|  |
| --- |
|  |
| Capstone Experience  FALL SEMESTER – IST 894 |
| Cyber Range Evaluation |

|  |  |  |
| --- | --- | --- |
| Carl Laneave | Cjl29 | Cjl29@psu.edu |

TABLE OF CONTENTS

Contents

[1.0 Five Focus Factors 3](#_Toc144673665)

[2.0 Evaluation: Cloud Range 5](#_Toc144673666)

[2.1 Evaluation: Tech Data 6](#_Toc144673667)

[2.2 Evaluation: Simspace 7](#_Toc144673668)

[3.0 Matrix Evaluations 8](#_Toc144673669)

[4.0 Overall Recommendation 11](#_Toc144673670)

# Five Focus Factors

1. **Cost**

The first evaluation factor going into a cyber range will be the overall cost. Cost is a driving factor for any business. Having a clear understanding of both licensing, upgrades and cost is crucial for the success of an overall cyber range product/program.

1. **Scope of Attacks and Complexities**

It is extremely important to understand what scope attacks and the overall complexity available by each cyber range. If a program is too easy without the ability to cover more complex attacks, then the value may be low. In the same regard, if the cyber range only includes incredibly complex attacks, it has no value for entry level individuals. This factor also includes the scope of attacks as well. Having a rich and robust library of attack types, including OWASP top 10 and most common CVE is critical to emulation of real-life attacks.

1. **Level of Environments (Cloud, VM, On Prem)**

The environment and infrastructure landscape has become incredibly diverse. While traditional datacenters as well as VM (VMware) are still an option, cloud has become a huge player. It is critical that the cyber range covers not only the traditional data center attacks but also misconfiguration and security flaws in cloud. The cloud especially has become a critical point of failure in organizations and is an absolute must in the cyber range.

1. **Updates and relevancy**

Attacks are ever evolving, which means the cyber range must be as well. The evaluation must include how often updates occur as well as the relevancy of such attacks. Are updates daily, weekly, monthly, or yearly? Do they include new zero-day attacks or not? By knowing how robust the updates will occur as well as the type of content being updated, we can determine the value of future usage of our said cyber range.

1. **Reviews**

Current and previous customer reviews are a critical insight to a cyber ranges value. By seeing the perceived value from current customers, it is easy to tell the value of customer service, product, and design of the cyber range platform. This factor allows for a snapshot into the cyber range platform prior to ever committing to the actual product.

# 2.0 Evaluation: Cloud Range

Cloud Range is a cyber range platform designed to accommodate all skill levels as well as scenarios available to security professionals. Through their platform enterprises can use pre-designed, as well as custom curriculum development to help their trainees in their security studies. The environments are integrated to provide multiple different types of security tools such as SIEM, firewalls, soc and cloud. The content itself is designed to provide a full-scale catalog of out of the box attack scenarios. These scenarios are a direct tie back to OWASP top 10 and other popular attack vectors.

As far as cost, Cloud Range is the most expensive cyber range that was evaluated. This cost association, as found in our research, reflects the large amount of content and customization that is provided by them. The model for their cost comes from two different options. The first is the per user licensing which is geared more towards smaller companies rather than large scale enterprises. This cost is much higher overall per user. The secondary option would be to buy an enterprise level support license that allows for a pool of users to be maintained and created by the organization itself. The cost is a flat rate and includes key functionality as well as enterprise level support and training.

Cloud range has the largest library of attacks and scope of coverage. Not only do they include attacks on traditional landscapes such as VMs, but also cover cloud centric vulnerabilities in both AWS and Azure. The scenarios and scenario design are extremely robust and allow for customization and scaling difficulty. Their overall design covers both key focus points of our evaluation in both level, volume, complexity of attacks as well as landscapes that are tested against.

Updates related to the platform occur as required to keep it up to date and are included in the license. The content itself is stored as a catalog that is updated as newer attacks occur. No official timeframe was provided but mention ‘as captured’ new attacks are added to the library.

Cloud Range had many positive reviews from customers. Each customer seemed extremely satisfied both with the platform and the level of support provided. The largest complaint noted was around the overall cost for the product itself. The interface, layout and design all received high marks as well. Overall, the platform was marked as worth the cost association.

# 2.1 Evaluation: Tech Data

Tech Data is a cyber range platform that focuses heavily on engagement with their team while using their platform. The focus, while mentioned to be a cyber range platform, is more heavily on certification and training through their program rather than a tool to support our overall organization.

Cost association was challenging when doing the Tech Data evaluation. There were costs related to platform use, hybrid training, certification using said cyber range platform and more. The model seems to focus more on tracks and associated costs to train in said tracks rather than just using the platform. The discounts focused more on the volume of users per track and not on the enterprise level of support.

The library of attacks was again more focused on training and courses at a high level such as mobile device security and penetration testing. It was hard to gauge the actual coverage of said cyber range as it was limited in visibility and seemed to only relate to the track of course selected.

There is no mention of any direct environments being tested against, but each course or track did not cover the scope of anything beyond traditional cyber esq training and infrastructure coverage.

Updates were also a challenge to rate as the updates were directly linked behind track and courses of scoped training. It seems that each track runs from multiple weeks to half day scenarios. There is no mention of how often each is updated.

Reviews were limited and seemed to talk more about the courses offered rather than the cyber range platform itself. Due to this, marks were given much lower compared to the other platforms as this lack of feedback generally means a lower user base.

# 2.2 Evaluation: Simspace

Simspace is the gold standard when it comes to cyber range platforms. The platform was built upon 15 years of research from MIT and boosts the largest number of users on the platform. Furthermore, there are multiple solutions as well-defined verticals of different areas of focus. These verticals include everything from government, financial to critical infrastructure. Beyond the platform itself, Simspace provides attack catalogs quarterly with detailed explanations to said attacks and targets. These updates are free and provided to everyone regardless of licensing.

In relevance to cost, Simspace is the best price per user. While still much higher than enterprise licensing overall, their cost model lends itself the most to smaller companies. The cost is average in comparison to over platforms and overall, not a large driving factor as noted previously by other companies such as Cloud Range.

While not the largest library of attacks and scope coverages, it still provides extensive tracks and verticals for specialized areas of attacks. These verticals such as governance or infrastructure all for IT professionals to focus directly on attacks that would directly impact their day to day professionally. This eliminates the noise and allows the user to train with the most relevant type of attacks for them.

The environments that it covers include cloud, infrastructure, SIEM, firewalls, networks and more. This is where Simspace has the clear advantage, as they provide the absolute largest scale of coverage when it comes to environments. As noted, though, there is no direct call out to an individual cloud provider but rather a blanketed mention that all are covered in different tracks.

Updates are quarterly and include excellent documentation while having no additional costs. Functionality to the platform itself from an update standpoint is quarterly as well and come at no additional cost to the user.

Simspace as noted has the largest user base of all the platforms reviewed. Not only does it have the largest user base, but it’s also got the largest number of reviews of all three platforms as well. The overall view from customers was uniquely positive, noting a great level of happiness with customer service as well as the ability to have unique verticals. The only negative noted was around the ability to create custom tracks and/or programs for users based on the provided catalog item of attacks.

# 3.0 Matrix Evaluations

**Matrix Company: Cloud Range [Score: 70]**

**A screenshot of a computer

Description automatically generated**

**Matrix Company: Tech Data [Score: 46]**

**A screenshot of a computer

Description automatically generated**

**Matrix Company: Simspace [Score: 86]**

**A screenshot of a document

Description automatically generated**

# 4.0 Overall Recommendation

The overall recommendation based on the evaluation of these three vendors is to use Simspace. Not only did Simspace acquire the largest score of the three vendors, but it was also the only tool to cover the scope of all our requirements. Simspace is a trusted industry leader that comes in at a cost that reflects the value being provided to us as a company. Their platform will allow us to grow our staff into better security engineers, as well as prepare us better as a company for potential attacks. Furthermore, all this progress being made is tracked in quantifiable metrics that can be directly fed to leadership to see our progress as a group both in skills and responses to events in emulated environments. Lastly, using Simspace ensures we are getting the best type of attack vectors and verticals. There is no fluff nor unnecessary scenarios for our team, but a focused track to assist in both education and potential prevention.