Notification Rules (Alerting) Video Transcript

Welcome. In this video, we're gonna cover notification rules, now known as alerting within CyberCNS.

So, before we get started, I'm gonna share a little bit of information with you guys about notification rules. As of early March 2023, notification rules have been disabled and can no longer be edited. We have migrated any existing rules that you had over to the event set and integration profiles. So, if you have any trouble with those that were set up prior, please let us know via email at support@CyberCNS.com. Open a ticket, and we will get you some help right away.

I also want to review the user documentation with you guys very quickly here. So, if you're on our website, connectsecure.com, go to resources and support, then click on the "View Documentation" link. On our left panel under "notification rules," we've got the CyberCNS alerting. Okay, and this is the doc, this is where I've got the snippet on this slide deck for you guys. And again, these documentation steps with screenshots will take you through this alerting setup in detail. I'm going to step us through it today on the video, but I wanted you guys to see before we get started if you want to follow along with the document, the documentation is out there and will step you through this as well.

So, I'm gonna go ahead and get us going here and we're going to get logged in. Once we get logged into the system, we are going to want to make sure that we're navigating up to that global view and then to integrations. And this is where we're going to configure our event rules, event sets, and how those notifications flow out. So, depending on what integration you're working with, you'll tacky accordingly. Today, I'm going to go ahead and work with our ConnectWise integration.

And once we're on the integration, we're going to go over to the company mappings area. You'll have to have this already connected in order to get here. If you don't have your ConnectWise manage integration set up, we do have a video on our YouTube channel that covers this step by step, and we also have the user documentation. So, if you need help getting that set up, that's out there. Otherwise, you're going to come over to the company mapping area where we're going to then see our event set, integration profile, and the mappings. So, these three areas are going to work together to create our notification engine, right? We need these three pieces connected in order for this to work.

So, we're going to start with our event set or the alert rule. We'll go ahead and tap "Add." And this is where we're going to give the rule a name and then select from our list what event set rules we want to be notified on. So, we've got a number of different categories here, and if you tap on the category, it will give you an accordion-style dropdown that'll give you the option.

So, under the "Agent" heading, we've got "Pro window" or a "Server Agent went down," and if you wanted to be alerted on those, simply tap those. And then we've got "Company," you know a new

company has been created. If we see that alert, we'll go ahead and tap that. So, you can go ahead and multi-select as many of these alerts as you want in any combination you want.

We do have a whole documentation page out there again on that site that explains each of these a bit in more detail regarding the remediation options and what we're including and how these are flowing across. So, if you have any questions, you want to see that, that is out there.

I'm going to go ahead and create an event set today. A popular one I get a lot of partners doing and asking me about is Active Directory stuff. So, I'm going to go ahead and use our Active Directory audit as our option today. And as you can see, we've got quite a few options in here for alerts. So, depending on what you want to know about, you can select every single one of these if you want.

So, I'll use an example where maybe I got a little bit Active Directory crazy and I said, you know, I want to get alerts for everything, any Active Directory alert that CyberCNS offers. I'm going to go ahead and pick them all. So, we'll pretend that I checked all those boxes off. And then I'll call this, give it a name. So, I'm going to call this "Active Directory - All Alerts." Where you would use your name, you would make it descriptive, and it lets you know what that event set is actually covering. Okay, so I've got my name, and I'll just check all the alerts. Let's save that.

So, there's one event set for Active Directory. Now, we'll move into our integration profile. So, this is where we're going to tell the system how to route that event into our integration. So, in this scenario, we're using our ConnectWise manage, so we're telling the event of Active Directory how to get into ConnectWise ticketing.

So, I'm going to go ahead and create a new integration rule for this. Now, I've got some existing ones here that you can see that I've already made from previously. You can edit, delete, and set these as the default from this menu for any rules that you've already made.

I'm going to make a new rule today since we need one for Active Directory that we don't have. So, I'm going to go ahead and do "Add," we're going to call this our "ConnectWise - Active Directory." The credential profile will already be selected for your advisor integration. Then we're going to choose the service board that we want to route this event to.

So, the Active Directory event, we're going to send to our "Alerts and Monitoring" board. You can choose the source. So, we've got some sources. Again, these are coming right out of your ConnectWise setup table choices. We've got some types. So, on our ConnectWise alerting Monitoring Service Board, we use our service types to signal what the platform or product was that is sending the alert through. So, we're going to choose "Connect Secure" in this instance. Then we've got subtypes that belong to that. That can tell us a little bit more information about what Connect Secure alerting to. So, I've got some choices. And again, I've built these in our ConnectWise environment. So, these already exist within our ConnectWise board. And I've got one for Active Directory. So, I'm going to go ahead and choose my "Active Directory" subtype.

You can see here, if I was doing applications or remediation plans or service items, I could also choose those. Again, create some additional mapping flow. But for this one, I'll go ahead and add. Not going to bother with items. I'm going to go ahead and do our "New Ticket Status." So, it wants to know when it creates a ticket from CyberCNS, what status should it go to. I'm going to use "New."

And then if we close a ticket from CyberCNS, what do we want it to go to? I'll use "Closed." Automation the priority of the ticket. So, these are our ticket priorities. Again, these are coming right out of your ConnectWise. We use P1 through P5. If you guys have different in here like the critical, medium, high, low, or whatever urgency you've got set, you can just find that. And then where you want the note to hit, external would be the ticket discussion, internal or internal analysis. I'll go ahead and use internal. So, I've added in the ConnectWise "Active Directory" integration rule. That top one is the one I just made.

Lastly, is connecting those two together with a mapping to a company. So, on our company mappings, we can see here any of the existing CyberCNS clients we've got, and then what they're mapped to in our ConnectWise environment. And then you can see here, if we had event sets and profiles assigned, they would feed in here. So, I'm going to go ahead and new "CW Advisory Group" for our test company today. And we're going to go ahead and edit this. So, we're going to edit the company. And this is where we can go ahead and enable our ticket creation.

So, I'm going to enable tickets, and then we have to tell it what event set. So, I'll go ahead and choose our event set that we made, "Active Directory - All Alerts," and then the integration profile. So, when we find that event, how do we push those tickets through to ConnectWise manage? So, we're going to choose our "ConnectWise - Active Directory" when we created earlier. And then we'll tap that plus sign that will give us a recap of what's been updated within that customer. And we hit update when we're done. If you want to sync configurations over to manage as well, this is where you can enable that sync, turn that on and off. So, I'll go ahead and check that because we always want that on.

Once those settings have been submitted, the screenshot and refresh, and again, you'll see a preview there of the Active Directory alerts and the integration profile side. So, I'm going to do one more here together with you guys. Okay, so we're going to go back to events. We're going to make a second rule here. So, we'll call this rule, we're going to look for a probe. Actually, let's do the remediation because this one's also very popular. So, remediation.

So, I personally like "Remediate by Asset and Product." And what this does is any item that shows up on a remediation plan or an asset will essentially create a single ticket for each remediation. So, I like to see tickets so that I know we can tie workflows, we can create accountability, we can make sure things are getting done in a timely fashion based on SLAs. All that starts to take place if you have the ticket. So, I like to do remediation by asset and product.

So, I'm going to call my event set just that, "Remediation by Asset and Product," but you would use your name. I'll just check the one box. Let's save that. Oh, there's my alert rule. And I'm going to do my integration profile. So, again, this is when that alert, when that event set goes off, how do I want it to map over to the ConnectWise system? So, we've got the "Active Directory" one, you can see here I've got a couple of others below for applications and remediation plans.

We'll go ahead and choose our "Remediation Plan" for this mapping. So, again, I'm going to just go edit here so you guys can kind of see the inside of this one. This one we've given it that name. And again, we've just told it, what board to go to, what's our source, what's the type and subtype on the ticket. So, for this one, I've got, you know, a remediation plan or an update versus Active Directory on the previous one. So, again, we're just telling it to do something a little bit different remediation plan. And then lastly, on the company mapping is where we assign the event set and profile to. So, I'll use "CW Advisory Group" again, we'll go ahead and edit these guys.

We can see here they've already got an event set defined for EDI. We're going to go ahead and do another one. So, we'll go from our event set dropdown, there's our "Remediate by Asset and Product," and then there's our "Remediation Plan" one. Go ahead, hit that plus, add it to the list, and hit update. Once the screen refreshes again, we should see that "EDICW Advisory Group" now has two profiles set. So, the more you add, the more you get, you know this view gets built up based on your event sets and profiles.

So, it's best to consolidate when you can. Right, you obviously don't want to have 30 individual ones because that can get messy. So, it's best to consolidate events and integration profile settings when possible. And it's really thinking about how can we logically group tickets together and minimize the options there. So, once these two are configured, that is the alerting rules.

So, again, back on our website, if you go to our support documentation, you'll see "CyberCNS alerting," this will step you through all of the things I just kind of discussed. It's got some breakdowns, it talks about the remediation options and all the details. So, if you'd like to docs and you want to get a little bit more detailed than the video show, that Doc's out there would also encourage you guys, you know, comment on this video, if there's other areas that you'd like to see around the alerting, other examples of integration profiles or event sets that we've done, or other partners or internally. We'd love to share those with you guys. So, let us know again, YouTube channel is out there, comment on those videos, or you can drop us an email directly at education@connectsecure.com.