Application Baseline Overview Video Transcript

Welcome. In this video we're going to review application baseline within the CyberCNS portal. Go ahead and get logged in here.

Alright, so application baseline is going to fall into the settings menu on the left. And right now we are at the company level. So, if you look up on the toolbar, always remember you got company versus global options. This is available under both. So, if you're at the company level, wherever you're under this would be the rules for the assets that belong to that company. If you do it at the Global level that would apply those same rules to all companies instead of just your own.

So, again, if I'm at the Global, and then I come down to settings, and I go app, these are going to be the rules applied at all customers. So, depending on how you want to create a rule, it can be global or it can be customer-focused. I'm going to go ahead and come back down to a client. And I'm going to use an application baseline client.

So, application baseline, in a nutshell, is the ability to flag a service or application as either denied or mandatory. So, if we detect a piece of software or a service on an asset, that is in the deny or mandatory lists, we'll go ahead and create an action item under the remediation plan to either install or remove certain software.

Right, so I'll go ahead and create a sample here today for us. We're going to create rules for an I have Snagit. Snagit is a piece of software that we're going to use, I'm using that just for no particular reason other than I know it's installed on one of the assets and I'm going to use that as our example.

So, the rule name can be whatever you want. I would recommend being descriptive here, but very clear if someone's looking at in the system, your OS type. So, you can choose either Windows, Linux, or Mac running on what you want to target. The OS name, I'll just leave windows and that will cover basically all flavors of Windows OS. If you want to target a specific OS like Windows Server, you can put in Windows Server 2012 or two or any version that you're trying to target.

And then below we've got the type. The type is either service or app. And depending on what you're on, you'll see that these boxes will change. Alright, now we've got services. If I toggle to apps, these will update the apps. So, again, you can target an app or a service. I'm gonna go ahead and do an app. And in the denied applications box, we're just going to start typing what we want to deny. So, I'll just start typing the word Snagit. And I'll go ahead and choose 2023. So, you can either do it as an exact match or as a regex match. So, if you were to add this to the list, it would go in and do that.

Similarly, you can go regex and you can do either or, or both, I guess if you want it to cover all scenarios. And I'll go ahead and give this a save. If you wanted to add any other additional mandatories you could or tags to include or ignore you could add those. I'm going to just make this a very basic one today. Well, there's a deny Snagit role. Similarly, if I wanted to do a mandatory application and signal Hey, every

endpoint or asset needs to have this application running on it at a customer level, you know this is a great way to check so for example, if you're supposed to be protecting your client's assets with your AV software like a Webroot or Sentinel one. You know you could set up an application or service level rule here that says check all the assets and if we find one that doesn't have Webroot installed, showing the remediation plan. And that's, that will help you guys identify or software missing so you can add as many rules here as you'd like.

Once the rules are added, I'm going to jump up to the probes and agents section for this customer and I'm going to run the offline vulnerability scan and that will check any of the application base rules and start to populate our scan results under the remediation plan. So, after the application baseline has been configured, after the scans are ran, those results are reported directly to the remediation plan

Okay, so, again, company level, global level, we can look at remediation plan so I'll stick with the customer that I'm on just jump over here to remediation plan. And I can see here I've got one item showing up on the remediation plan telling us that we need to remove an application and it tells us the asset that this is attached to. I can see here the rst legend asset as Snagit installed. And then I can see where the uninstall path was at and any version that it's on. And then if there were any vulnerabilities associated if this was like a legacy version, we would go ahead and identify those as well. But this is the evidence and then generally from here, you would go ahead and get this integration action, either as a short or long description depending on how much data you want to push. And then I would end up pushing this over to like connect wise an Auto Task to say or even an email to an email distribution list or an external ticketing system on Microsoft Teams channel. There's a bunch of different ways that we could go ahead and signal hey, let's push this over. And if I push that through that ticket ID that it creates will populate and the engineers will have what they need to go ahead and get that application removed, close the ticket out and then at the next scan, the system will check this asset, realized it under the inventory. It's gone. And we'll go ahead and clear the remediation item.

So, again, if I'm down on that asset so I'm back at the customer level, I'm looking at that asset, the RS diligent. So, this is that machine. I go down here. I can see under the remediation plan. There's that same view that I was looking at back here at the company level, this is just at the asset level. Right and I can see there's Snagit telling me to remove it. And then in under the inventory overview I've got the installed program list here. So, I've got 35 and I could go ahead and just search just to validate that we do see Snagit installed.

So, again, that's the remediation plan, pulling in actionable items based on the application baseline rules that we're defining. Well again, company level rules. We've got global level rules. And if you're at the global level and go to the remediation plan, this is where you'll get to see all of the different remediation items across all your customers and all your assets. So, here's a couple of examples where we're seeing some remove signals. And we're seeing some installed signals. So, we've got a rule that says we need to make sure that the CyberCNS lightweight agent is installed on every asset. And if we find one where it's not, we'll go ahead and tell you hey, that company, you know this company and this asset does not have the install. And so again, from these remediation plans

So, I can go ahead onto these through to a ticketing system to get our team to go ahead and get those applications or services either installed or removed. From the assets.

Okay, so application baselining is all about defining what you want on the machines as far as services and apps and what you want removed. Those items then feed to the remediation plans, where we're able to take action either creating tickets or updating through auto-patching schedules to take care of those remediations.

So, that is application baselining. We do have some really nice documentation out on our website as well. So, I want to remind my partners if you're looking for info about any in the area of CyberCNS, you jump out to the our website connect secure.com up under Resources and under support. And then just tap view documentation. And we've got everything over here on the left menu laid out really nicely. And we've we cover everything in really good detail. So, if you wanted to learn about application baselining and you want to look at the doc instead of the video. This is another really great place where you can come in and kind of go over what I just covered. This has got a really good step by step guide and talks you through all the field mapping and options. So, if you want to learn more, the documentation is a really good resource to find some additional content for this.

As always, you guys can comment the videos we'll be really checking those out. You have any feedback suggestions, recommendations, we'd love to hear them. You can always also email us to education@connectsecure.com. Thank you again for watching.