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

Better Incident Response through Scenario-Based Training

Key Message: Teams are better prepared to respond to incidents if realistic, hands-on training is part of their normal routine.

Executive Summary

Enterprise-level exercises, while valuable, do not meet the more agile, time-critical training needs of small teams, including military units. Small teams learn best when training is part of their normal, daily routine.

In this podcast, Chris May, Technical Manager for CERT's Workforce Development Team, discusses how security and IT professionals can be much better prepared to respond to security incidents by regularly participating in hands-on, scenario-based training.

PART 1: TRAIN AS YOU FIGHT: USE SCENARIO-BASED EXERCISES

Phases of Training: Crawl, Walk, Run

Being prepared and being ready result from practice and experience. Crawl, walk, run is a useful analogy for the stages of training that help staff members become well prepared

"Crawl" is generally typified by classroom-based training. This is useful for removing people from their normal work environment and setting aside dedicated time to learn, hopefully with a good instructor and a solid curriculum.

The downside is that as soon as students leave the classroom, they start losing what they've learned. If they don't use the new content in their daily routine, it dissipates over time.

"Walk" takes this a step further by providing web-based resources that students can access to refresh their knowledge and review course content. CERT's Virtual Training Environment is one example.

Crawl and walk phases are both performed individually. Yet responding to security incidents requires a team where many of the parameters are unknown – not predefined and structured like a real or virtual classroom setting.

Train as You Fight

It is critical to put students in a learning situation that simulates the real, live environments and threat conditions that they are likely to encounter.

Challenges in Developing Realistic Scenarios

Most scenario-based exercises operate at the enterprise level. They take a long time to develop and happen on an infrequent basis – a few times a year at best.

They can involve hundreds of people with a large number of scenario characteristics, multiple objectives, and a complex technology environment. This type of exercise isn't appropriate when working with small military units, teams, or organizations.

Working with Small Teams

Ideally, small teams learn best when training is part of their normal operating procedures and daily routine – an hour a day or a few hours a week. The goal is to offer this for reasonable cost and effort.

PART 2:TRAINING GEOGRAPHICALLY DISTRIBUTED TEAMS: CERT'S XNET

Training a Distributed Team

One typical approach is video teleconferencing (VTC). The best approach is to create virtual meeting space where the entire team can work together, using all of the assets they would normally have if they were meeting in the same physical space.

CERT's Exercise Network (XNET)

XNET provides a comprehensive, scenario-based exercise network by taking advantage of universal access to the Internet and to a web browser.

XNET's objective is to provide continuous access to unit-level operational readiness, training, and evaluation. The goal is to make access to training part of normal daily operations for CSIRTs (Computer Security Incident Response Teams).

XNET provides an Internet/web-browser interface to the same collaboration tools a team would have if they shared the same physical space: whiteboards, being able to look over one another's shoulder, chat, event logging, and access to wikis.

XNET uses visual, graphical images to display network maps/topology diagrams. Users can click on a network component to see what's happening, for example, with a firewall or intrusion detection system.

The objective is to be convenient, easy, and intuitive to use. This allows trainers to focus on the exercise, not on the infrastructure required to run it.

How an XNET Scenario Works

Objectives for an exercise address these questions:

- What are the threats that my responders need to prepare for?
- How can I shape the scenario to increase their readiness?

Typical scenarios include incident response, assessment, penetration testing, and network defense. A scenario designer can use existing library components or build custom ones.

Everyone logs into the exercise with specific roles as part of a team. The role determines the level of access. Using incident response as an example:

- The appropriate infrastructure components are provided, such as access to security systems (intrusion detection, firewalls) and logging servers.
- Access for network and system administrator roles may be limited to routers, switches, and email systems.
- The red team (the attack force) uses a script to insert controlled stimuli (suspicious events, attacks) into the network.
- The trainer evaluates students to see how well they detect and respond to each stimuli.

Trainers work with scenario designers to shape the exercise, model the target environment, and determine how the response team and security staff are organized.

PART 3: USING XNET FOR SIMPLE AND COMPLEX SCENARIOS

XNET for a Reserve Unit

Because a military reserve unit meets one weekend per month, their time for training is limited.

XNET is configured to present a short, 3-hour, targeted scenario called a Targeted Analysis and Response Challenge Track. Reservists log in and are presented with a well-defined directive or mission where they respond to automated attack injections. Team responses are also predefined.

XNET presents a graphical representation of the exercise timeline, where events can be dragged and dropped onto the timeline. Events are universally applied to all teams participating in the exercise.

Advance work to create the exercise definition (conditions, standards, expected responses, timeframes, etc.) permits the trainer or evaluator to monitor team performance against expectations.

Trainers can extend or stop the scenario at any point to walk through what has happened and discuss results with the team.

Each exercise finishes with an after-action report where everyone discusses what went well and what needs improvement.

Taking Advantage of Scenario Libraries

Trainers and scenario designers need to specify roles, timelines, expected outcomes, and trainer interaction well in advance.

XNET makes this critical preparation easier by providing a library of events and scenarios or situations that can be combined, reused, and customized.

Experience indicates that library content can be used to quickly develop an 85% solution for meeting a given training objective.

XNET's objective is to make it easier for trainers and students to practice for incident response and network defense.

XNET's Current State and Future Plans

CERT is currently piloting XNET with a number of government organizations to develop scenario libraries. This requires a direct engagement or relationship between the organization and CERT.

In the future, XNET will present a service model interface, where users can choose a scenario of interest and launch it with the push of a button. XNET will provide an interface where trainers can:

- control their user population
- build their user accounts
- allow users to log in, assume a role, and run a defined scenario

This capability is planned for calendar year 2009.

Resources

CERT XNET brochure (pdf)

For further inquiries, send an email to xnet-info@cert.org.