ReversingLabs Titanium Platform

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

ReversingLabs Titanium Platform

Read 2 reviews of ReversingLabs Titanium Platform

Review by a Real User

Verified by IT Central Station

Information Security Engineer IV at a financial services firm with 1,001-5,000 employees

Informat02f0

WHAT IS OUR PRIMARY USE CASE?

We haven't finished building it out fully but we want to use it as a pre-filter before samples go to anything else for analysis. Things are going to be coming to it and we're going to get a score regarding what ReversingLabs thinks of any file samples and, if it's a score that says it's a high threat level, we'll send it on for further analysis in other automated platforms.

HOW HAS IT HELPED MY ORGANIZATION?

The actionable insights that we've used thus far are from another ReversingLabs product, their APIs for hashes. We've been able to analyze thousands of hashes and then act on the ones which were deemed suspicious and malicious, by either retrieving a sample for further analysis or looking it up in other products. The head of my division has bought into the ReversingLabs group of products and their capabilities. One of the things that ReversingLabs has enabled us to do is look at new hashes and to do something with them, to act on them. When new files come in, we have at least one piece of information about them that we can query and find out further information. We might then do a pivot into other systems or other manual investigation methods. They've helped us begin to further automate our automated malware analysis and triage of new samples.

WHAT IS MOST VALUABLE?

We are primarily using it for its static analysis capabilities. It is valuable because it offers reports on a great many more file types than the other analysis solutions we have. It can give us a more in-depth analysis and better reporting on a larger number of file types. It also gives us a more comprehensive score on a number of things as well, and that's why we're using it as a front-end filter. It gives us more information, and then we use that information to decide whether or not we want to send it on and do further analysis. It's valuable because of its depth of information, as well as the breadth it gives us. There aren't a lot of tools that cover all of the different file types. While we have not extensively tested the detection, it has detected everything that we've thrown at it that we've known is malicious. From the numbers they've given us, the solution's malware and goodware repository seems huge. It easily integrates with our SIEM, Splunk.

ReversingLabs Titanium Platform

Read 2 reviews of ReversingLabs Titanium Platform

WHAT NEEDS IMPROVEMENT?

We would really like further integration with our threat intelligence platform, which is called ThreatConnect. We would also really like further integrations with an endpoint protection product we use called Tanium. The reason I mentioned both of these is that ReversingLabs claims to have extensive integrations with both of them, but they did not work for us. The integration may have not been tested all that well, because we don't have a complex setup in regard to connecting these things together. But when we tried the ReversingLabs integration with ThreatConnect, it flat out did not work. And we also haven't been able to get the Tanium integration to work. We are currently talking to them about some things we need in the next release. Mainly, they are security improvements and they know about those. They have done a great job in getting them to us, as soon as they can dedicate some engineering resources to them. Security improvements are the main things that we are working on with them right now because we do security scans of the appliance itself and there have been a number of vulnerabilities that have shown up.

FOR HOW LONG HAVE I USED THE SOLUTION?

We've been using it for about a year.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It's stable and capable. We've only had one issue where it needed to be updated because it had gotten into a weird state and there were memory issues and we couldn't run anything on the appliances. But there was only that one situation and that was fixed within a week to week-and-a-half, which I feel was good.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

We haven't tested it extensively, but we feel that it's going to be a very scalable solution which is going to handle the volume we intend to push to it. If everything is onboarded the way we want it, the entire company will be using it, in that all samples will be coming from all sorts of sources. It will be "under the hood" doing analysis constantly, 24 hours a day. Our company has 10,000-plus employees. We're not using it very extensively yet. We're still in the middle stages of implementation. We haven't integrated it with very many systems in our company yet, and we are still trying to figure out the engineering problems surrounding it, and are working on getting it secure enough to deploy in our environment. There are a number of different use cases for it. One of them is someone using it directly for doing threat hunting or threat detection. I'm not sure how many people are on those teams. But with the different threat-hunting teams and threat-detection teams, as well as forensic teams that might be using it, we could have at least 100 direct users. With everything else, it's being used indirectly by a number of services, under the hood. Anything that gets saved on a network share, any new updates on any of the operating systems - Linux, Windows, etc. - we want analyzed, as well as anything that gets saved or that gets brought in as an email attachment. We'd like, eventually, that anything that comes over the wire, that comes through our proxies and firewalls, downloaded by someone, to be analyzed. It's going to be the crux of a solution that does a lot of automated analysis. It's just one piece, but it's going to be a very critical piece because it's going to be the on-ramp. Responsibility for the solution will move to another team once I'm done with it, and that other team has about 15 people. But they support a lot of other things. They're a custom-support team, they support custom solutions.

ReversingLabs Titanium Platform

Read 2 reviews of ReversingLabs Titanium Platform

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Their engineering team has been great. In everything that we've done so far with ReversingLabs, they have been very responsive and very helpful on the support side. They're as speedy as they can be.

HOW WAS THE INITIAL SETUP?

This was my first time ever doing something like this, and I was working with a team to do it. The initial setup did seem, to me, to take a while, but I don't have enough perspective to judge how complex or straightforward it was because I've never done anything comparable. Our deployment has been ongoing for about a year. Our implementation strategy is to get a number of sources of file samples and hashes onboarded into the ReversingLabs ecosystem, whether it be the APIs or the appliances, including the A1000, and once we do that in development we want to export what we've learned to production.

WHAT ABOUT THE IMPLEMENTATION TEAM?

The "team," in this regard, is that ReversingLabs' team helped us greatly. They really provided the support and information we needed to get the initial setup going. But ultimately, it was an integrated team between them and us, because they did help us a lot. There were four on our side and it took us a number of months to get to the point where we felt that anything was happening with the solution, which may be typical. I'm not sure.

WHICH OTHER SOLUTIONS DID I EVALUATE?

We are also using FireEye and Palo Alto. As far as I can tell, the quantity of files that the ReversingLabs solution can process in a day is greater than many of these products. Also, the stability of this product seems to be much higher than some of the other ones that we've had issues with. Stability reliability volume of processing are the pros. On the other hand - and this is something of a pro and a con - there's a lot of tooling that we need to build up around the solution to get it to integrate with our existing setup. That's a plus and a minus, in that once we get it integrated, and once we understand all of the interfaces to this product and how best to utilize it, then it becomes a tool that we can extend in our own right. But the con side of it is that it takes all that engineering work, all that understanding, all that effort, and we're not there yet. And we've been doing this for some time. Other tools do not require as much of that sort of effort. ReversingLabs is going to be one of many things that we use. We don't want a mono-culture here, and we don't want information from just one vendor or one perspective. But we do respect ReversingLabs enough to put them in a very critical role in our infrastructure. We want to analyze pretty much everything that comes into our company, from email attachments to new files that are dropped by Microsoft updates, to files that people save on network drives, and we're going to use ReversingLabs to ingest all of those samples. ReversingLabs is supplemental for us. It will be a kind of filter before things get to the other solutions.

WHAT OTHER ADVICE DO I HAVE?

Anything we've pumped at this thing, it seems that it's just fine handling it. That's one of the big reasons we want it to be the funnel that everything comes through first. We want that determination of good, bad, or suspicious. We have complete faith that it can do that for us, and can do it at scale. It's stellar. I would easily give it a nine out of ten. I've had a great experience with it.

Learn more: Read 2 reviews of ReversingLabs Titanium Platform