Agent Deployment | Part 1 | Powershell Video Transcript

Welcome to the agent deployment part one.

In this video, we're going to cover agent deployment using PowerShell. So, in CyberCNS we've got three main agent types. So, those are probes lightweight and scans and probes are network based agents at can scan the network and give you information about assets and devices that is discovered on the network. In addition to the local assessment and local vulnerability scanning little do generally that would go on a server in the environment.

Your lightweight agent is probably the most commonly used agent generally installed over in our mental or manually for PowerShell or command line and this agent communicates the vulnerability assessment back to the CyberCNS portal. And lastly is our scan agent which is a one time scan for an asset where you don't want to leave an agent behind you just want to scan it you want to report those vulnerabilities back to the portal and but not leave the agent for regular scanning this is a good use case for scanning.

And all this agent types are supported by either the Windows operating system, Mac OS, Linux and HRM or Raspberry Pi devices.

So, let's go ahead and get into our CyberCNS. And we will do an agent deployment here. So, once you log in, you're at your company view and we'll make sure that we're under the right customer. So, I'm going to use XYZ test company which we've brought over from our ConnectWise manage environment.

So, we're using a clockwise integration to sync the company in and we're going to go ahead and click on probes and agents. This is where we would see a list of all the agents and probes that are out there for this customer. We've got none. We're going to go ahead and tap probe an agent to start the first one this is where we'll select the operating system. We'll leave it at Windows enter agent I need to go ahead and go with the lightweight today.

Once you choose the agent type, you'll be presented with the PowerShell command that you need to execute in order to run the agent installation. So, if you're using a RMM solution, this is also the same command lead that you could potentially use a portion of this to install agents now. I want to say that with err to the side of caution because some of these PowerShell commands are only good for a certain period of time and then they expire. So, you wouldn't want to reuse one that's going to expire on you and end up not working. So, we'll go over our min solutions in part two of our video. Series. So, for this one, we've got a nice copy feature here to copy the command to your clipboard so it's not ready to be pasted into PowerShell. So, I'm going to go ahead and launch PowerShell here and want to make sure you're running this as an administrator and then I'm just going to paste that into PowerShell with a right click.

And you're seeing now it's going to go with download the agent. And once it's done downloading and it's ready for installation, it's going to need a user return. So, we're at the screen we need to hit Enter on the

keyboard to start the installation. And we'll get some information about how the agents being installed to what customer ID what company and what agent type. And then it'll let us know about the service and if it's being created and once it started. And as you can see the PowerShell done and the agents installed.

So it's that simple PowerShell scripts pretty simple, right? It's installed. I can optionally, if I want, download the agent, right as an executable. If I needed to run that on any other machines for the short time being otherwise that agent is installed. If I go ahead and refresh here, you'll see that we've now got our first agent online. That's RST legend and we can see what agent type it is what IP what windows when it was installed. Once it runs its first scan the last time it scan will populate here. And then the last time it communicated or pink with the cyberspace form. Also got some additional options here that we can adjust for discovery settings when you're doing the pro uninstalling removing the probe or agent as well from that screen.

Another thing that I like to do when installing agents is I like to go to the View columns and be sure that I've got everything included. Or if you know I want to remove things like this Id probably don't need it. We can go ahead and remove it and you can also reorder things. So, if you want to reorder the way that things are sitting on the screen, you can grab these and drag and move them on to new positions. So, this will show you where your probes and agents are at. And the next step would be this asset coming online which once it checks in and does it scan, it will come up as an asset. So, in order to start that scan, we're basically going to select that agent.

Use that global action and we're going to say lightweight scan. Yes. So, that is initiating the lightweight scan. And once it's completed at last scan time timestamp will show up on that call. And then under our active assets that RST legend should show up there with the results of our scanning.

So that's the installation over PowerShell again, when you're in the customer, you tap probe an agent, you select your OS, you select your agent type and that is your PowerShell install must run it over administrator.

And that's it nice and simple. So, anyone has any issues installing. Let us know we'll be happy to help you out. Our support team can help you. And if there's any recommendations on future content you'd like to see us in demo, we'd be happy to add some additional videos to the library here for the education series. So, thank you guys again and look forward to part two.