Better Incident Response through Scenario-Based Training
Transcript

Part 1: Train as You Fight: Use Scenario-Based Exercises

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on security governance and software assurance. Today I'm pleased to welcome Chris May, the technical manager of CERT's Workforce Development Team. Today Chris and I will be discussing how security and IT professionals can be much better prepared to respond to incidents through scenario-based training. So welcome Chris, really glad to have you with us today.

Chris May: Thanks Julia, glad to be here too.

Julia Allen: So what do you see as some of the key issues, when you're faced with training security and IT staff to be as well prepared as they can be when a real incident hits?

Chris May: Well I think just having been immersed in training in various ways, over the past ten years at CERT and in my prior life working as a computer systems communications officer in the Air Force, I've experienced a lot of different — some very effective and some not so effective — ways of preparing my troops (and if I tend to have a more military perspective, forgive me but that's the perspective I'm coming from) is that preparedness, or readiness, really results in experience, and how much practice and experience you have in preparing yourself to respond to a given event.

And so in training, there's the crawl/walk/run phase; the kind of process that I look at when I'm trying to produce readiness in personnel. And the first area, crawl, is essentially you got to get people aware of the situation and introduced to the subject or the topic. Probably the most traditional means of preparing someone in this crawl phase is just general classroom-based training, right? And classroom-based training definitely has an absolute place in preparedness. It gets people out of their normal work environment and into a dedicated time, hopefully a good instructor, a good curriculum.

The problem with that approach is that it's a moment in time. So as soon as they leave that classroom-based training, they have — they start losing what they learned, and in six months they've probably lost half or more of what they learned. And the skills that they were introduced to, they probably don't recall and they have to refer back to any of the documentation, if they haven't used that daily in the normal routine of their job.

So in order to allow them to have a better retention and mastery of the stuff that they were introduced to in the crawl phase, we use a web-based or a maintenance approach, where we have — for example, we have CERT's Virtual Training Environment, the VTE, which allows people to retain knowledge that they may have received initially in a classroom setting. They're able to log into this website and they can take the class that they sat at again. And they can even go through some of the labs and watch instructors give them demos. But that's to not only retain what they learn but to expand upon it.

But again, that's just directed towards individuals in that phase, in that walk phase.

Julia Allen: Right, and of course as we know, this is a team sport, right?

Chris May: Exactly. And so in the real world, when you're having to respond to cyber events, or just general security issues, you don't do it in a vacuum, you don't do it in your own sandbox, right? So typically you're going to have all the policies, the procedures; what I like to refer to as the fog of war. Not everything is set up for you in a nice little classroom lab document that takes you through a very confined task. You have to be able to respond.

And the best way from my military background that I've ever seen, in the military is — this is how they prepare people — is they do something called "they train as they fight" right?, which means put people in a situation that simulates the environment that they're going to be called upon if they're actually asked to fight, right? So to provide these scenario-based exercises that really prep you for the environment you're going to see if you're ever called upon in a specific incident.

And so what we try to do is we try to through various means — whether it's at the end of a classroom-based course or as part of a larger scenario-based exercise — we try to put people in a situation that really simulates, in as realistic a way as we possibly can, the environment and the threat conditions that they're going to see. And therefore they'll have that experience, they've already seen and dealt with it before, and they'll have a better chance of responding in a way that'll be effective.

Julia Allen: Well I would imagine that setting up an environment like that, defining what realistic scenarios are, could be pretty darn challenging, in terms of making that as close to a live setting as possible, right?

Chris May: It is. And traditionally – again going back to large corporations and government organizations — because it's pretty hard, it just generally is, what tends to happen is that the events become further and further stretched apart, and they're bigger.

So, for example, the military will have, and the government will have, one big exercise, or a couple of really big cyber-exercises a year. And they have hundreds of people involved and it's just, it's a massive undertaking to actually produce this training exercise; crafting the scenario and the objectives, and getting all the

participants involved, and making sure that the environment is set up. It's just a massive effort. And therefore it's not really team building. It's not really going to help operators at what we call the unit level or the small organization. It's really dedicated to a more enterprise-wide, huge operation.

And so the idea is — again leaning back to my military days — every military unit, as part of their normal operating procedures, their normal daily, or what they have to do to prepare themselves, is that they have to carve out some of their day to train so that they're prepared when they're asked to fight.

Well the same investment — and hopefully organizations are going to start seeing that this investment is really worth it. And carving out what we used to call sergeant's time — an hour a day, or a few hours a week — to work on this kind of stuff, to prepare yourself to respond to certain conditions and events is really where it's at. And I think what we're trying to do is make it easier for organizations of any size to do that rather than just having to wait for the one massive scenario-based training a year. Or to do it regularly and provide them an environment that they can do it in, without a whole lot of effort or cost.

Part 2: Training Geographically Distributed Teams: CERT's XNET

Julia Allen: So I know that most of today's security and IT teams, both in commercial settings and in government settings, are geographically distributed. So when you're constructing a scenario-based training program that's specific to the needs of a particular team, organization, military unit, how do you take that aspect, that being geographically distributed, into account?

Chris May: Right. Well that's one of the big challenges. Typically what's done now is they use VTCs (video teleconferencing), traditional type of things to bring people together who are geographically distributed.

The best approach is to try to provide them an environment that virtually brings everyone into the same facility, into the same meeting room, all sitting around the same tabletop with all the assets that they would normally have if they're brought in together to respond to some kind of an event. But to do it over the web, and make it really, really convenient so typically from your web browser. Everybody has a web browser and Internet access for the most part. So we to leverage that in a new capability that we're researching and prototyping right now with some military organizations called XNET or Exercise Network.

Julia Allen: So what are some of your objectives for XNET? This sounds pretty intriguing.

Chris May: Well the main objective of XNET is to provide continuous access to unit-level operational readiness training and evaluation. So that's the scripted objective. Make it part of their normal daily operations, whether you're in the military, a large organization, a CSIRT (Computer Security Incident Response) team somewhere, that you can log into a website, and you have a network in there that

you can access from a web browser. You have all of the collaboration tools that you would have if you were in the same room, physical room: whiteboards. You can look over someone's shoulder and help them with a specific task on a server or a router. You can chat with people. You can log events. You can upload information to a wiki that people on your team can see. So we have to bring everybody into the same virtual room and give them very simplified access to their resources.

So what we do with XNET is we make most of the environment visual. So we'll have a network topology diagram, or a network map, that represents the exercise infrastructure. And people – if you've been in IT anywhere, people have become very accustomed to these Visio diagrams of their topology, right?

And so to gain access to a specific system — maybe your intrusion detection system or your firewall or a server – rather than having them try to find this and gain access to it via some SSH client, or some other means, we just have them double-click on that visual representation, on the topology map, and it brings up direct access to that system right from within their web browser.

So everything's got to be very, very convenient and easy and intuitive. Otherwise people simply won't use it. It becomes too hard. And the infrastructure should be the absolute last thing the trainer or the instructor should be concerned with. What they should be thinking about is the objectives: what are the threats that I need to prepare my incident responders or my staff to respond to and to deal with? How can I shape a scenario so that it'll prepare them and they'll have a greater degree of readiness if they have to actually respond to this kind of event in the real world?

Julia Allen: Let's take a candidate scenario. You talked about maybe a network intrusion or some type of event that's being represented in this kind of environment. Can you say a little bit about how many people might typically participate and how you keep the roles clear and control the interactions?

Chris May: Sure. Right now the XNET platform, everyone logs in and they're a part of a team with specific roles. So it depends on the scenario that we're dealing with. We have incident response scenarios. We have assessment and even penetration testing scenarios or network defense. There's a number of scenarios that we can build custom or draw from a library that we have. And when you log into XNET, via your web browser, you're within that specific role.

So, for example, if you're one of the incident responders, we can give you the infrastructure that you would typically have access to, right? You may have access to your security systems, maybe your intrusion detection system. Maybe you have access to your firewall and your logging server and some other things that you would have access to. And then maybe another team might be compartmentalized where you have a system or a network administrator team. And they have direct access to only certain parts of the infrastructure, maybe the routers or the switches or the email systems or whatever.

And so we can, basically we can very easily define what parts of the topology and what their roles are. And then we just basically either grey out or give them their own topology map that they can then access the specific systems on the network that they need, that they would ordinarily have access to.

On the other side, if you want to have a red team (which is a military perspective of having an attack force or an aggressor force that is trying to actually insert stimulus into the network) and see how the response team actually deals with that. And you can have that in kind of a scripted manner where the red team basically goes through the script and inserts controlled stimuli into the network. And then you monitor and evaluate the responders for how well they respond, given their systems, whether they can detect and identify what's going on, and then mitigate it or at least report it correctly.

So there's all kinds of scenarios. But it is very role-based in that, depending on what your role is in the team or in the exercise, we can control that very easily. And then we can give the actual trainer — so there's usually somebody in charge of these scenario-based events, someone who's shaping the exercise for their environment, to model their own network environment and the way their teams and their security staff are organized. And they'll guide us as we help them shape that exercise to really match what they're used to dealing with.

Part 3: Using XNET for Simple and Complex Scenarios

Julia Allen: If a team wanted to get involved and define an exercise, is this a half a day event, a day event? What are some of the timeframes?

Chris May: Yeah, well here's some examples. Right now we're piloting XNET with a few military and government organizations and they have different requirements. So one of them is a reserve unit and so they only get to get together one weekend a month. And typically the reserves have a bunch of military type of training and just housekeeping type of stuff that they have to do. And they only have really a small, narrow amount of time that they can really dedicate to training and preparing themselves to meet their mission, right?

So for them we do it on a three-hour block on a Sunday afternoon where we give them a more targeted scenario – we call it Targeted Analysis and Response Challenge Track — where they have to log in, and they're presented with a pretty tight directive or a mission that they have to do and accomplish. And then we'll walk them through — it walks them through this scenario and they have to respond to automated injects. So we'll have predefined what we want them to respond to.

And then we have what's called an exercise timeline. That's a graphical representation, what you might see as an Outlook calendar type of thing where you can drag and drop events onto this timeline. And then at the start of the exercise plus five minutes, you're going to have this particular event occur and it'll be universally applied to all the teams across the exercise.

And then because you've prepared this in advance, you know what the standard task is, what the conditions are, and what the standards or the expected response should be. So you can define that and then you can sit back as the trainer or the evaluator and say, "Okay, let's watch and see how well they meet the standards or what the expected response is." You can monitor that and then you can say, "Okay, here's the standard response, here's the reporting, and here's the — if you wanted to — here's the recommended or the normal mitigation strategy."

And you can give them a timeframe to do that. So by — this event should be done, everyone should be through this within 30 minutes or whatever in that scenario. And then if they're not, then you can either — you have, you can give them extensions of time or you can stop and say, "Okay everybody, now we're going to walk everybody through. Everybody watch me. So within your web browser watch me show you what the normal response should be or what you should do technically to mitigate this."

And then we can have what they like to call in the military a hot-wash, or an after-action report, which is basically everyone talks about what went right, what went wrong, and what they should've done. And that really sets the stage for not only understanding your current mission readiness or your capability but evaluating how you can then move and build your own capability, by continued training or whatever it is.

So that's one approach, right? A very short, narrow, three-hour, targeted response and analysis challenge. And then that can scale all the way up to a widely distributed, week-long, hundreds of people in the environment, all logged in on different teams, going through a very complex set of exercise events. And that doesn't have to be [incident] response necessarily. That can be targeted to whatever the mission is. Maybe they have some critical infrastructure systems that they need to deal with that aren't necessarily what you might consider normal security threats, network attack or whatever, but something anomalous in the environment. Or you have failures or whatever it may be.

Julia Allen: So it sounds like that the advanced planning, in terms of the scenario definition — the roles, the timelines, the expected outcomes, how the trainer orchestrates the scenario — this advanced planning is really critical.

Chris May: It is. But we can make it a lot easier for people. And one of the reasons, one of the ways we do that is we build all of our scenarios in a very modular way, so there can be maximum reuse, right?

So we'll have a library of events and a library of scenarios or situations that we can then draw from and customize. So let's say someone needs "Hey look, we need to really take a look at this DNS (domain name system) cache vulnerability or this latest exploit. Or we want to see how people do with some kind of environmental response."

We can draw from that and provide people a pretty, maybe 85% solution, and we can help them customize pretty quickly. So that way they can — again, the whole goal of this XNET idea is to make it easy for people to practice for incident response and

network defense, not to levy this huge burden on them. Because then in the end they're just not going to do it.

Julia Allen: Well how, if someone wanted to engage this environment, how would they actually get started?

Chris May: Well the way it works right now is we have, like I said we're piloting this with government organizations and even some corporations or public organizations that might want to, might have a specific strategic goal in mind. And then we would work with them, our XNET development team would work with them, to make sure that we understand their requirements.

And we try to again take advantage of what we already have built to customize, so there's not a ton of effort involved in producing something that is really relevant to their environment, their everyday working environment. So that's one thing. So right now it really involves us directly having an engagement or a relationship with an organization.

In the future, we want to have this more on a service model, where people can dial-up, choose a scenario from a drop-down menu, and launch it with the push of a button. But essentially just be able to say, "Here's a scenario." And there's a huge library of these scenarios. And give them an interface that they can then control their user population, build their user accounts, and allow people — and what role they fit in — and allow them to just log in and run through this canned scenario as well.

So there doesn't need to be nearly as much facilitation from the XNET development team, just setting the stage for them. So that's where we're going. That's not currently available but probably will be within the calendar year '09.

Julia Allen: So Chris do you have some sources where our listeners could learn more, either about XNET in particular or just about the concept of scenario-based training?

Chris May: Actually for scenario-based training, there's actually quite a lot of literature out there that you could find with a simple Google search.

If they want to actually interface with us, monitor the CERT website. We have a demo of the XNET environment that we're putting up on the web. We have some research papers that describe the capability and some other information that people can gain access to right from cert.org.

Julia Allen: Well Chris this has been a great introduction to what I think is a very exciting and valuable new capability. So I so appreciate your time today and sharing this upcoming work with our listeners.

Chris May: Hey no problem. I'm glad to help.