CONNECTSECURE

Active Assets Overview Video Transcript

Welcome. In this video we're going to cover active assets within the CyberCNS.

So, assets in the CyberCNS portal are defined as the workstations the servers, the switches, the printers, the routers, the firewalls that we discovered, either through our probing, or from vocalise agent installations.

The assets are broken up into three major tiers of information. Now, we do have some other information that we're going to cover, but there's three main sections that I'm going to highlight here before we dive in. So, first is going to be the dashboard we'll call it with the four tiles that display some recap. Data about vulnerabilities, the applications and software running on the asset, the port's that are communicating on that asset and a compliance check or benchmarking against different compliance standards on that asset Secondly, we'll find the asset security and compliance overview.

These icons that you're seeing here are the screenshot from the asset section and under that you will expect to find these key areas for that asset.

And then thirdly, we've got the inventory overview for that asset, which is a lot of the information that you may have already collected for that asset from an RMM tool. We're going to go ahead and show you what that also looks like. So, these are kind of the three main sections of the asset along with some other information that we're going to cover.

So, let's get logged into our CyberCNS. And we will go to, I apologize I didn't already have that logged in, my up token here. Okay, so once we get logged in, you should be at the company level. So, we'll make sure we're setting on the company. And in the drop down here you'll see the company that you're looking at. So, we're going to work with blue web company today. And then on the left, active assets.

Okay, so we've got 74 for blue eyed company, this would be a good sample size. And then just to give myself some more real estate, I'm gonna go ahead and tap up in the top left corner here on the three lines, and that will collapse that first window and bring it back you just happened again. So, this whole section here and we're just gonna kind of hide it because I don't need to see it. And so now we're in the active assets view.

So, in this screen, you can see on the left panel, we've got our assets and this is a scrolling list of all the different assets we've discovered through either probing or from agent installs. And so, by default, this list will be sorted. And there's a sorting here if you hit sort, you can see that it's sorted by last vulnerability scan. You can change the way that this is sorting. We've got some different options there. You can also search this list so if you wanted to say show me things with the word desktop in it, for example. I can see hey, here's all my desktops.

So, now that we can see our assets here is kind of take a look at the information we've got so on this toolbar, on the top are some actions that will follow across all the assets. So, again, we talked about sort refreshes to refresh the list here. If you were to do any searching here or you wanted to clear your filters out. You couldn't do some refreshing up there. You can add an asset. So, if you would use the air if you wanted to manually bring an asset into CyberCNS, you just tap there and you can manually build an asset. You can initiate a scan on an asset so if I wanted to initiate a scan on any one of these, I tap the asset and go scan now. And we can kick off one of the full scans, instant scan vulnerabilities and so on and integration actions. So, if you have integrations set up, or your CyberCNS portal, this is where you can interact with those from this asset. So, any of the integrations you've got tied in you'll be able to use those and show listen just a bit more in more detail. Snooze and activate this is where we can suppress a vulnerability on the remediation plans. So, this will be used for on remediation plan. So, we'll talk about what this is a little bit.

And then lastly, we've got a table view option here. So, Tapping this will allow you to toggle into what I call the line item, multi line view. So, this is our 74 assets. Now instead of that scrolling list on the left, we're getting them as lines. You can of course if you wanted to say hey, I want to see 20 per page or 10 per page, you have the option to do that. Then of course you can sort on any of the column headers just by tapping and you can sort things and then off to the far right. You've got some additional options again here to kick off scans, get details of the assets or remove an asset.

You also notice we've got pagination options here on the toolbars. You want to make sure as you're navigating the CyberCNS product that you keep your eyes up here because a lot of these options will follow on a lot of the screens. So, again, these are our refresh intervals. So, if you want this multi line to auto refresh itself, one five or 30. We've got filtering options here. So, if you want to filter data on any of the column headers without filtering, you can download this full asset list out. So, if you wanted to just say hey, I want all 74 of these either filtered or just the whole dataset. This will bring it out to an Excel file. Where you'll be able to do some of your own you know reporting or manipulation on this. So, this is all of the asset information here, over it out an Excel file and then this is to save setting so if you were to, for example, reorder columns, so I tap on my view columns and say, I really like the importance to be up at the front position. And then I want to see operating systems, and I don't care when it was first discovered.

Maybe I don't care about the manufacturer. So, maybe I like to look at things this way. I can save the settings here. So, next time I load this view, the system will remember how I like to look at this. So, that's the multi line view. I'm going to tap back out from the table view I'm sorry, and go back to this view. So, our original state, those are options along the top of all the assets.

Next, we've got the header information on the assets. So, we've got a little icon here signaling and this is coming from Microsoft Windows OS. So, we've got the Windows logo displayed, which it does automatically. We've got the name of the machine, or the asset, in this case, our STL legend and the local IP address. If you tap that, you can change that. So, if you wanted to give this a different friendly name and maybe you've got a standard, best practice for naming machines and the environments that you're managing, not managing. This is a way to create a new name or add a prefix or a suffix to this name, again to help with signaling to your team on what machines should be managed.

So, let's you need we've got a report for this asset. So, if you were to tap this icon, this would download our asset report. And if you notice if you just hovered over some of the items here on the screen, will give you a tooltip on what that item is actually displaying. So, asset or hostname, download asset record, you tap that. This will generate a Microsoft Word based report that is very comprehensive and it contains the information about this particular asset so cover page, this can be obviously customized and branded, you know for white labeling for you guys if you wanted to put your company's name information there or your customers information there.

And then, this is just a recap of everything about we've captured on that asset. So, all of the standard information that we're going to go through today on this asset is all here so programs and services and processes and how we scored this thing and how it's checking up against compliance ease. And this is a like I mentioned very comprehensive 447 pages long so I won't be going through this whole report with you guys today. But this asset report is available on any asset you tap to and you can look and download those.

Moving on, is next section is our remove assets. So, if you tap that this is how you remove or delete an asset out of your CyberCNS. Portal, delete it goes away. Production machine this is a flag if you tap that flag, we're signaling that this is a production level Machine and that's really just a signal for technicians or engineers that may be managing to let them know hey, this is a production level Machine. You'll see once you add that flag, we add this little stamp here. And then if you hit refresh, you'll notice over here, that that will also update with that little P. So, if you can imagine if I had a bunch of those stamps in here, it'd be nice to be able to see hey, what's the production machine what's not kind of at a glance without drilling down or knowing the machines and then to undo it use at the flag again so you can toggle it on and off despite given that click.

Next is the credentials. So, the key is where you can add credentials for an asset specifically. So, if you have a set of local creds, you could add them. If you're using probes you generally are going to have credentials stored especially in a Windows environment where you've got maybe a domain and you want to have credentials so that you can scan the network better. That's those will be useful when your probes and we've got your MAC address on the machine or the asset. We've got the last discovered time time and date stamp.

Same with the last time we did a vulnerability scan with the date and timestamp next is the importance on the asset. So, this is us categorizing an asset we feel how important it is to the organization low medium critical or high. And you can change it just by tapping and this will also affect how we score that asset and then we do some of the calculations so keep that and then lastly, we've got tags. Tags can be added to machines. And they can be useful for keyword searches later when we want to do sorting, reporting or filtering. You can see here I've got some sample tags that I've added to this machine. So, VIP production, SLA 24 hours, if I do not remove or connect should actually say remote connect. So, again, remove a tag add a tag. You can just type do not remote connect it might be a time in again you can sky's the limit here. So, any kind of ways you want to tag machines with attributes. So, that again you can report Sort Filter and later these can be shared amongst the other assets within the organization too. So, once you add those tags they will be you can tag your other assets.

And then lastly, if you look off to the right, we've got the risk score for this particular asset. So, we'll score the asset based on a number of variables and calculations that we do and if you want to know what those aren't exactly, you can tap on the score will take you to off to our documentation. And this will explain how we score the assets what those scores actually mean, where we're pulling them from. So, severity against vulnerabilities, the exploit scores, the way the weights are impacting etc. So, this is all documented out here. You guys want to look at that. All you got to do is tap that score, it'll take you out there. This score is also available all the way back here on that list. So, if we're scrolling through here we can see some of the scores have populated for some of our assets. I've got an E I've got a D. And if again, if you tap the score, it takes you to the documentation. So, either way you hit it, you can get that explanation.

Alright, and then next we've got the OS. So, what's installed from the operating system, number of CPUs, how much memory or rams installed, what built in version number or the OS and then the uptime, last time it was rebooted or shut down. And then when did we install our CyberCNS agent on the asset?

Both the next is some dashboard like tiles that we talked about. Early on in the video where we're going to just bring some high level data about vulnerabilities, applications, ports and compliance benchmarking against this asset. So, I can see somehow some of the values are populated here. And you'll notice that this asset happens to be pretty secured from the scoring. It's got an A, we've got no vulnerabilities and 35 apps 11 ports communicating you can see here how we got no vulnerabilities across this app. So, it's in pretty good shape from that lens. And then on the compliance forum. You can see here what we've got compliant versus non compliance through the lens of CIS. And we've got some other compliance standard checks out here that you can choose from. So, if you want to benchmark this machine against any of these compliance standards, you can just tap on it. It will recalculate and then it'll tell you how this machine stacks up.

If you drill down to these numbers, we do have, we do have some compliance information back on the left, where we'll give you some real good information about how to get compliant on these machines. I'm going to cover that in a future video. So, you guys are interested more about compliance checking and benchmarking. I will be covering that in an own focused video. So, more to come there.

So let's move down to the next two sections of the asset so the next section is the asset security and compliance overview. So, everything on this toolbar here so starting out is the security report card, where we're going to do some basic checks against that asset and see those that have a be installed doesn't have local firewall policy or profiles enabled what kind of ports are listening on it? Any vulnerabilities on the network scanning system aging? And is it a supported operating system meaning is it within a year end of its life support? And we'll score that machine based on some of those attributes we call that then we'll do a compliance report card. And again, this is looking at some of the basic security checks. And we will run those values and then tell you what we're finding. So, you know in this example LLMNR enabled, well registered if the registry keys and found we're going to assume that it's enabled. So, if we can't find evidence that it is not enabled, we'll always assume it is so this is how we're scoring that and again, there is some documentation out on our page if you'd like to get a bit more information about this. It's all documented really nicely.

Next is the remediation plan.

So, the remediation plan is where you will find any of the vulnerabilities that we've discovered how we can remediate those now we're seeing in this window on this particular asset is install. And we've got these three applications listed in Mozilla, WebEx, WebEx, MTA. So, what this is actually coming from is what we call application baselines.

So, we've got a rule in the system that says every asset must have these installed applications on them.

So we can signal to the system if an assets missing an application that we deem as mandatory and await whitelisting. If you will, and then we can also go the reverse of that. So, we can also say, Hey, if you see this application, flagged as a vulnerability, and we're going to run a signal to remove the app, so we can go both directions. Again, that's application baselining. And that's why you're seeing these in this list. I will again be doing another future shorter video, specifically around application baselines. So, if you're interested in how that whitelisting and denied and mandatory listing works, you can check out our application baseline video in on the YouTube channel.

Next, we've got our vulnerabilities if this machine had vulnerabilities, we would see them here I'm gonna go ahead and navigate to a different machine that's not my own, but we've probably got some so here we go. This machine this desktops got 36 vulnerabilities. And again, now you can start to see we've got them categorized by severity. And then if I go back down here to the vulnerabilities, now for this asset, you can see we've got data so we've got 36 vulnerabilities like the tile told us and if I want, I can kind of view these again, I like to see everything in one page. I don't like to have page older. So, here's 36 Right in the view, and again, I can see every piece of data, how we've signaled it, what it is, where it's installed, and then over to the right, how we've scored that and how it impacts the grading of this asset.

So, we've got, we got all that data available, you know, it's back down to five. And then if you notice the info section on any one of these vulnerabilities, if you're interested about what they are, you can tap the CVE and there's a hyperlink will take you out and we will link this article to the NIST information. So, you guys can, you know, learn and educate the team staff, colleagues, whoever it is, understand what these are, what the weaknesses is, and then how we can mitigate and resolve them. So, every one of the vulnerabilities in this list has the CVE linked to it. So, we're going to bring it to you and then we're going to tell you how to how to take care of it. So, really nicely done by our team to bring that bring that into view here. So, that's under your vulnerabilities. Now, this machine if I go back to the remediation plan, this one's got some data right my last asset steel legend didn't have any vulnerabilities. So, it didn't have anything to show you here. You'll notice that this one also has those, what I called application baseline mandatories. So, they're in the list because this device does not have those installed and then you can see the vulnerabilities or the other things we've signaled so hey, there's a vulnerability. It's not supported. It's at its end of life. And it's installed. And then you can see here that we've signaled how many critical how many hi how many medium vulnerabilities at this device accounts for.

And then lastly, we've got a signal here for a ticket ID. This systems integrated to our Connect wise managed environment. And so we're taking anything that shows up in our remediation plans and we're driving in them through to our PSA, that way our engineers and take action. We can run workflows we can hold, you know, accountability, that these things are getting done, and also going against their managed service agreements, right. Most of your clients that you're doing cybersecurity for should have some type of managed security services agreement in place with you. And any time and effort spent on this stuff really should be documented as a ticket against those agreements. So, we understand what the true cost of delivering the security services to our clients, right so that this helps drive and mash some of these things together. So, that's the remediation plan. And again, we're going to do another future video around remediation plans options specifically. So, you guys are interested in learning a bit more about this and kind of focusing on that. We will have a remediation plan video out there that you can look at.

Again, we're moving along we got our vulnerabilities. Then we got our network scan binding. So, if you're using a probe and the machine or the asset that you're on has the ability to scan it will go ahead and signal what it's what it sees in network scan binding. So, you can see here some various ports and protocols that are that are running across the environment that you can see TLS is running SSL certs being signed, RDP, etc and some additional similar to network scan, we've got some additional information. Again, this will populate from your probes, again running across the network looking at various protocols, various checks there.

We've got a quick compliance check against some of these applications. You can see and again, I like to see things all out. So, I'll kind of stretch this. So, this is saying hey, is this applicable this machine or this asset against these different packages, and you can see if it's compliant or not. And if you guys are interested in how we're how we're checking in flagging that as a yes or no, we've got the documentation out on the on the site for good to find check and then we've got our Windows 11 compatibility check.

So, any asset you pull up, you tap that this is our Windows compatibility check and we're going to show you hey, here's the minimum required for Windows 11 to run. And then we'll tell you, Hey, here's the value of what the machine you're running has. So, you can see here, it's just giving you Yep, this is all good. And if something was below threshold or not supported, we will get a red check. Similar to how you're seeing secure boot. I don't have secure boot enabled on my machine. So, you're seeing that that red.

And then, last but not least, is our PII scan results. So, if you're using PII scanning this will show you at the asset level, any PII data that's been revealed or found. We'll show it to you here back. I've got I was just working with another partner on this and I'd like you guys to see this, I believe this machine had and this is a newer feature that we just released. So, this is really useful. Yeah. So, here you go. So, this this asset, this desktop, you can see here, we've counted eight scan results that we've identified. And you can see here the category so we found surname five times we found an email twice and we found a credit card info once and if you tap down to these, you will filter the list out for you will show you what asset and it was a file, where that files located. Even the line number in the file, where it's located. So, this thing is really impressive. Shout out to the dev team at ConnectSecure. This is amazing.

Again, emails same thing Hey, we found emails, they're in these files. Here's the lines they exist in, in some surnames. So, any PII scanning compliancy that you have to adhere to. This is a really powerful way to get a quick look, understand what's out there and know that things are being protected. So, that's the PII scanning personal identifiable information.

Well go back to our so that's the asset security and compliance overview. Right, that's the sections of top.

Lastly, we're going to go to the asset inventory overview. As I mentioned at the beginning of the video, a lot of this information for you guys is most likely going to be coming from another tool and that's okay. It's great to have multiple checks going on in tools in case one of them is, you know, not right, something's wrong, you know, and trust but verify. This is a really, really nice way to do that. So, we've got your list of installed programs. So, again, if you'd like to see more, you know, when you say I want to see all these in one shot, there's 193 So I'll go to 100. Here's all the installed programs on the machine. So, we'll give you a list of all the installed apps.

We've got the extensions installed, so any browser extensions that they may be running in their in their browsers. So, picking up two from edge picking up a couple from Chrome, and what they are.

We've got Microsoft patches installed on this asset so reading any of the Microsoft patches.

Now, if you want to get more info on these patches, you know, one of the tips that I've been shown other partners is you can just double tap the highlight, right click and then search.

This will search and you can see the KB articles right on Microsoft. So, if you wanted to get down and actually read about that, A B will get you will take it to the articles direct. So, those are all available again, double tap right click search and then generally the first or second link are the ones that you know that you need to be looking at. And again, this is the article so those are your Microsoft patches and again, you know a patch you're looking for you can always come in and search for it like you know, hey, I know this patch ends and 372 you can always come in and search for patches here, filter them out, services running on the asset so any of the services whether they're start stopped running auto startups are reading those 290 times. And again, if you want to do your page items, you can sort on these, it also download these so if someone says hey, let's do some inspection here, right filter, I'm gonna go full data. Let me just download this file this data because I want to inspect this a bit more is 290 seems like a really heavy amount of services. And so now I got that same data set in here and then I can go through and maybe verify or validate what's here and say, Hey, this, this should or should not be here.

So, this is a again, nice way to export and again, any of this data can be exported off the line. So, just keep that in mind. These downloads are available on almost every single screen. So, anything you see and you're like, hey, let's look into that a bit more.

That was our ports. So, these are ports that are open communicating, what services what protocols are running on those ports. Are they compliant or not?

Against checks, so then we're listening to users local accounts, domain accounts, any users found on the machine, the shares on the machine, so what shares what rights we've got, what accounts they're on their local shares, SMB shares, network shares, etc. interfaces on the asset so you know, LAN, wireless LAN wireless virtual adapters, any interface we find will list here. We got storage.

So, we'll list out the local hard drive space and if that is encrypted or not. So, you can see here that unlock is in signaling to us that this is unknown, and it's not encrypted. So, you see that that's what that signaling. Go ahead. Go back to Legend Machine.

This one, as you can see this one, we got the green lock, that signaling BitLocker encryption with Microsoft. So, this is support for BitLocker only. So, if you're on an asset and you and you see that green lock, that's signaling to you that this machine has BitLocker drive encryption enabled.

This would be external scans. So, if you're running external scans from an asset, you will you will get some data back there. I'm not sure if we got that one.

And then lastly, we've got asset firewall policies. So, looking at the local firewall policies on the asset if they're enabled, not when they last been updated, and again, that's the asset inventory overview. As I mentioned, most, most partners, you guys will probably have some of this data, if not all of it coming in from an RMM tool. Again, this is a great way to validate and reconcile against it and make sure that we're not missing anything.

That's the asset overview.

So, I believe we've covered just about everything on our asset overview.

You know, if there was if there was anything on there, that we missed or that you guys would like us to, you know, cover over in more detail, we are more than happy to create additional content on that. As I mentioned, we've got several other videos on the YouTube channel. We'll be adding to it over time to focus in on some of those features we talked about application baselining some of the integrations, some of the remediation plans, PII scanning. So, we're going to we're going to focus on bringing additional content to you guys, again, to make sure you're getting the most out of a product. So, thanks for watching. If you want to connect with us, comment our videos, hit us on our YouTube channel @ConnectSecureEducation, or drop us an email education@connectsecure.com and we can get in touch again.