Using High Fidelity, Online Training to Stay Sharp
Transcript

Part 1: The Growing Need for Anywhere, Anytime Training

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 Jim Wrubel, who leads CERT's Virtual Training Environment Team. Jim and I will be discussing how high fidelity, online training environments are becoming essential for security professionals to add to and maintain their skills, anywhere, anytime. So welcome Jim, glad to have you with us today.

James Wrubel: Oh thanks Julia.

Julia Allen: So what is a virtual training environment, and in your experience how does this type of environment compare to or differ from in-person classroom training?

James Wrubel: Well the virtual training environment, as we've implemented it, is a web application. It offers a set of tools that allow organizations to record and publish high fidelity versions of their training and education programs in security and other disciplines, that they're already giving, and to make them available to learners around the world.

I'd say that VTE is a megaphone for in-person classroom training. Your average instructor can maybe handle 20 students in a technical, hands-on class. VTE can serve 20,000, and again all at the same time.

There's no substitute for face-to-face education, especially for some of the more specialized skills. But the reality is that logistics frequently gets in the way. It can be very challenging to get an instructor, a classroom, and a sufficient amount of students in the same time and place to deliver that sort of face to face experience. And VTE was built to solve that problem. It helps the best instructors with the best material reach the most students and ultimately, hopefully do the most good.

Julia Allen: Yes, and I would think with all of our travel restrictions, our time restrictions, the job requirements that we all need to fulfill, sometimes all you can do is get maybe a 30-minute or a 60-minute block of time and do a check-in, check-out on a particular topic, right?

James Wrubel: Exactly. Not only are demands for people's time are constantly under strain, but the ability to get away from everything and go take a class is becoming a

luxury that many people, especially those in the security field, can't afford. You know over the course of a month or two that you can complete a two-day technical class, but you can't dedicate any two days, within that month or two, to do so.

Julia Allen: What are some of the other reasons you've seen that these types of environments are becoming more and more important as a resource for, not only security professionals, but pretty much any professional?

James Wrubel: Right. Well everybody knows that networks are increasingly interconnected. You're seeing threats evolve extremely rapidly. An exploit will be published on, in some cases, the same day that a vulnerability is described. So the threats are moving at near light speed, and as security professionals we can't afford to be slower than those threats. We have to have training programs that can be delivered at the same pace.

Likewise I would say that the security training and education programs are being more formalized. We're seeing shifts in the community towards a set of standardized, commercial certifications in this field, and we're seeing more and more that a large amount of individuals are focusing on those types of certifications. You're certainly seeing this in the [U.S.] Department of Defense, other federal agencies.

So once you do start to standardize that type of education, you can actually make large-scale delivery of high quality training material economical, because what you can do is capitalize the cost of developing the absolute best training program over a very large student population.

Julia Allen: So that's an interesting thread, this idea of the body of knowledge for security professionals becoming more well-defined and the emergence of a growing number of certifications. Is that one of the reasons why CERT decided to embark on developing our own virtual training environment, or were there some other reasons?

James Wrubel: It is. We saw, I think like many organizations did, this trend towards standardization, and certainly again the government focusing on finding more objective ways to measure the quality of its security workforce. And we've been developing and delivering instructor-led training courses on information security and incident response, cyber forensics, for years. And we still do actually. But with the amount of courses that we're able to deliver instructor-led, again with that 20:1 ratio of students to instructor, we were finding that it would be a very good year for us if we could talk to 1000 students. And we just got numbers from the Department of Defense, out of their FISMA [Federal Information Security Management Act] reporting. Their numbers are over 90,000 people working in information security.

Julia Allen: Wow.

James Wrubel: It's a long road from 1000 people a year in instructor-led training to 90,000 people. We needed a way to reach these people without sort of penalizing our instructors by putting them on the road 52 weeks a year. We needed a better way.

So, the SEI has long had a history of distance education. Back in the '80s when we were doing software engineering as a discipline, we were actually filming courses and putting them on VHS tapes and putting them in the mail.

VTE is really just an evolution of this type of practice. We record the training class that we deliver and we make it available on demand.

Part 2: CERT's Virtual Training Environment; Lectures, Demos, and Hands-on Labs

Julia Allen: Why don't you kind of walk our listeners through a little bit more about the VTE environment and how it actually works?

James Wrubel: Right. The VTE environment is again, as I mentioned, a website, and it has a number of tools for delivering different types of education to meet specific objectives. I think at the core is the idea that there's an instructor and there's a classroom and a bunch of students. And what we do is simply put a camera in one of the student chairs and passively film the entire course.

We then post-process that material, we index it and we publish it to the web. And we do so in manageable chunks, ideally around 15-minute blocks of instruction each. And that gives, again, students the ability to access an entire training course in sort of a series of consumable modules so that they can go at their own pace.

Another tool that we use is what's I think more colloquially become known as screencasts. It's the idea of recording your desktop and actually narrating yourself walking through some sort of a practice. So this might be a firewall configuration. So we might actually record ourselves at a Cisco terminal entering configurations into the command line to actually harden or build firewall rules, and that sort of thing.

Julia Allen: So you can actually give a student a demonstration of how a particular tool and a particular practice would be executed.

James Wrubel: Exactly. The screencasts are meant to reinforce the lecture. So you've taught somebody a principle, you've given them some background information, and now you're showing them how to actually implement that in a real world environment.

The real differentiator in VTE is the hands-on training labs; the idea that an entire computer network is available to you as a student and all you need is a browser and an internet connection. And how this works is we have a library of virtual machine images, stored in a central server, and a series of configurations for those that are available for students to launch. Some of these are part of a class, some of these are sort of in an asynchronous library to allow students to practice on whatever they want, whenever they want.

So when a student initializes one of these labs, our servers actually go pull copies of the computer images that make up that lab and deploy them in a sandbox, and then give that student access to that sandbox for a number of hours. And we match that

with a manual that walks them through the purpose of this particular lab and the step-by-step instructions for how to complete it.

Julia Allen: So you're saying that they can actually get into this environment, they can access it through VTE, and actually put them in the practice of the "doing" part of what they may have just heard in the lecture or seen demonstrated.

James Wrubel: That's exactly right. One of the biggest challenges for any sort of technical education, and specifically information security, is that you don't necessarily have access to a scenario that can give you the context for learning. It's one thing to say that you might have a Cisco firewall lying around, but a firewall by itself doesn't do you much good unless it's protecting a network, or unless you have a reason to configure it.

So what the VTE hands-on labs give you are access to equipment that you would not otherwise normally have available at your desktop. You might have it in a training lab down the hall, but it's not available on demand and it takes a lot of time to reconfigure.

VTE abstracts all of the configuration from you. It gives you a starting point and a set of instructions to get it to a finish point. And the most important thing is that you can deviate from it. These are virtual machine images, which means they look and feel exactly like real computers.

Julia Allen: So you're saying it's not absolutely scripted or absolutely canned. It basically puts the student into an environment. They can follow the user's guide or handbook that they're given, but they can also experiment.

James Wrubel: That's correct. One of the biggest limitations of the previous generation of online learning, or what people have called computer-based training, is that they would use simulations to provide the hands-on experience. So they would take a screenprint of, for example, a Windows desktop, and you can click anywhere on the screen but it won't do anything until you click on the icon that they expect you to. It's a mockup, it's a facsimile.

The difference in VTE is that these are actual machines. You can go off the script, and they behave exactly like real machines, because they are. In fact, I've personally blue-screened several of the hands-on labs, trying something that wasn't part of the script. And that's a very powerful way. You can learn not only by doing the right thing but by making mistakes. Some people learn very well that way.

Julia Allen: Now do I understand correctly — you mentioned a student can get into this environment — but is it possible for small teams to actually interact with one another in these lab environments?

James Wrubel: We have a couple of other technologies that allow small teams to interact together. One of them that we're working on that's particularly exciting is

called XNet, which allows people to role play — attacker, defender, judge — and collaborate as a team.

VTE is really designed to remove the logistics from the active training so that you don't have to wait for a resource to become available, whether that be an instructor in a class or enough people to also be ready to train, that you can all go together.

Julia Allen: Right. So as you said, you can kind of proceed at your own pace.

James Wrubel: Exactly. It's designed to let you, as a learner, take control over the time and place where you are most comfortable.

Part 3: Using VTE: Initial Training, Selective Refresh, Event Capture

Julia Allen: So how have some of your team's customers, or CERT's customers, used this environment? What kind of feedback have you seen in terms of actual customer use?

James Wrubel: So there are a number of programs that customer organizations have implemented on VTE. Probably the most successful would be a program that actually DISA [U.S. Defense Information Systems Agency] is sponsoring to provide access to training courses on commercial certifications to allow Department of Defense organizations to very rapidly train and certify their staff for the DoD 8570 Directive, which mandates that within six months of taking a job in information security, that person needs to hold a commercial certification that matches the level of responsibility that they have.

This program's been in place now for nearly two years. We've put almost 20,000 students through the program. We've delivered a little over 130,000 hours of training, which is the equivalent, as we discovered, of four instructor-led classrooms running every week, full, since the inception of the program. It's a very powerful way to deliver this material to a very, very broad audience.

Julia Allen: Boy, that's very impressive, and certainly reinforces your earlier point about scale and span and outreach.

James Wrubel: Exactly, exactly. It has touched just about everywhere that the Department of Defense is. We've had support conversations with personnel in Iraq and Afghanistan and on ships. The Internet reaches much further than sort of instructors can go, especially into places, like in theater, where it may be too dangerous to hold an instructor-led training class.

Julia Allen: Right, and just to kind of go back to one of your earlier points. I recall from some of our work together that you said — you mentioned that you can get an Internet connection everywhere. But certainly there are cases where you can't, where it's — you also provide the capability to download at least the lecture and demo part of the course content for student use offline. Right?

James Wrubel: That's exactly right. Every time we create a training course online, we press a CD version of it, which has everything, with the exception of the hands-on labs, which require a reachback to a server farm. But this gives people the ability to take some of the training with them. And we've delivered a little over 2000 of these DVDs out to various locations. We sent an entire set to the point of contact for the Navy's Afloat Information Security Force, so that they can use it shipside. We've had some tremendous success there.

The program has been wildly successful. We're getting feedback that people are finding that the format is much more convenient, that they're passing their commercial certification tests on about the same rate as those who are going through instructor-led training. And the cost per student is dramatically lower than what you would get for sending somebody to a class.

Julia Allen: So you mentioned the DISA and DoD work. Are there some other organizations and customer sets that you've worked with that you could tell our listeners about?

James Wrubel: There are. We've done some work, for a little over three years now, with the Secret Service, focused on our cyber forensics material, making that available to agents in their Computer Crimes Taskforce. And that has, again, met with tremendous success and interest.

What we're finding is that these field agents are able to train on demand. So as they encounter unusual situations in their casework, they're able to reach back into VTE and very quickly refresh on the 15 or 20 minutes of material that they need to understand how to go out and implement some sort of a forensic acquisition practice.

We had one agent, in particular, who was performing an acquisition of an unfamiliar file format, and they actually had a laptop with the VTE lab that mirrored that environment up. So they would implement something in the lab, verify that it worked, and then implement it in real time. So they were actually following the real-time training model that so many organizations strive to achieve.

Julia Allen: Well that makes a nice point too, that you can use VTE for kind of an initial — to meet an initial training objective when you're trying to build confidence or, as you said before, get a certification. But then you can also dip into it very selectively to get refreshed or to validate on a particular, very specific subject. So I would imagine that having both of those, an ability to meet both of those objectives, is a pretty compelling business case.

James Wrubel: That's exactly right. One of the things that I've always found about going away to a training class is while I'm engaged in a training class, in an instructor led training class, I'll be very tied in, very in tune with what's going on. The moment I walk away, if I don't immediately put that knowledge into practice, it starts to fade. And the longer it gets — what I'm left with after six months very frequently is the memory of something that I talked about in that class that's relevant to something

I'm looking at right now. So I remember that we talked about this during class but I don't remember what we said.

Julia Allen: Right, you have no ability to kind of go back and refresh in a …

James Wrubel: Exactly.

Julia Allen: … in an effective way.

James Wrubel: Yes. So if I took notes, I can go back and look at those, but they're out of context now. What if I could go back and actually just re-access the portion of that training class that discussed exactly what it was I remember? And that's one of the things that VTE lets you do is immediately go back and just replay the very small portion of a larger training program that covers what you need to know right now.

Julia Allen: So have we finished the description of some of the customer use of VTE, or is there anything else you'd like to add there?

James Wrubel: There's one more that I wanted to call out. We've talked a lot about the idea of training programs, formal instructor-led training. That's not necessarily the only location and style of knowledge transfer that organizations are finding.

Very frequently organizations hold conferences, especially large distributed organizations will hold conferences for their staff to get together, share ideas, cross-train on various situations. But again, you have a logistic issue. Those conferences are typically held in a specific location and it can be very challenging to get all, or even a majority, of your organization to drop whatever it is they're doing and go to a conference for a period of time.

Recently we captured the Marine Corps' Information Assurance Conference. That, as you well know, is a very – an organization that's very globally dispersed, doing a very important job, can't necessarily drop everything and fly back to the United States to a conference.

So what we did is recorded the sessions from that conference and recreated it on VTE. So those Marines that were not able to attend the conference were able to watch the sessions that they were most interested in, at their own pace. Likewise, if a particular person was forced to choose between Session A or Session B, while they were at the conference, they could go through and sit in Session A and, at their own schedule, go back in and watch Session B online, after the fact.

Julia Allen: I know a lot of the big conferences do make either selected or all of their content available, and this seems to be an ideal use for extending training and education. In fact, one of the questions I wanted to ask you is how do you keep the content refreshed, given that this is such a dynamic changing environment? And what you just described about capturing this conference event could be kind of a case in point of doing just that.

James Wrubel: That's right. This is a style of instruction that again very much is a reflection of an organization's ongoing training and education efforts. We are an example of an organization that still teaches instructor-led training. We still do four and five classes a year, and we've made a commitment as an organization to refresh that material for the instructor-led portion. But once a year, once every six months, depending on how frequently we feel the information changes, we'll simply refresh the course with the latest version.

Julia Allen: Yes, well that makes a lot of good sense and — because we're all dealing with scale, with outreach, with a distributed and geographically displaced workforce. So having ways to push this information out is I think becoming more and more a critical requirement.

James Wrubel: That's right.

Julia Allen: So Jim, where can our listeners learn more about either the general subject or perhaps how to gain access to the portions of VTE that are publicly available?

James Wrubel: Yes, I should mention at this point that many of the programs that we have for information security education are specific to the sponsoring organizations — the Department of Defense, the federal government and so forth — and those programs are typically available to a closed community. So if you are a member of one of those communities, you certainly have access to those.

As an organization whose mission is to improve the state of information security across the globe, CERT makes a number of its training materials available through VTE, at no charge, with no registration required. And we do so using a library format that allows individuals to come and search the site.

The easiest way to get to VTE is to open up your favorite search engine and type V-T-E in the browser. I just checked earlier today and we're the top result in Google and Yahoo and number three in Microsoft Live Search. So that's probably the easiest way to get to it. If you want to go directly, it's vte.cert.org.

Once you're there, if you are a member of one of these constituencies, you can find the link for requesting an account and simply sign up. If you're a member of the general public and simply looking for resources to improve your security education, you want to look for the link to the library, and in there are about 200 hours of lecture and demonstrations.

Unfortunately we can't make the hands-on lab component available without registration. But that material is all individually linked. So you can actually embed it in your own training programs. You can forward it to friends. You can build bookmarks of security educational resources. And you can use this material. Please do. We make it available because we understand that security incidents on one person's network affect us all. We're all part of really the same networks.

Julia Allen: Well Jim, I so appreciate your time and sharing your expertise with our listeners today. It's been a great conversation. So thanks very much.

James Wrubel: Thanks very much Julia.