An Interview With Gus About the Evolving Cybersecurity Threat Landscape

Video Transcript

Federal Cybersecurity Practice Lead, Gus Hunt

Dave Gardy: Dave Gardy here for CyberSecurity TV at the AFCEA DC Cyber Security Summit. With me is Gus Hut who is Federal Cyber Security Practice Lead for Accenture Federal Services. Thanks for joining me today.

Gus Hunt: Glad to be here Dave.

DG: Give us an overview. You’re going to be speaking in the first session about the evolving cyber security threat landscape. What are you going to be covering?

GH: I’m going to talk a lot about how the landscape itself has increased in velocity and aggression. You just witnessed recent events by adversaries in our outside world – both nation states and cybercriminals. And the fact that the problem space has gotten to the point where we are going to have to act better together as a nation in order to deal with it and solve the problem itself.

DG: If you had to pick some of the top cybersecurity threats in that landscape, what would you pick?

GH: Wow. I think ransomware of course is a massive issue simply because of how easy it is to do and the fact that it relies on people who need better training and education to understand what they should and shouldn't do when they're working on their systems and clicking on emails, things like that. I think there is going to be a big push into tacking out T-systems, drones, you saw the article about hacking a while ago. Between skateboards and blue tooth toothbrushes and medical equipment and all those things like that they're opening up a massive additional number of potential entry points.
points into the system and if you think about IoT numbers we have seven billion smart devices today and we’re going to grow to 70 billion to a trillion smart devices by 2025 depending on whose numbers you look at. That just increases the attack landscape in ways people haven’t yet gotten their minds around to deal with.

DG: One of the series we’re doing on CyberSecurity TV is a cyber security national action plan; how do you spend that 19 billion dollars in fiscal year 17 that everybody’s talking about. Do you have any suggestions for how the federal government should work with industry to try to approach that?

GH: Yes. One of the things I’ve been trying to push hard for is what I call the national call to action. Think of President Kennedy’s ‘Race to the Moon’; his famous saying “We are doing this not because it is easy; but because it is hard”. I think we need a similar approach as a national call to action – a national grand challenge around cyber fundamentally because we don’t treat it in such a manner. And, use it to drive STEM education and improved capabilities across the board for everybody. I think we are going to be continuously fighting an uphill battle and never be able to get ourselves in front of what’s happening in this space. I think that’s a terrific idea.

DG: Can you give me just an overview of what you do over there at Accenture Federal Services as the Federal Cyber Security Practice Lead?

GH: Accenture’s been in the cyber business for a long time but hasn’t had a coherent, directed focus on it. So they built big systems and cyber goes into everything Accenture Federal builds. We’re now standing up a cyber focused practice to help us deliver capabilities to support our customers as we move into the future. So looking beyond the traditional modes of cyber we know that traditional modes of engaging in cybersecurity around infrastructure-centric approaches, things that came out of the perimeter-centric world – there is no perimeter anymore; that’s completely evaporated and it’s gone away. While necessary, traditional approaches are not sufficient any longer so now we need to step into things like data-centric security, building secure applications across the board, proactively hunting for vulnerabilities so we can aggressively find ABTs that are not singling out to the SOC and other things like that based off of the behaviors not their signatures and we’re going to have to bring the big data lens to bear on the cyber problem space. It’s going to be machine learning and AI that’s going to help us solve our problem particularly with a massive explosion of intelligent devices in the IoT world that are going to be out there.

DG: Well we appreciate the time you’ve taken before your presentation. Gus Hunt, Federal Practice Lead for Cyber Security at Accenture Federal Services. You’re going to be talking here in a little bit, we’ll have that also on CyberSecurity TV. Thanks for joining us here at the AFCEA DC Cyber Security Summit. Stay tuned for more.