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

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

CSOInfor4e0d

WHAT IS OUR PRIMARY USE CASE?

The primary use case is static analysis and retrieval of malware relevant indicators. We have multiple products in use. As far as the onsite product is concerned, we use the latest version of the product. The other version is a cloud-based solution, so I assume this is always the latest version. We are not integrating the solution with our bank technologies directly since we are employing the solution in a special infrastructure, which is isolated from the rest of the production network for security reasons. However, we do integrate the solution with a number of other analysis technologies that we use as part of our laboratory infrastructure. As far as this is related, integration is fine. As far as the static analysis capabilities are concerned, they're used extensively on a daily basis. We've just completed the integration of the cloud-based variant.

HOW HAS IT HELPED MY ORGANIZATION?

We are not compiling specific metrics for this product. We are integrating both products. The static analysis engine that we've been using for roughly four to five years, which this is fully integrated in our workflows and processes. Then, there is the cloud-based variant that we've been using for around a year. This is also integrated in our platform for analyzing malicious programs directly. For downloading reasons, we have integrated the product directly with our platform. So, if you search for specific malicious programs that are, for instance, referenced in threat intelligence reports. Then, the product would be automatically leveraged as a source, not the only source, but as one source. Therefore, the users have the possibility of searching through different repositories in order to find threat intelligence related information. As far as the analysis is concerned, we do this ourselves and mostly leverage other products for this. We use the product from ReversingLabs, mostly, for data enrichment or downloading malicious programs that we are otherwise unable to find. As far as the availability of the content is generally concerned and the number of malicious programs that can be looked up in the repository, these are very extensive. The solution helps to automate SOC operations when it comes to identifying the highest priority threats. We're leveraging the APIs, so the whole process with respect to looking up information and retrieving information about threats is fully automated. It's used as a data enrichment source. It is not used as the only source, but it's the information that is provided by the product and we retrieve from other sources, then we prioritize based on respective threats and corresponding risks.

ReversingLabs Titanium Platform

Read 2 reviews of ReversingLabs Titanium Platform

WHAT IS MOST VALUABLE?

As far as the cloud version is concerned, we mostly leverage the product to retrieve samples, or malicious programs, that we are otherwise unable to find. So, the ability to download programs directly from the platform is of importance to us. Other than that, we mostly leverage the information regarding static analysis. As far as URLs are concerned, we would use the product as a source to verify whether or not the URL has been flagged as malicious. As far as static analysis information is concerned, we use most of the information that is available in order to determine whether or not we might be dealing with a malware variant. This includes information that is related to Java rules. This is also related to malware families indicated or specific malicious software variants that are labeled by name. Besides this, packing or unpacking related information is something that we leverage a lot. As far as the malware repository is concerned, it's extensive. It's a good source for finding samples, where we are unable to find them on other channels or by leveraging other sources.

WHAT NEEDS IMPROVEMENT?

It's integrated in our product. We leverage the API, but it doesn't contribute to increasing the release time of the product itself. While the company is very helpful, it would be very much appreciated to have extensive proof of concept scripts for the different APIs available, though not for all the APIs that we have purchased. Respective scripts are available, but those scripts which are available are typically not of very high quality. This could be an area where the company can generally improve. It is not a big issue for us, since we have our own development team, but it could be an issue for other companies who are less mature.

FOR HOW LONG HAVE I USED THE SOLUTION?

We have been a customer of this company for around four to five years. This particular solution has been in use for around a year now.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

The product works fine. We had some inner issues for some special use cases, where we initiated Webex sessions with the support, who eventually helped us figure out alternative solutions. Some of them were very helpful, and others were not so helpful. All in all, the stability is definitely okay, with some minor problems as far as special use cases are concerned.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

The scalability is good. It's a scalable product. Only malware analysts and reverse engineers are currently leveraging the product, and those are around 15 users.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

The product support could be better at times. They are typically okay. They are definitely trying to reach high customer satisfaction. They are also available on a very short notice. Sometimes, the resources that they provide could be of higher quality.

ReversingLabs Titanium Platform

Read 2 reviews of ReversingLabs Titanium Platform

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

We did not switch solutions. We use an alternative solution in addition to the current product.

HOW WAS THE INITIAL SETUP?

The initial setup was straightforward. We were able to use the product within a day, then started integrating it in into our own platform. It was mostly access credential-based.

WHAT ABOUT THE IMPLEMENTATION TEAM?

We deployed the solution in-house. I have a dedicated developer team of six developers with two additional administrators. Not all of them are necessary specifically for this product, but some of them are able to set up this technology and also maintain it. The strategy was always to use the product as an enrichment source in addition to other technologies, then make all that information centrally available in a fully automated manner.

WHAT WAS OUR ROI?

We are mostly leveraging the API. All of this is automated, which in turn, helps to reduce response time.

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

We have a yearly contract based on the number of queries and malicious programs which can be processed. Currently, the license number of lookups that we purchased has not been reached yet, because the integration has only recently been completed. However, our usage is expected and planned to increase over the next couple of months.

WHICH OTHER SOLUTIONS DID I EVALUATE?

We evaluated most of the features that we were eventually licensing. That included, for instance, the possibility to download malicious programs from the repository. As far as the static analysis engine was concerned, we ran a very in depth evaluation. We also compared the results of those analyses with information that we had available from other tools. So, there were some quite in-depth technical assessments done before purchasing the solution.

WHAT OTHER ADVICE DO I HAVE?

It's definitely a technical product. Some expertise and experience with malware analysis and anti-malware operations is required. Only purchasing the static analysis parts, as well as the APIs, this typically requires some maturity in the Security Operations Center (in respect to CERTs). If this is not the case, then respective teams should opt for the graphical user interface, which provides more guided support. Other than that, it's a good product. I would rate it approximately seven and a half to eight. One of the problems is currently that the company offers three different types of products which are very similar to each other. It's not entirely clear during respective discussions how those different products can be truly distinguished from each other. Besides having a graphical user interface and a cloud-based variant, there was originally just one product, which eventually evolved into different directions. Then, it became a series of different products. For the customer, this is not that easy to understand. The other aspect is, as far as the APIs are concerned, the respective sample scripts are not of very high quality. Some of them are really basic, and that code base should generally be improved. We are not leveraging the product as part of SOC operations. We use it for contributing to our anti-malware related operations, which is slightly different. We don't use the solution's threat summary dashboards. We're not leveraging the whitelist so much, so I can't say much about the goodware.

Learn more: Read 2 reviews of ReversingLabs Titanium Platform