Attack Surface Mapper Video Transcript

In this video, we're going to cover the attack surface mapper feature within CyberCNS. And to go ahead and get us logged in here.

Once you log in, you will have on the left-hand panel. Once you're at your company, you will find the attack surface mapper module listen. So, right here under Scan Results window. So, from here, this is our attack surface mapper.

Now, what this does is it's basically an enhanced external scan if you're familiar with our external scanning module. We do have a nice explanation here of what this is actually doing what we're scanning, and we're gonna go ahead and kick one off here today so we can see what this looks like.

So, we'll go ahead and do RJs logo with one of our sample domains, what we'd like to scan to show you guys so once you scan to get your little magnifying glass, it will kick off and the scan depending on the domain size and where it's finding out there this scan can take anywhere from I've seen it running because 30 seconds all the way up to five minutes in some cases.

So, if you're don't have the time to sit here and wait for the little magnifier there to finish, you can always open a new tab and kind of continue on. You don't want to navigate away from the attack surface macro screen. If you do navigate away, the scan will stop. So, just as a tip, if you let this attack surface mapper you can always open a new window and look right and so once the results render on the screen, this is what you'll actually see.

So, here's the scan results for LG the domain that you scanned and then we give you vulnerability counts up in ports. What's the public facing target IP addresses that you know an attack attacker may be targeting? We look for any compromised emails or usernames out in the dark web scan. And we identify subdomains connected to our Jas logger.

Again, if I scroll down and show you guys some of the data you can pick up so again, public facing IP the ASN and location and see where it's being hosted at. We've got DNS record reveals here so any DNS records or tax records added will identify what's going on and DNS, got an email spoof checking and then demark status and record if it's available.

And then of course all subdomains that may be connected to this domain. So, again, this is a quick way to be able to scan client's domain and understand what are the attack surfaces out there. You know, sometimes we talked with our prospects and our partners and their customers and, you know, we asked them, hey, how many domains are you guys managing and, you know, the customer thinks that they only have one or two.

And, on this example, there's, you know, there's 10. In some instances, I've seen 20, and 30, and 40 subdomains depending on how many pages you've got, what kind of marketing you're doing and so on and so forth. So, this is a great tool that kind of do some extra exploring outside of just doing the normal external scan where we just scan once domain.

This will do some domain enumeration, do some crawling and give you guys some additional information that you can use when you know producing discovery audits, recording and really identifying your customers. Where are the gaps in security and where are they multiple. This is the attack surface mapper.

We've also got documentation out on our Confluence site for this so if you're in our Doc's and connectsecure.com/docs you can go look at the attack surface mapper Docs as well. Looking for any you know suggestions features enhancements on this, we're always listening so let us know what we can do to enhance this. You guys can email us anytime at education@connectsecure.com. You can also comment on the video. Let us know your thoughts and what features you'd like to see here. Thanks again for watching.