SECURITY OPERATIONS

The harsh truth about the next cyberattack

02.17.21 - James Dougherty

I don't know about you, but it seems like there's news of some big data breach every other month. The hard truth is that no one can really predict the next cybersecurity meltdown. There is no doubt in my mind that it will happen again (and again…). Over the past 15-plus years, the one thing that stuck out as being effective was the idea of always evaluating your security posture.

Start with endpoint assessment

It definitely is a cliché, but the saying "You can't monitor what you can't see" really does have some validity. Now, I know that every one of my readers out there runs a tight ship, but let's not kid ourselves; over the past year, the evolution of our networks has been on warp speed. We have to pay attention to everything.

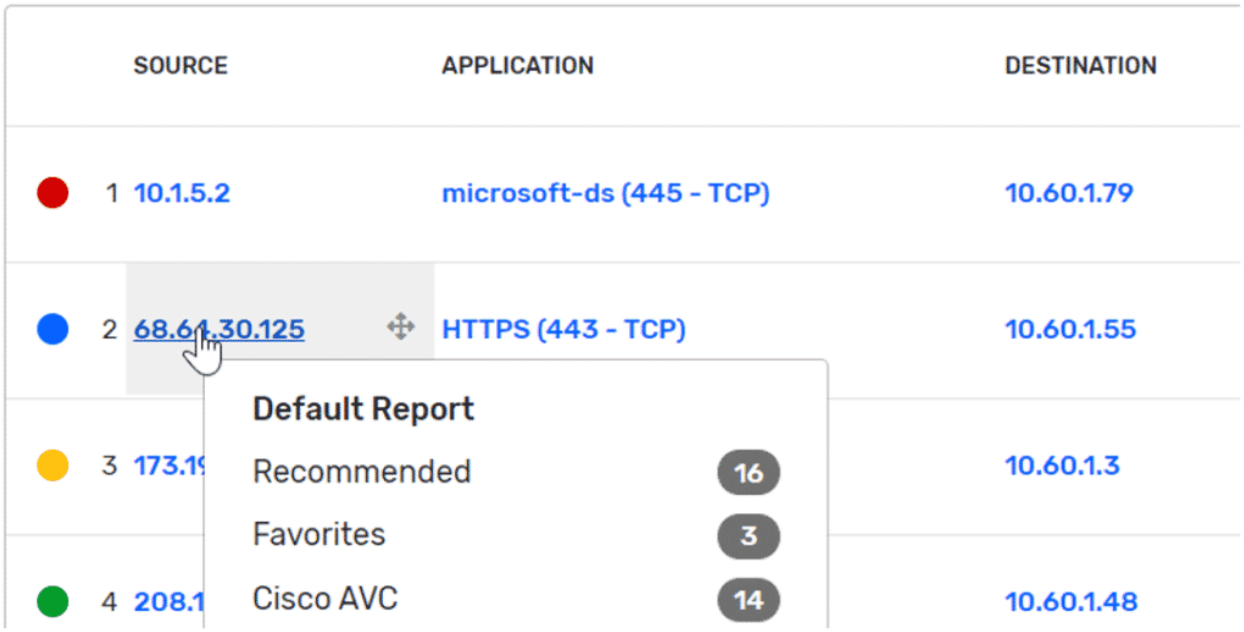
It's extremely difficult to know if your coworker spun up a VM session, if Kelly in accounting connected her phone to the network, or if an aspiring white hat decides to plug in his Pi and play

around during his lunch break. Unidentified devices, whether physical or virtual, are continually connecting and disconnecting from the company's network and not only does this add another dimension to your monitoring landscape, but it also increases your vulnerability.

So what's the solution? Get an endpoint assessment! I know what you are saying: "We already have XYZ and it does an endpoint assessment." That's OK, there are some interesting solutions out there that not only detect and profile all the endpoints on your network but also create a security profile. Trust me, kick some tires and use that as evaluation. What's the worst that can come of it? Either nothing new is found or you have a better idea of where you need to focus. Don't believe me? Try Beacon and see.

Get visibility

So you found something on your network. The next question you need to ask yourself is, what the heck was it doing? Again, I know this isn't you, but let's just say, hypothetically, a person like you was faced with a security breach or an audit. What do you think normal protocol would be for this? What would you do?



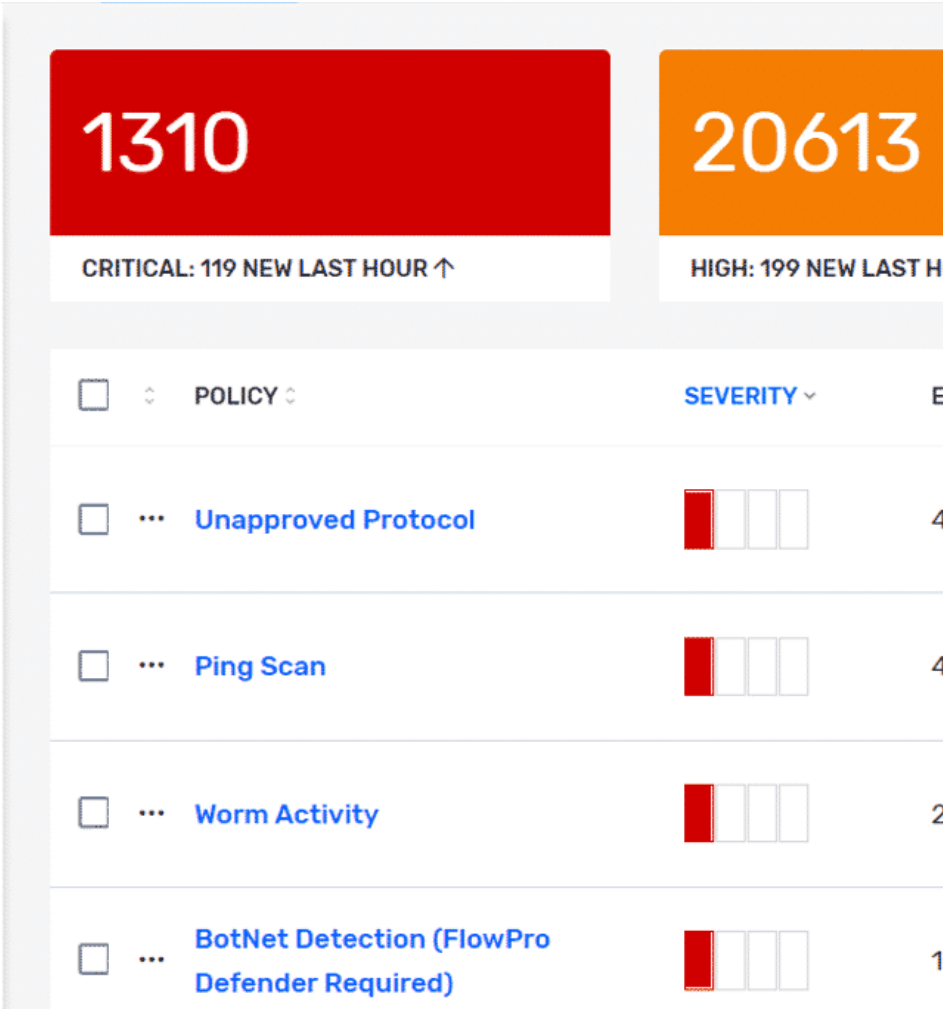
Earlier I talked about how today's networks are exploding in size. Well, along with that growth comes a huge rise in traffic. It seems to me that knowing what that device is doing and has done over time would be valuable.

In most cases, companies are incorporating conversation metadata, like NetFlow/IPFIX. Basically, the metadata is exported by your network devices and in turn, allows a company to reach the depth of visibility that is needed for monitoring and forensics. Due to the scale and size of today's networks, it's not news that metadata has become the de facto standard in monitoring network traffic for security. More importantly, it provides a way to achieve this visibility in a scalable way and that is key.

A great example of how to investigate a breach with metadata is the recent SUNBURST exploit. As my colleague points out, the malware used a domain generator algorithm to establish connections to a C2 server and a variety of IP blocks to facilitate communications. In this situation, the ability to see conversation data from certain IPs helps to eliminate guesswork.

Be proactive!

At this point, you've done an endpoint assessment and a traffic assessment. You've found some things you need to address. What's next?



There are many reasons why you would want to continually monitor endpoints and networks traffic. Sure, lessening the impact of the next mass data breach is top of the list, but failing audits and not meeting compliance can cost your company in the same way. As a matter of fact, data security had the highest average compliance cost per organization. In a 2018 Ponemon Institute study on the true costs of compliance with data protection regulations, they found that the annual cost of non-compliance to businesses was running an average of $14.8 million, a 45% increase since 2011. On the other hand, the cost of compliance was found to be less than $5.5 million.

OK, here is where you will need to review your current set of tools and plan for adoption Introduce the concept of NDR.

> "NDR solutions primarily use non-signature-based techniques (for example, machine learning or other analytical techniques) to detect suspicious traffic on enterprise networks. NDR tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect suspicious traffic patterns, they raise alerts. In addition to monitoring north/south traffic that crosses the enterprise perimeter, NDR solutions can also monitor east/west communications by analyzing traffic from strategically placed network sensors. Response is also an important function of NDR solutions. Automatic responses (for example, sending commands to a firewall so that it drops suspicious traffic) or manual responses (for example, providing threat hunting and incident response tools) are common elements of NDR tools." – Gartner.com

Overall, the concept of NDR is relatively new. As I mentioned in my post about picking the right NDR tool, things like the pilgrimage to fully remote offices have pushed management into looking for software that analyzes the enormous amount of additional traffic.

So how does this all work in real life?

I was talking to a friend the other day who had just installed a new head unit in his Jeep. He wanted to do some updates, so he connected the unit to the companies Wi-Fi. Well, the head unit had Huawei components, which is frowned upon due to the Defense Authorization Act H.R.5515. In this situation you would need to ask yourself a couple of questions:

1. How would you know that this device came on your network? In addition, how would you determine its security profile?
2. How would you determine who the host was, who they were talking to, and what they were saying?
3. How are you going to proactively monitor for this and other questionable activity on your network?

I don’t want to be the guy who’s preaching doom and gloom and promise that product X is your cybersecurity salvation. I think we can all agree that attacks are going to be part of everyday life. What I want you to ask yourself is how will you get all the information you need when the next attack or audit occurs? As I mentioned before, employing enhanced metadata will immediately help you expand your visibility and collect that data in a realistic and scalable way. Don’t believe me? If you’re looking for conversation-rich visibility along with the flexibility to integrate that data into your current environment, why not evaluate Scrutinizer?

James Dougherty

I have worn many hats in my professional life. Support engineer, developer, network admin and manager are all points on my resume, but the one common thread with all of these jobs is that I enjoy working with people; that is what I do here at Plixer. I make sure that everyone understands our product and can get the most out of it. It's just simple 'no bull' support!

Let me know if you have any questions, I would be happy to help.

- Jimmy D

Plixer

68 Main St Ste 4
Kennebunk, ME 04043

Phone: 1 (207) 324-8805