Shane McGraw
Hello and welcome to today's SEI Webcast Ask Us Anything- The Zero Trust Edition. My name is Shane McGraw, Outreach team lead here at the Software Engineering Institute, and I'd like to thank you for attending. We want to make our question and answer as interactive as possible so you can submit your questions in our YouTube chat area now or on LinkedIn or Twitter.

And use the hashtag Ask SEIZT and we will get to as many as we can. Our featured speakers today are SEI CERT Division Director Greg Touhill and Dr. Chase Cunningham. Now I'd like to introduce Greg who was appointed by former President Barack Obama as the first chief information security officer of the United States government. Previously, Greg served in the Department of Homeland Security as a deputy assistant secretary in the Office of Cybersecurity and Communications.

Before joining the SEI he was president of AppGate Federal. Mr. Touhill was also a 30 year veteran of the United States Air Force. Chase, also known as Dr. Zero Trust, is a recipient of several media companies Most Influential People in Security. Dr. Cunningham is the Chief Strategy Officer of Ericom Software. Previously, he served as vice president and principal analyst at Forrester Research, where he provided early and strategic guidance, on zero trust, artificial intelligence, machine learning and security architecture designed for security leaders around the country and around the world.

Prior to Forrester, he was a Navy chief Cryptologist at Fort Meade. Welcome, Greg. Welcome, Chase.

Greg Touhill
Hey, thanks. How are you today?

Shane McGraw
I'm great. Chase welcome as well.

Chase Cunningham
Hey, thank you for having me. I have to inflate my resume any time I'm on with Greg, trying to make myself look better so I have to write more stuff.

Shane McGraw
Absolutely. So it's a Friday afternoon. It's 70 degrees outside here in Pittsburgh. The NCAA tournament is all. But what better place to be here talking zero trust with you guys, correct?

Greg Touhill
Absolutely.

Shane McGraw
Great. So we have had lots of great questions come in already. So we're going to we're going to dive right into them. And again, if you have questions, feel free to put them in the chat area now.

So we have to level set here first. Okay, you guys are going to explain what Zero Trust is? What's its core principles? How long it's been around and why it's such a buzz phrase now? So, Greg, we'll start with you on that one.

Greg Touhill
Well, there's a lot to decompose on that one, but let me just give a quick overview here. You know, ultimately with Zero Trust, I contend it is a strategy and it's not necessarily all that new. Back in the early part of this century, 2004, the Jericho Project, which was centered out of New Zealand but had contributors from all around the world, posited a security approach that was focused on least privilege and ruthlessly enforcing least privilege, such that Greg could only see what Greg was authorized to see under certain conditions and entitlements.

And we always wanted to have that kind of approach, but we didn't necessarily have the technology or the mature infrastructure to go do that. And that's evolved into the zero trust approach. John Kindervag, our colleague that Jason I work with on a regular basis. John Kindervag was to Forrester and coined the phrase zero trust to describe this environment where you assume breach, you never trust but always verify.

And it's built on the tenets of strong authentication, network segmentation and if you can get the micro segmentation, all the better, ruthlessly enforced, at least privileged so that you only see what you're authorized to see and nothing else. And then also continuously verify, you know, and monitor to make sure that you don't have that situation where you turn it on and you're always on.

No, you're rules and your entitlements are always going to change. And you should always be continuously making sure that Greg can only see what Greg's authorized to see. And so I would contend it is no longer just a buzz phrase. It's actually a useful and I believe, a requisite security strategy. And finally, you know, we were doing this in the physical world for many, many years.

You know, when I was in the Air Force and a base commander, we certainly had zero trust. We had security forces personnel running around with use of deadly force authorized if you crossed into the wrong line. So we were doing zero trust in with nuclear weapons and high value assets throughout the military. Now we're taking that same approach into the digital world.

Chase, what are your thoughts.

Chase Cunningham
Well, I think the one thing that is interesting here is that the buzz is not a bad idea. I mean, I actually like that the buzz is the buzz because I want people talking about this. I had a call this morning with people in Australia. I had a two days ago with folks in mainland Asia are on the whole ZT thing so the buzz is not a bad thing.

I think we're also at a stage where the question kind of becomes, if you're not engaging in this strategically, what else have you got? I mean, we've got 30 years plus of failure. We've seen

what doesn't work and we continue. You know, you have two choices. Either continue to engage in a failed practice where you have seen major organizations, the DoD, etc., fall like a bunch of leaves in a hurricane or approach it differently and put this strategic approach in place and start to take back the initiative.

So I mean that I think that's really the crux of where we're at now, and it continues to evolve. That's the beauty of a really good strategy, is it is not this thing and nothing else. A really good strategy is it evolves, it changes, it grows, it migrates, it integrates, new technology. That's where we're at with ZT.

Shane McGraw
Thank you guys, both, for that one. Let's go. We got one from Ed- a little bit long but give me a second. I'll read it off to you. And we're going to point this one to Chase first. So, Ed asked, I do not think that ZT can avoid all threats to a system. I believe that is necessary to use a secure development methodology for each application where its threats are enumerated systematically, and countermeasures for each one are added to the system.

For example, how are the PE and PA protected? How about interactions between applications? I'm also concerned about the overhead introduced by checks that evaluate trust. What do you think about my assertion? Chase?

Chase Cunningham
So, number one, just systemic, right? I agree with any assertion that says that nothing can stop everything because that's a reality, right? There is no perfection. There is no you will stop everything carte blanche, whatever. There's no ZT button that will just make you never have a compromise. As a matter of fact, that's why we have this main tenet about assume breach.

I assume everything is compromised even when I have the strategy in place. So, agree there. The other piece, and I assume he's talking about 800-207 is talking about the PE / PA. Really, what I think you're scratching at is the need for visibility. And that's why I created the ZT X framework. When I created the framework, there's components in that framework that cover things like visibility and automation, analytics and orchestration, those types of things, because we need to see what's going on so that we know where to apply controls and can vector in on the problem set. Your last point really, and this is there's studies that are published on this and there's more coming out. Organizations that engage in effective security strategy actually see a freeing up of resources and better use of the traffic that is bouncing around their networks because not everything is of value like right now if you're just doing security, you're kind of sitting up on a hill with one pair of binoculars, chewing your fingernails, hoping you see when something comes by. But you've got to be just nonstop scanning the horizon. Not an effective strategy for actually dominating the space Instead, it makes more sense to have really good vectors, really good segmentation, isolation, control, see what's going on, see what's traversing. And then when a problem is evident, vector in on that, everything is not of value. And there is a difference between data and intelligence.

Shane McGraw
Greg, anything to add there?

Greg Touhill
I think Chase nailed it. I think it is. If you looked at a supplement that, you know, as you take a look at the concept of trying to isolate yourself from any attack, that's a fool's errand. For my military background, we always took a look at ourselves as the ultimate risk managers and the fact that the adversary is always going to get a say.

So the factoring in resilience is one of the key things in the risk management business. That you can take a punch and keep on going. And as we take a look at zero trust security strategy, we're not guaranteeing that you're not going to take a punch. But I would virtually guarantee that you're going to be able to keep on going once you implement the strategy.

Shane McGraw
Greg, we're going to stay with you for this one. Joe asked, I hear the term zero trust strategy and zero trust architecture, how do the two differ.

Greg Touhill
I think if you take a look at strategy itself. Strategy is a framework for addressing a series of actions. Normally you have a strategy and then you also have subordinate plans to achieve that strategy with the strategy telling you, basically, here's where we need to go. And these two things we want to accomplish. And the thing about zero trust security strategy, a lot of folks get wrong is the destination is not zero trust. Rather, it's the starting point.

And you start with zero trust by saying, I'm not going to trust my hardware, my software, my whatwhere, the people, you've got to verify that. For example, Greg has the appropriate access to my data, to the systems, even the physical aspects. I don't get into a facility if I'm not authorized to be there.

So you take a look at the strategy. It's an overarching concept of trying to get to a certain conclusion. When you take a look at Zero Trust architecture, it's a technical approach to achieve that strategy. And that zero trust architecture, it can be much more than just your standard information technology network topology. It should also incorporate such things as your personnel security, your physical security.

That also should be part of that zero trust architecture. And then further, you can drill down to a subordinate, to that zero trust network architecture. So they're complementary, but it all starts with the overarching zero trust strategy for the organization.

Shane McGraw
Thank you for that, Greg. Moving on. The one for Chase here from Paul asks, what are the current attack trends and does zero trust to address them all?

Chase Cunningham
Well, back to earlier, nothing addresses all. So that's a pretty broad term. But the most common attack trends, which are the same attack trends, other than a slight variation that we had ten years ago, are still pretty effective. Phishing, bad passwords, compromised VPN creds, those types of things. And then ransomware mixed into that whole fray. And I still, like I'll die on the hill, I fundamentally believe ransomware shouldn't be the problem that it is, because if you look how most ransomware is invoked, it's PowerShell. PowerShell is not something that most people need access to. Therefore, applications should be isolated to eliminate that type of activity.

Phishing just, you know, slightly controversial opinion here. Phishing should not continue to be the issue it is, if we had phishing training the way that it's in place and if we actually took controls and put them in place of the user where they can't interact with malicious content.

And then lastly, passwords and VPNs, we should be able to move past that pretty quickly. If we actually took the right approach and solved the problem the correct way, because it's not really that big of an issue. I haven't used a password in, I think 120 days. I'm all biometric now, and I'm not worried about whether or not my stuff gets compromised because I do have other ways of authenticating. But I'm also not worried about whether or not someone uses a crappy password of mine to log into my stuff.

Shane McGraw
Great. Thanks for that, Chase. So we have a little bit of a backlog here and the chats have been very active, so we're going to catch up on a couple there. Greg asks, and Greg will point this one to you. He asks, what is the best standard for measuring the maturity of our enterprise Zero Trust Architecture?

Greg Touhill
Well, thanks, Greg, and great name choice too, by the way. You know, as you take a look at the maturity of enterprise zero trust architecture, as you say, the folks at CISA, the Cybersecurity and Infrastructure Security Agency have put together an enterprise zero trust architecture maturity model under the leadership of my friend and colleague Sean Conley.

That's a good starting point for that, where you go and you take a look at the five pillars that they've proposed there. But you know, if you take a look at that, we are actually here at Carnegie Mellon, in concert between the Software Engineering Institute here that I belong to, as well as at the Heinz College, which I also subscribe to. And I'm a professor there. We've got some of our students that are working with us to put together an automated capability to quantify as well as qualify that maturity model. And I think you're going to see as our research and others continues to grow that maturity model that CISA has put out, we're going to be able to supplement that with some tools and capabilities that are going to help you better understand where you stand in that journey by better leveraging the data that you already have.

And I know, Chase, you've been an advisor to that group of students over at Heinz as well.

Chase Cunningham
Yes. I 1000% agree with everything you're saying that it continues to evolve, but evolution is what we're looking for.

Greg Touhill
And Shane. Looks like you're on mute for a sec.

Shane McGraw
So we had a question from Danielle and also one from Sridhar are in the chatroom that we will try to combine. Danielle's was how does zero trust reshape cloud security. And then Sridhar asked is about multiple things in the cloud. How do you make your product zero trust a multi-cloud environment? Is there a way we can combine those two questions?

Chase Cunningham
I'll take a quick swing. Really, when you're talking about multi-cloud we're all going to be hybridized in some way, shape or form. I mean, if you look at the data, the trends, the statistics, you're going to wind up in some sort of hybridized infrastructure that's actually not, in my opinion, a bad thing. It does make it a little more complicated, but it actually kind of, if you think about it, enables segmentation and isolation based on the hybridized model.

There are things you can segment within that that can help you there, instead of just the cloud. You have AWS for process and compute, you have GCP for this, you have Azure for that. And those things should be isolated and segmented, controlled along with the things and components inside of that. So I think that that's part of it. The other piece I personally am a huge fan of the is cloud migration. I think that that is the, quote, easiest place to build the ZT infrastructure from the ground up. It's really difficult to go reverse engineer something that's been there for 30 years or more and is generating revenue and is kind of a warm fuzzy box in a data center and make that ZT.

So it's a good thing that cloud is as pivotal as it is. And I personally believe the cloud is where you go to enable ZT make it quicker, better, faster.

Greg Touhill
Yeah. And I'll pile on onto that. As you take a look at zero trust in a multi-cloud environment or hybrid environment, you know ultimately you're going to have to trust at some point. And most folks can't even trust if they're running their own infrastructure, particularly with cyber workforce gaps and other deficiencies that are out there in the real world environment.

So going to a provider that has proven themselves through such certifications as FedRamp and some other activities, can help you in your zero trust journey from the standpoint of minimizing the amount of risks, having the ability to have auditing and some other controls out there, and then complementing with technologies such as software defined parameters that can give you more positive control of your data that's going in and out of those environments.

So as you take a look at the multi cloud or hybrid environment that is out there, you're never going to get the risk to zero, but you have access to actually increase your operational efficiency at scale, and at cost. Savings that could better manage your enterprise risk.

Shane McGraw
So Stephen had a question. Comment, if you guys can chime in on this. What can we say that Zero Trust is a setup that allows risk management by exception?

Chase Cunningham
Allows for its managed by exception.

Greg Touhill
I'm not sure I understand what that means. I go back to Stephen and ask for what does that mean? What's the context?

Shane McGraw
So Steven, if you're there still, can you chime in with a little more context on that question. We'll move on to the next one from Dan asking, again a little bit longer, but just bear with me. How would you describe the point where a minimally viable zero trust strategy is in place? Basically, what is the strongest key indicator that an organization has a minimally viable zero trust strategy operational? I'm thinking in terms of organizations currently utilizing a network cybersecurity approach, looking into transition into Zero Trust, it seems it could be a balance of the technology used, maturity and policies and processes and a threshold of data holdings protected by zero trust.

Chase Cunningham
Sir, you want to go first?

Greg Touhill
Yeah, I'll take a crack at that. And then you could provide color commentary. You know, I think as you're taking a look at a minimally viable strategy, it starts with the leadership. And leadership not only stating the strategy, but following up with the appropriate governance, funding and oversight of the implementation of the strategy, which has to be accompanied by a plan of action and milestones.

So I don't think a strategy is a viable strategy unless there's a plan associated with it- that it's funded, it's got good governance and oversight, and there's discrete milestones to measure it along the way. And then further, you know, as we were talking about implementation of the Zero Trust strategy and go back to Sean Connolly's model from CISA and taking a look at those five pillars, I want to see the plan touch upon all five pillars and how I address them and consistent with the zero trust principles that we already talked about, assuming a breach.

Never trust, always verify. Strong authentication, network segmentation, least privilege, and continuous monitoring and verification. I think those are components of that strategy and the implementation of plans to go with it. That's what I would consider the bare minimum. Chase?

Chase Cunningham
I think what's super useful in the context of kind of checking where you are in the ZT world, is do a red team event. I don't mean pentest, I mean call in some Red Teamers. Let them go at your organization like the bad guys would and see what happens and then take note and start implementing your ZT plan. Follow on from that.

Then I think you should go back and do the same thing again. I think you should do it at a certain regular interval, because if they continue to eat you alive the same way, something is wrong with your plan, your infrastructure, the way that you're putting things in place. And if you can't do that, then how will you ever combat the adversary, especially in a real world scenario? Because the bad guys are not going to come in and go, here's four IP addresses, here's three applications. I want to go with this. Can I do it from eight in the morning to four in the afternoon? That's not realistic. It's not a real world. And until you know, back to what General Touhill was saying, until you survive first contact with the enemy, you're not going to be prepared for when the digital lead starts flying.

Greg Touhill
Yeah. And Chase, you know, you and I have got plenty of experience with red teaming, but I'm not sure everybody in the audience knows the distinction between pentesting, hunters, and Red Team. You might want to expand on that a little bit.

Chase Cunningham
Sure. So when I say pentesting, penetration testing, that's basically where you'll contract with someone and they'll say that's a very quantified, very sort of minimized bounded approach and what's going on? And it's not there's no value and I think you should pentest, but the pentest is very structured and it's carefully curated. A red team is when you're going to get a group of individuals who are going to come at you with everything from social media exploitation to wireless exploitation, anything that you could think of that an adversary would use, in your crazy dreams, that's what a red team is going to do. And that is if you put a pentest against a red team, you will find different results every time because they do different things.

Greg Touhill
Yeah, absolutely. And one thing too for consideration is, you know, all too often we get targeted fixation on the digital enterprise. My experience with red teams is we were looking at physical attacks, physical penetration drills, getting into the facilities so we could monkey with critical infrastructure, all of the above. So when you're thinking like a hacker, you need to be thinking even more like an adversary and not limiting yourself just to the digital enterprise as well.

Shane McGraw
Great. Thank you guys for that. So we got a question in the chat as well. And I don't know if this is your expertise. I know we have staff at the SEI that work in this area, so if it's not your area we can maybe get an answer down the line, but how can we employ zero trust in the DevOps pipeline? Can we divide it along the pipeline? Could it bring benefits when it's applied as infrastructure as code? Either of you want to jump on that one?

Chase Cunningham
Well, I would say that you can employ the concepts and strategic values sort of side of ZT on to a DevOps pipeline. I personally am a fan of leveraging virtual infrastructure to do your testing before it ever moves anywhere before production, and then doing those things around that. But to say unequivocally, you know, here's an evaluated sort of reference on how to do ZT for devops that's still being built out and still being developed by folks that, like you said, are hard core DevOps engineers.

Greg Touhill
Yeah, I'll jump in and give an example. You know, as you take a look at DevSecOps, which I'm a big fan of more, I would say all DevOps should be DevSecOps, but we've got some organizations out there that have been doing some really great work in employing Zero Trust as part of the development of code. And Platform One that the Air Force have been using as one of their development platforms is built with Zero Trust as a key component to their strategic approach to building towards a DevSecOps environment, where they're using zero trust principles and not only the remote access for all the different coders that are coming into the Platform One environment. But also, how they control and monitor all the artifacts, the artifacts of the coding that's going on. So, you know, we've got some good examples out there of some of the software factories in the military now starting to adopt Zero Trust as a strategic approach to protecting the integrity of the processes as well as their code base. And I think we're going to see even more as this movement matures.

Shane McGraw
Thank you for that, Greg. Another great question here from Christopher asking, how do you sell zero trust to the rest of the business, especially when trust is a major part of the culture? Any comments there?

Chase Cunningham
I'm sure General Touhill can knock that one out oof the park.

Greg Touhill
Yeah, let me take a swig of my beverage here.

Christopher, that's a really good question. Here's what I hope is an adequate answer. The thing about it is, I wouldn't necessarily use the verb selling in this particular case. I think coaching might be a better verb for this. So how do I coach my corporate governance process as to the value of the zero trust security strategy across the organization?

What kind of return of investment can I show for that? I think really- is you go out there, you can take an evidence based approach as to what's at risk and how you can better manage your risk by implementing this strategy. And as you take a look at the key principles that are out there, if you're able to qualify or quantify that improvement and risk the lessening of risk exposure, sharing of data points from those who have already been victimized and those the lessons learned from those who have implemented the strategy, I think you can build an effective business case so that it'll stand on its own and become a much easier decision for not only the C-suite, but for the boards of directors out there as well. I'm aware of several companies that have implemented Zero Trust, and as Chase hinted at earlier, they actually saw a cost savings with a relatively rapid return on investment time where they actually streamlined and simplified their network architecture. They were able to retire older gear like VPNs and NAC, network access controls. You know, VPNs came out the same year as Palm Pilots and Network Access Control is almost as old as a kid getting his driver's license.

So, you know, as you take a look at some of the savings that are out there, the data is now gathering up to the point where you can make an evidence based argument to show where the improvement in security and the return in investment makes it a good business decision, regardless if you're in the public sector or the private sector. Chase, any thoughts on that?

Chase Cunningham
Well, actually, I'm working on a paper around this, and I think that there's a point to make here when you're talking to people that aren't in the security space. And I remind them of this in my workshops. It's zero trust, not zero faith. I'm not saying I have no faith in my employees. I'm not saying I have no faith in my business to do what it needs to do for the purposes of work. I'm saying I'm working to remove trusted, threatening relationships from within infrastructure and within IT. And that is a categorical difference. So that might be something you work into that conversation of this is a zero trust strategy. This is not I have zero faith in our employees.

Shane McGraw
Thank you guys for that one. Next one. And it may be this may be a similar answer to what you guys just gave Greg, because it's another kind of a hypothetical. But how do you get end users to accept the cost and inconvenience of zero trust security, the inconvenience of time and effort to set up increased management of varied users, more devices to manage, more complicated app management?

Greg Touhill
I actually thank you for that. I, I don't necessarily agree that it has to be complex. I think if you do it right and we're going to simplify so you know, having been engaged in the Zero Trust movement for pushing a decade now, I actually think there is an effort towards simplification. And let's remember this simplicity is the arch nemesis of our adversaries. Complexity, on the other hand, is the bane of security. So if you're doing it right, you should be retiring some of the old stuff. You should be kind of giving your network- say it's one of those things that they do with

the cardiac patients where you do the angioplasty and you're opening up the pathways. And then, you know, as you take a look at really what the biggest costs are.
You know, we did a survey of our alumni core from the CISO certification course that the Heinz College teaches here at Carnegie Mellon. And the survey showed that as we were taking a look at those folks who are in CISO roles and similar peerages, we said, you know, what is the biggest cost that's associated with implementing that zero trust journey? And, you know, as you take a look, we had 48.5% say that understanding and cataloging your data, as well as the access and control rules, you know, who should access that data under what conditions and entitlements. That actually was by far the largest cost that was associated with zero trust.

Now, I look at that and say we should have been doing that all along, not just as a trigger point for zero trust. We should have been making sure that we had positive control over data and know what data we had, where it is and who should access it and what rules. And Chase and I have talked on numerous occasions about, how many folks out there have an Active Directory structure that is properly populated and managed.

Yeah. I think that you take a look at costs. Some of those costs that folks are now attributing to zero trust are things that we should have been doing all along. And we're playing catch up on what the payoff is going to be lower cost, more simplicity, and most importantly, a better user experience and security for those who successfully make this journey.

Shane McGraw
Next, we got one from Carlos and I might combine it with one from Ademola as well. Carlos, his question was, what are your thoughts on Zero Trust strategy for embedded systems? Do you think it's possible to deploy to the significant performance impact associated with Zero Trust and low resources of embedded systems? And Ademola's question was, do you have a reference article or whitepaper that you can suggest for applying zero trust in embedded systems? Greg, you want to start with that one.

Greg Touhill
Well, hold on. I'm making a note here on that. Yeah, Okay. So, you know, as you take a look at embedded systems, it really depends on what your definition is and how far you want to go. But taking a look at the 20,000 foot level and then I can dive down from there. Ultimately with zero trust, we talk about network segmentation and getting into micro segmentation.

You go as low as you can go based upon what I call the FASA rule, feasible, acceptable, suitable and affordable. I'm not going to be able to segment down to the chip on an airplane at this point, you know, particularly something like an F-15 or an F-16 or operational technology that's out in the field. But I try to network segment down to the lowest level possible.

And I continue to use those principles down till I get to an acceptable level of risk. And I'm going to have to assume some risk at some point. So as I'm taking a look at embedded systems and that could be a weapon system in the DoD. It could be critical infrastructure or some sort of

operational technology. I'm going to get to a level of trust that is feasible, acceptable, suitable and affordable.

And then I'm going to say, okay, I have done my due care and due diligence, and I'm going to make sure that I have other mitigating controls and capabilities in place to maintain that level of trust, but I'm consistent with the strategy, and that's the way I look at it. Chase, you have some thoughts as well, because let's see you squirming on it.

Chase Cunningham
Well, I think that the embedded systems one is super interesting. I can't go into specifics, but I remember specifically working on penetration testing and exploitation around missile systems when I was still active duty. And I would consider those to be pretty embedded systems with lots of moving parts and, to your point, the issue was that there was actually being able to see what shouldn't occur, not that everything should be taking place and that there was the connectivity, because the connectivity was actually the flaw in the system, the open avenue connectivity. So I agree with you. I think that it boils down to an acceptable level of segmentation and isolation. However, there are still other things that you apply in the context of a strategy that would eliminate avenues of compromise. So just keep that in mind.

Greg Touhill
Yeah. And I'll just do a final double tap on that one. You know, we do have folks out there and I'll give a shout out to the Air Force for creating an organization that is actually looking at the cyber resilience of weapons systems. They call themselves the Crows Team. And in full disclosure, we at the Software Engineering Institute have been providing support to Crows, but they're taking a look at the embedded weapons systems and making sure that they have cyber resilience and, getting back to what Chase said, going in red teaming those type of embedded systems and seeing what your risk exposure is, is a really good starting point for determining the best approach to implement your zero trust strategy to better protect those types of embedded systems.

Shane McGraw
Okay, great question from Dennis asking, and we'll point this one to Chase, says ZT policy, and SP 800-207, is expressed in terms of subject, objects, the risk of that access. How do you see progression of the expression and orchestration, the zero trust policy over underlying zero trust architectures?

Chase Cunningham
So I think this goes to stuff that General Touhill's talked about a lot is, I think the next evolution of that will be, and we've had some calls with the folks at NIST about this around the ability to identify, isolate and add in the data side of that equation. Because right now it's great. And you also have to remember that this was kind of written around the concept in really big broad terms around like object oriented programing. So that's kind of why it was this thing that they put into there. But the last line in this will wind up being, I know where they're coming from. I know how they're getting there. I validated that they're supposed to be there. I've checked their posture.

They can get to the resource. Oh, and by the way, when they get to the resource, the only thing they need for the purpose of their work is X and that entire chain will be running inside of that secure pipe, that secure infrastructure, however that mechanism works.

So that's where we're going. And I think that that will be. And the reason I say I think is I know that that's what's coming within some of the iterations of 207 that is going to be part of that progression. And if you think about it, that makes so much sense, right? I mean, that is I'm from Texas. I say, that's your Alamo, all right. I want to make sure that the end of the day, well, it didn't work out really well for the guys in the Alamo historically. But anyway, the Alamo is a good thing if you do this correctly.

Shane McGraw
Next one. Let's go to let's go to Greg on this one. Greg, Terry asked, I have heard people mention that we can use existing technologies to implement zero trust concepts. Can you provide examples how an organization can use existing technologies?

Greg Touhill
Yeah. And well, let me take a step back, breathe through the nose on this one, because I'm pretty excited on this one. You know, having been a government CIO and I ended my military career as the CIO of US Transportation Command, which oversees the transportation of our logistics to our warfighters all around the world. Yeah, that's a pretty big job and a pretty big enterprise that's out there.

And we were doing a lot of great work on improving, for example, our identity management. And, you know, IDAM, the identity and access management controls, that's a key component of implementing a rock solid zero trust security strategy. Implementation is making sure that you have a great identity capability. And oh, by the way, there's lots of different vendors that are now in that space that provide capabilities so you can pick and choose and pick the business case that works best for you, and you can layer identity that's on there based upon your risk profile. So you don't need to, you know, rip out your identity capability if you've already got something that meets your risk capabilities and it's affordable, you keep it. But as you take a look at your whole network enterprise and as you're taking a look at building out your sort of trust network architecture, any CIO, any CISO out there, chief information security officer, they should always be looking at opportunities to do improvements to their architecture that's going to streamline it, make it simpler to operate and maintain at lower cost. So you're always looking for efficiencies, but you want to make sure that you're following the rule of effective, efficient and secure as you are designing, operating and maintaining your architecture. Do you have to rip everything out? No, but if you find that there is in fact a product that somebody is pitching to you to enable your zero trust journey, you should be asking, Okay, if I go and I buy this, what can I retire? What kind of savings can I have? And I picked on VPNs and NACs as an example. There are products in the market right now that are zero trust enabling technologies, such as software defined perimeter capabilities that can, in fact, help you accelerate the retirement of VPNs and network access controls which require a decent amount of manpower, have an effect on user

experience, and it cost more money than what the newer technology present. So look for the opportunities to economize but keep moving forward.

Shane McGraw
Next one from Anona as she asks, can you please share information about possible metrics or other probable questions related to Zero Trust that might be helpful in preparing for future FISMA Federal Information Security Act Management data calls. Any comments Greg or Chase?

Chase Cunningham
I would personally pass on that one because we don't want to go down a FISMA rabbit hole.

Greg Touhill
Well, I'll jump on that grenade because that used to be my office that would do that. Once we stood up the federal CISO office, you know, the FISMA reporting requirements that's managed out of that office. And I know that, Chris Derusha who is the new Federal CISO, Chris used to work with me when I was federal CISO and that's one of my staff and we worked together at DHS as well. Chris is demonstrating through his both his word and deed that he's trying to make sure that FISMA reporting requirements are rational and they're not an overdue burden on the different departments and agencies that are out there. So as did Chase, I'm not necessarily going to do a forecast on something I'm not 100% sure on, but I can say that having talked with Chris as recently as late last month, Chris and his team are making zero trust a priority and making sure that we have meaningful measures of merit to show progress on the journey towards Zero Trust adoption. Chris, I hope you're listening.

Shane McGraw
Next, we'll go to Chase for this one. Matt asks, Can you comment on using Zero Trust to manage a single domain Mission Partner Environment? Is it possible to tear down the network walls and still have sufficient security data segregation? I

Chase Cunningham
Is it possible. Yes. Is it advisable? No, I don't think that that's necessarily the best approach. Overall, you don't want to abandon controls that are valuable in the context of at least bounding where your defensive sort of avenue is. So I think that that's an important point to take away, but you just have to be. How would I put it calculated in the things that you are and aren't going to use to continue to bolster the focus of the security you're putting in place in that sort of scenario, continuing to just go, okay, we're moving to ZT. Let's just burn down the network stuff because we're all identity. Not a good way to do it.

Greg Touhill
So yeah. Spot on. You know, as you take a look at it, it's all about risk. And I want to minimize my risk within budget as well as operational capability and as I take a look at that kind of proposition, as Chase would, I would bring in a red team just to help me understand what

possibly could. Could somebody come up with the change my risk calculus. But just because you can do something doesn't mean you always should do something. So as you're making the decision as to how you want to apply some of this. Don't tear everything down at first make a rational decision based on the facts and make sure that you're not inadvertently exposing yourself to even greater risk in the zeal to jump forward based on, perhaps marketing hype.

Shane McGraw
Next one asking, can the average business implement zero trust with today's hybrid work environment? Chase, you want to take a stab at that one?

Chase Cunningham
Yes, you can. Hybrid again, does make things complicated, and it does introduce the additional areas of concern. But this is one of those things. I mean, I liken this a lot to being healthier. Everyone can have your own version of this, and you have things that are kind of key and core to it. And then there's things that you won't do because they're not applicable to you.

So can you do it? Yes. Any business, I think, can. There's lots and lots of businesses and organizations that are at all different size and scale and internationally, etc.. So the proof is in the pudding. But it does require, like General Touhill was saying, the focus and the initial sort of impetus of, here's a plan, we're going to do this. Let's march forward and go along those lines and not deviate from that over time.

Shane McGraw
Okay, we move on to the next one from Terry. And Greg we'll point this one to you. Terry asked, Is it possible to implement micro segmentation without purchasing SDN technologies? Consider smaller organizations which do not have as many servers.

Greg Touhill
Well, there's a couple of different ways you could do that, including you can outsource to different providers to help you with that. You know, folks that specialize in it. And I know a lot of folks say, well, it's an anathema to go to like an MSSP, a managed security service provider but I'm seeing more and more MSSPs that are out there that are adhering to zero trust principles and further, they'll run an infrastructure that has a software defined networking backbone, so you don't necessarily have to go out and buy yourself and set up your own enterprise conclave. You can go out there and you can go to an MSSP or others.

And as far as micro segmentation goes, even within your own environments, there's different technologies that you may already have or you may buy at a reasonable cost. And I'd mentioned previously software defined perimeter technology, because that's one of my favorites and became so while I was still in government service. I think you can be a really discerning customer and you may find that the costs once you go and you survey the whole market, you may find that you're going to find affordable capabilities that meet your needs while still being able to manage your risk.

Shane McGraw
Thank you for that. This is a question from earlier. So I'm not sure if it was tied to something else, but I'll ask if you guys could decipher. It was from Thanakorn asking what are the common verification techniques you guys have used before? Is that something we can address or is that something that needs more context?

Chase Cunningham
Pretty broad, I would say. Yeah. The question I mean, I mean, multifactor auth is kind of one of them.

Greg Touhill
Yeah. Yeah, absolutely. Strong, strong authentication has always been part of our identity verification. As a matter of fact, in the government, you're issued a PIV card, and it is the personal identity verification card where you literally are using a token. I've got one, nothing up my sleeve. Here we go. I've got one. Here's a PIV card and a PIV card you know, this is your identity validation verification card, something I have plus a PIN, personally identifiable number. So something I know. So I've got two factor authentication when I'm employing this. Similarly on the DoD side, yeah, I've got a card that looks like it, but it's a different card. It's my CAC card, common access card. So once again, something I have, something I know and that helps with the verification of my identity. And now you've got a whole big wide market of folks who will help with the digital identity and validation and verification of identity. So some examples for you all out there.

Shane McGraw
Thank you for that, Greg. Thanks Chase. So we've got about 8 minutes left, but I know I want to work in this question. Greg, we'll come back to you. What current research is CERT doing in this area? Can you expound a little bit what your staff is doing in the zero trust area now?

Greg Touhill
Sure. We're doing a couple of things. First of all, we are working with our partners on campus to take a look at best practices and zero trust implementation across that hybrid cloud environment. As well as what we're doing with our students and taking a look at how do I qualify the migration or the movement forward in that zero trust maturity model.

So yeah, can I automate some of the checks that are out there to help me assess where I stand on that zero trust maturity model? And can I do so in a manner that can be audited by my auditing and my controller functions that are out there? Further, we're taking a look at some of the technologies that are being offered in the marketplace and categorizing the strengths and weaknesses of them against certain use cases that our government sponsors are most interested in.

So those are three right off the bat, although we're exploring a few others that are still works in progress.

Shane McGraw
Great. So, Reed followed up with a question here. Asking, how would a warfighter in the field use identity management? A CAC card is probably not the answer during a battle. Is that biometrics question? What is the answer there? Is there a simple answer?

Greg Touhill
Well, it depends on where in the battlefield you are. You know, if I'm in the CAOC, the combined air operations center yeah. I'm going to use a I'm going to use an identity device like the CAC card to get into mission planning systems that we use to put together the air tasking order across all allied air forces. Further, I'm going to make sure that using that identity system in the CAOC where I may have multiple nations operating within the CAOC. And when I was deployed as the director of the CAOC in Al Udeid airbase in in the Middle East, we had 14 nations that were operating in there. And you didn't necessarily want to have everybody having the same access.

So we were using it clearly for the building of the combined air operations planning the air tasking order, as we called it. But if you're boots on the ground, let's say you're in a convoy you're not going to necessarily be using that CAC card for things like your radio communications back to the main control center for the logistics enterprise.

You may be handed a Sincgar radio, which is a typical light handset radio. And that's what we give our convoy folks. If you get in trouble, press a button and talk. But what we do give them from an identity standpoint, is we give them call signs, tactical call signs out on the road. Further, they have to file route plans so they would report Hey, I'm at this particular location, a grid coordinate X that would be verified against the route plan along with their call sign.

That's a measure of identity as well. So we use other means of identification on the battlefield that give us a reasonable assurance of identity and that's all overlaid along with the technology, such as with those Sincgar radios. We use a type one encryption so that that transmission is protected against intrusion from somebody who doesn't have access or need to have access to that data stream.

Shane McGraw
Thank you for that, Greg. We're coming up on time. So I want to give you guys any closing thoughts. Chase, we'll go to you. Just how can people get more information from you Chase? I'll put some stuff in the chat, but how can people hear more? Any closing thoughts, Chase, you have on zero trust and where it's going.

Chase Cunningham
Well, number one, thank you for having me. Number two, General Touhill, thanks for letting me ride your coattails, as always. And then on top of that, I think really the question becomes the

one that I think people should ask themselves often, is if we're not going to do ZT how are you going to be better than what we've tried in the past?

You have a lot of proof that the other ways don't work. So why continue to practice that failed methodology? And you have a movement -we're not messing around when we say this is global in nature. And this is big time deal. So that, in my opinion, is worth asking. And then if you're looking for me, I'm really easy to find on LinkedIn, Twitter. I do a LinkedIn live thing now on Wednesdays. I welcome folks to come out there and chime in and say what you want to say and interact. And then I do studies and publish papers all the time as well. So if there's something I can help out with, please let me know. I am always at everyone's service.

Shane McGraw
Chase. Thank you so much for your time and your expertise. General Touhill, we'll turn it over to you for some closing thoughts.

Greg Touhill
And thanks so much. And you know, if anybody has any questions that they didn't get answered sufficiently or if you want to learn more, reach out to us info@sei.cmu.edu. Once again, that's info@sei.cmu.edu. And you know, we'll get back with you. I also encourage you to continue your reading on this. You know, there's a lot of great research being done by Chase's old organization at Forrester. The folks at Gartner are doing some interesting work with SASE, their model, and then here at Carnegie Mellon and the Software Engineering Institute we're drilling down to make sure that we're helping our government sponsors, you know, DoD sponsors and critical infrastructure providers, and hopefully you as well, with some meaningful and relevant research that can help you understand how to better manage your risk and make more informed decisions. So don't hesitate to reach out if we can help you along the way.

Shane McGraw
Again, Greg and Chase, great discussion today. Thank you so much for sharing your expertise. Lastly, we like to thank you all for attending today. Upon exiting, we do ask that you hit the like button below the video window and share the archive if you found value. Also, you can subscribe to the SEI's YouTube channel by clicking on the SEI seal in the lower right corner of the video window.

Lastly, join us for our next livestream, which will be on April 13th, and our topic will be Developing Models to Support DoD Technical Reviews. Registration information is available on our website now and will be emailed out as well. As Greg mentioned, any questions from today, please send those to info@sei.cmu.edu. Thanks everyone. Have a great day.