Justin Robinson:

Hi, my name is Justin Robinson. I'm the CTO of Cybersecurity for Thundercat Technology. Thank you for joining us today. I'd like to talk to you guys about the current state of cybersecurity in the US public sector and how we kind of evolve and meet the current state. So it's a challenging space right now as a cyber defensive operator. When you look at the expanding footprint, multi-cloud, on-premise, hybrid and everything that goes in between, there's just a ton of attack surface that continues to grow. And as we approach protecting that attack surface, we're also faced with increased regulatory compliance. CMMC and GDPR and the executive order and all the regulations that have come with that, as well as the skills gap that continues to be widening. So if you look at the current state of the market, while threats are emerging every day, we aren't getting any closer to staffing to the levels we need or finding qualified talent to do so on the defensive cyber operations side of the house.

So how do we look at how we're securing ourselves today and move more towards what world-class SOC is? And how do we do that at the same time as meeting the expanding footprint, dealing with the skills gap shortage, and understanding that we can meet the regulatory and compliance controls that are necessary? So if you look at some of those controls, the executive order 14028, Improving the Nation's Cybersecurity, and then all of the memoranda that have come with it. M-21-30 for critical software, 21-31 for incident response and logging, 22-01 for endpoint detection and response, 22-18 for software bill of materials and 22-09 for zero trust, probably being the biggest in the defense of cyberspace. How do I look at reinventing SOC, reinventing how I do things today and still meeting those mandates, meeting those requirements? So if you look at traditionally how SOC have been stood up and how we've operated as defensive cyber operators, the SOC has been very role centric.

I might have a team of primer security folks that deal with my network sensors, my firewalls. I might have a separate team that does identity and deals with my ICAM IdAM strategy. I might have a third team that's strictly centered around governance risk and compliance, and is working in tools like Telos Xacta, RSA Archer or any other number of tools. And I might have a threat intelligence team that is just working with threat feeds and threat intelligence platforms and sort of enriching the data I have in my SIM. But all of those roles are separate, and that data is siloed. So the labor is siloed, the data is siloed, so if teams need to come together and data needs to come together, I have to bring people together from different teams and I have to move data. I have to copy that data, and that might be from cloud to on-prem or on-prem to cloud or a variety of all of those things.

As I look at role-centric security, it was a perimeter and moat, the firewall perimeter security, a centralized SIM, and something that was fine back in the early 2000s when we were dealing with worms like the blaster worm and security was attacks in the megabytes of security data. But as we've evolved, we're starting to collect gigabytes, terabytes, and even petabytes of security data. And so role-centric security doesn't work anymore, and we're going to have to evolve how we do SOC. So how do you move towards data-centric security and away from role-centric security? If you look at data centric security, what are the best SOCs in the world doing right now? How are they dealing with data? And if you look at some of the best commercial companies in the world right now, they're dealing with multiple cloud platforms. They're dealing with ingesting hundreds of terabytes of ingest of log and security data a day.

They're looking at multidisciplinary site reliability engineering teams where everyone has a base foundation in Python and everyone understands SecOps automation. So if you look at some of these leading teams and data-centric security, how do we move towards that? And if you really look at it, it's all about people, process and product. How do we change how we approach security labor? So from a people perspective, we can start to look at removing these role-centric, role-based silos and start to build multi-disciplinary teams. So instead of having a tier one, a tier two, and a tier three analyst, or a GRC team and an identity team and a perimeter team, I can start to bring things together and say, "I'm

going to have a multi-disciplinary SRE team." I bring in new security labor. And for the first six months they're there, they're working on identity. For the next six months they're there, they're working on perimeter. For the next six months, they're working on governance, risk and compliance, all the while touching the foundational undercurrent of the SOC; Python, security orchestration and automation alerting, rules.

So essentially having that multidisciplinary team and taking that SRE approach allows customers to start to hire people in a more efficient manner, have teams of people who are multidisciplinary and no longer siloed in roles, and it starts to allow for collaboration and automation process. All process in security needs to move towards security orchestration and automation. So if I have multidisciplinary teams and they all have a foundational knowledge of Python, they all have a foundational knowledge of how to code playbooks, how to deploy automation, now I can start to take what was legacy process and I can start to bring SecOps automation into my SOC. And then lastly is product. I can start to orchestrate my current security tooling, my current security stack in a more holistic way, and I can move towards data-centric SecOps. And so how do we get there from where we are currently in these role-based siloed security operations to data-centric SecOps?

Well, the first thing is having a data-centric architecture. So how do I build out a data-centric architecture that can inform my data-centric SecOps? The first thing I do is I deploy an enterprise security data plane. That enterprise security data plane is data in motion. So before I collect data and throw it into my Splunk or my QRadar or my Archer or my Elastic, I actually look at that data in motion and I actually remove the noise from that data so that I'm feeding pure signal into my enterprise security data lake. I enrich that data with threat intelligence from a third party, I enrich that data with my own intelligence, I take metrics as to what data I'm actually pulling in, and most importantly, I put the right data in the right place at the right time. So data that I don't need to move out of my cloud and pay cloud egress cost to do so and bring all the way back to my SIM, I leave where it is in that cloud. Data that I'm going to alert and visualize in my SIM, I bring that data back to my SIM.

And all the while I can, with data in motion, run metrics of AI and ML that are targeted and more supervised against that near realtime data. The secondary piece is enterprise security data lake, which is the follow on or next generation to what was traditional SIM and really breaking SIM into two different roles, the dashboarding and alerting that I expect from my security information and event management platform, but then also the distributed data query. So where we have been over the last 10, 15 years in cybersecurity is when I want to ask a question of my security data. I do that query in one place in a consolidated SIM that is drastically changing and going to continue to change over the next three, five, even 10 years. As we've moved into this world of multi-cloud, and I have log data in AWS, log data and Microsoft Azure, log data in Google Cloud platform, as well as on-premise data and maybe a Splunk, I need to leave some of that data where it is because it's going to be too costly and too prohibitive for me to move that data into a central location.

So if I have an indicator of compromise, an MD5 hash and an IOC something I'm looking for distributed data queries going to be important where I can look for that MD5 hash and I can query all those data sources and just pull the metadata back of where that's been seen in my environment without pulling all of the petabytes of data back into a traditional SIM architecture. So enterprise security data lake gives me the same SIM functionality I have today with an added distributed data query capability. The next foundational piece of this architecture would be SecOps automation. So your SOAR product, security orchestration and automation, your Splunk SOARs, your Palo XSOARs, your Google Simplifys, into your continuous configuration automation tools, Ansible, SaltStack, Chef Puppet, all the way to robotic process automation, UiPath automation, anywhere.

From simple to complex, all of these automations give me a foundation to take process, turn it into automation, which is going to be very critical. And then the last piece to this foundational data-centric architecture is detections as code. So traditionally I would have BARB working on my firewall rules and ED working on my SNORT signatures and [inaudible 00:11:16] writing CIRCIA rules for Brozik, and all those detections would live in silos. But if I take those and I put them in a GitLab repo, and I turn my SecOps automation onto them, now I can do things like automated hunt, automated response, automated security validation, and I can deploy those detections in my network at a speed and efficiency that I couldn't do manually. Why is that important? If you looked at how our adversaries attacked us even 10 years ago, it was having to be in a forum with other hackers, having to understand the trade craft, and then deploying my attack.

Then about five, six years ago, starting to just give Bitcoin to a malware mart, downloading the latest version of TrickBot, and now I just tweak it, and I can attack my adversaries. As these lingual learning models like ChatGPT, AutoGPT start to stand up, you are going to start to see malware.gpt type behavior where our adversaries are going to be attacking us in a more automated and more efficient manner, increasing the challenge to our defensive cyber operators. So it's critical that we bring the data in, we take the noise out of the data, we feed pure signal into our enterprise security data lake. We automate and have the automation tools to leverage that signal, to run our detections, to do automated hunt, automated response and automated security validation on our networks. So today we're all very role-centric.

Getting to maturity, rolling out an enterprise security data plane, rolling out enterprise security data lake, rolling out SecOps automation, become the critical piece, to get to world-class, moving towards detections-as-code, moving towards automated hunt, moving towards automated response and moving towards automated security validation are going to be critical into how we protect our networks. This is a challenge that's not just buying a tool, not just changing how I hire people, not just orchestrating or automating a current process, but re-imagining SOC, moving away from what was role-centric security towards data-centric SecOps. If we do this, we can stay in pace with our adversary or hopefully ahead of our adversary and protect ourselves in a better way. So once again, thank you for your time, and hopefully it'll be a good conference and any questions you guys might have, please feel free to stop by our booth. Once again, thank you very much.