Chad Kliewer: I'll say greetings and welcome to the discussion on cyberattacks. I'm your host, Chad Kliewer, holder of a CISSP and CCSP, and current $(ISC)^2$ member. I'll be facilitating our experience. And I'm extremely excited to welcome our special guest, Joe Sullivan, CISSP, and also an $(ISC)^2$ member. Joe's a former CISO in the banking and finance industry, who now specializes in forensics, incident response and recovery. So, Joe, you ready to get started?

Joe Sullivan: I am looking forward to this. I'm excited.

Kliewer: All right. Anything else you'd like to add about your background? I didn't give you much opportunity to do that.

Sullivan: Just a brief overview. I've been in information security for 2 years now in various aspects as you've mentioned.

Kliewer: Okay, awesome. Thank you much. So, I'm going to dive right into some content here. Because part of what we're trying to do is we're trying to look at how we prevent attacks, and then once those attacks happen, how they really impact the business and how they impact the companies. We all hear about these attacks constantly, but we never really look so much at how they impact each individual business. So, we're going to start out just talking a little bit and say, if we can't detect any future ongoing attack, how are we going to remediate that, and how are we going to stop it? And the one point we want to make here is how important it is to make sure that we're aggregating all that data using this Security Information Event Management system or SIEM, S-I-E-M. And what are your thoughts on using a SIEM to make actional intelligence, Joe?

Sullivan: Integrating a SIEM for actionable intelligence, I think you have to take a step back and think about, when do we trigger incident response, typically? Over the course of my career, incident response is usually triggered after something bad happens. They're on the network, or we see and exploit, or we've been compromised or there's a knock on the door that says, Hey, your data's out there. If we have a SIEM or user behavior analytics, whatever the case may be properly optimized and tuned, we can pick up on those indicators of compromise before the bad things happen. And when I say indicators of compromise, I'm referring to things like scanning, malicious email attachments, web application, enumeration and things like that. Attackers spend the majority of their time in the recon phase. If we can detect those recon activities, that's actionable intelligence where we can block IPs, block tools and things like that before they actually get on the network. Even once they get on a network, recon still takes place. I get on a machine, what's the vendor? What software am I running on this machine? What applications are installed? What's the network look like? And still, we're not to the point where a breach is actually taking place yet. Again, if we're detecting an activity in our SIEM with the appropriate logging, monitoring and alerting, we can trigger incident response well before the actual breach takes place.

Kliewer: So, what are your thoughts on the actionable intelligence and how we prevent threats? Do you think most of the threats or most of the, well, we'll say incidents, are actually detected by internal systems, or do you think they're mostly the result of receiving the indicators of compromise from a third-party organization, such as a government entity or something like that?

Sullivan: If you look at as far as detection, we have events determining what's malicious and what's just an event or a false positive is the challenge here. When you have lean running security teams, who don't have the time to go in and tune and optimize this (but then again, something is better than nothing) a well operationalized security program with the appropriate headcount has the chance of detecting these and getting those alerts and indicators of compromise and acting on those earlier; whereas, if you have a lean running program (a two- to three-headcount security department that are wearing many different hats) it's a little bit more challenging to tune and optimize that. It's in scenarios like that where it might be beneficial to outsource that to a third-party SOC or something, and let them say, “Hey, we've detected this going on in your network, it doesn't look like a false positive, you should go check this out.”

Kliewer: Awesome. So, I'm going to paraphrase a little bit and read between the lines and say that I didn't hear one thing in there about, ‘You need to buy this software product to detect all the incidents.’

Sullivan: You don't really need to buy a software product to detect all the incidents. You know, if you look at like the CIS controls in this CSF, this cybersecurity framework, or even this 853, if you implement those and get your logs where you just have some visibility into them monitoring something, you can detect these. It doesn't really need to have a high-dollar SIEM or something like that. Network segmentation, we'll look at that. Host-based firewalls does a lot of good for limiting the impact of an incident.

Kliewer: Okay, awesome. So now I want to kind of roll that just a little bit more, and we kind of talked about that that's more the processes to log retention, so do you think what we've talked about so far still holds true when it's cloud-based software products or even cloud-based, and I'm going to say cloud-based SIEM, like a lot of them are?

Sullivan: The concept still holds true, right? We still want to aggregate the logs. The challenging cloud is the threat surface is a little bit different. I have all these different authentication portals and command line tools that can be used in public cloud services. And your threat model is things like permissions and IAM—identity and access management—if you don't have the appropriate permissions set up, you don't know what a user can do (like in some cases with a particular public cloud service I won't name) if you have a certain permission where you can actually roll back permissions, but you're limited, you can actually roll back your own policy and do something where you had permission at an earlier date, but you don't now. It's those little gotchas like that that you need to be aware of. And then there is provisioning cloud services,

depending on how you provision certain virtual machines, RDP and SSH is enabled by default facing the internet, so you want to be aware of what's the context of if I provision that here or from the command line tool?

The logging, monitoring, and alerting, you can have a cloud-based SIEM third party, or a lot of public cloud providers have their own tools. It's a little bit different approach, a little bit different aggregating those logs and reading them, setting up the alerts, so there might be a learning curve there. And then there's things like the instance metadata service, which if you get in contact with that, you can actually—it's like getting all the metadata on your VMs, your hosts, your disk drives, your backups and things like that, and gives you a wealth of information. And we're seeing older attacks like server-side request forgery coming back. In the Capital One breach a while back in a public cloud service, we've seen that take place. And there's various controls and mitigations they put in place to mitigate the IMDS attacks, and you need to be aware of what those are and how you can prevent those from happening. So, it's a little bit different, a little bit more comprehensive. It's not the same as your traditional on-prem resources, so there's a learning curve going through there. It's a little bit more challenging at first, but I think overall, it's the same approach, you just have a different way of implementing it.

Kliewer: Awesome. So, thanks for answering that. Since you mentioned the recent Capital One breach that involved the cloud service, can you kind of give our listeners an overview, we'll say about a 15,000-foot view of that breach and what happened?

Sullivan: The Capital One breach was actually an insider threat. They actually had access to this system, had worked with it before, and the instance metadata service—so you hit the web application, which caused a URL on the back end to get data, allocate resources, authentication and things like that. Like say, you have data in an S3 bucket, you can actually hit that IMDS and get that information back. That server-side request forgery attack let that person enumerate those resources and get access to them and download them. So, they had to go back and determine, "Well, how can we prevent this from happening?" And implemented things like now you need a token to send to the IMDS to actually get that information back, or we're going to limit the response from the IMDS into one hop, that way it doesn't go past the machine out to the internet. So, an attacker can't actually get that.

Kliewer: Okay. Awesome. Thanks for covering that for us. I want to shift gears just a little bit, and we're talking about an attack here that involved some cloud components, but not necessarily in the cloud. And I wanted to talk just a little bit, because it was such a widespread incident—I mean, it can be called a cyberattack, we'll call it an incident with SolarWinds—it was one that was very widespread, gained a lot of notoriety because it was one that affected a lot of US government agencies, and I'm guessing probably a lot of other government agencies as well. And this was a very good example of a supply chain attack, where some malicious code or malicious programs were embedded within the supply chain or within an update package. So,

would you like to kind of lead us through a little bit, Joe, and just once again at a real high level of what steps that SolarWinds attack really took? I'm going to preface it by saying the reason it has such a huge impact was because it went undetected for so long. It went undetected, I think for at least, I'm going to say at least six to eight months that we know of, possibly quite longer. But if you could give our listeners an overview of that SolarWinds attack and how they actually utilized the cloud components.

Sullivan: Sure, no problem there. SolarWinds was a really, really clever attack. The initial foothold, we're not sure. They gained access to the internal network. We don't know if it was a spear phishing attack. There had also been rumor that a password was leaked as well. It could have been someone had set up a site for a watering hole attack. However, they did it, once they got access to the network, they focused on the build server where the actual code is compiled. And instead of actually implementing their malicious code in the build process, in the build, they coded as the output of the build process, that way it got packaged in and signed with the SolarWind software. They took that approach because, one, it keeps them off the radar for code scanning and code review. They're not going to see that code. And once they get signed, it's trusted at that point. So, once they got pushed out to the update server, all these individual companies who were running Orion SolarWinds download that, it gets on their network, but the attack didn't start or that malware didn't trigger for two weeks. And once it started triggering, it communicated with cloud resources where they set up their C2 network with AWS, GCP, Azure, GoDaddy and services like that and actually mimicked the Orion syntax. So, it looked like regular Orion traffic going back and forth. And that gave them access to the network. They could read email, obtain documents. They even got certificates where they could impersonate users. And it wasn't detected for a long time. It was a really sophisticated attack. They were very patient, and this was a really crafty attack.

Kliewer: Awesome. And just to point out there, because I want to point out in a little bit for our listeners and our learners in our courses that we've talked about some of these different components. I think we talked about C2, the command and control, which is what they're actually using to actually go back and obtain that information out of the host networks once they're compromised. And the fact that these command-and-control networks were propagated or stored in not just one cloud network infrastructure, but they used multiple cloud infrastructures and multiple cloud providers to do this, and all of that stuff helped them evade detection basically. So, like I said, I wanted to point that out a little bit. And I can tell you as one person who was part of an organization, who was named in that SolarWinds attack, and one of the initial organizations that were listed as compromised—I'm going to back this up to our SIEM conversation earlier and say that SIEM was absolutely priceless in showing us that, yes, we did establish the initial communication with their command and control, but nothing happened past that point. We can show beyond a shadow of a doubt that we did not exfiltrate data, that there was no other data that went back and forth between our internal network and that command-and-control service. So that's where that whole SIEM ties into it.

So, Joe, I wanted to talk about one other thing, which I know is one of those areas that's kind of near and dear to your heart as a hacker kind of guy, not to use that in a negative component, but I'd like to hear your thoughts on threat hunting versus pen testing, vulnerability scanning, and malicious actors. I mean, how do you know the difference between somebody that's out there doing threat hunting or vulnerability assessment across the internet versus somebody who's a real malicious actor or a real threat?

Sullivan: Well, I think when you look at threat hunting, pen testing and vulnerability scanning, if you're doing it internally, obviously you know this is happening. If you're a third-party performing this for another organization, obviously you're doing it with permission so they're aware of it; whereas if you see these activities taking place, then you haven't given anyone permission, they're not going on internally, you have bigger issues. And these are often used interchangeably today. Threat hunting, in my mind, in my experience is I'm actually going to look at my network and act like there's a potential attacker here, we've been breached and we're going to treat it like that. We're going to look at our business-critical systems. We're going to capture memory. We're going to do packet captures. We're looking for indicators of compromise to see if do we actually have a bad actor on the network? This is beneficial because of your attack dwell time, right? You don't always detect the attacker immediately. Hopefully you do, but usually there's four to six weeks or something like that where they're on the network. This helps shorten that time period if you perform regular threat hunting. Whereas pen testing, I want to know, can you actually get into my network? Is it possible to compromise my software, my configurations, my people? Can you get access into the building? And that tells you, like I say, people ask me, what do you do? Well, I hack networks and break into buildings to keep people from hacking networks and breaking into buildings. If you have a good idea of how this takes place, you can better shore up your defenses in those particular areas. Vulnerability scanning is something every organization should be doing. I'm running regular scans with whatever vulnerability scanner you like that fits into your particular context, that identifies these vulnerabilities as they take place or as they get released and you can set up a remediation plan to patch those.

Kliewer: Awesome. I think that is a great breakdown of those different pieces. So, I'm trying to figure out here if we have any other questions. And I want to take just a couple minutes here to—I want to roll back a little bit, and it's not so much in a cloud context, but still help define some of the rules and regulations we have in place today. But what I wanted to do, Joe, is I want to back up and talk a little bit about the T.J. Maxx incident. Happened quite a few years back, and I think it's probably used in a lot of textbooks. But there was an incident with T.J. Maxx, or basically, somebody was able to access their networks and use network sniffers, you name it, to siphon off credit card numbers, flowing from their front-end systems to their backend systems, and then turn around and sell those numbers on the dark web, you name it. Does that about sum that up? Do you have a better summary of it?

Sullivan: Yeah, this one's going way back aways, right? The T.J. Maxx hack is, if I remember right, was primarily, the initial foothold was they had an unsecured wireless network. Once they got on that wireless network, there was no network segmentation, so they were able to move freely. I think they got 94 million people or so credit cards. It was a huge breach, but yes, that's basically from a high level, what the T.J. Maxx attack was.

Kliewer: Awesome. And the reason I bring that up, because I wanted talk about that for our listeners a little bit, because everybody's also familiar with the PCI DSS or the Payment Card Industry Data Security Standards. And ultimately, that was one of the incidents and one of the cyberattacks that really led up to that PCI rule. And I want to be clear. It is a rule, not necessarily a regulation or a law, it's something that's set forth by industry. I mean, what are the pieces that PCI covers, Joe? I heard you mention several causes of that T.J. Maxx incident. Can you help us connect the dots between that incident and PCI?

Sullivan: Sure. Just to kind of step back and kind of recap what you were saying about PCI, a lot of times, it's misstated that this is a regulation or a law. It's actually a contractual obligation between you and the credit card companies. And the credit card companies got together and did all this because they wanted to avoid government regulation. So, they said, “Hey, we actually police ourselves, we don't need you to get in our business here.” So, they came up with PCI. The T.J. Maxx incident impacted PCI. They looked at what happened at T.J. Maxx, and they said, “You know what? You really need to better secure your wireless networks and need to be separate from your regular network, and your systems, actually whole PCI data, those have to be segmented. They have to have network access control as well. And you need to use the appropriate encryption to encrypt all this in transit and at rest.” And so, we came up with more strict PCI requirements, and you get into the network segmentation. And you don't want to apply PCI to all your resources, right. on the network (your systems, your servers, your devices) because then everything has to be PCI compliant. The secret to becoming PCI compliant is narrowing the scope, applying it just to those credit card related systems. There was something else on that one too. Just totally train crashed there. Oh, they also recommend using a higherlevel agnostic security or control framework, and then scoping down to your PCI system. So, then you're looking at something like the CIS controls or this cyber security framework as well.

Kliewer: All right. And I think that's a great point to make there is regardless of what country you are or geolocation, whatever, the PCI pretty much applies worldwide, but there are other frameworks and other tools you can use depending on your geographic location that can help implement those same regulations and rules, and I think that's a great connection to make there. And all right, I want to kind of start wrapping things up here just a little bit, Joe. Are there any other real last minute or overarching things that you'd like to talk about on the attack surface or what you'd like our listeners to know when it comes to the cyberattacks and what happens out there?

Sullivan: I think I'm going to sound like a broken record on this one, right? It still goes back to doing those basic things like you see in the CIS controls. Notice where you're at with asset inventory, know what assets you have, know what are business-critical assets, know where the crown jewels are, segment those, appropriate logging, monitoring, alerting, patch management, vulnerability scanning. In fact, it was June of last year, the White House actually came out with a document that said, these are the things you should be doing to protect your information security program—regular backups, penetration testing, vulnerability management. These things still hold true. And that was very much a watershed event. I don't remember a time where the White House actually came out and said, "Hey, this is what you needed to do to secure your network." Why did they do that? Because you see organizations like SolarWinds getting government organizations breached, and you see the Colonial Pipeline, which is supplying oil to the United States, and the meat packing processing plant, which also got ransomware at that time—provides food and meat to people in the US. It's where these incidents, these cyber events and these ransomware attacks aren't just affecting individual companies now, they're affecting people across the nation when you get to this level. So that really changed the criticality of what you need to be doing to secure your network. And you see, CISA came out with supply chain guidelines to protect your organization against those. I guess what I'm getting at is do the basics and determine what your context is. Do I need to focus on supply chain? Do I need to focus on vulnerability scanning, penetration testing—are my backups in place? And take care of the basics and build on top of that.

Kliewer: Awesome, great advice, Joe. And I want to take just a moment here. To our listeners, I hope you've enjoyed this discussion. I hope you found this useful, and I hope you found it helpful as the official training that you've been taking. And again, I want to offer many, many, many thanks to our special guest, Joe Sullivan for volunteering his time to share his experience with us.

Sullivan: Oh, good to be here, Chad, I enjoyed it. Good conversation.