Remediation Plans Video Transcript

Welcome. In this video, we're going to review remediation plans and CyberCNS is going to go ahead and get logged in here.

So, once we get logged into the CyberCNS portal, we will be down at our company level and over on the left understand results, we're going to be under a remediation plan. So, the remediation plan section is available at both company level and at the global level.

So, in this particular view, I'm at the blue Add company and I'm looking at 58 items for the remediation. That was to tap on the globe. Go back to remediation plan. Now I'm looking at 90 and this is across all of our customers in cyber scans. I'll go ahead and drive us back to the company. So, run blue Add remediation. We're back down to that customer.

And so, the remediation plan is a view of all of the applications that are either missing patches or are not up to date and at their current versions. So, we're going to identify those for you. We're going to give you the evidence, which is what you should do to fix them and then give you the ability to drive some action out firms.

So, from within the portal, I can go ahead and see some different action items that we have. Some will say Update, some will say remove depending on what the remediation action is. So, update is referring to an application 360 total security that is not on the latest version. And so if I was to look at the evidence on this particular line on this top line, our evidence is under the vulnerabilities and it's showing we've got three high just what those coloring schemes are. If you look here, we've got some mediums and we've got some criticals so it's telling you how many vulnerabilities we're finding and what severity those vulnerabilities are.

And the evidence is showing us what the product is what version we're currently on. So, ending in 15.0.3 and it looks like the latest version is ending in 15.3.1. So, we're a few patch levels back. And we've also provided you with a download to it. So, this link here is the actual executable download, which is no downloading to my machine here.

To go ahead and install the latest version of 360 total security or the evidence leads us a way to get the latest fix or the recommended fix completed. And that's on anything that's action of an update. You can also see here on the line we've got a ticket ID and asset column so it can be is if you're using an integration to one of the PSA systems. We'll go ahead and read the ticket number. In our case we've got our ConnectWise environment set up here. So, any of these ticket numbers are pushing over to our ConnectWise system.

So if you see a company here, for example, get I can see doesn't have a ticket ID. I can go ahead and push this over to our instance and you can push multiple remediation items at once. So, for example, you can see some of these have unique ticket numbers. But I could also like you're seeing down here in this

grouping, we can go ahead and select multiple lines from a remediation plan. So, for example, these three could get pushed over in a single ticket. Or I could create them one line for one ticket depending on oh you want to triage and treat these. You have the option to do that.

Once you select one of these items up on our menu bar up here, we'll use integration action. This will allow us to do a short or long description. This is the information that's basically getting pushed over in the ticket. I like more info so I like to use long you prefer different you can obviously use short and the if you hover over your tooltip will tell you exactly what info is being pushed. I'll go ahead and choose that. It'll give us our integrations and Actions menu.

From here we can signal what we want to do with this remediation plan item. So, I've got a couple options because we've got three integrations in this environment setup. We've got our Connect wise we've got an email method, and we're going to go ahead and use our ConnectWise system here. And we've got Creek close or update tickets within the system. So, in this case, I'm just going to go ahead and create. It'll fill in a summary and a description for us with some detail.

You can obviously add or change this you can come in here and change it if you'd like I'll just leave our defaults. Choose the Service Board. So, this is pulling from your ConnectWise environment. Whatever service boards you've got available will show up here. I'll use our alert monitoring board the source I'll choose our ConnectSecure option. Again these values that you see are all coming right out of your Connect wise systems. Whatever you've got set up in your Connect wise is what we're going to be looking for here.

So, once you set these values are given a status, open and closed. One and we'll see these are P2s and you got a note type. So, your notes external, external would be the discussion area of your ConnectWise ticket. So, session area generally used for customer facing stuff. I tend to use internal or internal analysis or anything that's an alert like this. So, I'll just choose internal. You hit submit, and this will get pushed over to your ConnectWise instance. You'll notice here it gives us success 11426 as our ticket ID and then on that line, you can see it's not filled in my ticket ID. And then this will tell us actually the number of assets that are affected by that particular vulnerabilities. So, in this case, it's just the one this machine if it was multiples, you'd get a count there. So, there's multiple on this one. So, there's the desktops in cyber scenes it's been so you get your counts at ticket that got pushed over for it. And we'll go ahead and open up our excuse me our ConnectWise instance here. And get a look at that real quick. Go out to our service board. And take a look here we've got blue web company doing that enforcement. So, 11426 that would have been that new ticket ID and this was for that good.

So, if you look here on the ticket creates, allows us, you know what application, what the fix is? Here's that link that we provide in in the evidence. So, the technician gets this ticket. They've got the link right here to go ahead and download that executable, install it on the machine to get it to get that addressed or you know, deploy it via your RMM solution. For those of you that will give you some information about where we found what we're that get installations taking place in where the vulnerabilities are. So, this is the ticket that gets punched over to your system. If you punch over multiples at the same time, you would just get you know three separations in that body or give you three titles at the same time. So, if you like one issue per line you have the option to either create one ticket earlier or like I mentioned multi-select and send them all over in a single ticket.

So, that's the remediation plan actions kind of at that company level. Again, I'm at Blue lead. I'm at that customer's level and the last thing on the toolbar is our snooze inactivate. So, this is used to suppress an alert that is picked up so if I wanted to take that 360 security and say you know what? We're going to go ahead and suppress this one we know about it. It's justified for this reasons we suppress it for one to 14 days. Or if we pick up a false positive in the system, we can go ahead and flag a false positive. Our team will be watching these and using those to eliminate them through updates and development cycles. So, appreciate any partners that let us know if you're seeing false positives, let us know let our support team you know, but that's what this news is up for is allows you to snooze and suppress an alert.

And so, when I'm in a remediation plan, I'm up here I've got these filters. I'm in the pending, so pending are things that need to get taken care of. They're still open, they're not resolved, or remediated.

Suppressed we just talked about so you can suppress things. And then you can look at the list of those suppressed items at the customer level. What they are how they got suppressed what tickets they're on. So, these tickets were in your PSA they'd be in hopefully in a waiting state. And you can kind of track these through.

And then we've got the remediated section. So, this will show us all the items in application that have been remediated in this case, or blue Add company. So, 24 times we've done remediation across different assets when we did it, what the tickets were, and what was actually updated.

So, that's the three views in the remediation plan at the customer level pending remediated suppressed. You can also filter by operating system if you wanted to look at you know, one OS versus the other. And then of course you can search so if you've got a large list growing over time, you can always use that as like hey, I want to find Java, or I want to find things with Microsoft, or maybe things with just that net. See the search is really responsive. It's really fast. So, I find this incredibly useful when I'm looking for stuff.

So, any searching you can always filter out there me and this is remediation plan at the company level blue. Now, you can also get to some of the same data. As I mentioned, at the global level, you can also do it at the asset level. So, we're kind of in the middle ground right right the company. By come down to active assets, we'll be able to do that same remediation plan data at the asset level. So, coming down into one of your assets, clicking on the remediation plan icon. We'll get those same view of things that need to be remediated.

Now, this is a good exam scenario. This remediation plan is signaling applications that need to be installed. Now these aren't missing updates, they're not invulnerable, but they're just not installed. And so, what this is a result of what we call application baseline.

Application baselines allow you to tell CyberCNS, what software needs to be installed like a mandatory install on an endpoint. So, if we detect that a machine in this scenario doesn't have Firefox doesn't have WebEx or MTA then we're going to signal that this needs to be installed and then at the next scan, we'll check in check the versions and then flush these out. But this is the remediation plan at the asset level. So, I'm on the steel legend asset. I'm down here I'm looking at the plan and I can see I've got some of those same actions that we talked about earlier as far as selecting off the items and then using the integration actions to go ahead and punch these through to your PSA as a ticket.

And that way your technicians or engineers are going to be able to get those assets resolved get that software installed, or get it updated. So Miss case we ran into an asset that needed installed software based on our application baselining. I'll just navigate to another asset that has vulnerabilities or remediation items. So, here's a pretty noisy one. This asset has 11 items on it and you can see here, this one has a remove. So, again, this is application baseline showing up where we're saying any desk software should be removed from any endpoint that we detected on. So, as part of a remediation step will signal if if software needs to be installed or removed off of an endpoint. So, in this case, we shouldn't be removing any desk from this endpoint. And then you can see the other apps that have the update signal. These need to be installed. And again we've got the evidence and how to fix these the URLs to fix these up to the pins or in this case products reaches end of life as of December 13. So, we'd want to get that you know, remediated and then got your ticket ID signal still.

So again, this is at the endpoint level. We can also go back and look at we can look at remediation plan at the company level. So you've got the granular look down at the desktop or you can come back at the company level and look at the company side.

Last is the global view. So, again, if I tap global and go back to remediation plan, this is now looking at that same data set, but this is for all of our customers in CyberCNS. So, instead of getting it down at the company level, I'm getting a bigger picture look across how many total items do we really need to have resolved so in my mind, that's 90 tickets right there, right? I need 90 tickets potentially created so that my engineering team might knock my sock whoever's responsible for these tickets and carrying out those kinds of services for our customers. These are their actionable items for the day. So, you know, I was coming in and starting my day, I would be coming here and saying okay, what do we need to get remediated and take place? Right, because once you get all the hygiene and all the machines up to date, these remediation plans will really fizzle out to mostly nothing, there should only be a few line items.

The majority of the works in common you onboard a new a new client. So, when an agent first gets deployed at a customer's network, and you first scan and we first discover all their assets, that's going to be when the most effort is going to be needed at the remediation plan level. But once we get the environment kind of standardized, to get the machines patched we get everything hardened and up to date based on our compliance and standards.

Eventually this stuff will fizzle out and allow your engineers and technicians to spend more time with your customers doing more proactive services. You know doing those things that we talked about in in the managed security services offering that they're most likely under. It'll give them some of that time back to look at that stuff. So, remediation plan globally. And again, we can also use our filtering at the global level. So, if I want to see suppressed alerts for all customers or remediated alerts for all customers, we've got those sand filters here and the searching so that is the remediation plan. I will be covering I know we kind of touched on the application baselines where we talked about mandatory applications. We will have a separate video covering application baselines. So, if you guys want to check that one out, we'll have that on the YouTube channel.

That will do it for the remediation plans. Thanks for watching. And again, if you guys have any feedback, or comments, feel free to comment that video on the channel. And if you have any future recommendations on content you can continue to use the email education@connectsecure.com.