

# **CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES**

## **Using High Fidelity, Online Training to Stay Sharp**

**Key Message:** Virtual training environments can deliver high quality content to security professionals on-demand, anywhere, anytime.

### **Executive Summary**

Today's organizations increasingly have to balance ongoing training and education needs with the logistics of large, distributed workforces. Day-to-day demands on technical staff and the need to minimize training costs are key drivers. High-fidelity e-learning preserves the quality of the educational experience while minimizing or eliminating the need for a student to be in a specific place at a specific time with a live instructor. This type of training environment is particularly useful for security professionals based on constantly evolving information technology and the threats to systems, networks, and information.

In this podcast, Jim Wrubel, technical manager for CERT's Virtual Training Environment, discusses how security professionals can add to and maintain their skills by using high fidelity e-learning environments.

---

## **PART 1: THE GROWING NEED FOR ANYWHERE, ANYTIME TRAINING**

### **Defining a Virtual Training Environment (VTE)**

Typically, a virtual training environment is a web application with tools to record, capture, and present training and educational offerings.

In effect, a VTE is a megaphone for in-person classroom training. An average class has 20 students. VTEs can serve 20,000 all at the same time.

A VTE solves the logistical issues of getting an instructor, a classroom, and a sufficient number of students in the same place at the same time.

In addition, a VTE can capture the best instructors presenting the best material for access by students on their own schedule.

### **Benefits of Using a VTE**

Based on work demands, students are often unable to carve out more than 30 or 60 minutes at a time, let alone travel for a multi-day course. Being able to take a two-day technical class over the course of one or two calendar months may be the only practical way to complete the course.

Threats and vulnerabilities are occurring at light speed. Students need access to training programs that can be delivered at the same pace.

### **The Move toward More Formalized Security Training Programs**

The growth in standardized, commercial certifications for security education and training makes large-scale delivery of high quality training material increasingly cost effective. You can capitalize the cost of developing the best training program over a large student base.

This trend toward standardization was one of the catalysts for CERT's investment in VTE, along with assisting

CERT's government customers in finding more objective ways to train and measure the quality of their security workforce.

As one example, the U.S. Department of Defense reports over 90,000 people working in information security, the majority of which require training. VTE provides an effective means for reaching this workforce.

---

## **PART 2: CERT'S VIRTUAL TRAINING ENVIRONMENT: LECTURES, DEMOS, AND HANDS-ON LABS**

### **Lectures**

CERT's Virtual Training Environment is a website, with a range of tools that deliver specific content to meet specific objectives.

VTE lectures capture instructors and students in a live classroom setting. All lectures are recorded and broken into 15 minute blocks of instruction to allow students to access content in short segments, thus being able to learn at their own pace.

### **Demos**

VTE demos are, in effect, a narrated recording of a desktop screencasts as the user walks through a specific practice such as configuring a firewall. VTE demos reinforce key points made in lectures.

### **Hands-On Labs**

VTE hands-on labs provide a virtual environment where students can perform practices described in the lectures and demos, just as if they were executing them in a live computer network.

Each lab has a companion step-by-step instruction manual.

This environment provides students with access to "equipment" that they would not normally have available at their desktops. Labs are not scripted or canned as in other types of computer-based training. Labs are available on-demand.

### **Small Team Work**

In the future, CERT's VTE will incorporate a capability called XNet which will permit small teams to collaborate and play a range of roles such as attacker, defender, and judge.

---

## **PART 3: USING VTE: INITIAL TRAINING, SELECTIVE REFRESH, EVENT CAPTURE**

### **Initial Training – Commercial Certifications**

The U. S. [Defense Information Systems Agency](#) sponsors a program to provide access to VTE training courses to help students prepare for several commercial certifications. This access allows U.S. Department of Defense staff members to meet their [8570 Directive](#) requirements.

This Directive mandates that each staff member must hold a commercial certification commensurate with their level of responsibility within six months of taking a position in information security.

In the past two years, 20,000 students have been trained, accessing over 130,000 hours of training material. Trained personnel include soldiers in Iraq, Afghanistan, and ships at sea.

If an Internet connection is not readily available for students, the training content can be easily captured on DVD and sent to specific locations.

Results indicate that students are passing their commercial certifications at the same rate as students who complete instructor-led training. The cost per student is dramatically lower when using VTE compared to in-person training.

### **Selective Refresh – Forensics**

Agents in the U. S. [Secret Service Computer Crimes Taskforce](#) have used VTE cyber forensics training materials to help train their field agents. They can use VTE on demand to quickly refresh on forensics practices and tools.

VTE labs have been used to test a forensics approach before using it in a real forensics examination.

In contrast to in-classroom instruction, VTE provides the capability to replay a specific training segment to help students recall what they need to know right now.

### **Event Capture – Conferences**

For organizations that are large and distributed, logistics can be an issue when conducting events to communicate key messages or training to their entire staff.

VTE has been used to capture the U. S. Marine Corps' Information Assurance Conference. All sessions were recorded and made available to Marines so that they could access those that they were most interested in.

VTE course content is refreshed as needed by capturing updated live instruction.

While a wide range of VTE content is available publicly, some content is tailored specifically to sponsoring U.S. federal agencies and, therefore, is only available to staff members of those agencies.

There are approximately 200 hours of freely available lectures and demos. The hands-on labs are only available to sponsoring organizations.

### **Resources**

CERT's VTE [web site](#)

[Wrubel 2008] Wrubel, James; Allen, Julia; White, David. High Fidelity e-Learning: SEI's Virtual Training Environment. CMU/SEI-2008-TR-022, Carnegie Mellon University, Software Engineering Institute, [to be published January 2009].

Copyright 2008 by Carnegie Mellon University