1/32/20201

Jon Mahoney

penn state university

Cyber Range Evaluation

# Introduction

For my evaluation of three different cyber ranges, I chose to take a closer look at Cloud Range’s platform, Raytheon’s platform, and Circadence’s platform. I chose these organizations because they each offer a unique experience and serve different corners of the cyber range market. When creating my cyber range rubric, I chose to include cost as a factor to be considered for grading. Through my research, I determined that it is unrealistic to grade most cyber ranges by cost because there often is not a price available without contacting a salesperson. This is due to the fact that many cyber ranges can be customized for an organization and their price will reflect that. For instance, the Raytheon cyber range relies on an emulated version of an existing network environment whereas something like Project Ares offers a less negotiable price for a less customizable package. For these reasons, I will be replacing the cost category with the category “level of technical support offered”. Technical support can consist of aiding an organization in creating a realistic environment for simulation or something as simple as solving glitches and bugs in an exercise. The criteria I will be using to grade the various cyber ranges are ‘the extent of graphical capabilities’, ‘level of technical support offered’, ‘ease of use’, ‘functional capabilities’, and the ‘level of training available on the platform’. After a breakdown of each platform, the rubric detailing the final score is included.

# Cloud Range Evaluation

Extent of graphical capabilities (10 / 10)

As for the Cloud Range’s graphical capabilities, the interfaces are standard with many aspects that are recognizable from other programs and tools. For instance, there are images of a network activity where a network topology is displayed in addition to a side panel of “training info” and a tracking list of the “training activities”. The cloud range graphical interfaces are a good example of providing useful information without distracting the user from the lesson.

Level of technical support offered (10 / 10)

Cloud Range provides above average technical support through their cloud range hosting services and their customization of the cyber range. Cloud Range’s cyber range hosting service can help reduce the overall cost of a cyber range program to an organization and prevent any unnecessary strain on the organization’s networking resources. Additionally, Cloud Range provides customized system replicas and customized lesson sessions which contributes to better learning overall.

Ease of use (do the platform systems enhance learning or are they intrusive/distracting?) (15 / 15)

Two areas that increase the cloud range’s rating is the presence of a learning management system, and the provision of live instructor-led classes. These two areas can be integrated to a training plan to enhance the exercises by providing further context and information. Instructors that are familiar with the exercises can provide criticism or alternate methods and solutions. Additionally, after-action reports completed through the learning management system provide an extra layer of analysis. Overall, these systems enhance learning.

Functional capabilities (ability to simulate the range of Cybersecurity problems/events in the "real world" (30 / 30)

The cloud range virtual training platform scenario library contains many of the most common cyberattacks like SQL injections and man-in-the-middle attacks. Additionally, the platform offers the ability to mirror an organization’s network environment to be used in the exercises. I would describe the functional capabilities and realism of the training platform as above average due to the provision of team exercises and the use of live industry standard tools.

Level of training on the platform available (25 / 35)

The cloud range virtual training platform contains a library of cyberattack scenarios of varying difficulty. All the listed scenarios begin with an identified attack of varying difficulty ratings and the user must implement the solutions necessary to prevent further damage and remediate the attack. The scenario difficulty ratings begin at “novice” level and progress to “intermediate” and “advanced”. I selected an attack scenario from each difficulty rating and took a closer look at the value being presented. For the advanced category, an attack scenario that caught my attention was the Ransomware exercise where an employee opens an attachment from a malicious email which results in the encryption of their system. The exercise description further elaborates that the trainee examines the image of the affected server. While it is important to be prepared for a variety of incidents that may occur, a reactive response to ransomware is less valuable than proactive barriers that can be put in place to prevent them such as well-established infosec policy training so the employee would not open the malicious attachment in the first place. This is an exercise in which I would describe as less than satisfactory for “level of training” as it uses a very basic method of exploitation (social engineering email) for a particularly serious form of cyberattack. In other words, It seems as though the “advanced” training of dealing with ransomware is undermined by the simpler solution to train employees to identify phishing emails.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Criteria | Insufficient | Sufficient | Exemplary | Score 85/100 |
| Extent of Graphical Capabilities |  | Standard graphics that aren’t distracting |  | 10/10 |
| level of technical support offered |  |  | Offers hosting of customized cyber range | 10/10 |
| Ease of Use |  |  | Cyber range comes with a learning management system and instructors | 15/15 |
| Functional Capabilities |  | Cyber range can be designed to mirror real system design |  | 30/30 |
| Level of Training on the Platform Available | Based on the exercise descriptions, some are too rudimentary |  |  | 20/35 |

# Raytheon Cyber Range Evaluation

Extent of graphical capabilities (10 / 10)

The Raytheon cyber range platform has underwhelming graphical capabilities. That being said, the lack of graphics better serves its targeted demographic of users. Because the Raytheon cyber range is marketed as a platform that teaches professionals to deal with advanced threats, it is best to have as little in the way of the information as possible.

Level of technical support offered (10 / 10)

Raytheon is an above average provider of technical support because they provide the ability to simulate advanced threats on an emulated version of an existing network.

Ease of use (do the platform systems enhance learning or are they intrusive/distracting?) (15 / 15)

As I mentioned above, the Raytheon cyber range has the bare minimum when it comes to graphical systems. Compared to a platform like Project Ares, the minimalist graphics are more conducive to an advanced learning environment, whereas Project Ares is best for beginner and intermediate learning environments.

Functional capabilities (ability to simulate the range of Cybersecurity problems/events in the "real world" (30 / 30)

The Raytheon cyber range is described as a platform that is designed to simulate existing and future systems against cyberattacks. While I could not find further information on the process of simulating futuristic information systems, I found that Raytheon provides functionality that allows users of the cyber range to create an emulation of a real system. The specific environments listed for emulation support include critical infrastructure such as power grids and water supply.

Level of training on the platform available (35 / 35)

As for the level of training available on the platform, Raytheon beats many other cyber ranges. Raytheon separates itself from other cyber range providers due to the facts that they offer training against nation-state threats. This is a slice of the cyber range market that is mostly uncontested as most cyber range platforms follow some sort of difficulty rating to teach beginner or intermediate users. Nation-state cyberattacks are often orchestrated by highly skilled and highly funded actors so the exercises are likely incredibly challenging and advanced. Before beginning a program with the Raytheon cyber range, it is important to consider the threat of a nation-state to your organization. It is far less likely for any single company to be specifically targeted by nation-state hackers. For example, an article from the website Statista claims there were 1.5 million known data breaches in 2019. Out of the 1.5 million known data breaches, approximately 40,000 of them were identified by Google as known nation-state sponsored cyberattacks which reinforces the idea that nation-state cyberattacks are far less common than other forms of cybercrime. Depending on the industry and size of the organization, this training varies in usefulness. For instance, for a professional who is training to maintain the systems that operate critical infrastructure, learning to deal with nation-state threats is likely far more useful than someone who maintains systems for a small retail company.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Criteria | Insufficient | Sufficient | Exemplary | Score 100/100 |
| Extent of Graphical Capabilities |  | Underwhelming graphics that sufficiently serve their demographic of users |  | 10/10 |
| level of technical support offered |  |  | Simulates advanced infosec challenges on an emulated version of the user’s network | 10/10 |
| Ease of Use |  | Minimalist approach to systems and graphics |  | 15/15 |
| Functional Capabilities |  |  | Simulated environment accurately addresses modern advanced threats | 30/30 |
| Level of Training on the Platform Available |  | Primary focus is on advanced threats, it is unclear the degree of training available outside of advanced threats |  | 35/35 |

# Project Ares Cyber Range Evaluation

Extent of graphical capabilities (10 / 10)

Of the cyber ranges I have described so far, Project Ares is without a doubt the leader in graphical capabilities. In fact, the entire premise of Project Ares is providing technical skills through a gamified experience and is likely the most graphically intensive cyber range on the market.

Level of technical support offered (10 / 10)

Unlike the other cyber ranges I described above, Project Ares does not allow the same level of customization and provides a uniform experience. This is largely due to the gamified nature where the platform resembles a large multiplayer game. Similar to how each player of a multiplayer game is playing on the same version, each user of Project Ares is interacting with the same cyber range.

Ease of use (do the platform systems enhance learning or are they intrusive/distracting?) (5 / 15)

While project Ares does provide a visually appealing experience, many of the gamified systems can be distracting to users. For instance, a Project Ares exercise environment is called a “Battle Room” where the user earns points that contribute to the user’s experience level. I am personally uninterested in turning learning exercises into game-like experiences and I think I would perform better in an environment more conducive to learning than entertainment. That being said, I’m certain there are demographics who could do better in an environment like the one provided in Project Ares.

Functional capabilities (ability to simulate the range of Cybersecurity problems/events in the "real world" (30 / 30)

Project Ares provides many scenarios that replicate challenges faced by infosec professionals in real life. These scenarios vary in difficulty and Project Ares allows for the scenarios to be tackled in different ways. That being said, the user’s score may decrease or increase depending on the methods they use and the amount of time they take. According to Circadence, Project Ares activities such as battle rooms and missions can be completed for the purpose of earning different infosec certifications. This process involves navigating to the Circadence website and confirming the different activities the user has completed. The user’s activity report is then reviewed by Circadence and if the activities fulfill requirements for certifications, Circadence then returns a Project Ares certification that can be submitted to infosec organizations such as CompTia. While users do not earn certificates outright, there is often overlap in the content provided in Project Ares and the content provided in certification courses. In the cases where there is overlap, users will often earn credit in their certification courses accordingly.

Level of training on the platform available (35 / 35)

Project Ares provides plenty of training on the platform through exercises. These exercises vary in difficulty but provide training at a level which is comparable to the training received from many infosec certification courses. According to Circadence, the Project Ares exercises have an overlap of approximately 30% - 70% with the content provided in different infosec certification courses. For this reason, Project Ares becomes a satisfactory supplemental tool for new members of the infosec community without experience or a large set of skills.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Criteria | Insufficient | Sufficient | Exemplary | Score 90/100 |
| Extent of Graphical Capabilities |  |  | Graphical capabilities are industry leading | 10/10 |
| level of technical support offered |  | Unlike other ranges, Project Ares offers a uniform experience among users (does not allow customization). More of a design decision than a drawback. |  | 10/10 |
| Ease of Use | For the demographic of undergrad students, Project Ares’ visuals are too distracting |  |  | 5/15 |
| Functional Capabilities |  | Provision of gamified training exercises |  | 30/30 |
| Level of Training on the Platform Available |  |  | Provides training in line with that which is expected of certification organizations | 35/35 |

# Sources:

<https://www.forbes.com/sites/daveywinder/2020/03/27/hacker-threat-google-confirms-40000-nation-state-cyber-attack-warnings-issued/?sh=9d917a73b71f>

<https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

<https://www.youtube.com/watch?v=ERTBYSSwYrI&t=1235s>