CMU Ghosts to Simulate a Cybersecurity Environment and Detect Novelty

Larry Holder, Vincent Lombardi, Timothy Reidy, Washington State School of EECS

Problem Statement
As the world becomes even more tech focused, there is a need for detecting possible security threats that cannot be detected by a person or team. The training and evaluation of AI-based techniques for detecting novel security threats would benefit from a realistic synthetic data generator for enterprise security scenarios.

CMU Ghosts
A framework built for simulating a user environment. Creates agents and their interactions similar to how an office or company would interact.

We are using this framework to develop an AI that can detect novel situations. More specifically, we want this AI to be able to detect possible insiders who are compromising security of the simulated environment.

-What is Novelty?
-Novelty is described as a situation or data that differs from the previous data, or data that has been introduced previously.

-What is an Insider?
-An insider would be an agent that is acting in ways that differ from the expected patterns of other agents but attempting to hide their actions, similar to how someone in real life could leak or steal secrets or volatile information.

Expansions on the System
In the future the system could be used to create active intervention scenarios, in which an AI or person could actively intervene as opposed to just using an AI to interpret data like we are using the system. The figure above describes how this scenario would be organized.

Ghosts for Data Generation
The purpose of setting up Ghosts is so that we can use the system to generate a log of user behavioral data and then use this data to evaluate an AI's ability to detect the insider.

References
-Software Engineering Institute, CMU, “Ghosts, A Framework for Realistic NPC Organization”
-CMU Ghosts GitHub: https://github.com/cmu-sei/GHOSTS

Acknowledgment
The Griffiss Institute with support from award no. SAA 10012021MM0336, a VICEROY Project entitled Northwest Virtual Institute for CyberSecurity Education & Research (CySER)