ReversingLabs Titanium Platform

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

ReversingLabs Titanium Platform

Read 3 reviews of ReversingLabs Titanium Platform

From IT Central Station, the leading review site for enterprise technology solutions.

Review by a Real User

Verified by IT Central Station

Forensic Lead, Global Security Fusion Center
at a insurance company with 10,001+
employees

WHAT IS OUR PRIMARY USE CASE?

We use it to analyze and pull out any indicators of compromise from malware that we get within the environment. We check to see if those indicators are seen throughout our infrastructure. We also do some type of open-source intelligence using the platform, at a basic level, dumping emails into it to see if it can parse out any of the URLs and the like. But that part is very basic. We're basically using it as a "sandbox" for static analysis. It's on-prem. Only certain people have access to it. It's not integrated into our whole environment as of yet. I would like it to be in our plans to do so but, currently, it's not deployed in that manner.

HOW HAS IT HELPED MY ORGANIZATION?

Because we are a young global fusion center, we have very junior examiners and incident handlers. This solution gives them a better way to understand how malware is constructed, what kind of indicators accompany it, etc. We use it for both junior- and mid-level people to get down and dirty and do analysis, on-the-go, when needed. What has been nice is that those junior-level people can use that information and push it forward for final actions if needed, or verification through senior examiners and incident handlers. They get them to confirm what they're seeing so that we can detect and remediate in a more timely manner. It's absolutely saving us time. We're not even using the full capabilities, but it has reduced our meantime to remediation by about 25 percent.

WHAT IS MOST VALUABLE?

The automated static analysis of malware is the most valuable feature. Its detection abilities are very good. It hits all of the different platforms out there, platforms that see the items in the wild. Also, the solution’s object and file analysis provide us with actionable insights. Its malware and goodware repository is very good. It's very robust. It gets all of the different repositories that are out there that do analysis and brings them under one roof where we can statically analyze for those indicators of compromise and look at them more deeply. If we need to go deeper into things, we can do that.

Continued from previous page

WHAT NEEDS IMPROVEMENT?

I would like to see if we could do a little bit more of bulk uploading of hash sets. Right now, I can only do them individually. If I have, say, a couple of thousand hash sets, I would like to be able to upload them. Currently, it's a very manual task.

FOR HOW LONG HAVE I USED THE SOLUTION?

I have been using ReversingLabs for two-and-a-half years now.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

The stability has been fine. We haven't had one issue with it. The only issue we have, once in a while, is our lack of getting to the RDP sessions into it, but that has nothing to do with ReversingLabs. It happens with our environment.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

It can be scaled a lot better than the way we're using it. The analogy I like to use is that I have an iPad and I probably only use 15 percent of its capabilities. We're using about the same percentage of ReversingLabs' capabilities. It can be scaled to be more broad-based within our environment. I hope to push that in the next few quarters. If the solution was to be integrated, we're talking about close to a million assets, worldwide.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Their staff has always been responsive and great. I have nothing but great things to say about them. They've been awesome anytime I have a question. I don't have to wait 24 hours for an answer; usually, it's no more than an hour to two hours. And I've never had to escalate an issue. I've had great relationships with the company. Even if somebody leaves and somebody comes on, they're very responsive. There's rarely a hiccup with their product.

ReversingLabs Titanium Platform

Continued from previous page

WHICH SOLUTION DID I USE PREVIOUSLY AND WHY DID I SWITCH?

We had nothing and that's why we went to the Titanium platform. We had nothing in the environment to do such analysis, so it's been a savior in many ways. We had nothing even close to what ReversingLabs does. Leadership realized we needed something like this because of the turnover of talent and people not having an understanding of malware analysis. We needed some type of reliable solution that would help with at least the static analysis of such items.

HOW WAS THE INITIAL SETUP?

We have a separate engineering and infrastructure side, so I can't talk about the actual deployment in detail. But I believe that once we set up the environment, we were provided with a VM of the system. But there was more of a connection with our engineering groups to get it deployed within the environment, so we could access it and use it for our analysis. It only took one guy a couple of days. And it takes just one person to maintain it, again within the engineering team. There are about 35 of us using it, including level-ones, level-threes, and forensics.

WHAT ABOUT THE IMPLEMENTATION TEAM?

It was our internal team and ReversingLabs. That's it.

WHAT WAS OUR ROI?

Our return on investment is in time saved as well as in producing indicators of compromise.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

We pay on a yearly basis.

ReversingLabs Titanium Platform

Continued from previous page

WHICH OTHER SOLUTIONS DID I EVALUATE?

I don't believe they looked into any other products before choosing ReversingLabs. And I've been very satisfied with ReversingLabs. If it isn't broken, why try to fix it?

WHAT OTHER ADVICE DO I HAVE?

Work with the ReversingLabs team. They're great to work with, and they're willing to help in any way. The biggest lesson I've learned from using it is that I need to know a heck of a lot more about the solution's power and how we can better integrate it into the environment for all our teams to use. We don't deploy it in a fashion where it is integrated with our existing security investments as of yet. We are going to look into those integrations in the next few quarters. Right now, it's more of a standalone analysis system that is not hooked up to any of our EDR solutions. We have also not looked into the Threat Summary Dashboards yet. We've had a lot of employee changes and leadership changes. That's one of those things that is on the to-do list, but no one has really sat down and gone over it all.

WHICH DEPLOYMENT MODEL ARE YOU USING FOR THIS SOLUTION?

On-premises

Learn more: Read 3 reviews of ReversingLabs Titanium Platform