THE IMPORTANCE OF GAMIFICATION IN CYBERSECURITY TEAM TRAINING AND READINESS

Laura Lee
Executive Vice President,
Cyber Training and Assessments
Laura.lee@circadence.com
ABOUT THE SPEAKER (}
<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key cyber terrain and risks</td>
<td>Organizational assets and data</td>
<td>Unauthorized access &amp; data breaches</td>
<td>To Cybersecurity Events and Attacks</td>
<td>Normal Operations and Services</td>
</tr>
<tr>
<td>Perform Asset Management</td>
<td>Manage Access Control</td>
<td>Perform Anomaly Detection</td>
<td>Conduct Response Planning</td>
<td>Conduct Recovery Planning</td>
</tr>
<tr>
<td>Proceed under Proper Governance</td>
<td>Secure Data</td>
<td>Maintain Detection Processes</td>
<td>Conduct Analysis to Develop COA</td>
<td>Improve Response Capabilities</td>
</tr>
<tr>
<td>Conduct Risk Assessment</td>
<td>Employ Info Protection Processes</td>
<td></td>
<td>Perform Mitigation Activities</td>
<td></td>
</tr>
<tr>
<td>Develop Risk Management Strategy</td>
<td>Manage Maintenance of Systems</td>
<td></td>
<td>Improve Response Capabilities</td>
<td></td>
</tr>
<tr>
<td>Employ Protective Technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Grey out are longer term tasks that are not part of an elite Cyber Defense Team.

Perform Mitigation Activities
- Report Attack
- ID Vector
- Prepare COAs
- Coordinate
- Conduct COA
- Validate COA

Course of Action (COA)
CHALLENGES FOR TRAINING CYBERSECURITY PROFESSIONALS

HIGH COSTS   SCALABILITY   AVAILABILITY   SKILLS RETENTION

"As technology changes the skills needed for each profession, workers will have to adjust….requiring a greater emphasis on lifelong learning and on-the-job training, and wider use of online learning and video-game-style simulation."

June 25, 2016
The Economist
TYPES OF PROJECT ARES ACTIVITIES

- **Missions**
  Missions where you prove you can think through a problem end-to-end

- **Battle Rooms**
  Battle Room with certification tasks for different work roles

- **Games**
  Games on concepts in cyber that need repetition
PROJECT ARES v3.0 (MAY 2017)
**PROJECT ARES CASUAL CYBER GAMES**

In this attack technique, the attacker guesses or observes which websites the victim organization often uses and infects one or more of them with malware.
BATTLE ROOMS FOR WORK ROLES
BATTLE ROOM INDIVIDUAL SKILLS

1. Using `iptables`, identify all rules that are in place on the Kali Linux system (id: 19).
2. Use `netstat` to obtain a list of all active (open, established, wait) network connections without doing name lookups (id: 20).
3. Use `nmap` to perform a version scan to identify services and software running on the target (id: 21).
4. Use `apt-get` to install the openvas package on the Kali Linux system from the configured repository (id: 22).
5. Use `hydra` to determine whether there are easily guessable passwords for the root user using the SSH service on the target (id: 23).
6. Use `apt` to get a list of all the installed packages on the Kali Linux system (id: 24).

Kali Linux 172.16.0.11

Attack Network

CentOS Router 172.25.42.250
172.16.0.250

Target Network

Linux Server 172.25.42.1

All Players

01/04/2017
rob_player 10:09
hello
rob_player 21:31
how do i discover open ports on host

04/01/2017
ilee 18:52
Good evening fellow team mates

04/17/2017
rprouty 21:46
good evening
ilee 21:57
Hello Mate

Enter text...
MISSION PLAY (INDIVIDUAL, CREW AND TEAM PLAY)
CYBER TOOLS AVAILABLE ON MISSION
Replay of user commands, chat and opponent actions
MISSION SCORE

**COMPLETE MISSION I - DISABLE BOTNET**
DURATION - 03:30

**203**
Quiz

**122**
Recon Network

**442**
Objectives

**767**
Total Points

**23 XP**

**22 XP**

**12 XP**

**57 XP**

**1,034,233 XP**
LEVEL UP 2,000,000

**LEADERBOARD**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Team Name</th>
<th>Duration</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Team Arasander</td>
<td>03:12:54</td>
<td>234,032</td>
</tr>
<tr>
<td>2</td>
<td>Team Tucker</td>
<td>01:21:33</td>
<td>212,840</td>
</tr>
<tr>
<td>3</td>
<td>Team Farmer</td>
<td>03:43:54</td>
<td>204,304</td>
</tr>
<tr>
<td>4</td>
<td>Team Price</td>
<td>04:22:24</td>
<td>203,697</td>
</tr>
<tr>
<td>5</td>
<td>Team Reid</td>
<td>01:14:55</td>
<td>203,232</td>
</tr>
<tr>
<td>15</td>
<td>Team Carson</td>
<td>02:33:21</td>
<td>150,207</td>
</tr>
</tbody>
</table>

Slide 15
MISSION COMPLETE: TROPHY CENTER

Current awards and past mission history is available to replay.
Players earn experience points as they play games, work in Battle Room or go on mission.
• Categories – Protect & Defend, Investigate (Digital Forensics)

• Specialty Areas (4)
  – Enterprise Network Defense Analysis
  – Incident Response
  – Infrastructure support
  – Vulnerability Assessment and Mgmt

• Work Roles (45)
  – Security Analyst
  – Incident Analyst
  – Penetration Tester...

• Competencies (~200 combined into 18)

• Tasks (~115)
Games Can Provide an Effective Method of Teaching Cyber

Generation-Z is Well Suited for Cybersecurity
- % Raised with DIY education and crowd sourcing
- % Digital Natives experienced in research and collaborating with others on-line
- % Talk about making an impact in the world
- % Routinely Multi-task across five screens
- % Over 60% list gaming as their primary form of entertainment
- % Not just “tech-savvy” – they are ”tech-innate”
EVERYTHING I LEARNED, I LEARNED FROM ENDER’S GAME

“I need you to think of solutions to problems we haven't seen yet. I want you to try things that no one has ever tried because they're absolutely stupid.” -- Ender Wiggins

The games are designed to harness the creativity of children and channel that to mold them into skilled soldiers, tacticians, and leaders to save the world.

Ender’s Game is a 1985 military science fiction novel by American author Orson Scott Card and 2013 LionsGate Film.