Carnegie Mellon University
Software Engineering Institute

GHOSTS

A Framework for Realistic NPC Orchestration

DELIVER STATE-OF-THE-ART CYBER DEFENSE TRAINING EXERCISES. As the need for cyber defense grows, finding effective ways to prepare cyber teams to face complex challenges becomes critical. More than ever, there is a need for high-quality simulations that help cyber teams ensure that they are ready for real-world operations.

Ramping Up the Realism

Introducing the GHOSTS Framework

From a training participant's perspective, realism is the most crucial aspect of a successful cybersecurity training exercise. When simulations convincingly mimic real-world scenarios, participants are more engaged, and cyber exercises achieve training objectives more effectively.

To create the kind of realism that makes training exercises truly immersive and engaging, we, in the CERT Division of Carnegie Mellon's Software Engineering Institute, developed the "General Hosts," or GHOSTS non-player characters (NPC) framework. GHOSTS uses sophisticated artificial intelligence to create highly realistic training environments.

During training, participants conduct missions where they interact with simulated characters that behave realistically without human intervention. The result is a training experience that looks just as real as what cyber teams might see daily during normal operations.

This level of realism offers training that approaches real-world experience. When cyber teams encounter realistic network traffic and personnel on the wire, they master the skills they need to perform their assigned mission capabilities at elite levels.

True-to-Life Characters

One of the most powerful aspects of GHOSTS is the unparalleled realism it achieves through the characters it creates. Participants in training are more likely to immerse themselves in an exercise when it provides authentic network traffic driven by a broad range of characters that behave with human motivations and biases, from office workers creating spreadsheets, to students shopping for shoes, or malicious state agents attacking networks. We aim for each piece of the simulation to appear as authentic as possible, from the documents created by an office worker to the network traffic generated by a shopper.

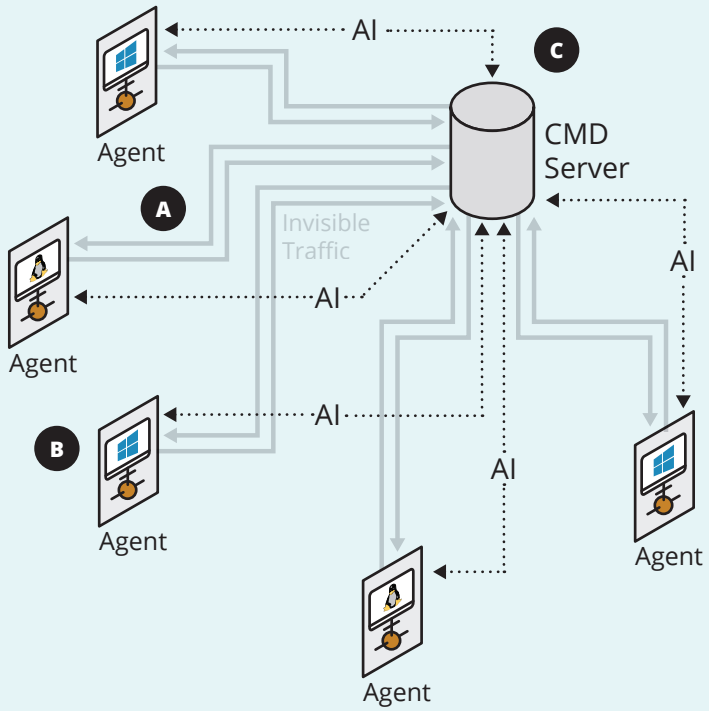
The simulated characters that participants interact with can perform many functions, such as web browsing, executing terminal commands, sending emails, or managing office documents. The functions appear as if real people were performing them, and none can be traced back to the GHOSTS software directly, making the training experience more lifelike and convincing.

How GHOSTS Works

The GHOSTS framework installs raw binary agent software on selected virtual machines. These agents check in to a command server where they receive instructions and alignment, giving them the ability to act as reasoning and biased characters in the simulation. When an agent receives instructions and alignment, they become non-player characters (NPCs) in the exercise..

Distinctions Between GHOSTS Agent and NPC Concepts

Layer	Represents	Actions	Capabilities	Alignment
Agent	Raw Software	General	Automated	Neutral
NPC	Human Persona	Specific	Reasoned	Biased



GHOSTS Highlights

GHOSTS provides the realism that is missing in cyber environments that lack random, independently generated traffic from multiple sources to multiple destinations.

A. GHOSTS uses vTunnel to hide the connection to the central command server from exercise participants.

B. Artificial intelligence powers non-player characters to create realistic and self-directed communications.

C. Event managers can give instructions to any number of GHOSTS clients from a central command server.

Explore Our Tools Online

SEI cyber training tools can be used to create cybersecurity training to help students learn in near-real-world situations without risking organizational assets.

See the latest information about these tools on our website at **sei.cmu.edu/go/cwd-tools**.

Get Started Today

GHOSTS has now been deployed to three live-fire cyber exercises administered by the CERT Division, and the feedback has been overwhelmingly positive from both participants and administrators. In the upcoming year, GHOSTS will be deployed to dozens more exercises.

Contact us today to discuss how we can help you improve your cyber defense training exercises.

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu