Amear Mitchell:

Hi everyone. My name is Amear Mitchell, account manager at GovExec. And I'm delighted to continue the conversation today with Meghan Good, Vice President, Director Cyber Accelerator at Leidos, and Doug Jones, CTO for the Leidos Corporation. Let's get into today's conversation. What does it mean to move to a readiness perspective? Meghan?

Meghan Good:

I love this question because readiness is the word of I think the decade right now. And it's really the one that we hear in a lot of different defense spaces. And for me, when we talk about that and particular with a cyber lens on it, I'm thinking a lot about resiliency. I'm thinking a lot about how we're moving beyond what we had with compliance in the past around cybersecurity and where we're going to really make sure that we're driving technical solutions that meet the mission demands, but that are secure and that are resilient, and that are adaptable to the changes that we're seeing across the threat landscape.

I use a couple words there. And I think it's really important to... Maybe it's all these mathematicians that I work with, of getting to first principles and easy definitions. But for security for us is a lot about how we're protecting confidentiality and integrity and availability of data. And that's really important for what's needed across our missions and when they're in really threat involved environments.

But resiliency is something a little bit beyond that. A resilient system is one that continuously delivers the intended outcome despite any adverse events. And that could be any number of different things that are adverse, not just threats, but it could also be misconfigurations. It could be changes that are happening within the environment that you really can't control, which is happening all the time.

And then adaptable for us is an adaptable system, is something that adjusts as conditions change. And when I look at cyber solutions, we really want something that has all three of those components. And what we're particularly thinking about for readiness is how we're really building in resilience. Security has been a focus for a really long time, and it's very important and critical. But it's part of the puzzle, especially when you think in a defense context, especially when you think about the great power competition... Especially when you think about even the battlefield environments that we're envisioning within the 2020s and beyond. It's about resiliency.

Doug Jones:

Yeah, I want to jump in there and add, I think when we look at the defense side as a focus multi-domain operations in [inaudible 00:16:17] two and we want to go and where the nation needs to go, especially in great power competition, we know our adversaries want to deny our ability to have a decision advantage. They want to deny us to be able to bring all of our assets to bear. Or they want them to be isolated so they're not working in a coordinated fashion. Because that decreases their effectiveness and decreases our ability to thwart whatever they're trying to achieve.

And so when you look at that as they're trying to deny these things, that goes back to that resiliency perspective. We also know that they've spent a lot of money in asymmetric warfare capabilities, specifically around cyber and things like electronic warfare and how those are used to neuter our information advantage and our decision advantage.

And so that's why we need to be focused on resiliency. We need to be able to prevent things such as DDoS attacks which denies availability or jamming, right? We need to be able to be ready for supply chain style attacks and looking at traditional network as well as data poisoning and things that decrease our confidence in our decisions, especially as we're looking at the speed at which data is flowing to just to be made. Because now you're looking at algorithms that are informing decision makers don't.

We're not quite at the area where war fighting is being done by algorithms, but those algorithms are looking at massive bounce of data and informing the war fighter on decisions they need to make. And if you create distrust from a data perspective, from an integrity perspective, now that resilience, that ability of the systems to be adaptable. And our war fighters to be able to be effective is hampered.

When we look at these lenses, we look at how do we prepare for that resiliency piece. And look at we also have to do it in this adaptable environment. Everything is software defined now, so change is a lot faster than it used to. It used to be to roll out new capabilities would be years to decades, and now things are changing. We have software defined radars and software defined EW. And those types of capabilities are critical that we have to be able to react to them as well. same thing with the cyber world.

That resiliency piece is critical. We have to be resilient and adaptive. And we have to be able to apply that to all of our mission sets in the defense world if we want to be able to be a player in this great power competition.

Meghan Good:

And I like Doug, if I can just add on that you emphasize speed there, that things are changing and adapting faster and faster. And I think that's the other big component of readiness that we talk about a lot is the continuous nature of this, and that the decisions that we make today will continue to compound and also make it so that we are able to be more resilient in the future. And so it's decisions today to make an impact for tomorrow. And then but they also make an impact today.

Amear Mitchell:

Meghan and Doug, thank you. Speaking of change, how does moving to readiness change your approach? Doug?

Doug Jones:

I think it's important to think about things from a threat perspective and understanding what is the threats that the adversaries are providing, and how do they want to prevent our mission outcomes and then understanding based upon that, what is the risk to the mission? And then once you understand the threat and the risk, how do you prioritize the resources we have? Because we have constrained resources, both money and talent and time.

We need to be able to optimize and prioritize those and factor those into how do we do our solutions. This gets beyond focusing on just capabilities and compliance. When the way we used to design and build systems and networks is about what capabilities we're going to have and are they secure from a compliance perspective. Now we need to understand what are the threats and risk and how do we prioritize and build those in from the beginning.

We now look at how do we do that from a design perspective. As you're designing a new application or [inaudible 00:06:26] as an application, designing a new network you need to support, what we start now with is what is the threat? What's do a tabletop red team exercise of the design? If someone knew what capabilities this application or mission or network supported, what would the adversary want to do they want? Do they want to deny it? Do they want to block it from happening? Do they want to [inaudible 00:06:50] the data out so they know what our intelligence services are saying and they know where our war fighters are, our readiness capabilities are? Or do they want to create distrust in them from an integrity perspective?

So we understand what would the adversary want to do with that asset if they got in there, if they were able to thwart a mission capability. And then you want to understand how would I put countermeasures into that From a design perspective. This goes to things like zero trust, it goes to design capabilities that you could build the resiliency and from design. We start a design. But then now we're taking the next level, how do you evolve that all the way through to your ecosystem from your tools and your engineering process to how do you deliver it?

I think it's incredibly important to think about that adversarial view and what they want to do from a threat perspective into how do we build, design and operate and continuously evolve the systems that we're building for the war fighters.

Meghan Good:

And I think with that, to your point about the change of the approach, I don't know that it's all that different to do red teaming, right? Because we've done that for a while, penetration testing. We've been trying to take where one team builds and one team tests. And that's something that we do that's very time intensive, but it's often really limited in scope too, and so that you're only testing certain portions.

And what we're talking about here, there's scale involved in, there's a lot of heterogeneity, that's a hard word to say, amongst all of the systems. And it's even harder to then think about how they'll be resilient to threats. And what we need to get to with this really big emphasis on that adversary mindset, what would they do about it, is how are we attacking and defending at the same time when we're doing that red teaming. It's more the purple team, the red and the blue coming together. And how do we do that in a tighter loop throughout the entire life cycle of our engineering design and even the deployment side of it?

How are we continuing to adapt? Again that adaptability word, to make sure that we're resilient to those now unknown or evolving threats as we go forward. And I think for us, a lot of what we're finding that is it's how we're getting to really operationalizing DevSecOps. It's that DevOps mindset of you develop it.

Security here we're going to figure out like an adversary what's going to happen to it, and then we operationalize solutions from it. And it's how to make that a really close tight loop so that it's really enabling all these missions that are so impactful and important.

Doug Jones:

It's funny you talk about DevSecOps. When I look back at the early days of DevOps, they're trying to figure out how to include security in it. And a lot of the early team names were rugged DevOps instead of DevSecOps. And maybe we had something there because it's more about the resiliency and readiness and not just about security. But we're really passionate about how do we bring that security piece through the entire lifecycle and ecosystem. Everything from visibility from a monitoring perspective to countermeasures to additional areas of failover and resiliency capabilities, that can allow the mission to keep being performed even if we're having thwart adversary or adversarial impacts that are ongoing.

Amear Mitchell:

That brings me to my third question. How do you actually bring all of these things together at scale in an operational environment?

Doug Jones:

I think one of the key things is at scale. When you look at what Leidos does, we are the largest provider of IT services, federal government. And when you look in the DOD, we have those franchise programs, the GSMO over DISSA where we operate the [inaudible 00:10:18], the Navy engine contract, where we are operating massive scale IT for the Navy across the entire enterprise, multiple other massive scale IT jobs.

We also... One of the largest cyber providers in the DOD from a CSSP perspective, that's a cyber security service provider, we operate six of the tier twos inside the DOD, multiple tier twos over a DHS. We try to think about those scale aspects. And what do we learn from how do you scale massive scale IT? And I think one of the struggles we have is how do you modernize it. When you've got a global scale?

You've got networks literally across the world when you talk about the [inaudible 00:10:56] and the DOD IT services network is all across the world. How do you modernize that? It's like the problems they have in casinos. When they clean it, they start at one end, they finish and they start over at the next end and keep going. It's a continuous process. You have to do the same thing when you're talking about massive scale. And so it makes things a little bit more challenging when you're trying to do these at scale. Because you can't just sort of rapidly put in a prototype when you're talking about operating mission critical functions globally.

Those are the challenges that we bring to bear in our understanding. And one of the things we've been thinking through in that space is how do you scale something like a zero trust? One of the things that we've seen people struggle with is how do you get to zero trust. Because it's an architecture and a construct. It's not something you can just buy. We developed something called the zero trust readiness level or ZTRL. And the idea is understanding where are you? A lot of the DOD has been focused on defense in depth. They're a little bit more mature from a zero trust perspective because they've been building that in based upon the way adversaries were attacking us for years.

And so we understand where are you in that readiness level and then where do you want to go. And then how do you evolve to that? What are the right technologies and solutions you need to get to that next level step and the benefit of that next level step? So as part of that, we've integrated our zero trust proving ground where we can go and evaluate products, not just evaluating for whatever capabilities they have, but evaluate them against a use case. What is the problem we're trying to solve? How are we trying to advance from an existing zero trust rate readiness level to the next level? And how do we achieve those outcomes?

And not just what are the tools, how are they configured? How they integrate into the ecosystem of other existing tools that you may have, whether they're monitoring tools or data aggregation tools or identity access management tools. You're not going to replace them all. You're going to be augmenting them or improving them through configuration and other tools.

We try to look at it through how do you time them all together, what are the gaps. And then how do you now develop the deployment approach at scale so you can incrementally roll them out without impacting that scale mission. That's one of the hardest things that we try to look at as we look at the lab.

Meghan Good:

And I think adding to it, to tie back in what you were talking about before, Doug, about adversarial mindset to that, It's really important to apply that to your zero trust readiness. And an interesting side of it of being a full spectrum cyber company is we can really apply that offensive thinking into this defensive strategy around zero trust.

Because the whole point is you're adding all those solutions, you're doing a lot of modernization. What's the value? What's the impact of it? How are you making sure that you're really addressing those threats

and that you're resiliently operating through it? So we take a lot of our zero trust lab and we actually get to use it as an environment where we figure out maneuvering around still in a zero trust environment. We figure out how you can start to identify some of the gaps in the defensive systems and the visibility so that we can then plug those gaps along that purple team thread, of you have to have that attacker mindset so that you're really supporting your defenders and you're making those decisions much more quickly.

But all that said, I think zero trust often gets applied to enterprise systems and it's like, "Oh, we're doing it. We're doing great with zero trust." But what about all these other systems that are connected within into the same environments? I think for us with resilience and with readiness there, we have a large focus around cyber physical systems. Those platforms, those capabilities that we've been developing over the years as part of the R&D functions that we have, and now that they're getting more integrated for multi-domain operations, how are they really going to communicate well and effectively and still be resilient in a threatening environment?

A lot of those systems were never meant to really be connected. Or if they were, it was a specific channel and you would never think about some of the other areas, or you would, but it was acceptable risk at times. But as we're moving forward, it really isn't. So a lot of our emphasis now is about how do you emulate some of those infrastructures and start to identify where their weakness is there and similarly iterate in a purple team construct of how are we improving the resilience of these platforms in these capabilities over time. And how do we do that in a more automated manner?

I think today it's very much manual and human intensive, much like we were talking about penetration testing. And so for Leidos we're using our 40 plus years of reverse engineering these cyber physical systems to really develop the tools and capabilities that are needed as we're rolling them out and integrating them much more into these multi-domain operations constructs. The effort that we do there is called Leidos Secure. And so it really is implementing those secure design capabilities that we talked about that are helping ensure resilience and adaptability going forward.

And a lot of it is the aim of all of it is so that we are making sure that these systems operate through adverse events on a continuous basis and that they're adapting to changes within their environment from a cyber threat perspective. Our goal really is to outpace and out maneuver those increasingly sophisticated cyber threats.

Doug Jones:

And Meghan, I think you hit something big. There is a lot of the focus has been on the enterprise IT side and if you look at a move to multi domain operations and [inaudible 00:16:17] two, we're now connecting weapon systems. And we're connecting them with data moving its speed, and we're connecting the cloud. And we're bringing cloud capabilities to the edge.

And when you start pulling all those together, you're now creating great capabilities that allow us to move data around and have information decision and turn a lot of our platforms and more effective sensors for us to make more effective decisions out of. The same time, you're creating a massive threat profile. You have to factor into resiliency of it. And it's not just from a cyber threat perspective. It goes back to that data poisoning, that trust factor, the whole CIA triad, which is confidentiality, integrity and availability, all those into the mission ecosystem of where they're all being connected.

And that's why it's absolutely critical that when we think about this problem set, we're not just thinking from an enterprise IT perspective, we're thinking it from a mission IT and a mission outcome perspective that is really driven by data and decision making across a wide variety of platforms that include legacy systems and modern systems and partially modernized systems.

Ultimately, the key is how do you get that resiliency and adaptability at scale for the war fighter? And that's what we're trying to get to. In the end, it really is about speed, scale into security and applying that to our customer's hardest problems.

Amear Mitchell:

Excellent. Unfortunately, that's all the time we have today. Meghan and Doug, thank you so much for being here today and for the important work that you are doing. And thank you to Leidos for helping us make this event possible. I hope you'll stay with us for our next session. For GovExec, I'm Amear Mitchell. Thanks for tuning in.