Cyber Range as a Service®
CRaaS

January 2023
Update

Introduction

For companies that have or make use of production network infrastructures whether private or public, in the cloud or a hybrid, there is a need for developers, consumers of the infrastructure, and the administrators of the infrastructure to perform cyber training, testing, and exercises on a replica of their production infrastructure or Cyber Range. Delivering this Cyber Range as a Service® (CRaaS) allows for the fastest and most economical way to for users to perform their required tasks. The myriad of services, applications, processes, methodologies, and tools such as traffic generators, SIEMs, malware simulators, public/private clouds, Software Defined Networking (SDN), Lab as a Service (LaaS), web catalogs, LMS products, event scheduling tools, simulated training environments, and hypervisors provided by many different vendors complicates the management and automation goals for delivering Cyber Range capability as a Service.

This complex problem prevents the cyber range infrastructure from being optimized to meet the needs of the administrators, developers, and users. Without full control and automation of the cyber range infrastructure and the applications and services running within the cyber range infrastructure, organizations cannot keep up with new technologies, enhance the performance and capacity of the infrastructure, and service the growing demands of the cyber range consumers.

The key to the successful deployment of a cyber range infrastructure is to implement a methodology that manages the infrastructure using an agile life cycle approach offering standardization and centralization of management and consumer activities, while giving developers, administrators, and users appropriate control and automation of their worlds with the ability to share cyber range infrastructure resources, networks, and automation IP across many use cases. An agile based, highly automated, and lifecycle managed cyber range delivers maximum utilization of the services to allow for the greatest return on the investment.

Cyber Range Environment Types

Cyber Security Range environments encompass a number of different types that share some common characteristics, but also have their own unique requirements:

Red Team vs Blue Team (Cyber Range Exercise) And Purple Team

This type of environment is more common in military cyber defense for training of personnel and assessing network security in both offensive and defensive scenarios. Generally, a "cyber arena" is created that uses a network that looks as close to that of the production network as possible, and a traffic generator creates traffic that simulates normal network traffic patterns. The "Red Team" attacks the network using cyber hacking techniques, and the "Blue Team" reacts in real time as the network monitoring group that identifies the hacks and attempts to stop them. The latest capability is the concept of a "Purple Team" where the Red Team and Blue Teamwork as a Purple Team together to learn how each side works and thinks.

Development, Test, and Experimentation of Cyber Tools and Techniques

This type of environment is used primarily for evaluating the use of new security tools and techniques and determining whether they will improve network security in organizations. With this type of testing organizations once again attempt to model the typical production network. Traffic generators are used to simulate typical user traffic in that network, and the new security tool (hardware and/or software) that is being developed and/or tested is inserted into the network. Disruptive events are added to the network and the new security tool is evaluated for how well it captures and responds to the disruptive events. This approach is used for developing and testing security tools and techniques, as well as for customers who want to evaluate those tools before implementing them for their own networks or products.

Penetration Testing and Recovery Practice

Organizations typically hire external test consultants to test the organization's cyber readiness with a series of penetration tests of the infrastructure to find and report gaps in compliance and cyber protection. This sort of testing is typically expensive, requires downtime of the production network and is only a snapshot in time of the cyber protection status of the infrastructure. A duplicate of the production network allows for continuous penetration testing to provide more assurance that there are no gaps in cyber protection. Recovery response from a successful cyberattack requires practice and training to perform these complex operations. A duplicate of the production network with a compromised set of assets allows for a practice testbed that cyber recovery engineers can hone their recovery skills on.

Application Compliance Assessment

Compliance assessment is very similar to cyber tool testing, except that the tools remain fixed and new applications or hardware are inserted into the network, or the existing infrastructure is upgraded. Testing with load, traffic, and disruptive events is performed to determine whether the new application, hardware, or upgrade might create a new vulnerability in the production environment. Evaluation criteria includes privacy and data protection regulations, security requirements, and any other

business compliance standards that the organization is subject to such as Mitre Att&ck exploitations. This testing is performed prior to pushing any new upgrade, application, or equipment into production, to ensure that compliance requirements will be maintained.

Performance Based Assessment – Training
Security testing for training purposes is common with cyber ranges, but also for cyber security testing. This type of testing allows organizations to train their infrastructure architects, security administrators, and end users to respond in real time to a variety of security threats. The focus of training is to train, practice, and measure the performance of an entire organization.

Traditional Education – Training
New users of services and applications of almost any kind need cyber security training to gain certification and other degrees of accomplishment, and to build expertise in cyber tasks and methods. This type of training allows for a greater adoption of cyber expertise into the user community. The goal is to provide the building blocks for users to tackle other types of cyber security tasks.

Physical and Virtual Cyber Range Management

Many entities today are struggling with how to efficiently manage their Cyber Range infrastructure with the continuous pressure to reduce cost while increasing performance, capacity, and ease of use for their consumers. These entities have identified the following infrastructure management needs:

- Control physical as well as virtual resources
    - Scheduling, reserving, managing, deploying (lifecycle) environments
    - Auto provisioning of resources (physical and virtual)
    - Supporting converged infrastructure and legacy hardware
    - Support of new technologies
    - Support of cross domains (public and private clouds)
- Automation of infrastructure activities (both physical and virtual)
    - IT admin activities
    - Auto-discovery, lab resets, resource health-checks
    - Powering down devices when not in use
    - Spinning up new resources on demand, etc.
- Supporting multiple tenancies and domains
- Configuration management
- Enabling user automation (testing, DevOps flows, sandboxing, etc.)
- Sharing of intellectual property
    - Support processes, automation, configurations, resources, use cases, etc.

    - Community based and open source focused
- Integration with other tools such learning management systems, simulators, malware traffic generators, training labs, scoring tools and more
- Metrics on the processes/activities, resources, usage, and users, to manage the lifecycle of the environment

This list is by no means complete but it does address the majority of the problems seen by these entities. All of the above actions need to be handled in a standardized and centralized approach in order to be effective and consumable by the different roles involving the use of the cyber range infrastructure. The actions need to be managed with a lifecycle approach for both the management of the range infrastructure and the activities within the range. The maintenance of resources, the roll back of configurations, and the validation testing of an environment before releasing it to the consumers are all examples of actions that are repeatable yet highly configurable and complex.

Management needs to understand how well the Cyber Range infrastructure is functioning so that decisions about the maintenance and lifecycle of the range infrastructure can be made from the data analytics available. The infrastructure needs to have tools in place to support not only these actions, but the lifecycle management of these actions as well. Most importantly, the environment needs to support new tools and processes as well as share intellectual property (IP) developed across all levels and users of the environment (administrators, developers, end users, etc.).

The Risk of Not Managing or Automating your Cyber Range

Given the financial cost of a Cyber Infrastructure and its importance to the rest of the organization, it's foolish to make the significant capital and operational investments while neglecting the lifecycle management of the infrastructure. The highly manual processes associated with lifecycle management typically used in Cyber Infrastructure labs are the enemy of reliability, repeatability, and auditability. Manual or non-managed processes are often visible in a number of ways:

- *Absence of live inventory visibility.* In most Cyber Ranges, equipment inventory is not tracked in a way that provides live visibility to engineers. While most IT organizations perform asset tracking for financial purposes, what passes for the inventory management used by engineers is a spreadsheet that is often ill-maintained. As a result, it can be difficult to tell without exhaustive work what resources or equipment exists, is being used by whom and what is truly available.
- *Offline topology design.* Since there is no usable inventory visibility, it follows that topology design is done completely offline without regard for resource availability. Visio or other diagramming tools are most

common, and basically produce the electronic version of a paper drawing, which is usually then printed to aid in a time-consuming manual hunt for relevant equipment.

- *Chaotic connectivity management and costly errors.* Once inventory is found that is at apparently available, engineers must manually re-cable connections between the equipment. With multiple engineers making adds, moves and changes, typically without up to date documentation, errors such as disconnecting someone else's infrastructure inevitably occur.
- *Private and public cloud virtualization solutions are isolated.* Often tools and processes are locked into a particular set of virtualization tools and infrastructure, greatly limiting the sharing of these environments across private and/or public clouds for different use cases and end users.
- *Use of custom environments instead of COTS (Commercial Off The Shelf) tools.* Using these custom tools to manage the environment leads to excessive cost, limited use within different groups, and limited industry expertise to lower maintenance costs for the management environment. Different custom tools and environments without a common control interface across different user roles can cause limits in adoption of the environment due to increased training and expertise needed to support multiple management environment tools and processes.
- *Lack of device configuration baselining.* Engineers using the infrastructure must often change OS images, apply patches, and create new configurations on devices. Unfortunately, it's all too easy to forget to set devices or environments back to a baseline state, which means that when the next engineer uses the device they may wrongly assume that it is configured at a known baseline state and execute a series of test protocols on an incorrect configuration.

The result of these manual processes is inaccuracy, inefficiency, and waste, evident through a number of indicators:

- *Lack of process integrity and repeatability.* Manual processes tend to experience operator errors that compromise process integrity. The lack of repeatability that results means that it is very hard to offer sufficient verification of processes.
- *Poor process documentation.* Manual processes are by nature difficult and time-consuming to capture in documentation for auditing purposes. When changes occur in procedures or processes, it is too easy to miss documentation steps, which can impact the audit trail.
- *Incomplete process reporting.* Process methodologies can generate voluminous results of data. Manual analysis processes struggle to digest this data and provide sufficient reporting for auditing purposes.

- *Imbalanced ratio of setup to actual usage.* Infrastructure engineers can easily spend days in the setup process for a procedure that takes less than an hour to run.
- *Very low asset utilization*. Millions of dollars in capital equipment are typically only 15% to 20% utilized. This represents a huge waste of annual capital depreciation costs.

There are significant implications of the inaccuracy and waste created by manual operating processes in infrastructure labs:

- *Risk of errors and non-optimized range infrastructure due to process integrity, repeatability, and documentation issues.* Even if the processes are painstakingly performed in an accurate fashion most of the time, the inefficiency and slow pace of manual or separate custom processes may make it nearly impossible for allocated personnel to achieve fast cyber infrastructure delivery, which causes a reduced utilization of the infrastructure.
- *Cyber Range Infrastructure lab asset utilization under 20% represents a significant waste of capital depreciation costs.* Low asset utilization also means that as demands for infrastructure deployment grows, the pace of investment in infrastructure lab capacity will rise at a rapid rate. With large infrastructures costing anywhere from $1K to $3K per square foot inclusive of equipment costs, this can lead to huge, unnecessary CAPEX outlays over time.

Implement a Cyber Range Automation Framework Solution

Using a Cyber Range orchestration and automation framework solution to manage the lifecycle of a cyber infrastructure environment can help users achieve dramatically higher accuracy, utilization, and productivity. This will lead to significant CAPEX and OPEX savings, faster infrastructure cycle completion, and sustainably documented processes and reporting for metrics and auditing of the cyber infrastructure's performance. A sound automation and provisioning solution which delivers a fully integrated, object-oriented software framework for automating development, administration and end user operations on the cyber infrastructure whether physical, virtual, or hybrid includes:

- Centralized live infrastructure and resource inventory
- Inventory-aware cyber topology design
- Shared calendar-based resource and topology reservation
- Connectivity mapping and automated connectivity control
- Easy to create automated provisioning tasks

- Non-programmer friendly automation workflow creation based on a library of highly reusable, template based, objects that can be created from a wide variety of sources and leveraged to create:
    - Auto-discovery, auto base-lining, and other automated maintenance routines
    - Full test automation workflows
- Community sharable IP for automation and management of cyber training and simulation infrastructures and processes
- Powerful automated reporting that provides a verifiable and sustainable audit trail
- Resource agnostic (any device, any cloud, any hypervisor) to support new technologies
- Ownership of all logs and datasets produced by the toolset
- Built in Learning Management System (LMS) instruction portal
- Over the Shoulder support for Trainers and Trainees

If designed properly, the automation architecture avoids the pitfalls of script-based approaches to automation, which cannot scale due to their high maintenance costs. Best of breed commercial solutions deployed by industry leading organizations worldwide provide them with the fastest path to successfully and sustainably automated framework environments. This is the path which leading power utilities, enterprises, government and military agencies, telecom service providers, and technology manufacturers have chosen to transform chaotic manually driven environments into highly efficient infrastructure operations.

These organizations have the ability to manage infrastructure inventory including SIEMs, testing equipment, L1/L2/L3 switches, and virtual resources such as virtual machines, virtual switches, and containers in a live, searchable database of resource objects tagged with searchable attributes. This capability eliminates manual searching for equipment in racks and allows engineers to interface with the datacenter infrastructure efficiently via software. An inventory and resource management tool with object support and hierarchies can represent relatively simple nested resources such as chassis, blades, and ports, or complex, pre-integrated resources stacks such as converged infrastructure and “cyber range in a box” solutions. (See Figure 1 Full Cyber Range as a Service Framework)

- Create variable or abstract topologies via a software GUI that allows drag and drop of resource objects onto a canvas, visually ascertain availability, design, and sanity check connectivity. Save the entire topology as a high-level object in the resource library, so that it can be reused later or by other engineers. (See Figure 2 Web Portal for Self Service Catalog for Ranges and Training)
- Use a large library of resources available for standing up entire cyber training or exercises. (See Figure 3 Cyber Range Resource Library and Search).

- Schedule resources and entire topologies through a common calendaring system, preventing use case disruptions. (See Figure 4 Scheduling)
- Manage connectivity remotely by generating patching or cabling requests to lab administrators, or if Layer 1 switches are in use, to automatically connect topologies.
- Make use of Layer 2 switching as Layer 1 to deploy new topologies without re-cabling or the use of expensive Layer 1 switch resources.
- Make device and service provisioning error free by building automation objects for common provisioning tasks and execute them from a graphical test topology view. Device/VM provisioning can include uploading OS images, resetting device configurations to baselines, or creating routing adjacencies between virtual switches. (See Figure 5 Resource Automation Commands)
- Create auto-discovery and auto-baselining processes that leverage an extensive array of control interfaces, GUI automation and scripting capabilities to streamline the management of inventory and device states to a compliant baseline.
- Automate complex provisioning and configuration management tasks in a fully documentable and repeatable fashion. Automation can be created through integration of existing automation scripts as objects, as well as creation of new automation objects through screen, GUI, and other capture processes.
- Build, configure, and rapidly deploy complex virtual networked environments through an easy to use, multi-tenancy web portal GUI. (See Figure 6 Complex Cyber Training Virtual Environment)
- Embed other tools to allow integrated Learning Management Systems and Cyber Training Simulation tools into a single pane of glass environment for easy to consume interfaces for end users.
- Use compute, storage, and networking resources in an optimal and hyper-converged deployment for shared resource pools to meet on-demand needs of users
- Support virtual resources from any hypervisor and any physical resource vendor, allowing for a universal user interface for all consumers of the infrastructure. (See Figure 7 App and Service Support for Clouds)
- Allow multi-tenancy in a secure virtual and physical environment to meet security compliance validation. (Encryption of passwords, SSO, single file virtual network containers)
- Support enterprise-wide deployment of Cyber Range use cases with role and domain control with support of AD, LDAP, SLDAP solutions
- Support integration of Cyber Training tools and Cyber Training Labs and Content for both classroom and remote self service cyber training (see Figure 8 Example Training Content Cyber Range Sandbox)
- Training Instructor and Student over the shoulder capability (see Figure 9 Over the Shoulder shared GUI experience)
- Generate comprehensive audit compliant result reports.

- Produce custom business intelligence dashboards to allow for managers to analyze and collate data from the testing activities and metrics for input into planning initiatives. (See Figure 10 BI dashboard)

The Automation Framework's Beneficial Impact on the Cyber Infrastructure

Adoption and deployment of an automation framework methodology on your infrastructure leads to significant, positive impacts:

- ***Sustainable auditability.*** With automation comes built-in documentation of automation processes since the object-oriented method of creating, modifying, and maintaining template elements creates an ongoing and live documentation for process composition and methodology. Automated equipment maintenance processes with documented schedules provide proof of the compliance of the testing environment. Automated results analysis offers robust reporting that offer solid proof of compliance and compliance efforts. Complete control of all data sets produced by the framework allows for control and ownership of all metrics and outputs produced by the toolset.
- ***A dramatic increase in the velocity of infrastructure delivery.*** Organizations routinely report time savings upwards of 70% in their deployment cycles once they have automated the process of allocating devices, device/VM provisioning, running automation processes, and generating reports.
- ***Significant savings in infrastructure CAPEX and OPEX.*** Organizations deploying infrastructure automation software report increases of 50% to 200% in device utilization, leading to capital budget savings, less depreciation waste, as well as accompanying savings in space, power, and cooling costs.

Conclusion

Large and small cyber range deployments are under tremendous pressure to maintain a sustainable compliance regimen for continuously evolving and increasing the usage and optimization of the deployment of services and resources to their user community. Deploying a framework set of tools and services to automate the lifecycle management activities of the cyber range can dramatically increase the usage and optimization of the resources within the cyber range, allowing entities to deliver the cyber range infrastructure faster with less cost and greater performance to their user community. Using this COTS approach to managing the infrastructure ensures that the process of managing and using the cyber infrastructure is reliable, rigorous, repeatable, and highly auditable. Entities using an automation framework for their cyber range Infrastructure

can build a sustainable platform for delivering an infrastructure that leverages their users' performance and capability to ensure that their bottom lines are maximized.

About the Author

Charles T. Reynolds (Chuck) is the founder and CTO of Technical Systems Integrators, Inc. (TSI). TSI is a leading provider of Infrastructure Management solutions serving customers globally since 1987. Chuck holds a BS in Computer Science/EE from Duke University and a MS in Engineering Management from Florida Institute of Technology (FIT). Chuck is a member of ITEA, AFCEA and has over 30 years of involvement in electronic design, testing, and infrastructure management tools. To learn more about TSI's product solutions, please reach out to us:
https://www.tsieda.com
https://www.tsieda.com/craas

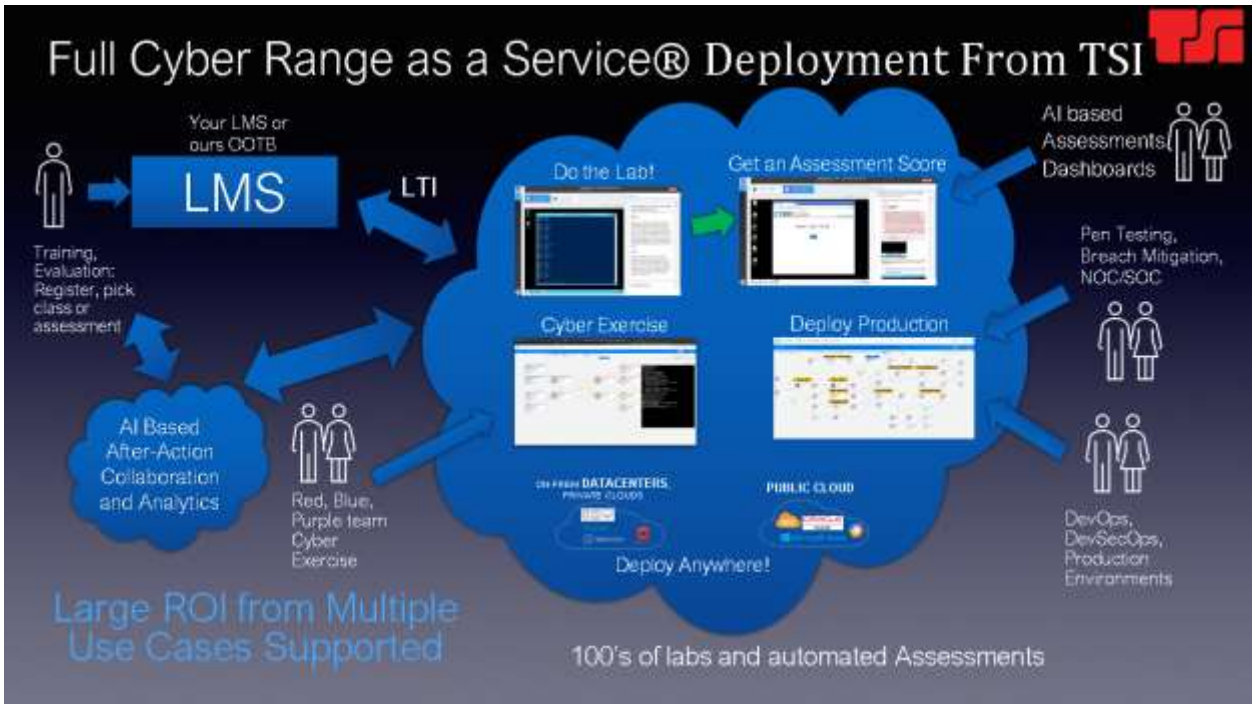

Figure 1: Full Cyber Range as a Service Framework

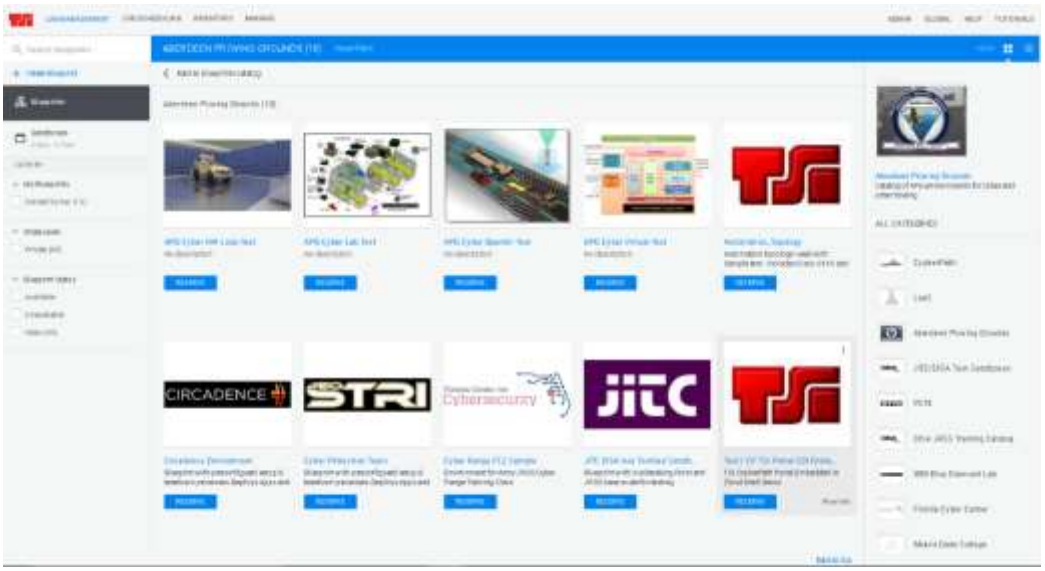

Figure 2: Web Portal for Self Service Catalog for Ranges and Training

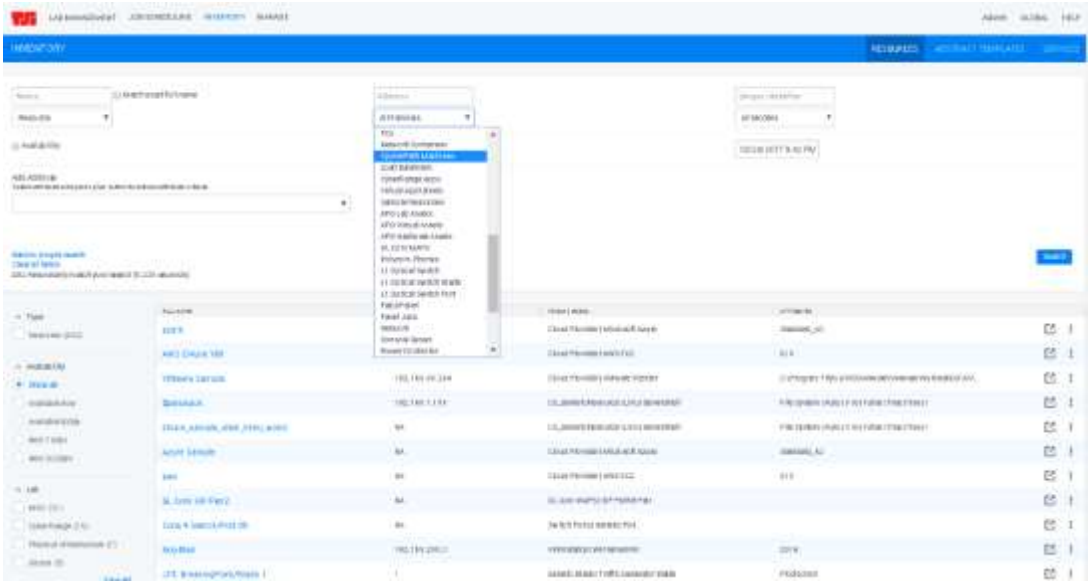

Figure 3: Cyber Range Resource Library and Search

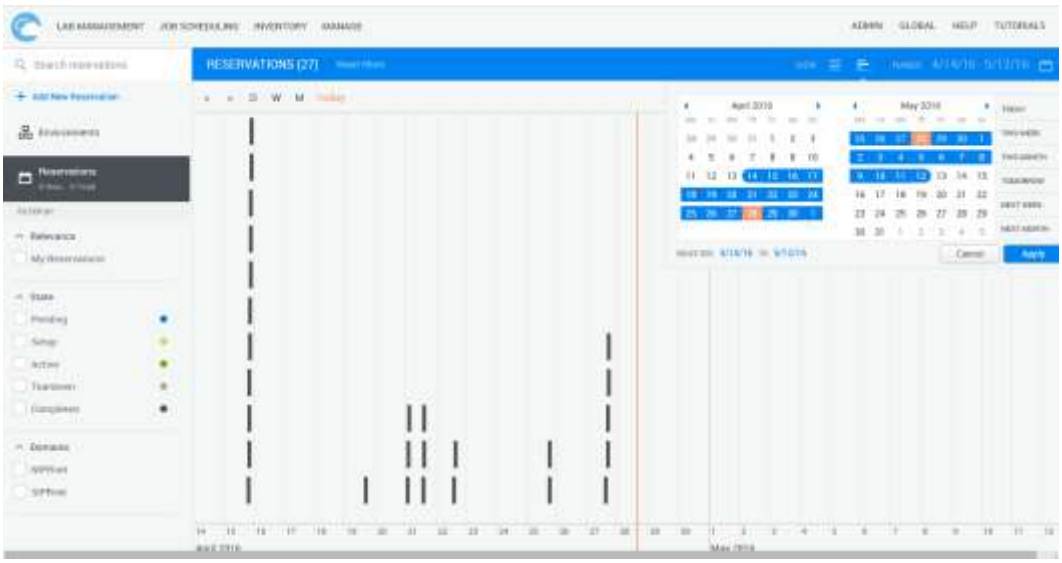

Figure 4: Scheduling

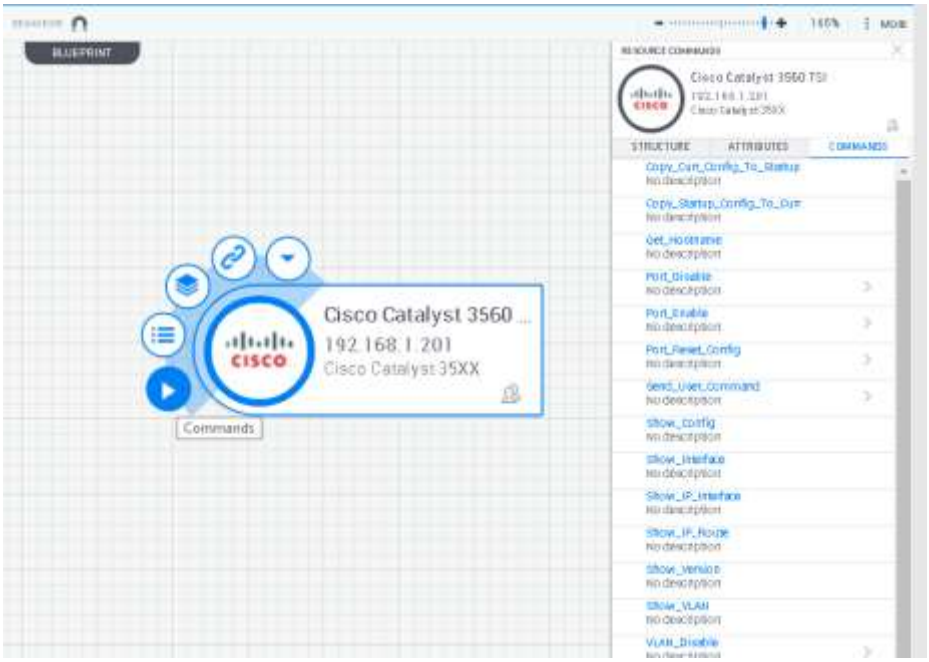

Figure 5: Resource Automation Commands

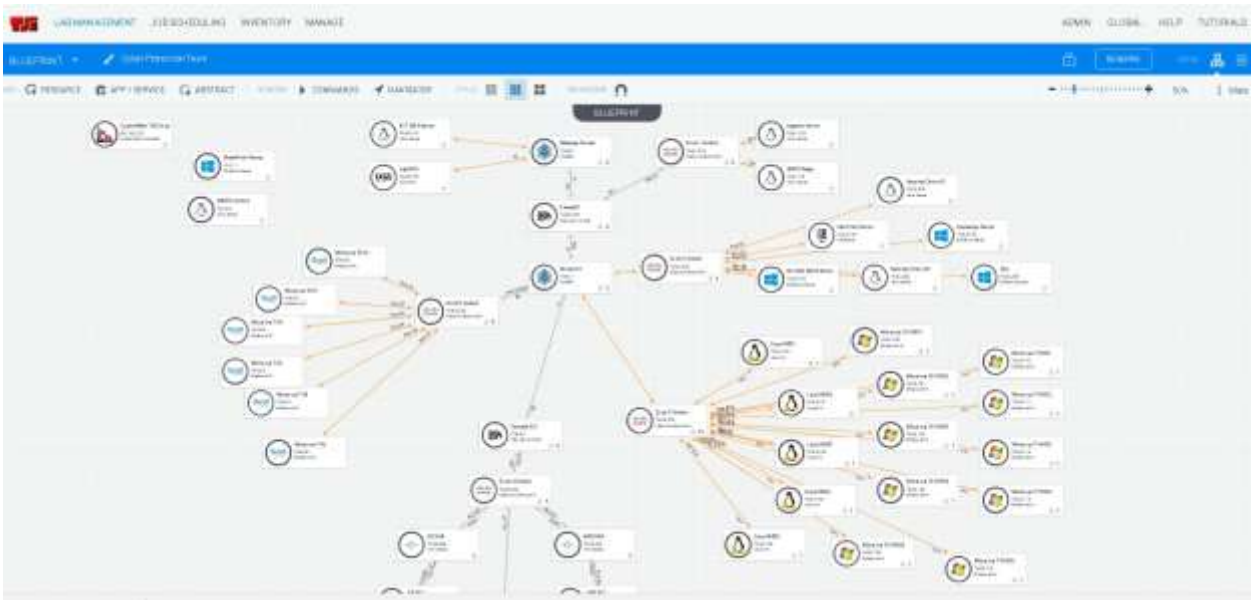

Figure 6: Complex Cyber Training Virtual Environment

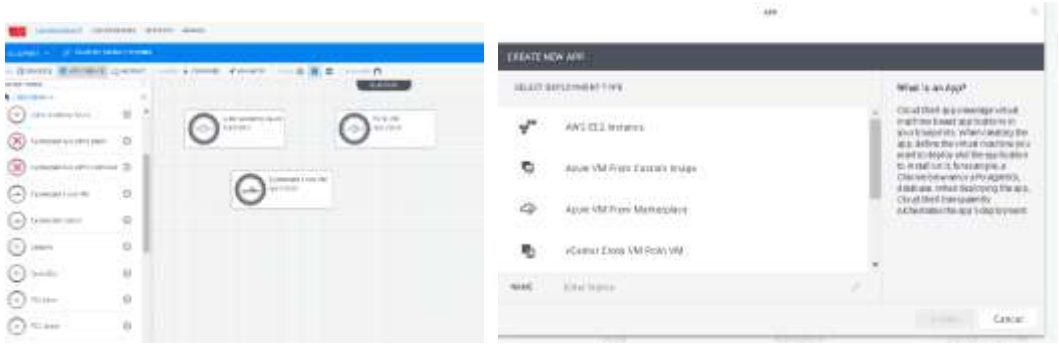

Figure 7: App and Service Support for Multiple Clouds and On-Premise Support

Figure 8: Example Training Content Cyber Range Sandbox

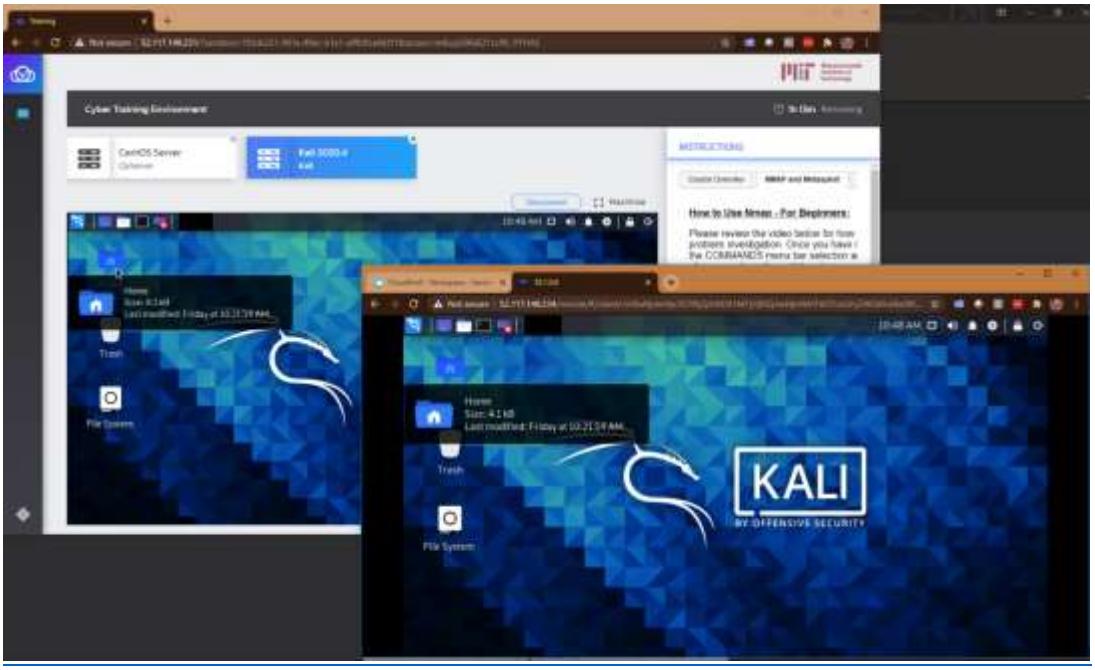

Figure 9 – “Over the Shoulder” shared GUI experience

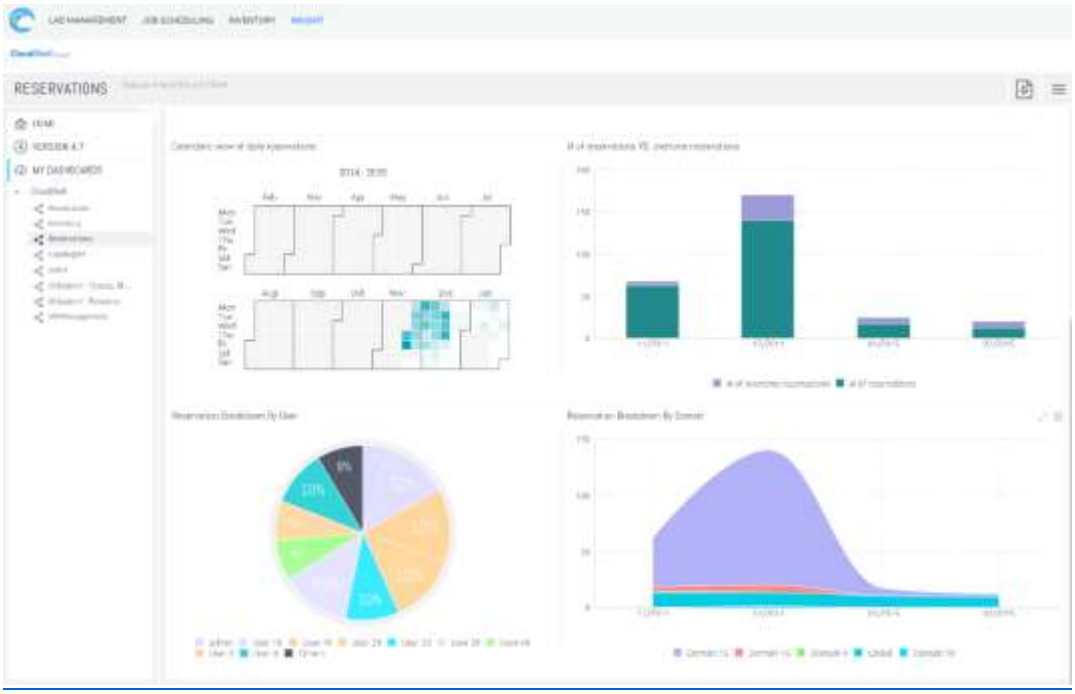

Figure 10: BI Dashboard (example of reservations dashboard)