Shane McGraw: Hello, and welcome to today's SEI webcast, "Zero Trust Journey." My name is Shane McGraw, Outreach Team Lead here at the Software Engineering Institute, and I'd like to thank you for attending. We have a worldwide audience today. I see attending members from United Kingdom, Pennsylvania, Maine, Bulgaria, so keep adding your location in there for us. We love seeing that worldwide audience. We want to make our discussion as interactive as possible, so we will address questions throughout today's talk, and you can submit those questions in the YouTube Chat area, and we will get to as many as we can.

Our featured speakers today are Geoffrey Sanders and Tim Morrow. Geoff, Tim, welcome.

Geoffrey Sanders: Afternoon, Shane. Thanks for having me today.

Tim Morrow: Shane, thanks so much.

Geoffrey Sanders: Thank you both, and so Geoff is a senior member of our technical staff within our CERT Division here at the SEI, and is a member of the Situational Awareness Team. He supports SEI sponsors in multiple areas of network systems security and survivability. His current areas of interest include analytics, big data, data fusion, and zero trust.

Tim is our Situational Awareness Technical Manager within the CERT Monitoring and Response Directorate, also here at the SEI. He has experience with system-of-systems, systems and software architecture and analysis methods, full lifecycle development and support of Model-Based System Engineering tools in his 18 years here at the SEI.

Now I'd like to turn it over to Geoffrey Sanders. Geoff, again, good afternoon. All yours.

Geoffrey Sanders: Hey, great. Thanks, Shane. Basically what we're going to do here today is just talk about some of the research we've done as it relates to zero trust. Really this domain is about 10 years old, still growing very quickly, and we're starting to see great progress in actually implementing the tenants, and our research really has come down to understanding that much of this is a journey as much as it is a strategy for organizations, a very unique thing for each organization that tries to do it. So we're just going to go through of how we're approaching this now and some of the neat things we've found with the journey itself.

Tim Morrow: Yeah, and I think one thing that you'll hear a little bit different with our--part of our webcast here is our focus on the implementation. So a lot of times--and Geoff's going to talk very well about this, what zero trust is and what it means to think about transitioning to that, but we feel it's very important to get a good vision of your system, have that big picture, and be able to analyze so that you know where you are in your journey. And so we're going to talk a little bit about some of the techniques that we use that kind of ties the two together and gives you a

good sense of how you could accomplish this. So yeah, we're looking forward to a good webcast here. Thank you.

So I will--sorry?

Geoffrey Sanders: Great. Thanks Tim. One back, please.

Tim Morrow: Yeah.

Geoffrey Sanders: Great, thanks. So what we're going to really start with today is just really short overview of kind of what zero trust is so we're all starting off with the same definition and the same understanding. We'll look at some of the challenges we've run into talking with organizations and things they've encountered while trying to do zero trust and implement it. Then we'll get into our unique view of what zero trust is and how it's really a journey for an organization and how we approach that in a particular way and some of the next steps we're going to have as an organization to help grow this research out.

Tim Morrow: Yes, sir.

Geoffrey Sanders: So when you get through most of the documentation and artifacts that are out there to help organizations get their hands around zero trust and trying to implement it, you can get into the real technical details of how things are supposed to function, but when you kind of roll them all up you're really kind of looking at three main tenants in a zero trust architecture, in a zero trust strategy, really, which number one is you're assuming that attacker presence in whatever system you're trying to secure.

So the traditional method has been a perimeter security approach where you have a firewall and there's not necessarily tight security controls on the inside as compared to what you're trying to keep from coming into your network. So that changes with zero trust and that you're assuming that attacker's in wherever you're working, and because of that, the goal is to remove any type of implicit trust that's in the design and implementation of that architecture in those systems. So rather than assuming that somebody should be trusted to access a service or something else, you're saying, "We're going to deny access to everyone. We're going to remove any implicit trust between two endpoints, per se, and we're going to design the architecture and the implementation, the security and all the technology around it," and using that approach.

So to do that, what we're really doing is we're moving the traditional security from the network, and we're moving that to the user, the application, and the workloads that serve those applications.

How about you, Tim? Anything else you want to add to that?

Tim Morrow: Yeah. I know for me I had a tough time in the beginning thinking about this implicit trust and what that meant, you know. I mean, I could look at the--some of the documents you're going to be talking about and it would draw circles around things but it didn't appreciate, "Well, how close is close for something like implicit trust?" Is it something you're going to talk to us a little bit about during your discussion here?

Geoffrey Sanders: Yeah. We can get--in one of the diagrams we'll get into some more specifics. We'll actually look at kind of an abstract view of some zero trust components, so we'll talk about that a little bit.

Tim Morrow: Okay, great. So Shane, I was wondering, is this good opportunity check for some questions?

Shane McGraw: So I'm just actually going to put one in there now, Tim, just to our audience saying make sure they get some questions in there, and if they have any way that we can kind of direct this. So I'll chime back in once we hear from them.

Tim Morrow: Sounds great. Thank you very much.

Geoffrey Sanders: Okay. So here's the diagram I was basically referring to. This comes out of the NIST Special Publication 800-207. These are what are termed the logical components of a zero trust architecture. At the bottom here you're seeing the data plane, where you have kind of three main things. You have a subject, a resource and a policy enforcement point, and the subject is usually a person accessing some type of system over an untrusted connection, and they're trying to access a enterprise resource that is being served from some location, wherever that may be, and in between those is some policy enforcement point that's saying, "Okay. We're going to restrict access to this resource based on some particular policy."

If you see at the upper part of the diagram, they have the control plane there, and that's made up of the policy decision point, and that policy decision point's getting input from both the left and right sides of the diagram. You have things like threat intelligence, compliance, log data, SIEM alerts. All that information is being brought together and is being utilized in some dynamic way by that policy decision point.

So when you look at this here, what we're really speaking to this type of architecture is it's much more dynamic than what we've been used to in the past, right. We have a lot of manual intervention where you have an analyst looking at data trying to decipher what's going on on the network, tickets back and forth, and when you look at some of the artifacts coming out, speaking to how these dynamic things work, you're actually talking about implementing security orchestration automation response and things like that where because of the complexity and the

amount of data that's coming in here, you're having to rely on some automated decision-making too to go on, which means you really have to know your environment well and you have to be able to identify activity within that environment very specifically in some automated way, and it's not that every step will be automated. You're obviously going to have some human interaction here, but the key is is to reduce that work, right.

When we talk subject, understand that a subject can be a human or it can be what they call a non-person entity or some type of NPE. A good example of that is like a container, okay. So it isn't that it's always going to be a human. You can have automation in there. You can have a IoT device, something like that, and then you're going to have to make decisions based on those types of context as to what that user is.

So how this typically plays out when you're talking about implementing that technology is you'll usually have some type of agent on that subject side that's understanding what's going on either at the container level or at the system level that that person is using and is communicating with the decision point and the enforcement point, sending data back and forth, and that's kind of where you get that dynamic interaction.

Anything else that you think we should cover here, Tim?

Tim Morrow: And, you know what? When I look at the diagram, my eyes always jump up to the policy decision point block up there, and I get the idea that, you know, there's all these inputs coming in and I should be able to go out and find a good tool that's going to let me connect these all up, you know, just putting the wires in the right spot and making this happen. Is that reality today?

Geoffrey Sanders: I think you're getting some pieces that help you build that full puzzle, that help contribute to that picture, but there isn't one particular thing you can buy, and especially in today's modern age when you're talking about hybrid cloud computing and orchestration and containers and unique applications where people are leveraging open source components to build their own app and their own services. That makes it much more complex in that you're going to say, you know, "I can buy these two things and generate that." There are building blocks that help you accomplish that, but there is no one component that you're going to be able to find.

Tim Morrow: I appreciate that. Yeah, I think that's what makes I think our work exciting, is being able to put together that picture like you just described, the things that you need to think about for your environment and how that'll work for you. So we're going to talk more about that, but thank you. I thought that was a great description here.

Geoffrey Sanders: So when going to look at zero trust and how you're actually going to implement that and the guidance around how to actually start your journey and execute your

journey, there's a lot of different guidance out there we just want to point out to you. Multiple different government entities, commercial folks who are actually publishing their work. The "Zero Trust Security" book by Garbis and Chapman is a great resource for anyone who's looking to actually get down to the nuts and bolts from folks who are actually implementing these ideas on networks, and of course the government guidance is great because they're spending a lot of resources and actually defining what all these components are and how they work together.

Tim Morrow: Yeah, I think that's one thing in our position, we work with so many different customers. I think--we work with the DoD, we work with federal agencies, we work with commercial, and so they have a variety of things that they need to consider as part of their government, and so having a lot of these different documents, it makes it good for us to help understand different points of view, but I know for me when I look at this stuff, I do like the DoD zero trust reference architecture. It provides the detail. It tells me a lot about the interaction. So that was another one that I thought was very helpful, and I think people if they can, take a look at that.

Okay. Let me go on to the next one then.

Geoffrey Sanders: Okay. So there's a lot of challenges when you're talking about the complexity that goes with this type of architecture and all these interacting components and subjects and resources. We see them breaking down into four kind of common areas. This isn't exhaustive by any means, but these are kind of some of the general areas we see of governance being an issue. To do a zero trust implementation and to start that strategy and to execute it, you really have to have a good asset inventory. Asset inventory meaning--really anything that generates data is considered an asset. That can be a container, that can be a mobile device, that can be a server. It really gets very broad when you talk about assets, just as one example of governance.

Architecture. You really have to have a great awareness of your architecture and everything that's working together, but also it must be accurate, right, and historically a lot of organizations are used to doing artifacts and diagrams but not necessarily having an ongoing awareness of what that architecture looks like and how it's changing and growing or maybe shrinking. So when you're doing this type of stuff, you really have to have an ongoing and continuous awareness and accuracy of the architecture you're working with and being able to maintain that. You know, when you're trying to implement what we say as kind of a default deny security posture, understanding what type of shadow IT functions are occurring in your enterprise or your organization is very important.

Cost. You know, if this is very new to you and you may not have some of the technologies that zero trust is looking to use to achieve that strategy, it can be a very large curve just to get started. So, you know, how do you understand what the cost is? And really that is up to the organization

to define kind of what their business drivers is and what they'll be purchasing. In general, we see on average that most zero trust journeys, when you're starting to try and implement the strategies, it's going to be a good five-year journey form kind of getting where you're started to getting where you're more mature in implementing those types of things.

And again, you know, whenever you're doing these types of large strategies or any strategy, measurement is a key challenge. How do you measure your success, understand your risk, and understand not only where you're at on your journey but what your risks are and what gaps you might have to fill and, you know, kind of where your next steps are for the new iteration that's coming up so you can get further down your journey?

Anything else you want to add for that, Tim?

Tim Morrow: Yeah. Because I look at this list and I'm like, "Okay. I've been around the block a little bit. I've seen these things before. Is there anything much really different that I should be doing for zero trust in these areas, or is this a common problem that we've been experiencing for a while and now's the time to kind of refocus on really getting down and doing some of these things, tackling these challenges?" What did you think about that, Geoff?

Geoffrey Sanders: Well, I think many of these, and at least this list here is very common to just, you know, my career in the security domain, so they aren't new, but when you're talking about the automation and awareness and asset, because you have this not only policy but dynamic policy, these types of things are much more critical. So organizations may have been able to do them at a lower maturity level, but now they're becoming much more critical to being successful with the zero trust journey. So it's not necessarily that they've changed. They're just much more important and they have a larger overall impact, I think.

Tim Morrow: That makes sense to me. I think--another one I was kind of wondering about is the cost part. Because I think about, you know, some of the things that, like, to purchase a tool and things like that, okay, there's a cost associated with that, but I think a lot of times people don't think of the cost that goes into some of these other things that you've described, and I was just wondering, do you think that's something that is missing today, people are not taking that into account in their adoption cost?

Geoffrey Sanders: Yeah. I think it's a large unknown, because when you talk about governance, for example governance and asset inventory, the largest lift that's pretty common across industry when we look at this is data. Understanding your data, where it resides, who should have access to it. That is probably the largest lift on a zero trust journey and a zero trust implementation, and it can take the most amount of time and most amount of resources, and it's not something that you're purchasing or implementing. It's kind of a hidden cost, because you're going to have to do a lot of work and a lot of expenditure and resources to do that data

inventory and understand those data flows between subjects and resources, right, and that isn't something specific that is on the list, and that's really why we're doing zero trust, right. It's to protect the data.

Tim Morrow: Right. No, that's very good, and I appreciate you digging into those one a little bit deeper. That helps me out there.

So we'll go to the diagram here, and if you could describe a little bit about this and then maybe we'll check in with Shane to see if there's anything we need to do after this slide.

Geoffrey Sanders: Sure, sure. So going through the artifacts we've looked at, this is kind of how we break out approaching a zero trust strategy and a journey to implement the tenant and the ideas, right. Really we see it breaking out into kind of four areas here. We see it as a prepare, plan, assess and implement, and it's not that this is a linear, you know, start/finish type diagram. This is just kind of a framework that you can iterate through and apply the steps in each one of these areas as they apply to your situation, and in many organizations, when we walk in and work with them, they may already have started their zero trust journey and have gone through the prepare stage and plan, but this framework helps us get in there and say, "Okay. Here's what we see as the repair, here's where your plan, here's your gaps," so we may need to go back into this step and execute a couple more things to make sure we're able to finish the plan phase appropriately.

And across this diagram here, what's another key thing to understand, is we have an assessment framework that helps us come in to an organization and really understand where they're at from a mission perspective, not specifically a controls perspective. So we're coming in to look at really what's the mission of the organization? Kind of what are some of their key business functions that they're doing and can we actually break out what those work flows look like and how they operate on a day-to-day basis and look at the journey from a mission execution view rather than specifically a security controls view?

When you look at the prepare phase here, key things. I mean, this stuff sets you up for success. You're looking for, you know, executive endorsement. If you can't get that executive endorsement from the top then it's not going to go throughout the organization to finish the rest of the initiative.

So as you see, these are really key piece and key components to a full-on journey when you're trying to do something over, you know, five or long-year period. What about you, Tim?

Tim Morrow: Yeah. No, I think that's a good start. You know, when I look at it, I get the sense it's a full lifecycle, and that's the way you need to think about these things, but honestly, I was surprised myself by how many times inventory's in here, and I know that's something you

stressed as a challenge earlier, but I didn't appreciate I guess all the different inventories, and I was just wondering if you could expand a little bit why you think these inventories are important.

Geoffrey Sanders: Well, the different types of inventories here are really setting you up to understand your subjects, your resources, and the data that they're accessing between the subject and the resource. How that data moves, which also forces you to understand where that data resides, and the work flow piece, and then understanding, you know, "Why is that data important?" and that helps you actually fill out that mission execution piece, because you got to understand, "Why are these business functions occurring and where is all this data coming from?" and how many different areas or services a user may have to access.

So, you know, typically, when you go through a regular assessment, it may not be in-depth to understand how the mission actually works and what's critical to the mission, so these inventories really help you get very specific in what you're looking for and what you really need to assess to really understand what that journey is going to impact and what needs to be included in it.

Tim Morrow: That's excellent. It's--really, it's music to my ears. I love architectures and systems and those are the key things that come out as you're doing that type of architecting, is understanding the, you know, what you have in these inventories, where it's located. So I think this is a very important message that people need to consider, part of the, you know, what we're talking about today.

So how about before I flip to the next slide, Shane, is there anything you'd like to...?

Shane McGraw: Yeah, I got lots of great questions and comments, so if we could catch up on a couple, this would be great. I'm going to direct this one towards Geoff. This is from Mel. She said, "I read a definition that says, 'Zero trust is simply that we no longer trust where the request comes from but need to know who is making the request.' Is that a reasonable simplification?"

Geoffrey Sanders: Yeah. I think it's even simpler in that a core component of zero trust is identity. Understanding who that subject is, right. So the removing implicit trust, and typically we've done it in the past, is, you know, like nowadays, even in many websites that you use, you have a username and a password, right. There's some assumed trust in there that that password hasn't been compromised, that that user is who that is, and as that dynamic piece comes in, but when you look at the actual architecture, it all resides around, you know, who that subject is and what they're trying to access. So yeah, in a general term, yeah, that--I think that's a real good way of simplifying it.

Shane McGraw: Okay. Let's go to Tim for this one from Narayan, asking, "What is your view about justifying extra complexity and implementation overhead, specifically in the context of complex enterprises, parentheses (multi-layer application architecture)?"

Tim Morrow: Oh, man. I like that. That's something that we deal with every day here. You know, the big push on like DevSecOps and agility and trying to do things quickly, I understand that in that, you know, the waterfall has not been a good method for everybody because you kind of got stuck in steps. But I think getting a vision--and that's what we're going to talk about here in the next few slides--a vision of your system, having an understanding of what's important to you, what it needs to accomplish, I do think that takes multiple layers, multiple ways to view a system and understand those communication, those interfaces.

So I'm in a field where you need to have some architecture out here, and we'll talk about big systems, but we'll also talk about what do you do if you're just a small organization too? But, you know, I think that's a key part in here, yes. I hope that addressed that.

Shane McGraw: Great, thanks, Tim. So let's squeeze in one more if we can, from Joseph, and then we can move on. We've got some other questions and comments we can address later, but Joseph asks, and we'll direct this one towards Geoff, "What challenges are you seeing people encounter when considering implementing zero trust?"

Geoffrey Sanders: A lot of it is current architecture design, right. They don't necessarily have a great handle on what their current architecture looks like, and, you know, you need to have a good understanding of that before you can identify what the delta is to start that journey, and again, the one main thing that everyone is talking about is understanding your data. Where it is, who accesses it, and that ties back to that identity piece we talked about a few minutes ago. Data is, aside from the technology that you're having to implement to--implement for the strategy, the data is actually the largest lift, and it's the largest challenge for pretty much most every organization we've talked to.

Shane McGraw: Great. Thank you for that. We can move on, Tim. Thank you.

Tim Morrow: Yeah, great. No, thanks a lot. That was awesome. I appreciate the feedback we're getting, questions.

So this is where we're talking about the--how to implement the approach. So I think Geoff's done a really good job emphasizing the inventory assets, understanding your missions and things like that. So we're going to talk a little bit about each of these five areas and how they all kind of play into it. Is--and I always like to say, we're very fortunate at the SEI to be involved in so many different organizations at different levels and getting to see the challenges that they face, and one--these are some of the mechanisms or methods that we've come up with that help us

deal with that size or complexity. It doesn't really matter. We're finding that we can apply these in many places, so just wanted to share that a little bit with you.

And these are--we talked business mission threads. We're going to talk little bit about Systems Security Engineering, Model-Based System Engineering. I think a lot of people are hearing about Continuous Authorization, and then Geoff had mentioned our cybersecurity engineering assessments.

So I'll tell you little bit. So lot of times these terms are not familiar and lot of times you hear more on the DoD side of things, but, you know, when we talk about developing mission and business threads, you're really talking about getting a picture of what you're trying to build or what your system is. A lot of times you have existing systems. The people that made it aren't here, or the documentation isn't here, or even if you're trying to come up with new systems or emerging technologies in there, it's hard to get everybody on the same page. So we use an approach that you develop a vignette, which is kind of like a contextual diagram of your system and the interfaces it goes in, and then you want to run--have these threads that run through that system, and these threads, whether it be in a DoD side, you talk more of a mission which you're trying to accomplish, on the business side it's more of a work flow.

But you want to have examples that go across that whole system that allow you to look at what it is to do it successfully, and this will give you an opportunity to come back later once you've got a good picture to say, "Well, then where could I have problems?" and I think that's important. So having these threads--and these threads don't have to be complicated either. A lot of times I want it to be front and back, one page. I have 10 to 15 steps. So you want to go through at a high level. You kind of list out all your assumptions, your constraints, who's all involved in that thread, and documenting that, and a lot of times once you can do that and have two or three of these together, it's good to get the people in your organization to look at that and to verify that is reality and that is something that makes sense to you, and we wanted to incur operational lifecycle and development context so people are very comfortable with, "How do I work day to day?" The lifecycle is, "Well, do I think about my system 5, 10 years from now?" and development is like adding in new technology or content.

So I was wondering, Geoff, did you have anything you'd like to add in this area of your experience?

Geoffrey Sanders: So one of the great things I've seen about this, Tim, is not only the how the thread works in identifying the key components of an organization and what impacts their ability to operate, but all the external dependencies that they rely on that may not be completely obvious until you actually start talking across the organization. So this thread work is not only a great tool to document that, but it's a really great way of bringing the organization together. It's a mechanism, not just specifically a technical thing, but a mechanism to bring teams together to

understand completely across the organization and the organizational lifecycle what really matters from a day to day basis.

Tim Morrow: That's good to hear. To me, this is also some of the creative part of our work, because a lot of times people don't have this information in hand. So we get a chance to kind of think about it ourselves, do some research, then go back and talk to the stakeholder. So it's always a pretty engaging experience. I think it's a lot of fun to do this type of development.

The next area was dealing with systems security engineering, and most people--well, they always used to say, if I talked about systems, it's like, "Well, you're with the Software Engineering Institute. Why are you talking about systems to me?" and it's like, "Well, this is what feeds into what we have to work with with the software." If I don't have good processes in how the system is being built and developed and engineered, then, you know, it's kind of that garbage in, garbage out, and I didn't want to deal with that.

So we push more to the left in terms of a lifecycle, looking and focusing in systems engineering. So 15288 has been around for a good number of year. I recommend that for people, if you're architects or engineers, to understand your systems. Spend some time with that. That's a good standard to get used to the terminology for lifecycle for a system. The (inaudible) to the 160, both Volume 1 and 2, take the security focus on that, and then 60--the Volume 2 one is more of a cyber resilient. So it's kind of tuning in and focusing on specific areas throughout that lifecycle what you need to do to focus on security. The last NIST one is 800-37, it's the risk management framework.

So I kind of lump these all together and say, "What we're trying to do here is I want to identify some cybersecurity goals and I want to be able to build that into my system," and it doesn't matter if I'm just getting started or if I'm later on in the process, lifecycle process, there are things that at each stage in the process you need to have into your system, you need to be documented or you need to be figuring out how you're testing that information, and what we found is very important for us is we like to analyze systems. You know, I'm not the expert on a lot of areas, but if you give me a system and you give me these things that I'm talking about, the mission threads, the architecture, and an understanding of what you're trying to do, I can show you how to analyze that stuff. So that's why this is important, I think here.

Geoff, did you have anything you'd like to share in this area?

Geoffrey Sanders: Yeah, I think it's important also to take away too that, you know, we're talking really about a multi-year journey, a multi-near--a multi-year initiative here, and when you consider how quickly things are changing, personnel churn within a organization, people coming, people going, this is really essential, because when you're coming in to help an organization, the historical context may not be there. They may have been a startup and now a

couple years down the road they're much more mature, but all the business drivers as to why they were doing some particular security initiative within their organization, historically what that is, and does it match where they're at today, right.

So this whole process, in many cases when you're going within an organization, you may be--depending on where you land within the organization to help with this types of journey assessment, you may not have access to a lot of the lower-level details. So this process in itself brings that, not only that framework to bear, but actually helps you draw all those crucial details in that are going to be important to implementing those cybersecurity goals.

Tim Morrow: That's a great point, because I think we experience this every day now with--especially with the pandemic. We're seeing turnover in our staff and so multiple organizations are doing that, where, you know, you have different opportunity than we had before the pandemic. So coming up with some level of documentation around these things so that you can withstand losing people and be prepared for your future road mapping efforts, planning in what you want to be doing when, is very key, and it doesn't have to be these big, thick documents and things. It's more about what's important to you and what do you want to convey? So I think that's a good one.

We'll go to the next one then. So this is one, and this is one of our pretty pictures, and we talk about Model-Based System Engineering, and this is definitely something that is very important to the DoD right now in trying to improve the speed that you can get new technology into systems. Interoperability is huge, not only within, like the Army and the Navy being able to communicate, but with coalition forces where we're trying to talk with our friends and we see that, you know, it's very complicated. It's very hard to do these types of things, and one person can't think about that. I remember I worked on Joint Strike Fighter 10 years ago, and it's been around for a while, and I met the chief architect for the whole program, and, you know, it was amazing person but they burned out because there was just so much and they didn't have quite these tools.

So this is where I think it's really important whether you have a tool or you come up with a process where you do these things, where you have a system definition of what you're trying to do. It's a context diagram. You have a vision and a roadmap of, you know, "I know what my threads, what's important to me. I understand what's important in terms of system qualities." You know, for my performance aspects, my resiliency aspects, and being able to have a roadmap, have that plan ahead of where I want to get to in my system, and then we start talking about function.

So functional is, you know, you talked--spoke earlier about that happy day path, where if things were all going good, I want to have a path and a good understanding of my system of how it's really supposed to work, and then you can see what would be impacted if I have a problem, and

that's--some of our later analysis focuses on those areas, but functional again is just doing the things right. It's not worrying about the qualities as much there, and then we start to get to the logical and the allocated, where you actually apply it to something.

So you have some basic architecture that you get a sense that, "I understand how my system's working," but if I have to move it to the cloud or if I have to combination of--have some stuff that's on premise or some in the cloud, how you allocate that information, where that data is is very important, because you're going to need to capture logging information about that, and knowing where that is and how to get that, because as you go between clouds or what you did on on-premise, it's all a little bit different and it requires different skills from your staff to do that. So I think this is to be--important part for us, I know, more on our DoD side or the large organizations.

With smaller organizations, you can have diagrams that do this in real simple PowerPoint or whatever you like to do, but you just got to have things like this to have that vision and understanding of your system.

Geoff, did you have some other thoughts you'd like to share on this one?

Geoffrey Sanders: Yeah. What was really amazing to me, because I hadn't done a lot of systems engineering recently. It had been a few years ago, but when we started working with this in some actual MBSE focused tools, it was really amazing to me how these things link all these important elements together and help you understand how they relate, and not only just relate, but you can trace them throughout the architecture, the relationships, the requirements.

So having come from a background where much of the systems engineering was done with, you know, you have some requirements tools and PowerPoint and you have a lot of Word documents as artifacts, these MBSE focus tools are actually taking all the important stuff of the details, putting them together, and then you can take that out if you need to and put those into other artifacts that will hold the information and reserve it. But the MBSE tool is great in that it actually gives you a living, changeable model that links everything together, and if you're going to propose a change you understand how that one change affects everything else.

Tim Morrow: Right. Yeah, it makes our life easier, I like to think. I get--gives me time to think about other things, right, because in the past I'd have all these different volumes, requirements documents. I'd have, you know DoDAF views or I'd have different architecture views, test procedures, but now, with a tool like this, you can link that--all that together, and that's what's invaluable. So if you can do something like this, it's well worth it for bigger programs and things. But it's a good feature. I like it, so we'll go on to the next one.

Continuous authority to operate. So this is when, again, it's in a heavy focus on our DoD side of things, and what that is is trying to incorporate the Risk Management Framework. Your security controls how things are implemented, and I took this definition from--I'm sorry to jump around--there was a really nice article in "CrossTalk" in August, where these gentlemen kind of broke down continuous authority (inaudible), right, and I lifted that to make use of it here. So it's how you incorporate your controls, but then you have to monitor it. So like Geoff was saying about being in a multi-cloud hybrid environment, knowing where that information is that you need to show that you're satisfying your security controls, and doing it in a way that you can be resilient.

So I liked, you know, the first condition there was talking about the supply chain. It's one we've all been living through, and you--we've been warning us about for years, but, you know, understanding that supply chain and how that impacts your work and making sure that you understand how your controls are applied in that area. I think understanding the system--I always, like when we talk about a system, I draw a circle around something and I want to see every line that goes cross that, all my interfaces, all the way that that potentially impacts. You know, like Target years ago when they had a third-party, you know, coming into their network. Things like that is what you need to be able to visualize and understand, and the last one you think is exciting, because it's active cyber defense, and you think, "That's the thing that we're trying to get," as I think if you tie these all together and you have a good sense of what your system is, how those controls are tied together to your activities, to your threads, that you can see when an incident comes up what could be affected, because you've got, you know, some type of model and you have that understanding, but then also as a change comes in, you'll be able to adjust your system and be able to know where you have to focus on things.

So to me I think we're going to get to the point where continuous ATO is something that we can apply to a system, you could apply to your system, and have the level of comfort that you're doing a good job, and right now I think people struggle to feel like they're doing a good job. So that's kind of what I was thinking, but Geoff, did you have something you'd like to share?

Geoffrey Sanders: Yeah. I mean, having gone through assessments for decades now, it has--historically has been a very static type of thing where, you know, you'll have your assessment, your report. That'll be delivered and, you know, sometimes that can take weeks to months to a year, depending on how big the system is and how big the initiative is. With these Agile frameworks like DevSecOps and things like that, it's much, much faster, much quicker, big changes, should be a little smaller, and that pushes that whole static approach to now needing to be agile, continuous, and especially when you're talking about supply chain, where you may have some open source code that you're bringing in, you do not know how that has changed, this continuous method really is an automated thing that needs to be considered, and it's much different than the static approach organizations have taken in the past. So one of the key things is is not only understanding that but understanding that, I mean, even like DevSecOps in the DoD reference architecture is called out as a capability under a zero trust architecture.

So when you're talking about removing implicit trust and all those moving components in a DevSecOps environment, it's very important that someone has a continuous view of what they're accepting as a risk perspective within their systems and their architectures.

Tim Morrow: Right. No, I really appreciate how you tied that together, Geoff. Thank you very much. So we're going to go one more, and then we're going to check in with Shane to see how the questions and things are going.

So the fifth area that we focused on and that's part of the zero trust journey is the cybersecurity engineering assessments, and so (inaudible) Chris Alberts was someone I work with that developed this view for us, and I think it makes really good sense. So we have different levels of assessment, and, you know, it depends on what type of organization, what your size is, what your system you're worried about, and that's what we tried to tier these things to to help, to be able to figure out what's the appropriate thing.

So at the first level we have something called a Mission Risk Diagnostic, and it's kind of like a health check, where, you know, you take your temperature, you see where you're at in the system, just real simple thing, comparison, and then the next tier down is there's a SERA method which focuses more on the architecture. So again, this is where we're trying to make sure that we have the right information to be able to make assessments on.

The Cybersecurity Engineering Review is one that's more focused to that system security engineering, about are you doing the right things at the right point in a lifecycle? The information, the documents you produce, are they containing the right information to help you meet your cybersecurity objectives?

And then the last level is, you know, we have teams that do penetration testing, they do code analysis, vulnerabil--so there's things that once you pinpoint an area of a problem you dig down and actually go find out that problem.

So the remaining slides I have talks a little bit more about each one, but I thought it might be a good time just to check with Shane to see if there's some questions, because people would rather talk to us about their questions than hear about this method that would mean more to us.

Shane McGraw: Great. Thanks, Tim. Yeah, couple more questions coming in. We got a follow-up from Narayan asking, "Is there any example you can share where you've seen successful implementation of full-circle zero trust journey?"

Geoffrey Sanders: Yeah. I can't name specific organizations just based on privacy type stuff, but I can tell you there are some very large global organizations that are having great success in

implementing zero trust. But again, it really starts out with defining what it is that you're trying to accomplish with it, making sure that its initiative that the entire organization is buying into, and then starting small and iterating over those changes over time.

Shane McGraw: Great. Tim, anything to add there?

Tim Morrow: No. I think that that's a good approach, as trying to see that in a zero trust journey though, it talks about pilots, and that's what you need to do is you have to plan and you try to be successful because it's a challenge when you change things, right, and so that small planning gives you that opportunity to do that.

Shane McGraw: Great. So let's go to Tim for this question from Alexander, came in earlier, regard--it said, "How does NIST or other models fit into operational technology network, such as that found in electric power system?"

Tim Morrow: So I think the thing is NIST is just providing examples or frameworks of things of how, you know, they can be applied to a different situation. So yeah. I can apply that. I know NIST has its own standards dealing with electric power systems that you can follow, and I know co-workers had worked on this a few years back here at the SEI. I think if, you know, if you're looking at a system, it's still like from a lifecycle point of view, the ones that I mentioned, work out just fine to be able to break apart your system and think about it, you know, whether it's a electrical power plant or if it's, you know, an airplane or a ship. We applied these things, you know, the same type of way, so I'm not sure if that's a good, crisp answer, but I have no problem--I guess the answer's always good from my point of view when I use a NIST standard or a, you know, a document to help me figure out or analyze a system.

Geoffrey Sanders: Just to add on to that, Tim, kind of one good example that I've seen us doing is our Model-Based System Engineering tool, is when we're actually modeling that architecture, the capabilities and all those types of things, and this applies to zero trust, is you're able to take a lot of those NIST control mechanisms that you're wanting to validate against and put them into that model and add them to your traceability and actually link them to particular views of your architecture. So as Tim said, these--the NIST tools are great frameworks. They're great pieces, and one of the key things is, really the question back to you, is how are you going to take those and implement them in how you're managing your lifecycle?

Tim Morrow: Right. (Inaudible), Shane, for us, I think we have--we'll have our--Next Steps would be the next slide that we do. We'll kind of skip over some of the assessments if you have a few more questions, because I think we're I good shape for that.

Shane McGraw: Right. So we do have two more, if you said you do want to take them now, Tim, or...?

Tim Morrow: Sure.

Shane McGraw: Okay. So first, just a comment from Rinaldo, and then we got a Terry--a question from Terry. Rinaldo's comment was, "A research project I would like to see is inferring data relationships from network traffic." So I don't know if you guys are aware, is there any research at the SEI or otherwhere going on in that area?

Tim Morrow: I was going to say that's one thing that my boss has told me about needs to be important in our work going forward, and I think it's the, you know, the architecture's going to get me to the point where I understand what data is going over, you know, which communication paths, and then I think going forward is for us to set up some prototyping efforts and pilots to start to look into questions like that. So a lot of times I like to say the work that we're doing is putting together enough of a, like, a testbed, a shell, so that the people that are really into doing data analytics or different things are able to start and think about it without all this other clutter going on. So we're getting to the point where we can make that easier for people to do but I think I would share that with somebody else can be doing that stuff. I know there's line--at our place, line proposals talking about doing this type of stuff, but maybe Geoff, you know more on this or can share anything?

Geoffrey Sanders: Yeah, I can't point to anything specific by name. What I can tell you is when you're working with organizations, and it is on our radar for research, because in typical perimeter defense models, you're having to do things like intrusion detection system alerts, SIEM tools, flow collection and analysis, and when you're--now when you're transitioning to zero trust, you're now looking at pretty much, you know, a total encryption model where flows between information systems are encrypted. There's really nothing for an IDS unless you're putting it in line somewhere where it has decryption access.

So much of this, this journey, is because that organization may have a very unique monitoring model, is, number one, understanding that data that we talked about is, you know, what does your organization require to identify intrusions and to monitor, and then change that to how does that translate to when you're outsourcing your ICAM, when you have a hybrid cloud where you're having logs that are not necessarily totally under your control? So this framework in itself does help that, and we are looking at some of the specifics, you know, how to, "Okay. Here's how we've done monitoring in the past. How does that need to switch to these new types of integrated environments?"

Shane McGraw: Great. Thank you both for that. We'll--one more question from Terry, and then we'll let you guys wrap up with your closing thoughts. Terry wants to know, "What are technology options for implementing micro segmentation? I know VMware NSX is a common solution. What other options are available?"

Geoffrey Sanders: So as have--already see, we don't go out and pick any particular product. I would say look at all of the solutions out there. When you talk micro segmentation, really you're going to be looking at your architecture in two different ways. You're going to be looking at traffic from north/south, and then you're going to be looking at traffic from east/west. East/west is typically that micro segmentation model where you have containers that are talking to each other and a very dynamic environment that's changing when you're talking about containerized applications.

So one of the big words with zero trust is called software defined perimeter. Okay. That is a particular type of technology, not a particular vendor, but if you look up for zero trust architectures, zero trust solutions, and start digging into the details, you will find that there are different providers, and then you have to do that tradeoff analysis. Does it integrate with our ICAM? So saying that you have, you know, five or six things to look at, it really isn't accurate either because you as an organization need to sit down and define what those requirements are to even say that, "This is a zero trust solution we should be looking at."

Shane McGraw: Great. Thank you for that. We're all caught up so we can move on.

Tim Morrow: Okay. Sounds great. So Shane's going to make the slides available. I'm going to just jump through the assessments that we talked about, but we have reports at the SEI website on these assessment methods that you could go look at, as well as you can reach out to us too. So I'm going to jump--whoop, sorry. Jump on down to Next Steps, and I think this is back to you, Geoff. You want to take a pass at this?

Geoffrey Sanders: Sure. So really next steps is, you know, where does this research go? Well, we're looking at actually piloting these assessment methods, documenting the specifics, definitions and all, into a zero trust journey paper so we actually can define what this means from taking that diagram he showed with those four areas and the assessment across all of those areas. We're going to actually start specifying what that really means, and then looking at, you know, how do we apply the cybersecurity engineering assessment practically? How you take this journey and actually execute it, and then going through and providing some type of example enterprise journey using it. So, you know, we're pretty excited about--because a lot of this is historical work that we're just able to adapt to zero trust and add those zero trust specifics in, and we've had some great success, so we're looking forward to leveraging it for zero trust as well.

Tim Morrow: Absolutely. I think the thing that we enjoy is the application, the implementation, working with people in that, because we always learn it's--everybody's unique, and I think that sometimes that people forget about in these areas. That we try to have a cookie cutter approach or a standard thing, and it's like, "No, you really have to listen and help people adapt to what

their world is, help them understand what's really important to them," and I think those are the fun things that we are looking forward to doing in terms of pilots coming up, so thank you.

Shane McGraw: Great. So we got one more question. We got about two minutes left, so if we could just squeeze in one more question, then we'll wrap up, if that's all right with you guys, and maybe I'll start this one with Geoff, and then we can let you add on, Tim, is, "What organizational commitment challenges do you have for zero trust adoption, or have you seen for zero trust adoption?"

Geoffrey Sanders: Well, so when we do assessments, in many cases, you know, depending on where you come into the organization, they may need help with something specific, so you're really pulling teams together. The overarching challenge with any initiative is, number one, buy-in, so if you're working with a small group that wants zero trust and that hasn't been either propose to the higher-lever C--the C-level folks who are actually going to allocate the funds to do that, that's an important thing you have to consider. So it's not that we have seen any unique challenges. Really at the end of the day, when you talk about enterprise initiatives, typically these are not technology problems, right. It comes down to a combination of people, process and technology, and usually the hardest part of any initiative is the human piece.

Tim Morrow: Right. I think the other thing is a lot of times these things are mandated. So like federal agencies are being mandated to implement zero trust in two years. So, you know, when you think about that, you're like, "Jeez, that's an awful lot to try to figure out and do in such a short period of time," and, you know, as Geoff said, you can't just go out and buy a complete solution, so it's going to take some work, and I think these are the challenges, real challenges that someone has to face in terms of zero trust.

Shane McGraw: Geoff and Tim, great discussion today. Thank you very much for each of you sharing your expertise.

Geoffrey Sanders: Thanks for having us, Shane.

Shane McGraw: Great.

Tim Morrow: Yeah, appreciate it.

Shane McGraw: And lastly, I want to thank you all for attending today. Upon exiting, please hit the Like button below and share the archive if you found value. Also, you can subscribe to our YouTube channel by clicking on the SEI seal in the lower-right corner of the video window. Lastly, join us for our next webcast, which will be next week, on October 13th, and our topic will be, "Five Things to Consider When Threat Modeling Cyber Physical Systems with DevSecOps

Practices." Registration information is available on our website now and will be emailed out as well.

Any questions from today's event please send to info@sei.cmu.edu. Thanks, everyone. Have a great day.