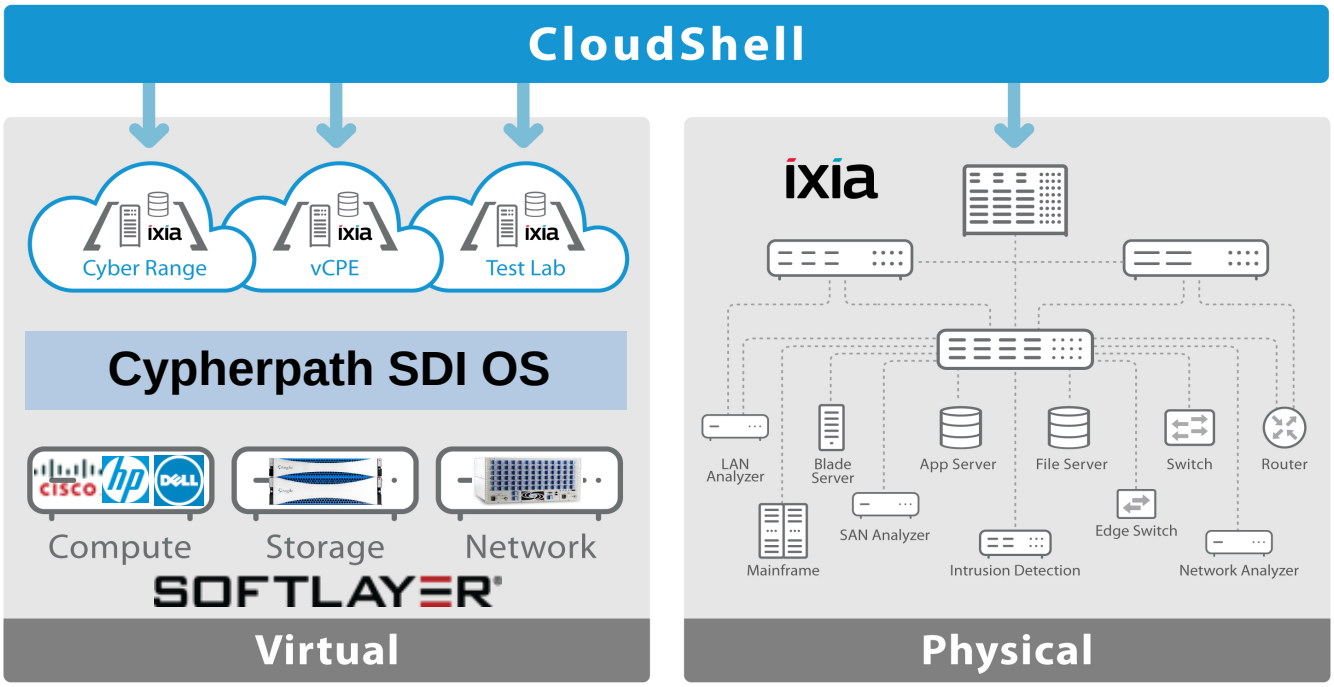
Virtual or Hybrid Cyber Range

TSI provides a COTS orchestration, automation, and virtualization platform for deploying, exercising, and resetting cyber range infrastructures and applications. Our web portal based framework, **CloudShell**, provides a ideal user experience to easily build, deploy, and utilize cyber ranges for **training and exercises**. The automation itself includes but is not limited to **asset/device communication, infrastructure orchestration, application/service delivery, processes within and outside the infrastructure, test/lab/exercise execution, discovery, data aggregation, and analysis**. TSI can provide these virtual, physical, and hybrid platforms via either hosted or delivered environments. In addition to standard network appliances, these environments can also include network loading and strike capability VMs such as those from **Ixia - PerfectStorm (Breaking Point), Developer, IxLoad,and IxNetwok**. While typically the the user provides range or lab resources and content, TSI's automation can help to make deployment and management a true easy button.

TSI's solution can also provide a unique Software Defined Infrastructure Operating System from **Cypherpath** which allows **virtualization of the entire infrastructure (Cloud) AND all associated VMs within a single file.** This technology provides support for **Hyper-converged hardware** which offers unparalleled security, speed, and portability of your cloud/range at the lowest cost available.



Additional Products from TSI to Complement the Solution:

- Solutions to test, validate, secure, and optimize networks
- 3D MEMS Optical Switching
- Layer 1 electrical and OEO switching solutions
- Flash and hybrid storage arrays

Key Features

Full Stack Cyber Environments

Automate the deployment and configuration of all the infrastructure components necessary to replicate any cyber threat scenarios, from physical networking, storage, servers, and test equipment, to virtual resources, cloud components, tools, and applications. Model and provision complex L1, L2, and L3 networking as well.

Self-Service, On-Demand, Multi-Tenant

Publish cyber range environments for on-demand deployment by IT, QA, and security teams. Complete REST API allows access to cyber environments by DevOps and Test Tools as well. Single tool for managing and automating multiple sites allows federating and consolidating cyber labs and data centers.

Rapid Blueprint Modeling

Quickly and easily model complex cyber infrastructure blueprints. Drag and drop physical, virtual, cloud, and app components onto a visual canvas; easily model network configurations and quickly set custom attributes and configurations.

Rich Orchestration

Manage the entire lifecycle of cyber sandboxes with orchestration that supports automated setup, provisioning, teardown, monitoring, and scaling. Snapshot and restore environments to known states for reproducing threat scenarios. Provide custom orchestration commands for specific use cases like security validation, training, and support/remediation.

Live, Interactive Environments

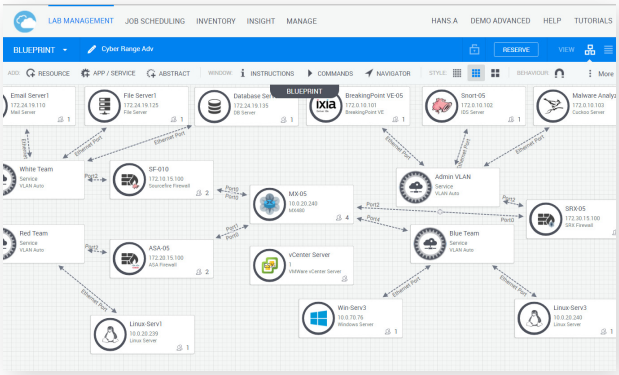
Give users SSH and RDP access to resources directly from within live cyber sandboxes; live graphs and charting provide compelling visual feedback; custom instructions and guided tours enable faster on-boarding of users.

Resource Optimization

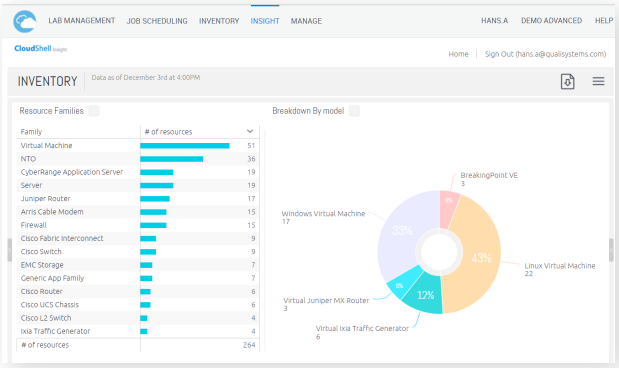
Optimize cyber range infrastructure utilization through intelligent resource sharing, management of resource contention, scheduling,and automated control of physical layer connectivity (L1 and L2 Switching).

Reporting and Analytics

Provide visibility into user scheduling, environment, and infrastructure usage for predictable spend and resource planning. Tie analytics to automation data for valuable insights into cyber scenario behaviors andtrends.



Full stack, real-world cyber infrastructure environments.



Rich reporting and analytics for resource planning and threat behavior analysis.