Speaker 1 (00:00:03)
You are listening to the one HCL podcast series, the place where industry experts, analysts and veterans help us identify, understand and prepare for the upcoming cybersecurity technologies and trends. If you haven't subscribed for the channel already, do it now for regular updates.

Speaker 2 (00:00:25)
Hello ladies and gentlemen, I am Robin Tiwari. Your host for this edition. Today I'm talking about HCL eVerity application security framework that provide end to end security solution for entire vulnerability management lifecycle as well,
I will talk about what are the customer objective from the application security program as well. What are the industry best practices?
What are the industries challenges they're facing to managing the security vulnerabilities?

And how, HCL provide better solutions in this area to overcome these kind of challenges. So I'm talking about the HCL eVerity which is a complete service that is designed to deliver comprehensive application vulnerability management program to provide an effective and efficient management of security vulnerabilities. From the detection till the remediation of the issues.
One of the customer objective in this area about managing the vulnerabilities is the fact that as we know that vulnerabilities and exploits are growing exponentially and modern enterprise has a poor middle mediaeval challenges to ensure vulnerability management program consistently achieve their principles and business outcome.
We at HCL understand that customer is looking for a solution to maintain and deliver an end to end application vulnerability management program to a certain and comprehensively identify the application vulnerability and consistently limited from the environment within stipulated time period.
As we mentioned that one of the challenges we are facing in this area that a traditional Vulnerability management program is only run by the security team to deliver prioritize vulnerabilities has been properly addressed by the industry and its practitioners.

Collaborative outcome driven vulnerability remediation that result in cross functional organization efficiency and more security involvement remain uncharted territory for the most.

The literally challenging but achievable with fully utilized tools, willing people and a mature process. Industries are facing many challenges in terms of management vulnerability, which is diversified in nature and lead time increase the remediation of the vulnerabilities. So some of the basic challenges like organizations are using different technologies, so they use different set of tools to assess their application. That may also increase the lead time to remediate the vulnerabilities. Many of the organizations are moving from traditional opposed to the dev OPS part for faster execution, so they miss to remediate the vulnerabilities on time because many times the developer have been missed due to their execution time have been delayed and some other organizations are managing the vulnerability manually.

Which again leading time to increase the remediation time of the vulnerabilities another some of the challenges which we have seen that people are following the very standard approach for the protection of the vulnerabilities. So they missed the critical patches which need to be updated

very frequently as per the exploitation is available those are the thing that has not been considered while we are prioritizing the vulnerabilities. And when we're talking about managing the vulnerabilities there are, it means we not only for the developer or the Infra team, but for the CIO or CISO level. It should be highly visible to them so they know drag their particular vulnerabilities so less visibility of the vulnerabilities is also one of the challenges we have.

In in this area and there is a wide gap between the security person who are doing the security assessment and the development team. They have lack. Of coordination between them when they are doing this kind of application security program, or they're developing some applications, though they get the information about the security vulnerabilities, but they missed the deadline to remediate those vulnerabilities. So there is vital gap between them, so due to the different type of challenges faced by the organization in terms of managing a vulnerability we as HCL bring a solution E Verity solution that helps CISO & CIO level people also to easily manage their vulnerability management program to remediate from their environment as soon as possible.

What is this particular solution we're talking about? So this is a Verity framework that is enablement for the significant risk predictions through effective prioritization of the vulnerabilities, governance and automation on the various layer of application security program. It has various features like aggregation, deduplication and compression of abstract vulnerabilities.
Vulnerability management need risk measurement to use remedy cross team collaboration process orchestration, integrated remediation automation and visibility into the progress and outcome from scanned to the fixing of all those vertical vulnerabilities.
Our solution will provide a seamless integration and orchestration of abstract tools within the DevOps pipeline also for consistent repeatable scanning at scale without changing existing workflow or impeding productivity, its support or leading commercial as well as open source tools also, to align with the customer preference. To streamline the service delivery, it provides the analytics dashboard and report that deliver a single source of truth on AppSec risk or the application portfolio from the executive view to the granular details. Organizations must systematically optimize its vulnerability management process at each level to move on towards its goal as data driven well-orchestrated smart vulnerability management program. So this particular solution that we're talking about it is a framework which provide from platform for detection, tracking, and support for fixing those vulnerabilities and enhance the effective governance process.
Easy integration with the enterprise existing tool, asset management, configuration management, deployment and so on allow for them to be orchestrated into a seamless remediation track. So our HCL platform will provide a dashboard and source of truth for the remediation in process with all team kept continuously updated as to the progress and status of the vulnerability to the. To the CIO and CEO development team, infra team and all the application owners to know about what is the status and they can easily track those things. So this is platform we will just want to explore and we happily to give more information when we need it on this.
So thank you for listening to me hope you have enjoyed this particular edition with that allow your host Robin Tiwary to sign off. Thank you, thank you for listening.

Speaker 1 (00:07:14)
This episode of the One HCL podcast series has ended. Be sure to subscribe for more insights on how to identify, understand and prepare for the world of possibilities around the new and upcoming cyber security technologies and trends. Don't forget to rate and review this episode so we can keep bringing you the most relevant content.