

Traditional classroom training and paper-based “tabletop” exercises are only moderately effective in preparing organizations to respond to real-world cyber events. There is simply no replacement for experience and practice. The goal of XNET is to provide organizations with convenient and continuous access to realistic and flexible cyber-training scenarios. This experiential approach allows leaders to assess and improve the cyber-readiness of their personnel and command and control processes.

The CERT XNET development team can work with your organization to shape these scenarios to model your environment, mission requirements, and training objectives. The use cases for XNET are extensible and can range from weekly, 3-hour threat management challenges for small teams to annual, enterprise-wide, multi-day cyber-reaction exercises.

If you want to “raise the bar” on your organization’s cyber-readiness program, email: xnet-info@cert.org

For more information, email the XNET development team:

xnet-info@cert.org

www.cert.org

About CERT

CERT engages in cutting-edge research and development and also provides robust training and education programs focused on ensuring that software developers, internet security experts, network and system administrators, and others are able to resist, recognize, and recover from attacks on networked systems.

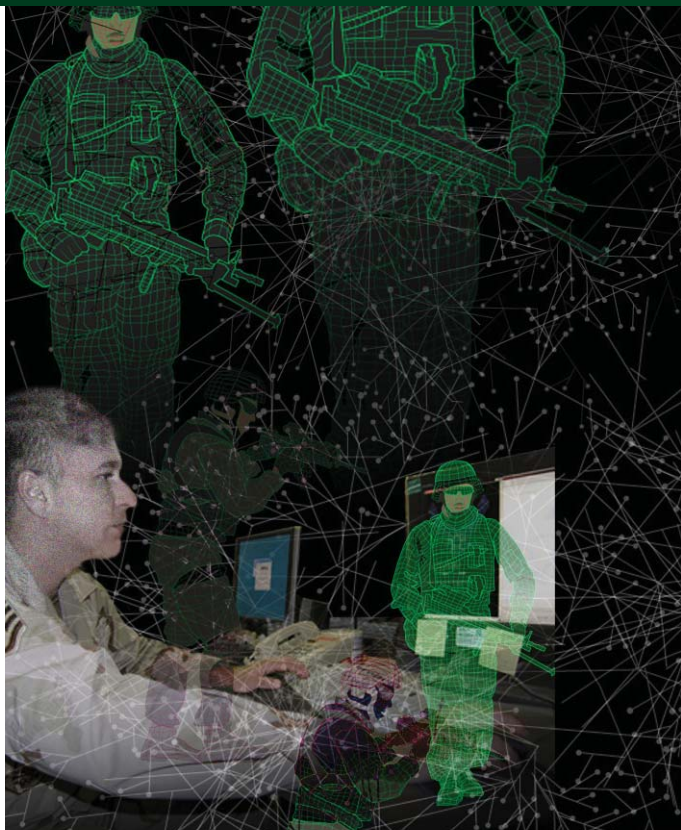
The CERT® Program is part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania.



XNET
CERT® Exercise Network

CERT® Exercise Network (XNET)

Government and large corporate organizations regularly conduct cyber-training exercises to improve network defense and incident response operations. Developing, organizing, and administering these exercises poses many challenges, and resource constraints are often the weak link. It is expensive to build scalable training environments and problematic to assemble and organize the participants.



Addressing Challenges

CERT's XNET was designed to overcome and mitigate these challenges. XNET can provide "push-button" deployment of multiple, simultaneous exercise environments where participants interact within their customized scenario. A centralized, isolated, and dedicated exercise environment significantly reduces the setup and configuration time associated with hosting an exercise. As a result, exercise preparation can focus on developing training objectives and scenarios, rather than on configuring infrastructure.

Traditional approaches are flawed for a variety of reasons:

- Some of the exercise activities are simulated or otherwise artificial in nature, thereby detracting from the operational value.
- It is often difficult to objectively measure the effectiveness of the event as it relates to mission readiness.
- After achieving a successful, realistic exercise event, it is difficult to reproduce that event at other locations with different participants.

XNET is designed to specifically address these challenges to operational training. XNET is an extensible training environment that provides a realistic and scalable multiple-team, scenario-driven exercise capability.

Flexible Scenario

The training network can be configured to suit the specific type of training required. Scenarios can be developed for incident response and forensics, vulnerability assessment/penetration testing, computer network defense, intelligence acquisition, critical infrastructure protection, and more. These scenarios simulate realistic operational conditions and provide context, exercise command and control, and structure to the event.

The computers and network devices of the XNET are virtual, rather than physical, which provides push-button control for switching scenarios or modifying existing scenarios. The virtual nature of the exercise infrastructure simplifies administration while allowing training events to scale to hundreds of globally dispersed participants.

Universal Access

Participants in an XNET training exercise access the environment through a standard web browser. They are presented with an "exercise portal" from which they can communicate with teammates and access their training network resources. This portal essentially assembles the team in the same "virtual room," so participants can be physically located anywhere in the world and yet experience exercise events and accomplish the training tasks together. The exercise network is isolated from the participants' home networks through controls in place at the portal; however, it also provides for "out of band" upload and integration of participants' favorite tools and applications.

Structured Control

Structured control maximizes training effect. Exercise controllers or trainers initiate events to guide participants and teams into and out of situations that facilitate certain training objectives. XNET includes components that provide a robust threat model so that many situations can be developed without the use of a full-scale Red Team. Further, the environment can be equipped to track events and actions, allowing the controllers to quickly and comprehensively assemble the teaching points and lessons learned during an exercise. XNET also provides for "on-the-fly" management of the exercise infrastructure, so controllers can start, stop, and reset network resources at will.