Black Sabre Response

Project Closure Report

# Performance of the Project Management Team

The Team successfully created an IRTx where red and blue playbooks were tested and made to simulate a real life scenario. Each member had clear roles and these were followed.

The team successfully met the project target as set in the Project Charter e.g. create playbooks, test, run the scenario etc.

Better timeline could have been done when starting the project but the team still managed to get all work completed in reasonable time. The playbooks could have also been made more clear

Each member took on their roles and fulfilled all responsibilities of that role to the best of their abilities

# Project Management Closure

The original timeline of events and expected results is inaccurate as the dates initially set were incorrect and 2 months too early. However all parts were completed in reasonable time and still followed the same structure as the original planned timeline

The team kept all risks to a minimum meaning there were not disruption doing the exercise. No recommendations are needed for the risk strategy.

The team performance was viewed against three major objectives

1. Evaluation of current IRP
   1. The team created an evaluation of Midtown IT’s current IRP and made recommendations to it. This was then sent to the CSO
2. Creation of playbooks
   1. The team brainstormed and created the playbooks for both red and blue team. These playbooks were also tested to ensure everything works and the attacks will get detected.
3. Running the Scenario
   1. The team ran the scenario with another team using the red books to perform the attacks on our network. Our team successfully identified all attacks that the other team performed thus making the IRTx successful

Improvements

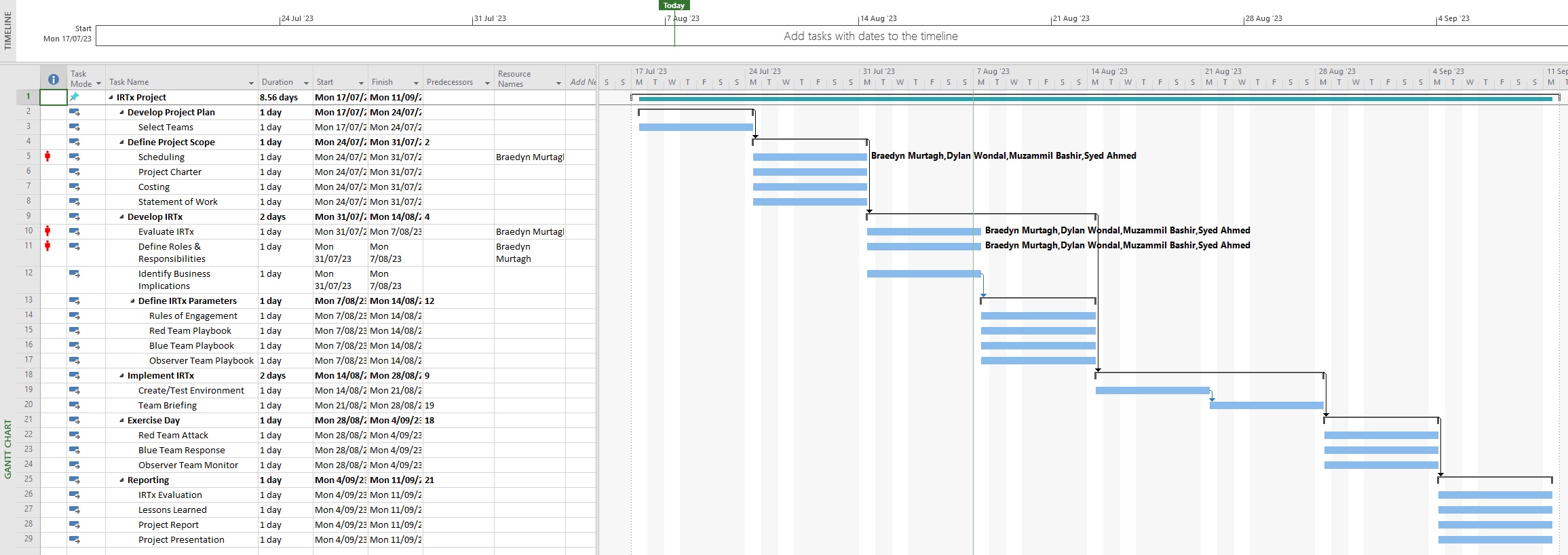
1. Create a better timeline with accurate dates as per stakeholder information
2. Make the runbooks less vague so they are easier to understand and follow
3. Give the attacker machine internet access so that reverse shell code isn’t stored on the desktop thus making the scenario more realistic.

End user training

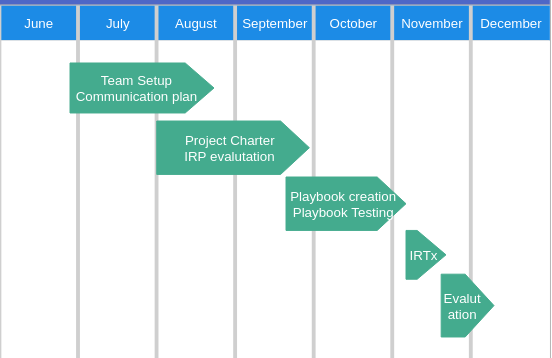
With any new tools installed as part of the updated IRP, user training will need to occur so that the user will know how to use the new tools. This training can be official from the tools company or unofficial inhouse/online training on how to use the tools.

Expected vs actual timeline

expected:



Actual (everything completed later due to incorrect dates on original timeline)



SIGN-OFF