Global Scheduler Video Transcript

Welcome. In this video, we're going to cover the scheduler overview within CyberCNS.

So the scheduler is going to be found under the Global Settings, under Settings and then scheduler. So, what the scheduler is, in a nutshell, is it allows you to do custom defined schedules for three major functions within CyberCNS. And so first being our standard scheduler, where you can automatically define when you want scans to be kicked off. And we've got a list here of the scans that are supported. So, all of the major scan types in the skin can be initiated using that scan scheduler.

Second, we've got a report scheduler, which is how you define when and how reports are delivered outside raciness. So, we've got you know, we've got standard reports out there. You could also use your custom reports if you've built any and then you can schedule when those get delivered. And then thirdly, we've got our auto patch, which is the third party patching engine included in CyberCNS, where we can define when we want to patch and what application we want to patch. Okay, so that's our auto patch scheduler. We're gonna go ahead and dive in here to the system and look at this together in an instance. So, once we get logged into CyberCNS, we will be at the customer level we'll want to make sure we're navigating back up to that mobile view.

And on the left hand side, we will find our scheduler.

If we tap on scheduler, here's going to be the three major scheduling functions that I showed you in that slide. So, we've got the scan the report scheduler and the auto patch. We'll just start with the scan scheduler. So, as you can see here, if you've got any scheduled scans already in the system, they're going to be displayed in the window. You'll get some heads up info about what those are, what they're scanning, how often they're scanning, so on and so forth.

And then we'll also get some actions for existing scheduled scans to either go in and edit them, or if we no longer need them, delete them.

We'll go ahead and add a new one just to take us through some of the options so to add a new scheduler, just tap the Add button we give this a name. So, we'll call this our daily bull scan.

And then in the Scan Type, we have to tell the system what type of scan we're initiating.

Okay, so we've got, again, all the different scans available. Within CyberCNS. As our documentation page does have details about each of these scans, if you're interested in want to see that document, we do have a document patient page out there for the scheduler that will talk about these scans in detail. If you're interested in I'm going to go over them just kind of very quickly the cliffnotes version of them. So, asset discovery, this will scan and do asset discovery, Discovery settings of a probe. So, if you've got probes installed on the Discovery settings of your probe, where you define the IP ranges to scan, you

provide credentials, you provide SNMP information. That's what the asset discovery will do is run the scans based on parameters on your probe and discovery settings.

Both scan will kick off a full scan, it'll do a vulnerability scan, it'll do an SNMP scan it'll do the firewall scan vulnerability basically does the whole the whole thing there. So, full scan is everything in one Active Directory scan will use your LDAP and SMB scanning, and it will use the Active Directory credentials provided on the Discovery settings of a probe and that will scan specifically the EDI environment.

Your lightweight agent scan is for any of the lightweight agents installed and those will kick off vulnerability scans and inventory scanning. So, any agent that's installed with a with a lightweight that will kick off vulnerability scans baseline application updating and inventory. So, installed applications installed extensions, ports running services running so on and so forth.

We've got our PII scanning or personal identifiable information. So, if you're using PII scanning, this will initiate the PII scans, got an SNMP scan. We've got an external scan for you know scanning external IPs static or IP range or domain.

We got an auto patch. Again, this is to kick off the auto patching and then lastly a firewall scan if you're using any of the firewall integrations. So, those are the different scan types. So, again, tell it which one we want to run. I'm gonna go ahead and just do a full scan for this example. So, we'll call this our daily full scan. Then we can select what companies the scan runs against. So, you can either say I want this to go against everybody or you can pick off from the list the companies that you want to include in that scan, and they will fill up. You can either choose all or you can go in multi select use and

then you're going to define the schedule. So, in this scenario, we've got some ranges pre-selected here for you. So, if we want to say every day, tell it what time if we really can tell it, how long you know what that interval, we've got, you know, choices from one to 23 hours. He's got the weekly so you can choose days in the week, and the times and days in the month, and then you can choose what days, what calendar day, months that you want to run it on.

And then yearly, again, defining the months, the days and the time. So, scheduler has complete flexibility to cover almost every in any scenario that you need to schedule scans on. So, for our daily scan, I'm just gonna say let's do this every day. And we'll just use nine o'clock and you say that, once you add a scan schedule in, it'll refresh the screen. They'll populate your list here, and you'll be working on your scans. So, again, I'll just update this on.

I'm sorry, if you look at the updated column we can find the newest one we just added which was right here our daily full scan. And I can see it's a full scan every day, nine o'clock. runtime.

If you had any filters applied, you obviously would see them in the screen.

And as I mentioned, once a scan is created if you wanted to edit it or remove it, you can just use the actions and tap that choice. And that'll go ahead and kick it off.

You also notice we've got checkboxes on the left so if i multi selecting some of these, you got some global actions here where you can delete and clean up the screen and mass if you need to. Otherwise, the scans will kick off on their on their schedules as defined. Okay, so that's our skin scan scheduler.

Second will be our report scheduler. This will work very similar to standard scheduler except it's for the reports at a CyberCNS. So, again, any reports that are already scheduled. You'll see them in the window. We've got the heads up display on what parameters are set within that scheduler, and then we've got our actions to edit, delete, and then again, we've got our global actions if we wanted to match them.

Same in our same interface layout. We'll go ahead and do add make it through this one.

So, this give it a name. And again, just as a tip, I always find it better to give it a name after we define the schedule. Sometimes you don't really know what the name should be until you define a schedule. So, I'll work backwards on that. So, I'm going to skip the name and we're just going to kind of work through the rest of the fields and then we'll give it a name when we're done. So, the first thing is what companies do we want this to run it so if I wanted to report delivered to me, for a particular customer, or maybe for all my customers, I can indicate that here. I'll just go ahead and choose our three test companies.

We can exclude companies so again if I was choosing maybe the all companies option, and then I wanted to exclude a couple or some a test company, for example, or our own internal company, maybe we don't want to get a report for us. We can exclude companies using these.

Then we've got the reports that we want to select.

These are all the reports built into the CyberCNS system, whether they're in the standard reports, the report builder reports to be executed. These are here and you can go ahead and search for reports to us in the search bar. So, maybe you want to find things board computers. So, we've got Active Directory computers and Azure computers. Maybe I'm looking for user accounts, and then looking for vulnerabilities.

I'm looking for network stuff, right? So, you can kind of type what you're looking for if you know what you're targeting. If you don't know you can easily just scroll through and pick off the ones that you like. So, if you can just scroll through this and you say hey, I want to go ahead and move agents report on include asset report. And I'd like to do a browser extension report as well just those three. The type is how we want the output of that report sent to us. So, we've got PowerPoint, Excel, Word doc PDF, you can choose one or any combination of those. So, if you wanted to get this into PowerPoint and an Excel file, you could choose all three or you can choose any combination and your password this is optional. If you want to put a password in here. This is if you want to send the report encrypted when it gets delivered.

It's important to also note that these will be delivered via your email integration that you have set up in CyberCNS. You'll have to have an integration configure for email and the email that you configure is how this will be delivered. And again, that password if you enter a password here that will be used to encrypt that report. And the end user must have that password to access that. If you don't need to encrypt it, then you do and leave the password field blank and send it off.

Then we've got the scheduler, again same options as our scan scheduler where we can define daily, hourly, weekly, monthly yearly. And then when you choose an option, you will get the additional breakouts here so on a report maybe I just want to get this you know on a Monday morning, let's say at 8am Monday mornings I want these reports. So, now that I kind of know what these reports are, when I'm getting them and also what reports I'm receiving I might then give it a descriptive name. So, this is my bi weekly agent slash assets slash report. Right? And that might be what I call this.

And again, you can call it whatever you want. And then who gets the report here. So, we can start typing a name so maybe Ryan at connect secure.com And we add and if you want to add additional names you just start typing so it could be you know, name at Domain Dot Coms. And you can add as many recipients of that report that you want.

You need to remove them you tap the trash that'll remove them.

And then lastly, if you want to do filters on the particular reports, we do have an ability to do some filtering down here. So, we do have, you know pre canned filters that you can apply to your reports. If you guys are interested in seeing more about the report filters. I do have a reporting video that we've done out on the channel where we go into Report Builder, we go into report customization and we talked real heavily about filtering options. So, if you want to see some of that you do got some content out there to take you through additional once you're done with your parameters, give it a save and again once that save is completed, it will show up in our window. So, here's that weekly agent asset report we just made. I can see again, when it's on schedule, what time it's arriving when it was created and when it was last updated.

So, that's how you schedule the reporting. Very simple.

Lastly, we've got the auto patch.

So, this is where we can define a schedule. And what third party applications we want to be patched by CyberCNS you must have your patching enabled. So, again, use this feature we'll want to make sure under Global Settings under our patching that we've got patching enabled, basically it's a toggle to turn it on and agree to the EULA or the End User License. Once that's on, patching is enabled. And here's where we can start to define this schedule. So, again, we give it a name actually here, let me know, if you had schedules defined in the previous screens, as you saw, they would be populating here and we would see them and have some editing options, just like the previous two screens. Since we don't have anything we've got no data. We're gonna go ahead and add one today. So, we'll define a patch schedule. So, we're gonna call this about we'll call this daily patching.

And I'm just going to use Adobe as our example today.

Again, tip sometimes naming your patching is better after you build it because sometimes you don't really know what you're going to do. So, just keep that in mind. If you guys want to change the name after the fact. You can always choose our companies where we auto match. Are we doing everybody? Or are we doing certain customers? So, I can define customers or I can use the all companies option.

Remove them back the ex.

Boom, there's my three is enough. And you've got included applications. And we've got excluded applications. So, if you want to include for patching, you can use all apps. This will do all applications within the CyberCNS system that we support patching for. If you want to call out specific apps, like maybe I want to look for Adobe stuff, so if I do Adobe, I can see all right, we do reader, Creative Cloud, Shockwave, IR and Acrobat and I can include all my Adobe titles there.

If you want to do your thing, so men, maybe this isn't Adobe one, maybe I just wanted to exclude the shockwave player out of here. I would make sure that I exclude it and obviously we would want to have it.

So, this is if I wanted to do some inclusion and exclusion on the Adobe daily patching. And then of course our schedule.

Again, just like the scanning report scheduler, we've got the flexibility to cover any and all scenarios to patch. So, every day, we tell it what start and end time our patch window is weekly, what days of the week and again, what is our patch window? Days in a month, we select the days and we pick the patch window time. So, each of these will include the date, the times, and the patch windows.

So, every day and we'll run our patch window for example, let's just say 6am. To me there's no reason I'm picking those values other than I just randomly decided that's what I used. You guys have complete control flexibility or this I would align this up against your current maintenance schedules, or patch windows that are already established. Many of our partners are already doing the MSP services with their clients. You've probably got a tool out there an RMM tool that can do patch management and you've already got patching policies in place. This is just you know, again, a second way to come behind and really make sure it's being done. So, I would try to align the schedules maybe to what works best with your clients and or with your current patch cycles. So, just keep that in mind as a tip so once I've got this schedule defined, I can go ahead and save that.

Once it saves will get a preview in this window of what we're patching here. So, I can see daily patching or Adobe every day six to 10 when it was created and updated.

As I mentioned, once we've got one in here, if we wanted to remove this or click edit and go back into it, this is how we jump back in and make edits to it. So, maybe someone said you know what, let's go ahead and do this for all our customers. We're going to swap that to all companies and to do that and save easy as that to make updates.

So, that's our patch scheduler.

Real real simple to use really easy to navigate. If any of the partners are needing help with your patch schedules or having problems with it, you can always get in touch with us contact our support team, support@cybercns.com, put a ticket in we'll get you some help.

If there's other, you know, information or content around the schedulers that you'd like to see maybe some more examples of packing schedules.

Again, we'd be happy to put those out just let us know. You can you can either comment these videos, we'll be watching those, or you can email us directly. We've got the education@connectsecure.com inbox up. We're watching it, we're monitoring it, so let us know thanks again for your guys' time. Thanks for watching.