifications for threat and intelligence analysis tools

●=yes ○=no

Product	Analyst1	Anomali	AT&T	Bandura	Dark Owl	DomainTools	EclecticIQ	IntSights	LookingGlass Cyber Solutions	ManageEngine Log360	Recorded Future	ReversingLabs	ThreatConnect
Covers the Dark Web (closed source intelligence)	●	●	●	●	○	○	●	●	●	○	●	●	●
Live analysts in Dark Web Forums (i.e., not screen scraping of automated access)	○	●	○	○	●	○	●	●	○	○	●	●	○
Focus on threat analysis	●	●	●	○	●	●	●	○	●	●	●	●	●
Focus on threat intelligence	●	●	●	●	●	●	●	●	●	●	●	●	●
Integrates w/SIEM	●	●	●	●	○	●	●	●	●	●	●	●	●
Integrates with IDS/IPS	●	●	●	○	○	●	●	●	●	○	●	●	●
Integrates via API with Maltego	●	●	●	○	●	●	○	○	●	○	●	●	●
API	●	●	●	●	●	●	●	●	●	○	●	●	●
Accepts open source (free) threat feeds - if so, how many are available out of the box?	●	●	●	●	○	○	●	●	●	●	●	●	●
Accepts commercial (paid) threat freeds - if so, how many are available for purchase out of the box?	●	●	●	●	○	○	●	●	●	●	●	●	●

PICK OF THE LITTER

ReversingLabs Titanium Platform maps threats to the MITRE ATT&CK Framework to accelerate investigation and response activities, while its massive known-malware repository ensures organizations keep pace with the ever-growing threat landscape. Titanium always issues descriptions in plain language so that even analysts with less experience can actively and effectively engage in threat hunting and response. This exceptional threat intelligence solution provides valuable information while maximizing actionability. Such ease-of-use, transparency, and scalability make Titanium an attractive option for organizations of all sizes coupled with the fact it is one of the less expensive options we looked at this month, making this product an SC Labs Best Buy.

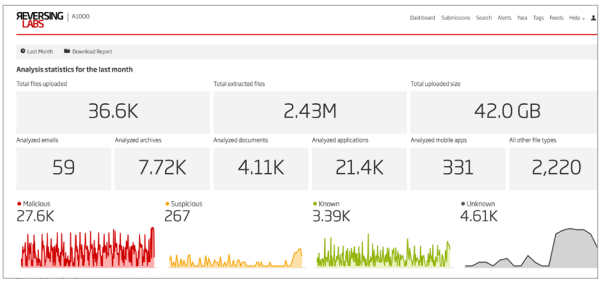
Recorded Future Security Intelligence Platform is a strong contender in the threat intelligence space, especially considering its robust integration catalogue and fully documented API. It provides analysts with transparency, explaining the reasons behind the threat ratings it issues and supporting these explanations with evidence and details. While many platforms with a multitude of options become heavy and difficult to navigate, Recorded Future remains easy to use for even novice team members. The ease-of-use balanced with advanced capabilities to optimize analyst efficiency and reduce response times make this our SC Labs Recommended product for this month's round of testing.

delivering information. In our testing, we saw great strides towards enhancing integration capabilities to drive the actionability of intelligence, versus just providing data for which analysts then must do the investigative and response work. Security teams are overwhelmed with too much information and too few resources. Integrating these platforms with SIEM solutions and other security investments offers the ability to act, often automatically, on the discovered threat information. Empowering security teams with products that help carry the burden of threat response and prevention lets them focus their efforts elsewhere while simultaneously closing gaps in the security perimeter.

Many times, organizations purchase multiple threat intelligence products. This might seem contrary to tackling tool fatigue. However, because these products are designed to highlight the information most relevant to an organization, deploying multiple threat intelligence products means receiving more targeted information. Although too much information can be a hindrance to threat detection and response, the more targeted information an organization has, the better decisions it can make.

We strongly recommend those looking to incorporate these effective threat intelligence products into their environment take the time to decide what they are trying to achieve and then commit to the product (s) best suited to the organization's needs. Although these products are all threat intelligence solutions, many of them come with different approaches or focus points. Therefore, align security needs prior to committing. Companies don't want to feed the vicious cycle of too much information without enough context or targeted reporting. The goal for CISOs and top managers should always be to keep security teams proactive.

— Katelyn Dunn



ReversingLabs Titanium Platform

DETAILS

Vendor ReversingLabs

Price $10,000 per year

Contact reversinglabs.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★★

Strengths It maps threats to the MITRE ATT&CK Framework to accelerate investigation and response activities, while its massive known-malware repository ensures organizations keep pace with the ever-growing threat landscape. Titanium always issues descriptions in plain language so that even analysts with less experience can actively and effectively engage in threat hunting and response.

Weaknesses None that we found.

Verdict Overall, ReversingLabs Titanium Platform is an exceptional threat intelligence solution that provides valuable information while maximizing actionability.

SC MEDIA BEST BUY

ReversingLabs Titanium Platform presents TitaniumCloud, an important threat intelligence tool that continually harvests files and intelligence information from various sources across the internet. Enriching threat intelligence data in this way makes it more actionable and relevant, drives security team efficiency, and even encourages inter-organizational collaboration since this file and data analysis reservoir is accessible to good faith actors all over the world.

Organizations often struggle to improve SOC efficiency and to optimize their existing threat intelligence programs that protect their environments against high risk threat vectors, while analysts face more alert fatigue and skillset gaps than ever. Yet, non-optimized threat hunting tools still miss threats and lack the indicators of compromise enrichments that they need to drive information value. ReversingLabs seeks to reverse these trends with three offerings that make up Titanium Platform: TitaniamCloud, which provides reputation and intelligence; TitaniumScale, which offers a scalable and elastic hub worker module; and A1000, an investigation console complete with malware analysis.

This solution focuses on growing attack vectors, specifically large destructive files and objects that are otherwise too large and complex for other analysis tools. The sheer volume of unpackers and supported formats that this solution offers allows organizations to process almost all data across all operating systems and application layers. It maps URLs to corresponding malware files, continuously and recursively crawling and breaking down each component so that analysts may discover every URL to which a particular malicious file has attached itself, not just the URL that delivers it into an environment initially. It also assigns every file a dynamic severity rating on a scale of 1-5, with 1 being the most benign and 5 the most severe. This rating may change depending on the results of the recursive analysis.

TitaniumCloud reveals the reasoning behind every threat determination it makes. Such transparency gives security teams confidence in all of the machine-generated insights and recommendations they receive. The platform also offers many opportunities for automation, issuing configuration recommendations with similarly transparent explanations that encourage organizations to adopt them. The reasoning is also important for sufficient depth and understanding of a threat to formulate customized automated responses to threats via the API.

The A1000 dashboard is quickly digestible and displays monthly statistical analysis trends. It collects approximately 8 million unique threat samples daily and combines them with internal threat intelligence to gauge threat maliciousness and severity. It categorizes all platform data, highlights the most critical information, such as the top malicious family detections based on malware type, and prioritizes remediations. The metrics in the dashboard give analysts useful overviews of current environment security posture and trends over time.

Overall, ReversingLabs Titanium Platform is an exceptional threat intelligence solution that provides valuable information while maximizing actionability. It maps threats to the MITRE ATT&CK Framework to accelerate investigation and response activities, while its massive known-malware repository ensures organizations keep pace with the ever-growing threat landscape. Titanium always issues descriptions in plain language so that even analysts with less experience can actively and effectively engage in threat hunting and response. Such ease-of-use, transparency, and scalability make Titanium an attractive option for organizations of all sizes.

Pricing starts at $10,000 per year and includes 8/5 phone, email, and website support. Organizations also have access to a knowledgebase and a FAQ list, both of which are rich in content and easy to use.

— Katelyn Dunn
Tested by Tom Weil