PennState
College of Information
Sciences and Technology

Cyber Range Evaluation Report

COURSE:	IST: 894
ASSIGNMENT:	CYBER RANGE EVALUATION REPORT (PART II)
SUBMITTED BY:	BRANTLEY PRICE
DUE DATE:	JUNE 1ST, 2025
INSTRUCTOR:	DR. BARTOLACCI

Table of Contents

Introduction

This report evaluates three commercial cyber range platforms: RangeForce, CYBER RANGES, and Cogent Cyber Range. Its purpose is to assist a mid-sized company's decision-makers in selecting a solution that optimally balances cost-efficiency with the user experience necessary for effective enterprise-level cybersecurity training. It is important to note that this theoretical evaluation for a mid-sized company can only be conducted objectively using publicly available information, as I am unable to simulate a mid-sized company accurately. The evaluation uses a custom-built rubric (Appendix A) that assesses each platform across five key factors: Real-World Simulation/Application, Scalability and Performance, User Experience (UX), Quality of Pre-Built Content/Scenarios, and Cost Efficiency. Each factor is scored on a scale from 1 (Poor) to 5 (Excellent) based on available information, vendor transparency, and alignment with recognized best practices. I do my best to maintain objectivity and critical analysis, acknowledging where claims are well-supported and where gaps or uncertainties exist, with my focus on providing a clear basis for strategic investment.

Clarifying Cost-Efficiency vs. Cost-Effectiveness

When developing the rubric for this assessment, I opted to use cost-efficiency over cost-effectiveness. I believe there are subtle but important distinctions between the two, especially for a mid-sized company's decision-makers. Cost-effectiveness is an overused metric that often feels like a catch-all, despite not always being the most appropriate measure. Additionally, while often used interchangeably, these terms reflect distinct evaluation lenses. As Thompson (2023) defines them:

- **Cost-effectiveness** focuses on whether the desired outcome is achieved at a reasonable cost. It asks, *"Did we get the result we wanted for what we paid?"* This is a retrospective view often concerned with baseline achievement.
- **Cost-efficiency**, on the other hand, assesses how effectively resources are maximized in relation to outcomes. Here we ask, "*Are we getting the best possible value per dollar spent?*" There is nuance between the two, and this forward-looking perspective prioritizes optimizing resource allocation to achieve the greatest possible training impact and measurable skill enhancement for the corporate workforce.

Cost-efficiency is evaluated by considering several key factors. These factors include pricing transparency, pricing flexibility, clarity of the value proposition, real-world training outcomes, and administrative overhead. I felt it was necessary to break down cost-efficiency into several sub-factors because, while it is a more thorough metric, it is difficult to truly determine how cost-efficient an option is until learning outcomes have been realized.

Narrative

RangeForce: 21 out of 25 (Excellent)

RangeForce offers a cloud-based cyber range platform specifically designed to build and refine high-performing defensive cyber teams within enterprise environments. The company's mission revolves around closing the cybersecurity skills gap for corporations by providing continuous, hands-on training that mirrors real-world operational challenges (RangeForce, 2025). A significant strength of RangeForce lies in its deep integration with widely used commercial security tools such as CrowdStrike, Splunk, Palo Alto Networks, and Fortinet.

Integrating commercial tools is an advantage, both in the rubric for this evaluation and from a corporate training perspective, as it ensures that employees can gain hands-on experience with many of the same technologies they use daily.

RangeForce supports various pre-built exercises, including Red and Blue Team scenarios. For a mid-sized company, this is attractive because it will provide the ability to simulate realistic threat actor tactics and practice defensive operations. Specific training modules delve into areas such as cloud security, network security, web application security, malware analysis, and security operations, which will help develop a strong foundation of knowledge within a Security Operations Center (SOC). Additionally, RangeForce provides learning paths explicitly aligned with recognized frameworks such as NIST and MITRE ATT&CK.

While the content catalog and tool integrations appear impressive, there is limited public evidence that RangeForce offers the most advanced, multi-domain, hybrid cloud simulations or fully supports the intricate, cradle-to-grave lifecycle of highly sophisticated advanced persistent threats (APTs) with the same depth as highly specialized, bespoke ranges. Its scalability is largely assumed based on its SaaS model and proven capabilities for team-based training; however, independent performance metrics for extremely large-scale enterprise deployments do not appear to be publicly available. Because of the lack of public availability of this information, I cannot objectively confirm or deny.

In terms of user experience, RangeForce consistently stands out. With an average user score of 4.6 out of 5 stars (G2, 2025), it features a well-designed, modern interface with intuitive navigation, which minimizes the learning curve for busy corporate professionals. Their platform includes dashboards that provide users and managers with actionable feedback, enabling them to track progress effectively and ensure the appropriate focus is applied where needed. Reviews suggest that the UX enables users to engage with complex cybersecurity scenarios without being hindered by interface intricacies. My personal evaluation of the UX is also positive.

Pricing is transparent, with clear tiers ranging from approximately $200 to $250 per person for specific, focused modules to $5,000 per person annually for full access (Solomon, 2021). This tiered structure offers flexibility for a mid-sized company's budget and will allow scaling investments based on specific training needs and team sizes.

CYBER RANGES: 9 out of 25 (Fair)

CYBER RANGES presents itself as a versatile platform engineered to cater to both corporate and government clients, emphasizing highly customizable training environments and flexible deployment options, including both cloud-based and on-premises configurations (CYBER RANGES, 2025). While its marketing materials describe a broad catalog of cyber exercises, specific technical details, such as the exact number and complexity of scenarios, the variety of operating systems explicitly supported within its custom environments, or the depth of integration for advanced, multi-vector attack simulations, are less publicly documented than those of its competitors. The lack of detail here makes it more difficult for corporate decision-makers to understand the full scope of capabilities and how they align with their specific, evolving threat landscape.

The platform claims to support a wide range of training needs, and the promise of customizable environments is appealing for tailoring to unique corporate IT infrastructures or proprietary systems. The lack of transparency around specific tool integrations and detailed technical features limits this evaluation’s confidence in the platform's ability to deliver truly enterprise-grade, cradle-to-grave APT simulations or highly specialized, deep-dive training for corporate security teams. Examples of simulating these scenarios are not readily available, which is a significant concern for any mid-sized, budget-conscious organization needing practical, relevant training.

CYBER RANGES highlights its scalability through marketing materials, suggesting it can adapt to diverse organizational sizes. Again, however, data demonstrating its capacity for high-concurrency enterprise deployments or the efficiency of lab provisioning under peak loads is not publicly available. This requires prospective clients to take vendor claims at face value, which introduces an element of risk for large-scale training initiatives where consistent, reliable performance is necessary.

UX appears to be a mixed picture. It appears that the platform likely offers good functionality, especially considering the suggested focus on customizability; however, there is limited public information about its quality. Without public demos or extensive user reviews, it is difficult to say whether the UX is practical. To top it all off, there is a notable lack of pricing transparency, which significantly hinders the platform's cost-efficiency rating. While flexible subscription models, e.g., Platinum or Pay-As-You-Go, are advertised, the complete absence of clear figures makes it extremely difficult for decision-makers to conduct thorough cost-benefit analyses, compare to alternatives, or justify expenditures. I believe it is important to caveat this assessment by acknowledging that a company could reach out to CYBER RANGES to request clarification on the pricing model, as well as their other offerings. That said, for this assessment, the available information is lacking. This prevents CYBER RANGES from scoring higher, despite the platform’s promises. CYBER RANGES says they are “the official cyber range” of the United Nations, which lends some credibility to their claims, but any real verification requires demos and sales calls. Ultimately, the scores for CYBER RANGES suffer because of a lack of publicly available information to assess what is being presented correctly.

Cogent Cyber Range: 21 out of 25 (Excellent)

Cogent Cyber Range offers a platform designed for organizations, particularly smaller businesses or departments, seeking flexible and cost-conscious cybersecurity training options. The platform provides a logical progression through three distinct levels: foundational skills development labs, individual and team exercises, and more advanced Red Team scenarios. This tiered approach may be beneficial for corporations looking to establish a baseline of cybersecurity knowledge across their workforce, provide initial training for new hires, or develop intermediate skill sets that already exist.

The platform's content offering, although solid, appears narrower than those of some competitors. While it provides valuable training for foundational and intermediate skill development (Cogent Cyber Range, 2025), it does not appear likely to fully replicate the highly sophisticated, multi-domain attack environments, advanced forensic analysis, or large-scale incident response drills demanded in high-stakes corporate training scenarios faced by mature security operations centers. Like RangeForce, Cogent offers NIST, ATT&CK, and other framework-centric content. The content appears to be generally well-suited for individual skill acquisition in areas like network fundamentals, basic exploitation, and introductory forensics, making it effective for specific, targeted learning paths. Additionally, Cogent bills the platform as one that a company could build private cloud-based labs within. If this is a company’s desire, great; however, pre-built scenarios carry significant weight in this evaluation.

Cogent's scalability appears to be a point of strength. It effectively supports self-paced, browser-based access for individual learners and provides some support for small to medium-sized team exercises. Additionally, Cogent says their CYRIN cyber range platform can host hundreds of concurrent users and has been used by organizations with more than 100,000 participants (Cogent Cyber Range, 2025).

The user experience for Cogent Cyber Range appears generally positive. It operates on a straightforward, accessible, and adaptable model, making it approachable for entry-level professionals and those new to cyber range environments. As a result, the platform has been identified by the Arizona Cyber Threat Response Alliance (ACTRA) (2025) as its preferred vendor. Cogent also offers dashboards and performance tracking, similar to RangeForce.

Where Cogent appears to excel is in cost-efficiency: its pricing is fully transparent and publicly available. There are several different pricing tiers to choose from. These tiers range from approximately $695 per individual for a six-month subscription to $5,995 per person annually for the most advanced content, with enterprise and educational discounts available (Cogent, 2025). This clarity in pricing and clear descriptions of content offerings make Cogent an attractive option for organizations of varying sizes, particularly for a mid-sized organization. This information enables the prioritization of budget transparency, predictability, and a more easily justified value proposition to financial stakeholders.

Scoring Matrix

Factor	**RangeForce**	**CYBER RANGES**	**Cogent Cyber Range**
Real-World Simulation/Application	4	2	4
Scalability and Performance	3	2	4
User Experience (UX)	5	2	4
Quality of Pre-Built Content	5	2	4
Cost-Efficiency	4	1	5
Total	21	9	21

Recommendation and Conclusion

This report contains an evaluation meant to provide an assessment of RangeForce, CYBER RANGES, and Cogent Cyber Range in order to provide decision-makers of a mid-sized company with information they can use to select a cyber range platform that aligns with their needs. RangeForce and Cogent Cyber Range score the same overall. Based on the rubric provided in Appendix A, Cogent Cyber Range is the recommendation. It appears to have the best mix of each factor, as described in Appendix A, and offers the best cost efficiency for a mid-sized company. RangeForce finishes in a very close second place, and with more specific research, may be a slightly better choice, as the scoring mix is quite strong. CYBER RANGES finishes a distant third because while they advertise broad capabilities, it was very challenging to verify the veracity of their claims. Ultimately, the decision between RangeForce and Cogent Cyber Range depends on the organization’s specific training goals; however, the results of this evaluation provide the target audience with a well-informed path forward.

References

ACTRA. (2025). *NACRA Preferred vendors*. Retrieved June 1, 2025, from https://www.actraaz.org/nacra/nacra-preferred-vendors

Cogent. (2025). *Course offerings and pricing*. Cogent Cyber Range. Retrieved May 30, 2025, from https://www.cogentcyberrange.com/course-offerings-pricing/#:~:text=Costs%20range%20from%20%241275%20to%20%242200%20per%20person.

Cogent Cyber Range. (2025). *COGENT Cyber Range: FAQs*. Cogent Cyber Range. Retrieved June 1, 2025, from https://www.cogentcyberrange.com/faqs/

CYBER RANGES. (2025, May 15). *CYBER RANGES: Cybersecurity exercises for training and capability development*. Retrieved June 1, 2025, from https://cyberranges.com/

RangeForce. (2025). *RangeForce Cloud-Based Cyber Range*. Retrieved June 1, 2025, from https://www.rangeforce.com/

RangeForce Reviews. (2025). G2. Retrieved June 1, 2025, from https://www.g2.com/sellers/rangeforce#profiles

Solomon, H. (2021, May 29). *RangeForce adds mid-priced packages to cybersecurity training offerings | IT World Canada News*. IT World Canada - Information Technology News on Products, Services and Issues for CIOs, IT Managers and Network Admins. https://www.itworldcanada.com/article/rangeforce-adds-mid-priced-packages-to-cybersecurity-training-offerings/444779

Thompson, C. (2023, November 8). Cost Effectiveness vs Cost Efficient: The Difference. *Precursive*. https://www.precursive.com/post/cost-effectiveness-vs-cost-efficiency-what-s-the-difference

Appendix A – Creation of Cyber Range Evaluation Rubric

PennState
College of Information
Sciences and Technology

Creation of Cyber Range Evaluation Rubric

COURSE:	IST: 894
ASSIGNMENT:	CYBER RANGE EVALUATION REPORT (PART I)
SUBMITTED BY:	BRANTLEY PRICE
DUE DATE:	MAY 25TH, 2025
INSTRUCTOR:	DR. BARTOLACCI

Introduction

A strong rubric is necessary to ensure a strong assessment. In part two of this assignment, this rubric will be presented in a matrix and will ultimately serve as the framework for my evaluation of specific cyber range platforms in the second half of this report. This rubric should help to facilitate informed decision-making regarding the selection of a cyber range platform best suited for cybersecurity education and training initiatives. It could, in theory, be used in a real-world scenario. The individual factors of the rubric are not necessarily presented in any particular order. Each factor has a grading scale at the end of the justification. The final score is the total of each factor. The grading process will consider user and professional reviews of each cyber range.

1. **Real-World Simulation/Application**

I believe this to be the most critical factor in evaluating a cyber range. As noted in a guide published by the National Institute of Standards and Technology (2023), a cyber range provides a safe and legal environment for developing cyber skills and plays a crucial role in development of cybersecurity professionals. Therefore, a cyber range's ability to effectively simulate a wide array of real-world issues, attack vectors, and defensive scenarios is the most important piece of criteria to judge. A high-performing cyber range in this category will support multiple operating systems, be able to simulate complex network topologies, and simulate vulnerabilities and exploit techniques. Users need to be able to practice scenarios that they will experience in the field; otherwise, the range is an exercise for the sake of exercise.

1 (Poor)	2 (Fair)	3 (Good)	4 (Very Good)	5 (Excellent)
Limited in network configurations, supported operating systems, and vulnerability representation.	Basic network configurations with limited customization. It supports more than one OS, e.g., Windows and one Linux distro. Supports slightly more vulnerabilities but lacks complexity. No integration with standard defensive tools.	Moderately complex network configurations. Supports a good variety of vulnerabilities and attack vectors. Supports more than three operating systems, but fewer than five. Some, but limited, basic standard tool integration.	Can simulate complex, realistic enterprise-level network topologies. Supports a wide variety of vulnerabilities, attack vectors, sophisticated exploits, etc. Supports many operating systems, and in some cases, even legacy operating systems. Allows for integration of industry-standard tools.	Can simulate highly realistic, customizable, multi-domain, and complex real-world network environments. May include hybrid cloud simulations. Seamless in integrating current known vulnerabilities, allows for the simulation of sophisticated, multi-vector attacks, and cradle-to-grave advanced persistent threat lifecycles. Supports an extensive number of operating systems and may support custom environments. Provides the ability to integrate with commercial and open-source tools.

2. **Scalability and Performance**

A cyber range that meets the requirements outlined in factor #1 will almost certainly have a large number of schools, businesses, and individuals who want to use the service. The cyber range should efficiently handle varying loads and concurrent users without compromising performance. The cyber range should accommodate large numbers of concurrent users who are running simultaneous labs. This could also look like supporting team-based training with large-scale incident response exercises. If the cyber range struggles with scalability, it will ultimately degrade the learning or training process. Performance considerations also take into account the responsiveness and stability of the environment. A cyber range with a high score in this area will provide a smooth and reliable experience.

1 (Poor)	2 (Fair)	3 (Good)	4 (Very Good)	5 (Excellent)
Frequent slowdowns or crashes. Lab deployments are slow.	Fewer slowdowns, crashes, and long lab deployment times, but issues are still noted during peak usage hours.	Generally acceptable performance across the board. May still experience some slowdowns, but they do not affect the experience noticeably. At this level, it is fair to consider the complexity of the labs on offer.	Consistently high performance across the board. Almost no noticeable performance issues. Especially noteworthy if environments and labs are complex.	Exceptional performance. No noticeable performance issues. Especially noteworthy if environments and labs are complex.

3. **User Experience (UX)**

A cyber range with a good UX will provide an aesthetically pleasing interface that will be easy to navigate. Additionally, supporting documentation will be readily available and easy to understand. Though UX almost always devolves to subjectivity, a lot of research has been done into the topic. There are even full design foundations that specialize in teaching these research methods and how to apply them (What is UX Research, 2024). A cyber range with a good UX will not leave the user facing face a steep learning curve to access the platform's functional capabilities. The content within the range is potentially difficult enough. A cyber range with a high score in this area will ensure users can focus on the cybersecurity concepts they are trying to learn, not navigating the interface.

1 (Poor)	2 (Fair)	3 (Good)	4 (Very Good)	5 (Excellent)
Interface is cluttered, non-intuitive, and requires significant effort to execute basics. Very high learning curve.	Interface is functional but needs work. Key features are challenging to locate. High learning curve.	Interface is generally straightforward and easy to navigate. Should they exist, some advanced functions may require additional effort to locate.	Interface is intuitive and well-designed. Users are effectively guided throughout the platform. Very little to no learning curve.	Exceptional interface featuring a streamlined and aesthetically pleasing layout. Users are subtly guided throughout the platform via contextual help and workflows. The learning curve is non-existent.

4. **Quality of Pre-built Content/Scenarios**

The availability and quality of pre-built labs, exercises, and training modules can significantly accelerate deployment and reduce the burden on instructors or trainers. This factor may seem similar to factor #1, but there is a clear difference. These scenarios take the real-world application factor to another level by placing real-world issues in realistic, pre-built scenarios for users to assess their capabilities against. Customization is nice, even necessary in some cases, but strong pre-built scenarios offer an out-of-the-box factor that could be extremely enticing to schools and companies alike. The quality of this content, the realism, clarity of instructions, and alignment with industry certifications or frameworks (e.g., MITRE ATT&CK, NIST) is also important. A cyber range with a high score in this area offers high-quality, relevant content that can immediately deliver value, reduce the need to develop custom courses, and help jumpstart a smooth learning experience.

1 (Poor)	2 (Fair)	3 (Good)	4 (Very Good)	5 (Excellent)
Very limited number of pre-built scenarios. Those that do exist are simplistic and lack realism.	Limited number of pre-built scenarios. Scenarios are basic with limited real-world applicability.	Solid number of pre-built scenarios. Topics covered range from basic to intermediate. Scenarios are generally realistic and moderately align with common industry frameworks, e.g., NIST.	Large library of pre-built scenarios. Topics covered range from basic to advanced. Scenarios are highly realistic, well-designed, and provide clear instructions and hints when users struggle. Strong alignment with industry best practices, frameworks, and certifications, e.g., Sec+	Exhaustive and regularly updated library of high-quality, highly realistic, layered pre-built scenarios. Complex red and blue team scenarios are likely to be found. Scenarios are clearly designed by experts and directly map to industry best practices, frameworks, and advanced industry certifications, e.g., OSCP.

5. **Cost-Efficiency**

Finally, as with any service, the financials are always important. This factor does not just look at the raw price. The reason cost-efficiency is used instead of cost-effectiveness is due to the nuances in the two definitions. Cost-effectiveness is achieving the desired outcome at the lowest possible cost. Cost-efficiency, on the other hand, is a measure of how well resources are aligned with the results achieved (Thompson, 2023). Cost-efficiency is a more valuable metric to evaluate because of the previous four factors that have been identified and will allow for an evaluation the overall value proposition in relation to the cost. Cost-efficiency is about maximizing value. The efficiency of the instruction, how quickly users are able to effectively complete and learn from the range exercises, and the overall cost to the school or company will go into creating a cost-efficiency rating. Companies understand cybersecurity is very important, yet it is often it is necessary to justify cybersecurity-related expenditures to C-Level leaders. Focusing on cost-efficiency gets beyond just how much money is being spent and focuses more to the "why" a particular amount is being spent.

1 (Poor)	2 (Fair)	3 (Good)	4 (Very Good)	5 (Excellent)
Very high cost with limited features provided. Little to no flexibility in the pricing structure.	High cost relative to the features provided. Pricing structure is somewhat inflexible or contains hidden costs. Value proposition is difficult to justify.	Competitive price relative to the features provided. Pricing structure is generally fair and the value proposition can be justified, if only at a basic level.	Strong value relative to the features provided. Pricing structure is flexible and can be scaled as needed. Options exist for single user, multi-user, and even enterprise-wide access. The value proposition can easily be justified.	Exceptional value relative to the features provided. Pricing structure is highly flexible and transparent. The value proposition is clear due to effective learning outcomes, minimal required administrative overhead, and detailed content library. Partnerships with certifying bodies may exist to prepare users for certification exams.

References:

Cyber Range Project Team & NICE Community Coordinating Council. (2023). *The Cyber Range: A Guide* [Report]. National Institute of Standards and Technology. Retrieved May 23, 2025, from https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf

Thompson, C. (2023, November 8). Cost Effectiveness vs Cost Efficient: The Difference. *Precursive*. https://www.precursive.com/post/cost-effectiveness-vs-cost-efficiency-what-s-the-difference

What is UX Research? (2024, November 30). The Interaction Design Foundation. Retrieved May 23, 2025, from https://www.interaction-design.org/literature/topics/ux-research?srsltid=AfmBOoqVPkFhaVAvqURqvmcyFaLcJlVGbLcja_kL5UfRDhcv8nHTU--V