Active Directory, Part 1 (On Premise) Video Transcript

Welcome. In this video, we're going to cover the Active Directory integration to CyberCNS. This will be our part one, we're going to cover on premise Active Directory today. We'll also have a part two, which will cover Azure Active Directory. So, we're going to go ahead and get logged in here.

Once we get logged into CyberCNS, we will be at the customer level. We want to make sure we're on the company we want to work with. And once we've got the customer that we want to do the ad scanning on, we're going to go to the probes and agents area for that company. Now we want to make sure that we've got a probe for this, so we'll have to have a probe installed generally when I do an ad scan, your probe is going to be installed onto the domain controller directly. So, you have a backup domain controller that's also a good alternative. So, either the PDC or the PDC. We're going to install the fro and once that agent comes online on this pro, we're going to go to the discovery setting so I'll tap actions and I'll tap discovery settings. And then I'm going to go to Active Directory credentials. So, these are where we're going to store the on premise version of Active Directory credentials. Okay?

And here, you can see if you've got credentials already stored, they will show up in this list on this panel. So, I can see here I've got a set called ad from January 12. I can see when they were created, and then if I wanted to edit those or remove those, I can hit the actions and tap an option there to do so. Alternatively, if I want to add a new set of credentials, I'll go ahead and tap Add. This will allow me to add an additional set of credentials for the Active Directory scan to use Okay, and once you've got your credentials in, you're ready to Active Directory scan.

Once the scan is kicked off, adding on the size of the environment, resources and with that scan can take you know, half an hour up to a few hours. And once that scan is completed the scan results will flow down into our Active Directory area under the Scan Results section. So, once you've got that data set in here, we'll get a panel shot of your users, the computers, the groups and GPO. And then below, we're going to have the same data panels with some additional information about each of those areas, in addition to the overuse from AMD.

So, you can see here I've got my O us and then below that I'll have my users computers groups and GPIOs and then on these panels within the CyberCNS interface, if you got the ability to do searching, so if you wanted to search through any of the data fields or columns here, you can search this and reload the data. So, if you wanted to reload the table because of additional scanning or additional agents checking in or being depreciated, filtering, so if you wanted to do any column filtering here, you can choose and do filtering on the column headers. And then you've got to download so if you wanted to download any of this data out, you can tap the download arrow and either go filter or full data. And once you download that, it'll just take it out to wherever your default downloads is. Here's my Excel file. And this would contain all of the user data and all of those columns that are in CyberCNS over now for Excel.

And that's across all the pins. You can also drill down into some of the values where we've got blue hyperlink. So, when we're looking at some of these tiles, for example, I've got my computer's you I'm sorry, my users. You can see about 82 here. I want to see those 23 disabled or not logged in you just tap on those numbers. And you can see now I've got my 23 Those are my false and that's that filtered list for me. Again, if I want to see additional highlights, you know, like me, I like to see a little bit more than five. So, here's my 10 and then of course you got the ability to sort ascending or descending on any of the column headers along the top, simply tap on them and that will give you a sorting option. And you can remove your filter, you just tap your x that will return you back to your full data. Even if you wanted to filter disabled tap that one. There's my disabled user looks like it's wind on me that's okay cool.

So, you can drill down so those are your scan results on the active data directory that we're discovering. Next, we've got the Standard Reports section understand where the Active Directory data is going to be fed to our standard reports. So, we have a number of reports in here starting with our login attempts. And then underneath we've got you know, several Active Directory reports that pull some of that data right out. And you can download them into various formats. So, we've got you know, PDF, PowerPoints, Word or Excel, you can see the different options based on those reports. And to download these you just tap on the ones you want. So, once you tap on one of these icons that will initiate the download of the report. So, I'll just have those two and you can kind of see they're letting us know that those reports have started.

And when they're done, if they're available right away, they'll hit your download folder right away. Otherwise larger reports will get fed right into here under our standard report jobs. So, you can see here once you've selected reports off, you could multi select the ones you want download using your global actions and either terminate those jobs or you can go ahead and download these. I'm going to go ahead and download this one right here our Active Directory computers just to give you guys a quick view this so this would be our Active Directory computers report in Word. These can be customized so if you're interested in doing your report customization and we will have another video on that on the YouTube channel to talk about customization of these reports. The white label them or you know change logos and whatnot. But this is our EDI computers. Again, we've got a table of content here. This is a 24 page report and there's a breakout of what we're going to display. So, all of your you know KPI high level Active Directory data points that you might expect to see on an Active Directory Users or computers report. Risk assessment based on you know, some of the computer settings. Some of the enabled computers with the data that belongs to them, groups, policies that they're connected to spidering versus non expiring computers without passwords required. And again, report data. You can add some additional panels here if you wanted to include more data here. So, again, if you're interested in report customization, we'll do another one but I wouldn't encourage you guys to check out the ones we've already got built out on our standard reports.

Got some really useful ones here. Again, scan results, standard reports and you'll have your ad stuff there. That's for your on premise Active Directory. Lastly, I'm going to take us to the company overview where we've got the open source dashboards so if any of you are using the dashboard, or the DQ ls to do reporting, or dashboard views, we've also got some Active Directory data here. So, I'm on again, I'm at the company level. I'm up at the overview. And then from here, we can change our drop down these are all the different dashboards we've got. So, we'll scroll up. You can see here some of the Azure AD ones and then up above those. We've got the actual Active Directory one so this has been on premise version. So, we'll use Active Directory computers report. Now this is currently looking at the last 30 days so we're

not getting any data here. We're going to go ahead and just swap this out this filter. So, you can see here we've got some actions to quick select the number of days, months, weeks years. I'm just going to click and say last one year just so we can get some data in here. Again, here is our Active Directory computers report dashboard. Again, so now we're looking at enabled computer ratio, some of our risk assessment based on passwords logged in and then your Active Directory detail table. And we've gotten like I mentioned we've got several other reports up here. So, in the dashboard overview, you can swipe through these reports, check them out. Remember, you got date ranges. So, if you're not seeing some of your data, you have to keep in mind what when or what your date ranges are. And for those of you interested in dashboard customization, as I mentioned, we will again have some additional video content out there for report and dashboard customizations.

So, once you've got your Active Directory, probe, an agent, got your discovery settings, you add the credentials, you take the scan off, and all the data starts to flow in right into our Active Directory scan results, along with our standard reports are now available to us. The dashboards are available to us. And then we've also got notification rules and alerts that can be used on the integrations that you're using. So, if those of you that are taken advantage of some of the integrations for your with your ticketing systems, we're able to take some of these actionable alerts out of Active Directory and drive them into ticketing. So, if you're interested in looking at that we've got a video out there on notification rules and it hones in on how you can tap in to Active Directory learning so take advantage of the ticketing site.

So, as I mentioned, this is our on premise Active Directory setup. I will be doing another short video on Azure Active Directory setup. So, if you want to, you're using Azure and you want to see that one. I'll take you through that. Very similar to what we've done here. As always out on the support site. We do have documentation, our step by step guides on how to set these things up. So, if you're, you know, you'd rather see the docs jump out to connect secure.com upon the resources on the support our documentation, we've got the Active Directory, both of them with step by step guides. If you'd like to see any of their information on this, let us know comment the video, comment the channel or drop us an email education@connectsecure.com Thanks again for watching.