Project Host Organization: Microsoft Corporation

Description of the Organization: Microsoft is a technology company with interests in software development, computer hardware, consumer electronics, cloud computing, and video games.

Contact Person Information:

Name: Mark Yu
Title: Support Eng Manager
Department: Azure Security, Identity and Management
Phone: +1 778-812-5201
E-mail: markyu@microsoft.com

Project Title: Wilson: Azure Cloud Lab Chamber

Project Members: Carter Codell, Jason Hewgill, Stephen Neville, Sheetal Singh, Brianna Weinstein

Project Description:

This project revolves around the idea of a "Blue Team Lab Builder" for Azure. The plan is to create a tool that allows a training manager to easily build an automated environment for blue team practice in Azure. The training manager writes a Terraform configuration file to automatically build Azure resources. In a second configuration file, the manager specifies cloud attacks to be automatically run at certain times. This simulates a live environment for analysts to detect and stop attacks.

Expected deliverables:

- Platform for building and deploying Azure labs
- Sample template files for Azure training labs
- Configuration files and scripts that demonstrate the various cyberattacks for the labs
- Answer keys that show how to identify and stop the attacks using a SIEM

Tools/Resources/Skills Required for the Project:

- Azure
- Terraform for Azure template creation
- Jenkins for Azure template management and pipelining
- cron or another automation tool for automatically replaying attacks
- Bash and Powershell for scripting attacks
- MITRE ATT&CK Matrix for identifying common attacks
- ELK or Azure Sentinel for the trainees' SIEM
- Azure Playbook for implementing changes to the environment