You're listening to the one HCL podcast series, the place where industry experts, analyst and veterans help us identify, understand and prepare for the upcoming cybersecurity technologies and trends. If you haven't subscribed to the channel already, do it now for regular updates. This episode starts in 321.

Hi, everyone. Welcome to the cybersecurity and GRC services technical podcast on vulnerability management. I'm your host for today. And with me today I have Saurabh Singh, who is leading service security consulting team and has extensive experience in various cybersecurity technologies and offering so Saurabh has an extensive experience of around a decade and vulnerability management domain, which is a topic of discussion for the podcast. So let's start our today's podcast and gain some in depth industry information in the field of vulnerability management from our guest, welcome to our podcast Saurabh Thank you. happy to be part of your podcast today.

Thank you Saurabh. So as a kickstart since the pandemic has occurred, we have a multi fold increase in the cyber-attacks and even the repeated organisations like who was the main central point in the current pandemic was also compromised and attacked. So, sort of can you explain our audience how we should have played a role through which these attacks could have been avoided?

Exactly. So, I mean, how vulnerability management can come to rescue in this specific area is by decreasing the attack surface, well established vulnerability management programme will help us to not only reduce the vulnerability landscape, but also to proactively identify the vulnerabilities if there are zero days proactively it can get us visibility into that area and then help us to proactively remedy it or close the vulnerabilities. Hence, in a way we are reducing our attack surface area and that is the benefit which are well manageable number two management programme can bring in for any organisation

Okay, so, I think now, we are pretty much sure that our audience could be able to relate the importance of liberty management in their organisations. So, sort of what are the specific ask the client have been coming up over the period of time after the corona pandemic has occurred? So, are there any new asks is the client are talking about
I mean, that kind of discussions we are having or the engagements that we have seen a lot says specifically for the advanced VM, but for example, from last year, we have seen the focus or trend towards adoption of advanced VM, advanced VM has gained more traction or attention during this pandemic. Okay,

so Sir, can you just explain our audience that what advancement This is bringing to the earlier VM programme, which was running in the organisations and how it is more effective in managing the end to end threat landscape for any organisation? Definitely.
So we have to understand what is the advanced in this vulnerability management, you can consider vulnerability management as being an actus udic engage. The vulnerability scans were run in accordance with predefined frequency. And then the output was treated in accordance with the output that we're getting from now, but if we talk about advanced VM, what are the features that make it advanced? So I'll just list a couple of those features and then I'll explain them What are those features. So, the first and foremost will be the asset visibility, that is attained dynamically the dynamic discovery and in in winterization of

assets, second, would be then the coverage of attack vectors followed by real time monitoring and analysis. This is where we move away from the episodic scanning frequencies. And then the later features which are understanding context business risk and bringing the threat Intel perspective. And then last feature would be bringing the remediation capabilities. So that we as an organisation has an idea of which are the focus areas or the priority areas from a remediation perspective when they have to focus so these are the some of the features which make vulnerability management programme, an advanced vulnerability management programme.
Sort of we are now hearing a prioritisation as a constant Central most focused on being used during the vulnerability management programme. So, how effective is this word advanced multi management programme is helping in the prioritisation and the remediation which we just talked about.

Yeah, so, I think it is paramount in a nutshell. Now, the features that we talked about and how it helps in prioritisation or remediation for that matter. So, first one would be the asset visibility. Now, we are working in an area or we see that there are various asset categories such as the management manager assets in my data centre, cloud based mobile IoT x etc. So, first step is to get a visibility on those kinds of assets and then bring in the aspects of asset criticality from this point on we take this asset criticality forward and once when I'm doing the vulnerability scanning, I understand the context. So, context in terms of while the asset criticality is with me, what is the context what is the business risk if that asset is compromised, so, I bring that context as well. And the third visibility that I bring is what is the exploitability or the nature of exploitation of the vulnerability which is reported is it is if there is a exploit which is readily available for the vulnerability in the market. So, bringing in all the three views I as an organisation, bring prioritisation aspects. So, I give a prioritised list of all amputees which have to be focused the messaging that we have here is organisations have to focus their energies on the areas where it matters most hence, prioritisation becomes of paramount importance, another feature in the same top discussion discuss remediation in advanced VM the remediation code becomes very important so that while vulnerabilities are being reported, how are they being closed? Or are the exception management practices that we are following? For example, if some of them it is cannot be closed because of valid business reasons? How are we going to manage exceptions for those? So, those are few of the aspects that we focus on in the advanced vulnerability management.

Okay. So, sort of we generally hear a lot about automation in the ICT industry which is going ahead. So is this advanced vulnerability management programme utilising automation as well?

Yes, I think the major discussion drivers or engagements that we are having a thing a lot of integrations recently. So the trend now for all the organisations is to have an integrated environment. And the typical integrations that we are seeing or we are engaged in doing are the integrations with solutions like same patch management, the ITSM solutions and the CMDB solutions in the environment. And output of this integrated environment is being fed into the compliance monitoring tools of the organisation.
So what we can understand is there the increased monitoring, and the end to end visibility is always available in the advanced VM programme.

You're right in saying that I'm
so sorry, that was really in depth technical information. And I believe or a cybersecurity enthusiast, they will believe this utilise this knowledge and will increase their awareness about the advanced VM programme. So sorry, moving ahead. We talked about the best practices earlier in a podcast. So in the advanced VM does his best practices, the first as for industry, reason, manufacturing, or financial, whatever industry? It is?
Yeah. So I mean, it still is a firm believer of the fact that if we talk about vulnerability management, there is no one size fits all strategy. I'll give you two live examples of two environments. If we talk about manufacturing as an organisation and BFSI as an organisation. In the manufacturing side, what we are seeing more and more is the visibility. Now clients want a continuous visibility, not only in the IT environment, but also in the OT side, what are the assets being added into the OT environment? And what are the Wm vulnerabilities without disrupting the normal business? What are the vulnerabilities which exist in their oT? So that is the focus area. Now if I come to a BFSI sector, what we're typically seeing is the hybrid nature hybrid nature of environment is hybrid is not only on premise and cloud landscape for vulnerability scanning is on prem and multi cloud, in essence, that there are multiple cloud options. And also, there is extension of applications to go by so that extending the coverage and reach of their banking facilities
Okay, so it's clearly visible that they are dynamic solutions defined based on the industry requirements. So, sort of as we have been hearing since long that the validity management always takes place the last place in the budgeting of an event of any IoT farm or maybe any organisation. So, how do you see the organisation expenditure on vulnerability management being increased over the period of time?

I think I mean, from where we started, we have seen like I mentioned in this podcast that will MBT management was seen as an additional responsibility, but the scenario today has changed drastically, vulnerability management has gained substantial mindshare of the CEOs of any organisation and what we are seeing that the vulnerability management discussions initiatives are being taken seriously and also it is being represented as one of the major lines in the balance sheet of organisations. So, yes, there is focus there is management driven initiatives for vulnerability management and also investments which are happening in this space okay,
sort of as a practitioner, how are you seeing the V model evolving based on the scanner based approach or the agent based approach or other organisation now preferring the hybrid model as you discussed?
summit like we touched on the fact in our initial discussions, it has come a long way the vulnerability scanning tool, if that is the question earlier when it was only one hardware or software based scanning solutions, now organisations want it hybrid, so that there is holistic coverage. So, the adoption is clearly for scanners and with agents and then there is third component which is being heavily relied on or heavily adopted is the use of passive visibility being achieved by continuous monitoring or scanning scanner. So, those are the three components that we see as an adoption. And yes, yes, it is pretty much hybrid that organisations are adopting today.
So it's not clearly visible that there is a continuous monitoring shift and the vulnerability management perspective that earlier the clients and organisation have to sort of since it still has a huge client based on the validity management side, what are the specific VM based offering ACLs engaging with this client

committee, we are capturing the entire spectrum of vulnerability management a so if you talk as a service model in this area for vulnerability management, for policy compliance and web application scanning and the cherry on top of the consulting initiatives that we are doing, wherein we are engaging with a lot of organisations in advanced integrations area wherein the integration is bringing the holistic upwards and downwards view in along with the vulnerability scanning solution,
okay. So, sort of how also is it still managing the specific ask and maintaining the good momentum with the good with the time where the attacks are increasing ever since. So, how is it still managing its offering accordingly,
we have been very proactive in managing or aligning ourselves to the scenarios. Hence, what we have done is we on a service model as well, we started with vulnerability management. But now what we are focusing is a risk driven vulnerability management programme, wherein, what we are doing is we are enriching the data or the output that we are getting from vulnerability scanning solutions or web application scanning solutions, Enriching it with the risk and the threat which might be prevalent for that organisation or for that vertical industry vertical. And with this, we are thriving in the remediation bringing into governance. So those are the enrichment that we have done in our as a service offerings,
sort of your answer clearly depicts that how well it still is evolving itself with the ever changing client requirements. So now, I think with this podcast, our audience had got an overview about the availability management and the advancement of multi management, which is just taking up the industry standards, and the various industry solution offerings and our latest client requirements, which is sales volume demand team is going through. So well that's for today's episode of sales consulting, and I sell cybersecurity and GRC services podcast. Thanks for listening. And thank you so much for joining me today for sharing your valuable experience on the most important pillars of the cyber security domain. That is the vulnerability management. Join us again, when we will talking about the penetration testing, which is also another important cybersecurity pillar to thank you everyone.
Thank you, man. Take care.
This episode of the one HCl podcast series has ended, but be sure to subscribe for more insights on how to identify, understand and prepare for the world of possibilities around the new and upcoming cybersecurity technologies and trends. Don't forget to rate and review the episodes So that we can keep bringing you the most relevant content. Thank you for listening