Knowledge Objectives

ThreatGEN® Red vs. Blue Cybersecurity Gamification Platform

Author: Gerald Auger, Ph.D.
Director of Cybersecurity Education && Cybersecurity Manager, ThreatGEN

Date: June 13th, 2022

Purpose

This document outlines knowledge objectives for students using the ThreatGEN® Red vs. Blue Cybersecurity Gamification Platform as a learning utility. These knowledge objectives align with Bloom's Taxonomy1. The experience and learning outcomes differentiate based on which cybersecurity simulation role a student assumes.

Background

Platform

The immersive simulation platform allows students to operate in an environment that simulates a business Information Technology (IT) and Operational Technology (OT) production environment. Students assume an attacker perspective (e.g. Red Team) or a defender perspective (e.g. Blue Team) within each simulation. Students may play against other human opponents or an active adversary computer-controlled opponent.

Bloom's taxonomy

Bloom's taxonomy is a recognized utility for developing educational objectives for students and allowing these objectives to be properly mapped to learning levels that are appropriate. It allows educators to enable students to build upon basic learning elements ultimately developing higher-level thinking.

Knowledge Objectives

The knowledge objectives are categorized by cybersecurity simulation role assumed by the student. Student experience and learning outcomes develop over time as the students becomes more engaged with the platform. This is explicitly identified with sub-knowledge objectives based on iterations of simulation experience, and highlights students begin learning as early as the first play through. These learning objectives are intended for a student without prior experience in information security.

Students experience immersion, rules and goals for defending or attacking an IT and OT environment, and managing conflicts in a realistic production environment.

The following knowledge objectives align to student experience operating as the "*Blue Team*". Bloom's taxonomy level is included as a preface for clarity and convenience.

1) Game level objective (Blue)

    a. (Evaluate) By the end of the course, students will be able to compare the efficacy and choices in building an information security program.
    b. (Understand) By the end of the course, students will be able to explain red team and blue team operations and how they relate to each other
    c. (Understand) By the end of the course, students will be able to generalize techniques to secure an organization's IT infrastructure

2) Course level objectives (Blue first play)

    a. (Remember) By the end of first play through, students will be able to name different types of cybersecurity controls
    b. (Understand) By the end of the first play through, students will be able to discuss the resource costs associated with building an information security program
    c. (Remember) By the end of the first play through, students will be able to recognize normal operating conditions and incident response operating conditions

3) Course level objectives (Blue multiple plays)

    a. (Remember) By the end of multiple play throughs, students will be able to label a basic network diagram
    b. (Understand) By the end of multiple play throughs, students will be able to explain when incident response is activated and why
    c. (Remember) By the end of multiple play throughs, students will be able to name different types of vulnerabilities
    d. (Understand) By the end of multiple play throughs, students will summarize different conditions that could lead to catastrophic organizational failure from a cyber incident

The following knowledge objectives align to student experience operating as the "*Red Team*".

1) Game level objectives (Red)

    a. (Understand) By the end of the course, students will be able to explain red team and blue team operations and how they relate to each other
    b. (Apply) By the end of the course, students will be able to express the order of operations for a successful cyber-attack (i.e., cyber kill chain)
    c. (Understand) By the end of the course, students will distinguish between Internet-based and on-premises attack techniques

2) Course level objectives (Red first play)

   a. (Remember) By the end of the first play through, students will be able to name different types of offensive security activities
   b. (Understand) By the end of the first play through, students will observe target IT environment visibility increase over time
   c. (Remember) By the end of the first play through, students will recall the activity and output of reconnaissance

3) Course level Objectives (Red multiple plays)

   a. (Understand) By the end of multiple play throughs, students will classify different types of cyber attacks
   b. (Understand) By the end of multiple play throughs, students will explain how organizations can be compromised by a cyber-attack over the Internet
   c. (Analyze) By the end of multiple play throughs, students will differentiate between denial of service and manipulation attack impacts

Conclusion

The ThreatGEN® Red vs. Blue Cybersecurity Gamification Platform has educational "*scaffolding*" incorporated into its design to guide students through the simulation while allowing them to make their own decisions and learning through immersive exploration. This scaffolding manifests in allowing students the choices and paths to pursue that would only be appropriate for that point in the simulation, unlocking decision points when prerequisites are met.

Copyright