Sonatype Nexus Lifecycle Review From A Customer

IT Central Station
Unbiased reviews from the tech community

Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle

Review by a Real User

Verified by IT Central Station

Achitekt at SV Informatik GmbH

Axel Niering

WHAT IS OUR PRIMARY USE CASE?

Our use case is to check and evaluate third-party libraries for vulnerabilities and licensing problems. We are integrating it into our build pipeline as well.

HOW HAS IT HELPED MY ORGANIZATION?

We're still using it in a PoC and it's not as integrated as it could be so it hasn't changed too much for us right now. But of course, what we want to do is to keep safe, look at the vulnerabilities that come from third-party libraries. It will change our development process and help us improve the security part, the development process. In the way we are using it now, we have checked several applications manually and gotten some information about vulnerabilities. And we have been able to fix these vulnerabilities with help of the product. The solution helps automate open-source governance and minimize risk. For example, a developer decides to use an open-source component, so he is going to add Wire Maven into the application. In this phase, he can already get information about possible vulnerabilities. If he ignores this, we can still absolutely detect such a problem later on and prevent it from being sent to production. This is a process which has several steps, of course. We also want to use the firewall to prevent such libraries from downloading, but this is something we haven't done yet. It has also improved on the time it takes us to release secure apps to market. It was not possible for us, before, to ensure really secure development. But we are still on our way in that regard. Without a tool like this, you can't really find out which vulnerabilities are present. It's only possible if you use such a tool. Because we didn't have this kind of tool before, I cannot say how much time it has saved. I can only say that now it's possible to develop secure applications.

WHAT IS MOST VALUABLE?

The most valuable feature is that I get a quick overview of the libraries that are included in the application, and the issues that are connected with them. I can quickly understand which problems there are from a security point of view or from a licensing point of view. It's quick and very exact. The onboarding and policy grandfathering are quite useful, to keep in mind what we have already discussed around parts of the application, and to identify our own parts of the application which are not discovered by Nexus Lifecycle. The data quality is really very good. We have also checked other products and they do not provide such good quality data. Still, we must look very closely at a single vulnerability from a single issue. We have to understand what problem it's indicating. However, without this tool there would be no way to do this. The data quality is really very good. It was very easy to integrate into our build pipeline, with Jenkins and Nexus Repository as the central product. It was very easy to integrate the evaluation of the application to be built into the Jenkins process so that we had the ability to check how good the application is thus far. It also helps when you look at the stage we are at in building this application, whether test or production.

Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle

WHAT NEEDS IMPROVEMENT?

If there is something which is not in Maven Central, sometimes it is difficult to get the right information because it's not found. And if you look at NPM-based applications, JavaScript, for example, these are only checkable via the build pipeline. You cannot upload the application itself and scan it, as is possible with Java, because a file could change significantly, so the applications are not found anymore. This is something that could be improved in future. Also, I have seen in Black Duck, for example, that there is also information about exploits there are known for a given vulnerability. This is something I haven't seen or haven't found yet in Nexus Lifecycle. If there is a known exploit to a vulnerability, this could be something that is useful to know as well.

FOR HOW LONG HAVE I USED THE SOLUTION?

Less than one year.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

Nexus Lifecycle has had no problems until now. There is just a small circle of people using it directly, so this is not a critical mass of users. I cannot say what the stability will be like when there are more people using it. But right now, there is absolutely no problem. It just works. The users in our company are developers and software architects.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

We are using just one instance right now, I don't know how it scales.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

We have always had quick responses to questions we had, and they have always been very helpful. The people involved are very smart. They know what to do.

HOW WAS THE INITIAL SETUP?

The initial process is straightforward. It took half an hour. We had everything working and then the integration into Jenkins took another half an hour. This was very straightforward. Of course, you must look at the rules and the metrics that are important to you. You must do something regarding the applications you are using and your organizations that are involved. But this is true for every tool.

WHAT WAS OUR ROI?

We are still on our PoC, so there has been no investment up until now. We have just decided to invest in Nexus Lifecycle. I am sure that there will be a return on investment very soon.

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

Its pricing is competitive within the market. It's not very cheap, it's not very expensive.

Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle

WHICH OTHER SOLUTIONS DID I EVALUATE?

We also evaluated Black Duck. We selected Nexus because of the data quality and the ability to integrate it into our build process.

WHAT OTHER ADVICE DO I HAVE?

Look very closely look at Nexus Lifecycle to check whether the system is a possibility in your environment. It has good data quality and good integration in our build environment. Everyone must check for themselves whether it is the right solution for them. But I would always advise to have a close look at Nexus Lifecycle, if there are similar requirements to ours. The Success Metrics feature is something we have not used too much up until now. It's unused because when we started was it was very basic. However, it is a very good means for seeing how successful we have been in reducing the issues that are connected with applications. We could improve the quality of the third-party libs we are using, and the SDLC is something we are going to improve as well. In this area, we hope Nexus Lifecycle will help us to do so. It's just a part of what there is to do, but Nexus Lifecycle will be very helpful in this kind of process. We can get the information about vulnerabilities and licensing problems very early, when integrating a library into Eclipse, for example. Further on we can scan applications manually and integrate the evaluation into the build pipeline. These things are important as early as possible, but it's also good to have the last look if there is something we do not want in production. In terms of blocking undesirable open-source components from entering our development lifecycle, we could configure the solution to do so but we haven't done so yet. This is, of course, something we want to do. As for the tool increasing developer productivity, I would say yes and no. Now we can better deliver secure applications but, on the other hand, there's more to do. Of course, it was just not done before so it would be comparing apples and oranges. It is possible that we will extend the tool to other development departments, or even to those who are looking at the licenses. We are using it on-premise, right now, and this is something we would continue. We are integrating it with our Jenkins and Nexus-based build pipeline, which is also here on-premise. This is what we are going to do in the next weeks.

Read 10 reviews of Sonatype Nexus Lifecycle