Cyberoperations Enhanced Network and Training Simulators (CENTS®)

Technical Capabilities Document

Stephanie Harwell, VP, CyberCENTS® Programs
Stephanie.harwell@bylight.com
Cybercents.sales@bylight.com
+1 618-624-7800

Metova Federal (a By Light Company)
CyberCENTS® (a By Light Offering)
1472 N. Green Mount Road
O'Fallon, Illinois 62269

www.cybercents.com

Last updated: January 2020

TABLE OF CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

What is CENTS®? CENTS is a line of advanced, turn-key cyber range environment solutions – used for training, exercises, tool development, and test and evaluation. The underlying software driving each CENTS product is the simulator's SLAM-R© *(Sentinel, Legion, AutoBuild, Myrmidon, Reconstitution)* appliance.

2 CENTS TECHNICAL CAPABILITIES

The CENTS platform solutions provide a relevant, integrated, Live-Virtual-Constructive (LVC) cyber range environment for cyberspace training, exercising, tactics evaluation, tool development and evaluation, and individual and crew standardization/evaluation without risk to the operational network.

Metova's CyberCENTS division developed cyber environments for organizing, planning, developing, and conducting cyber training, exercises, competitions, validation, and tool development. CENTS is currently in use supporting Air Force, Air and Army National Guard, Navy, Joint Service, State, Universities, and commercial industry requirements.

CENTS provides a realistic network management and cyber practice and test range in a controlled environment. Malicious and risky attacks and/or problems executed in the environment, either from the library of provided scenarios or 'live events", pose no threat to any operational system or network.

The CENTS solution permits both closed-network engagements as well as multiple interconnected virtual private network (VPN) engagements. Each CENTS unit has Institute of Electrical and Electronics Engineers (IEEE) Request for Comments (RFC) compliant traffic generation that features dynamic traffic flows and protocols that can be manipulated to follow a customer profile. The emulated elements of the environment (e.g. users, traffic, attacks, the Internet) interact with the virtualized and physical elements of the system providing true-life system response (no pre-programmed responses; events will continue to run/impact the target until stopped or mitigated). All elements are user configurable, and accessible to the Media Access Control (MAC) level. Each cyber range environment is self-contained, requiring Internet connectivity only for remote user access or interconnection between systems at other locations. The Range Global Internet (RGI®) has social media services and multi-layer, dynamic websites. All Internet Protocol (IP) addresses and websites Uniform Resource Locators (URL) resolve in the cyber range's Domain Name System (DNS). The RGI IP space uses real-world geo-located IP Addresses. The cyber scenarios execute in either automatic or manual mode. Each CENTS solution can be reconstituted within minutes to a previously defined state.

Through our Air Force program, our solution has an Authority to Operate (ATO), issued by the Headquarter Air Force accreditation authority, on the United States (US) military network. In addition, the Air Force cyber mission force solution has been certified (issued a "SIMCERT") as meeting all requirements to "mission qualify" the cyber forces on the cyber weapon systems.

What makes the CENTS platforms unique from other cyber range environments is Metova's patented simulator/range automation engine – SLAM-R®.

2.1 SLAM-R© Range Automation Engine

SLAM-R is the CyberCENTS cyber range automation engine that brings fidelity and realism to our cyber range/test environments. SLAM-R brings the features and functions of real-world networks and operations centers. SLAM-R interfaces into the networked environment, both internally and externally, to complete the look and feel of the real-world network. The SLAM-R appliance is controlled/operated through a single web-based User Interface (UI) – our "single pane of glass" for simulator control.

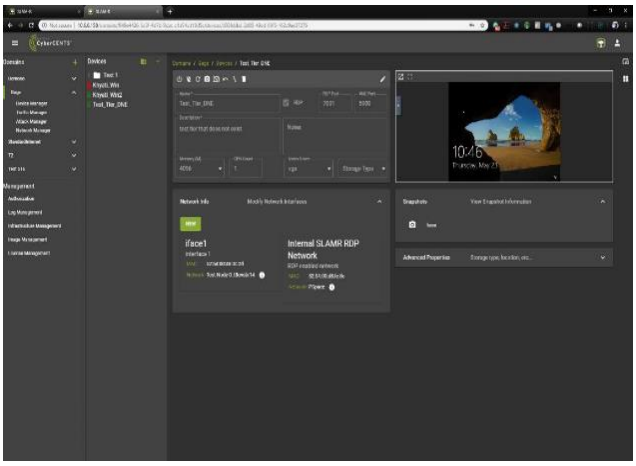

Figure 1: User Interface (UI)

Through the UI, instructors, trainers, engineers, and administrators manage the configuration and integration of VMs in the blue and gray space through the device manager, manage and configure traffic generation and profiles, configuration and manage individual attacks/exploits and group them into scenarios. Network engineers and administrators also configure the network environment, manage the infrastructure, and create and restore snapshots through the UI. Role-Based Access Control (RBAC) and Users are managed by the administrator through the UI as well.

The **SLAM-R** appliance provides network monitoring with **S**entinel – traffic generation, user emulation, simulated internet, and root DNS through **L**egion – rapid simulator duplication through **A**utoBuild – scenario building and network attacks through **M**yrmidon – and rapid system baselining through **R**econstitution. A management console is used to manage the SLAM-R hardware.

The **Sentinel** module monitors and reports on the status of system actions. System actions are tracked through Log Management. Info events are logged for each event as it executes in Myrmidon, the attack/scenario module, and the traffic flows in Legion.

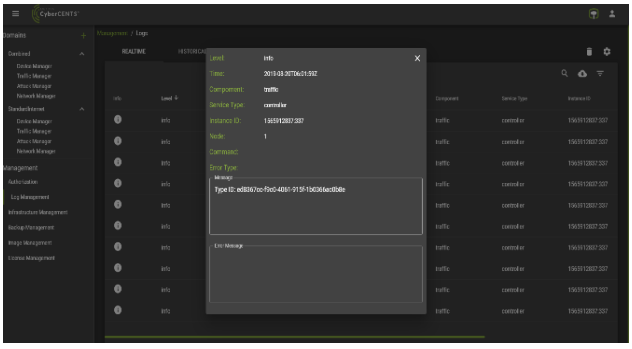

Figure 2: CyberCENTS Monitoring

The **Legion** module provides the realistic and programmable (model based) user behavior. Legion provides RFC compliant network traffic, root DNS, and the Internet environment. Traffic is varied, complex and random; it emulates actual network traffic providing high-level, realistic representative network traffic flow into, out of, and inside the network. The volume of traffic and the traffic patterns are programmed to map to the scenario to model user behavior. The traffic protocols are those used abundantly in daily operations (e.g. Hyper Text Transfer Protocol/Secure (HTTP/S), File Transfer Protocol (FTP), Internet Relay Chat (IRC), Simple Mail Transfer Protocol (SMTP), ICMP, DNS, Lightweight Directory Access Protocol (LDAP), etc.). Traffic generates from external/internal sources, traversing the global grid, or leaving any node for another network. It provides a global DNS architecture including Root DNS servers, which emulate the expected behavior found in Intranet and Internet environments. Internet web sites such as www.cisco.com, www.apple.com, and www.walmart.com are emulated across the customer CENTS network. Legion's user emulation capability affords operators realistic client computers that gain IP addresses via DHCP, join the Active Directory (AD) Domain, and register hostnames in DNS. Simulated users, fully qualified on the domain, conduct routine activities (logon/logoff the network using Kerberos client authentication, send e-mail, and surf the web

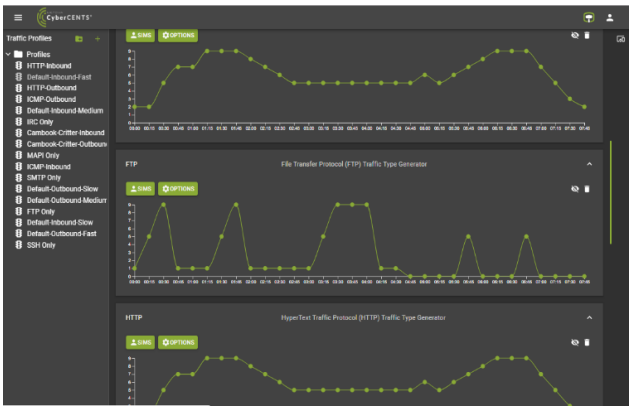

Figure 3: CyberCENTS Traffic Management

The CyberCENTS Traffic Tracker visualization tool provides real-time mapping of traffic flows. Traffic flows are characterized by protocol, packet size, and volume of traffic. Utilizing Geo-located IP Addressing, the traffic flow starts and ends on the global map based on source and destination IP. This provides insight into range activities and is especially suited for demonstration.

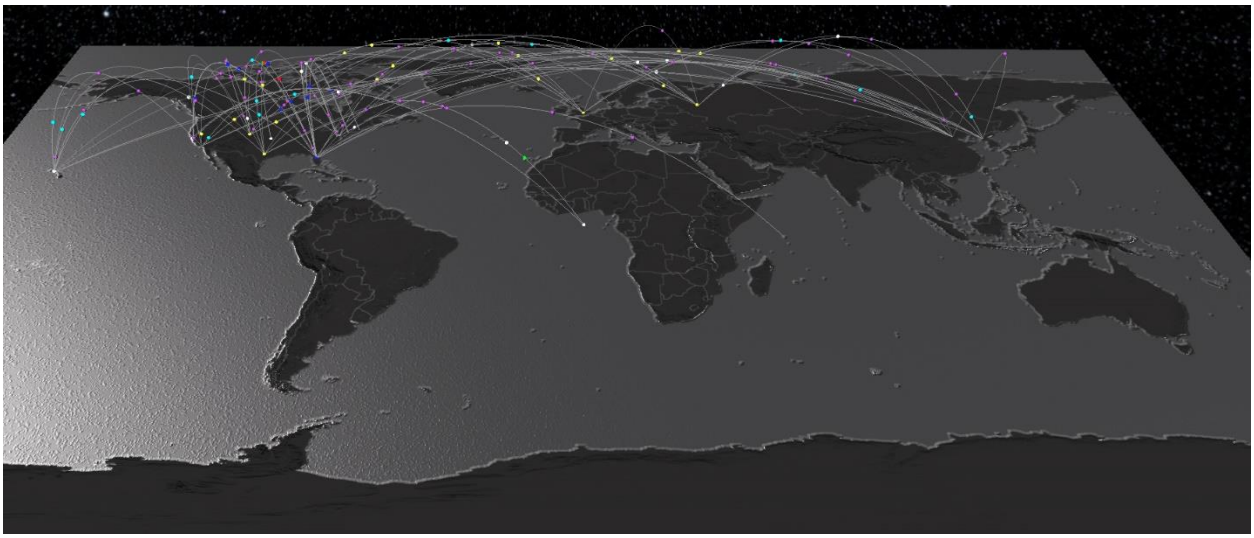

Figure 4: CyberCENTS Traffic Visualization

The **AutoBuild** module connects to the appropriate servers or devices and builds them from standard configuration files. AutoBuild and its image library provides the drag and drop entities. This automated build results in a consistent baseline by removing the element of human error and allows the simulator to be built more quickly. In SLAM-R, there are two VM "libraries". One is the "template" library, the other is the "image" library. All processes are automated using the configurator function in the template (workstations, servers, routers, vulnerable boxes, etc.) and image libraries. The template library contains the configured images of all VMs deployed within the system (blue and gray space). Templates are configured to work within the specific blue and gray space domain unless it is marked "shared".

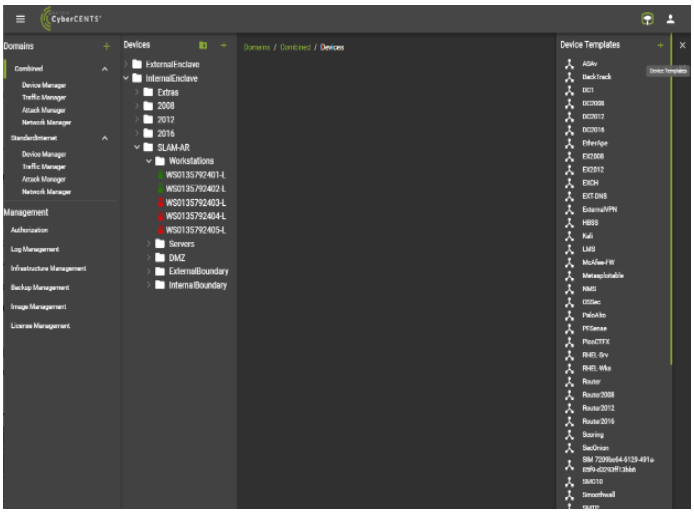

Figure 5: CyberCENTS Template Library

The master image library contains the images of all VMs and appliances CyberCENTS has available in QCOW2 format (Linux KVM format). Images in this library may be incorporated into the system baseline and configured for a specific function (If it is a commercially licessed product, a license must be obtained). Once the baseline configuration is established, a new template is then automatically created and added to the template library. The "add a site" and "add a device capability provide the expansion/adding of VMs to the network. The CyberCENTS AutoBuild and virtualization is Linux-based and uses Kernel-based Virtual Machine (KVM) as its virtualization software.

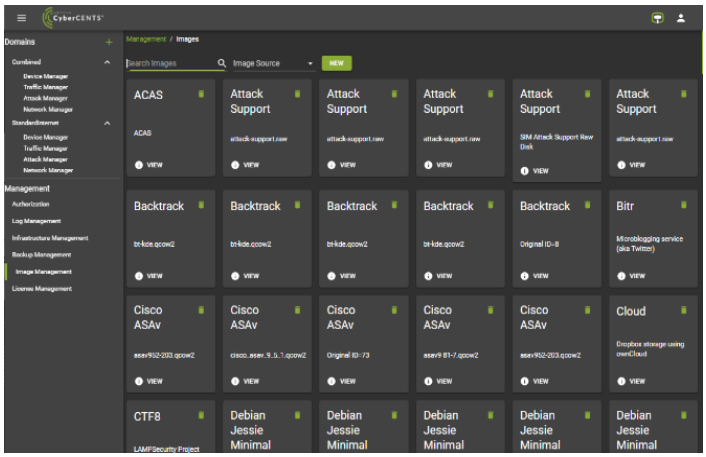

Figure 6: CyberCENTS Image Library

SLAM-R also provides the capability to import new VM images. Through the UI, VM images not already in QCOW2 format, can be converted to QCOW2 and imported into the master image library then templated and made available for integration in the cyber range. This feature permits new virtualized technologies to be incorporated in the range.

Myrmidon is a multi-faceted tool that provides the automated opposing force permitting "real-world" scenario-based cyber training. Myrmidon automates attack scenario development and execution. Whether the system is being used to train individual operators, entire network teams, vulnerability assessments, or test and evaluation, Myrmidon provides the stimulus for students to identify if an attack has occurred, contain the attack, remediate, and defend. It is comprised of nodes and controlled from the primary UI. It provides both scenario management and attack generation. Scenarios are built and executed from the UI through either automatic (pre-set time of execution for each event) or à la carte menu (manual mode) with the capability to select a variety of attacks. Individual attacks can be selected for a single event or multiple attacks can be connected using a timed interface to create a complete (repeatable) scenario. Scenarios and individual events can be started, stopped, and re-rolled to provide maximum training capability. Used in a testing or evaluation environment, Myrmidon provides an off-line capability to perform penetration testing against an operational configuration to identify and mitigate vulnerabilities before they are exploited.

Figure 7: CyberCENTS Attack Management

Through the UI, instructors/trainers are able to manage the entire attack framework. Instructors/trainers can create, load, and execute individual events and/or complete scenarios. The UI has individual wizards for applying new configurations to existing event templates, configuring new events to add to the event template library, and for grouping events into scenarios.

The attack library is updated with each SLAM-R release that is published. Events that are already configured will stay in the templates; the addition of a new version of a particular event will not adversely affect any event in the event templates. The attack library presently contains 2900 events. Using the scenario builder feature in the UI, the instructor/trainer will easily be able to create new attack scenarios without the need to write new code.

When configuring new events and scenarios, the configuration wizard provides a set of text boxes to provide a description of the scenario/event, the objective, the indicators of compromise,

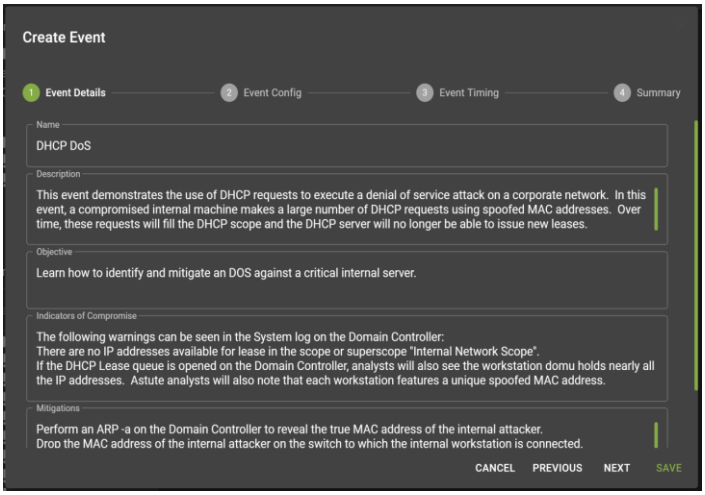

Figure 8: CyberCENTS Attack Description

and the expected mitigation steps for countering or defeating the event. When the playbook for the scenario is printed all the information related to the scenario and each individual event is compiled into a Word document. Event details can be extracted from the Word document and put into student materials for them to have available. All preconfigured scenarios delivered with system will have all the data fields filled in, so the playbook is ready for immediate use.

Reconstitution allows easy re-roll of events or execution of a new scenario by returning the range environment to a previous state by keeping "snapshots" of the VM baselines. At any time, the operator can rapidly restore any or all of the devices within the range to a preconfigured state. This is not a full reinstallation and configuration build, but rather a restoration of the stored virtualized baseline. Snapshots can be taken and saved of individual machines or groups of machines. Multiple sets of preconfigured baselines can be kept providing differing levels of complexity based on training, exercise, or testing objectives for a scenario.

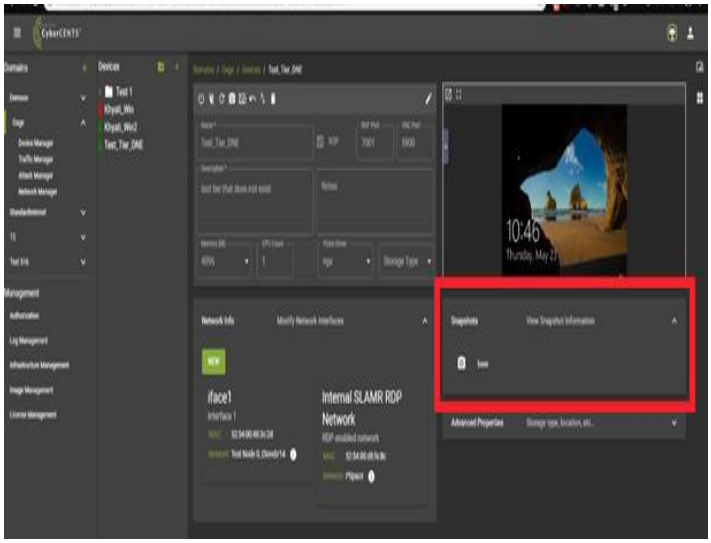

Figure 9: CyberCENTS Snapshots

When either a virtual machine is reverted to a previous snapshot or when an entire system of virtual machines is restored via a group snapshot (VMs must be shutdown first), the range can be completely reset. Multiple snapshots of the same baseline or individual machine can be taken in order to put the range in a particular state in advance of a test, training scenario, or exercise. Once a snapshot is restored, all previously running processes are stopped and previously utilized resources are returned unless they are restarted in the new state.

Domain Isolation, Networking, and Scalability

The implementation of Domains in SLAM-R encapsulates common virtualized network devices and interconnectivity. The relationship within the domain is subjective. A domain can represent a specific exercise or training environment, a portion of a larger network, an internal production environment, or any other user defined relationship. Multiple virtual environments can be created and isolated from each other. Each domain manages its own virtual machines, networks, traffic, and attacks. The Internet becomes a shared resource that can be tagged as exclusive or as shareable. This provides flexibility in managing range resources and only locking down components when necessary.

The SLAM-R Network Manager provides users the capability to manipulate the virtual networks

in a number of ways to scale and add flexibility to the environment. In addition, users can Start, Stop and/or Restart Networks without fear of corruption or compromise. Users also have the ability to interconnect other off-line networks or components to an available physical sever Ethernet port or toggle a switch for promiscuous mode. Networks can be added, bridges can be changed, VLANs can be configured, and network attributes and the attached devices can be viewed through the network manager.

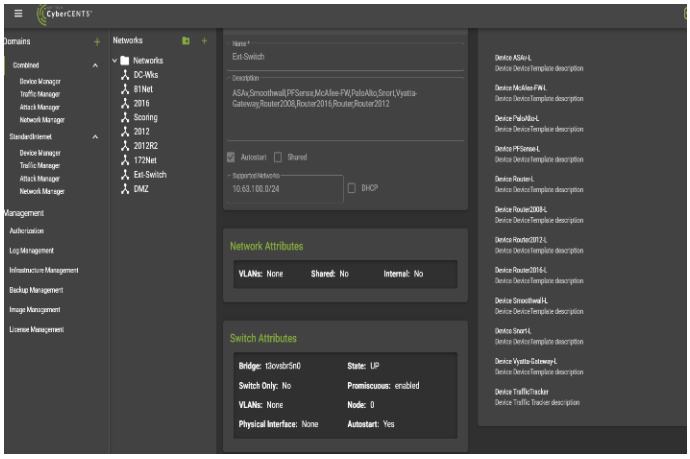

Figure 10: CyberCENTS Network Manager

By managing the networks, bridges, virtual devices, and compute nodes, the range can be expanded to add new technologies into the system.

Role Based Access Control (RBAC)

RBAC is implemented within the SLAM-R baseline. RBAC provides secure access into the range and allows for the isolation of different training environments to only authorized users. Access controls are placed on each of the domains restricting access to only authorized range managers. By restricting access and isolating domains the risk of data spillage across tests and testbeds (whether online or archived) is mitigated. RBAC also permits different instructors/trainers to create and operate their own domains without the risk of another instructor/trainer mistakenly making changes to a domain that is not theirs.

System Auditing/Reporting

Through the Audit capability in the Authorization module of SLAM-R, the administrator has the ability to customize audits being handled by the system. Auditing can be turned on/off for token refresh, login attempts, password changes, claim requests and account operations. Auditing for all options is on by default.

- Audit Successful Token Refresh: Logs all successful token refresh for the web browser.
- Audit Failed Token Refresh: Logs all unsuccessful token refresh for the web browser.
- Audit Successful Logins: Logs all successful user logins.
- Audit Password Changes: Logs all password changes for users.
- Audit Failed Logins: Logs all failed login attempts for user accounts.
- Audit Claim Requests: Logs all token claim requests.
- Audit Account Operations: Logs all user account changes (i.e. name, e-mail, etc.)

Instructor Oversight

SLAM-R provides the capability for the instructor to "shoulder surf" student activities. This is done through the UI and sending each student a unique URL for them to access their particular virtualized workstation via a web browser. The instructor is then able to connect to each student's workstation and work with the machine or observe student actions without interfering with their session.

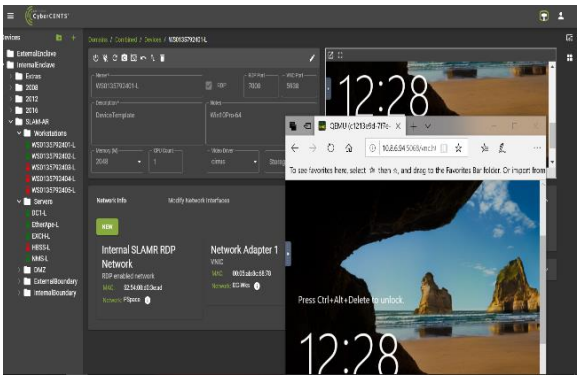

Figure 11: CyberCENTS Instructor Oversight

3 CYBER RANGE PLATFORM SOLUTIONS

All Metova CENTS® platforms are powered by Metova's SLAM-R© appliance which provides the automation/simulation/emulation capabilities such as traffic generation, users, attacks/events/scenarios and Internet functions (Domain Name Services (DNS), Network Time Protocol (NTP), and global web sites). There are four (4) platform solutions in the CENTS portfolio: Hands-On-Training Simulator (HOTSIM®), CYbersecurity Network and Training Simulator (CYNTRS®), Virtualized Cyber Classroom Environment (VCCE®), and Range Global Internet (RGI®).

Each CENTS platform includes typical resources like network sensor systems, switches, routers, firewalls, servers, domain controllers, e-mail, and various other network services normally found in most computer network architectures (depending upon requirements). CENTS with its open systems architecture, provides the capability to integrate additional hardware (physical or virtual appliances) and software (either applications or operating systems) for assessment and validation of potential tools and technologies. The open architecture facilitates expansion either locally or as an enterprise.

Each CENTS Node is designed with expansion, testing, tool development, innovation, reconfiguration, and evolution in mind. **If a product/service has an IP interface, it can be connected to a CENTS unit**. The CENTS solutions are flexible and quite capable of accommodating changes resulting from new and changing requirements, technology, resources, and/or architecture while still emulating the real world operational environment. The solutions are scalable, and can be operated both as a single system or a network of systems interconnected by a VPN architecture.

The HOTSIM and CYNTRS are used for training, capstone events, exercises, and test and evaluation. The HOTSIM unit is primarily a classroom trainer used for individual or small team (up to 3 people) training. The CYNTRS unit is for team (Security Operations Center) training and exercises and capstone events. Both use the same architecture concept having nearly the same network capabilities (depending upon customer needs) and the operating systems, infrastructure, and security appliances are tailored to customer requirements.

The VCCE is primarily used in college/university environments and for competitions. The solution has a very small footprint (2 rack units) and is entirely virtualized and the network infrastructure and appliances are open source tools. The VCCE solution is designed to train up to 28 students within a single range environment. The VCCE has seven individual pods with four seats each interconnected through a single virtualized Internet space. As an analogy, the HOTSIM is a single local area network; the VCCE is seven local area networks all interconnected.

The RGI is a virtualized "Internet in a Box". The RGI provides world-wide routing and traffic flow capability through a series of virtualized tier-1 backbone Internet routers. These virtualized routers are configured with the actual principal data routes of the core routers of the "real" Internet.

3.1 CENTS® SYSTEM ARCHITECTURE (HOTSIM and CYNTRS)

The CENTS architecture and associated framework is an innovative and unique solution for training and exercising full-spectrum cyberspace capabilities in a safe environment. The persistent cyber training environments architectures most commonly developed are for cyber protection, national mission, network operations, network defense, and intelligence operations. The actual technical architecture depends on customer requirements; the intent is usually to emulate the customer's selected operational network architectures when conducting cyber training and exercises. Logical separation of the training network from the operational network permits open and free activities to occur without any concern for operational impact or risk of spillage from any of the scenarios conducted.

A representative CENTS network node for network operations and defense utilizes a defense-in-depth architecture It consists of network architecture designed to emulate a typical network environment.

A "stock" HOTSIM and CYNTRS unit contains the necessary components of a single site network. Although each CENTS unit delivered is customized to the customer's requirements, this response will refer to a 'blue-print' architecture. It contains virtualized internal core network services (e.g. domain controller, email server, web server, network monitoring servers, mail relay, and host based security system). HOTSIM and CYNTRS also contains routing, switching, firewall, routers, switches, and a web proxy.

The HOTSIM solution is a completely virtualized solution utilizing open source tools for network management, network security, and infrastructure. The HOTSIM utilized Microsoft Active Directory for the blue space network. The HOTSIM single network is further described in the Virtualized Cyber Classroom Environment (VCCE).

CYNTRS components are vendor agnostic permitting the use of multiple products, emerging products, or upgraded products within the range environment. The main firewall also provides the separate demilitarized zone (DMZ). In the protected DMZ space, there are External DNS, Web, and Mail Relay virtual servers. The core switch, internal router, internal switch, firewall, proxy, external switch, external router, and Service Delivery Point (SDP) switch can be accessed via Secure Shell (SSH) from the internal accessible workstations hosted in the SLAM-R environment. (Figure 1) More complex architectures can be incorporated when the simulator is designed.

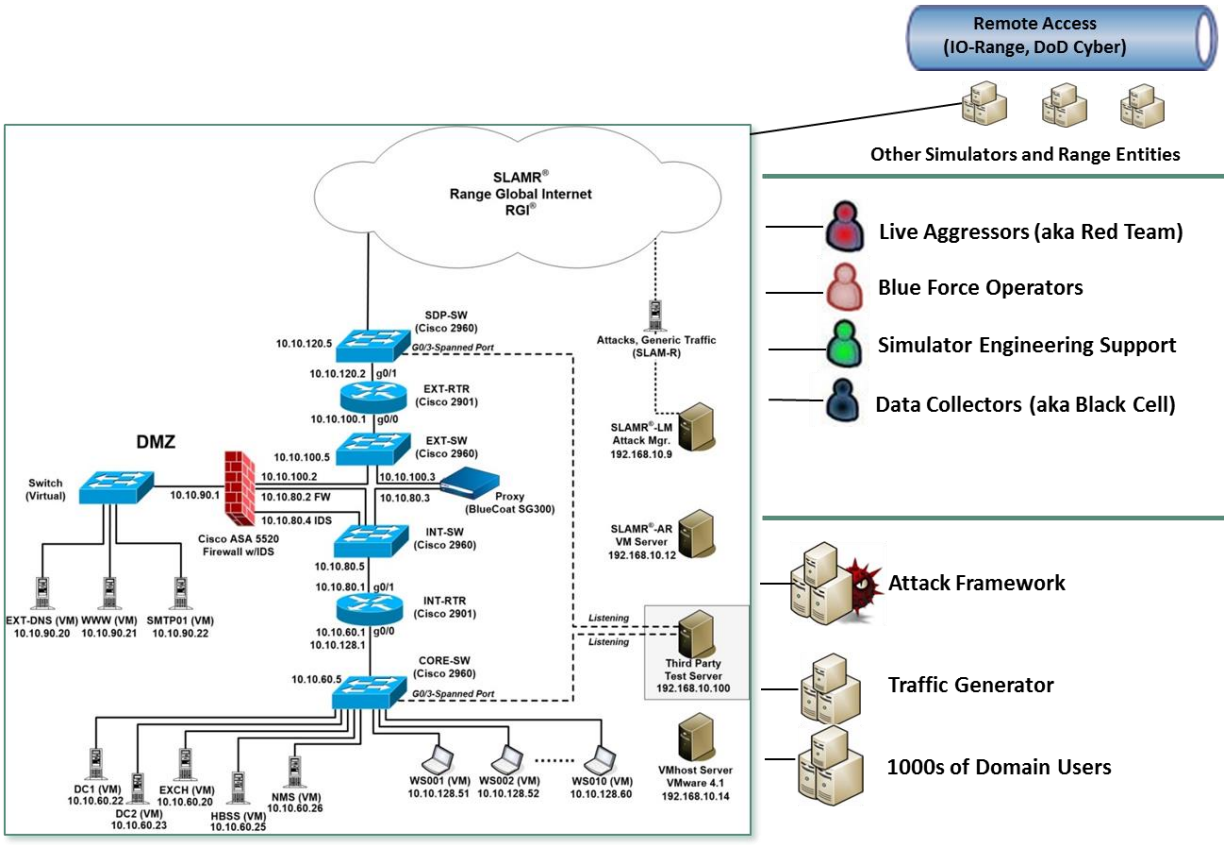

Figure 12: Representative CYNTRS Architecture

The CYNTRS can be designed to support tiered operations. The CYNTRS unit has a wide area network (WAN) services module for tiered operations and simulator interconnection. With its network capabilities (depending upon customer needs) and tailored to customer requirements, the CYNTRS can be used for training, capstone events, exercises, and test and evaluation. The CYNTRS WAN services hosts a Tier 1 Internet router, a simulated Internet, Root DNS, Network Time, and the social networking/media services of Cambook (Facebook) and Critter (Twitter). The CYNTRS unit can be interconnected through the WAN services module off a single Tier 1 router or through the Range Global Internet (RGI®) permitting multiple units on diverse (or similar) range environments to participate in events from an individual location, locations across the US, or anywhere worldwide while in the same cyber range environment (Figure 2).

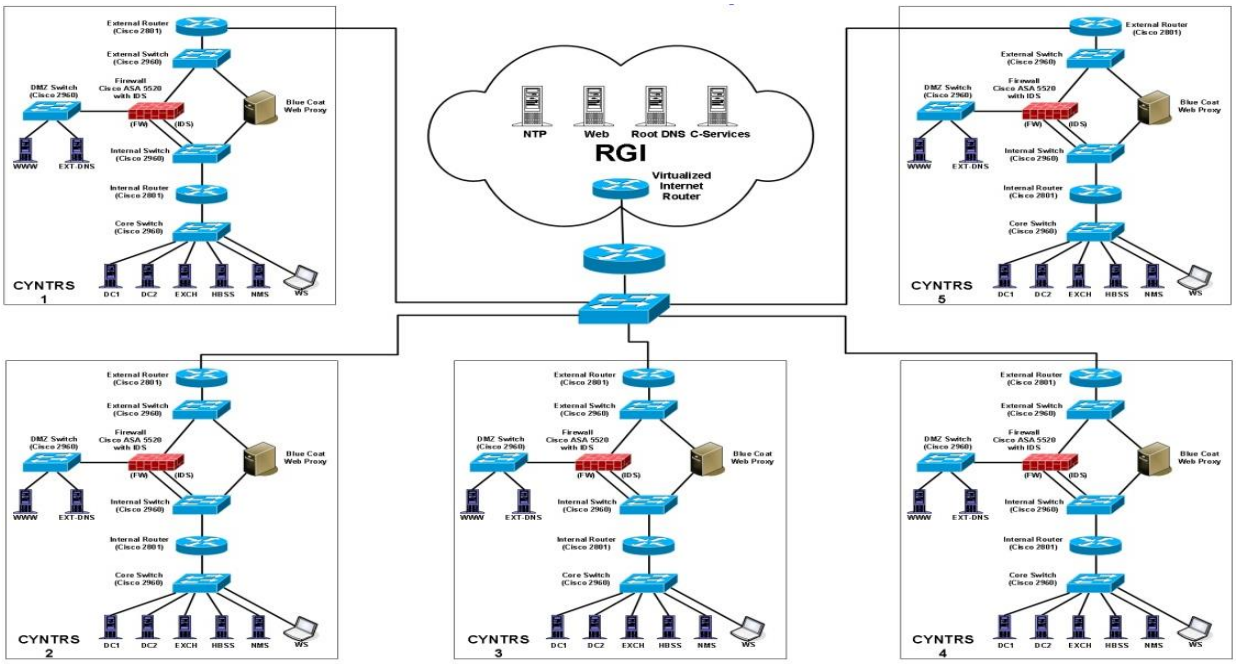

Figure 13: Interconnected Simulator Range

As part of the growing cyber mission, using the CYNTRS platform has also developed a mission forces cyber range solution. For the latest in Cyber Protection Team (CPT) requirements, Metova has designed and deployed systems to train and exercise the "Protection" forces (Figure 3). As with the solutions for the network operations and defense systems, the CPT persistent cyber training environments are designed to be able to emulate the functions of (or interconnected for training/exercise purposes with) a garrison, mobile, or deployed platform. The actual toolset integrated into the range is selected by the customer. Multiple CPT simulators can be interconnected through the Range Global Internet.

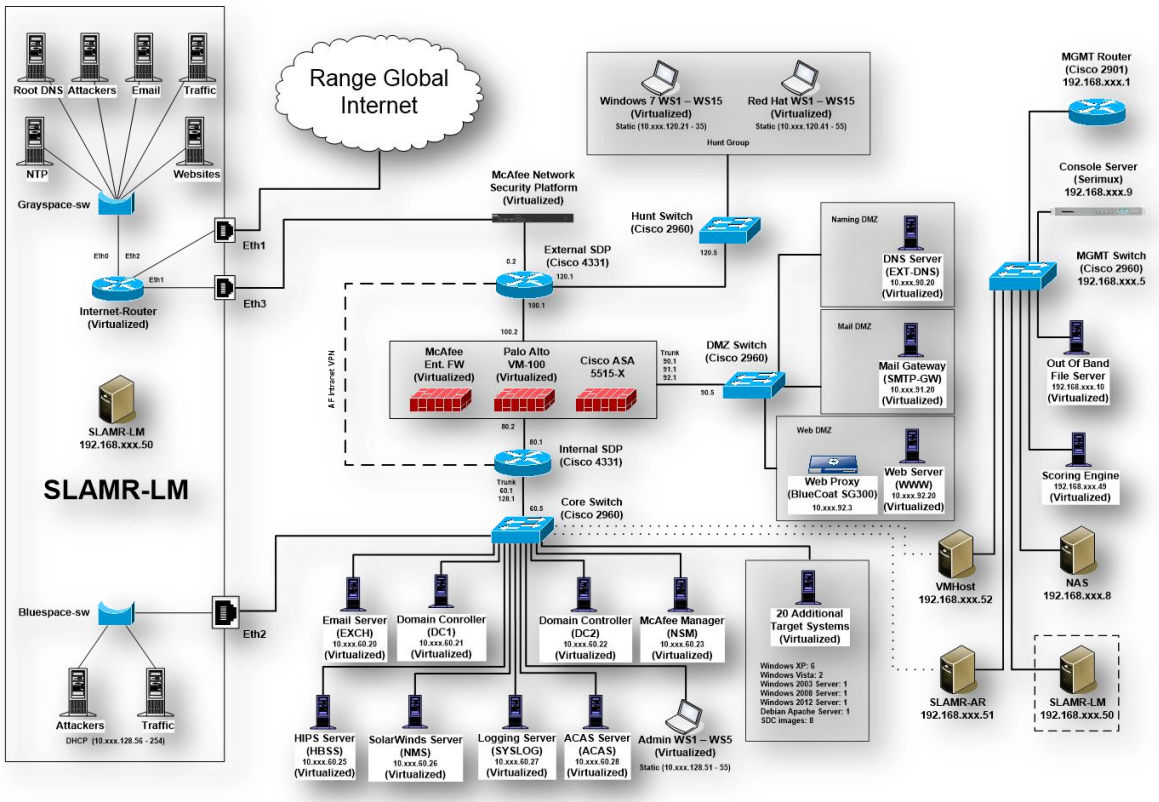

Figure 14: Defensive Cyber Ops Sample Architecture

3.2 RANGE GLOBAL INTERNET (RGI®)

The RGI has a look and feel comparable to the actual Internet. It provides for controlled and secure testing and training scenarios outside of the public realm. The RGI is completely virtualized, using open-source utilities where possible, and utilizes real IPs found in the global Internet structure. With the same open architecture as CYNTRS and HOTSIM, the RGI's flexibility permits the incorporation of physical equipment (e.g. network or threat systems) and virtual appliances.

The RGI is made up of 76 backbone routers, supporting 400+ domestic and international websites and social media sites (Cambook and Critter). The RGI also includes fully functional e-mail servers along with global DNS and Network Time Protocol (NTP) services. RFC-compliant Internet traffic-generation provides routine traffic activities between Internet routers, DNS queries to actual servers, website "GET" request, e-mail generation, along with other miscellaneous random traffic (e.g. ICMP). The traffic provides communication from both internal and external network interfaces (Figure 4).

Figure 15: Range Global Internet Representation

The RGI is spread across six (6) continents. Once inside the customer's spaces, multiple location types (red, blue, gray) can be represented and built out around the globe (e.g. hospitals, banks, universities, cyber cafés, commercial business, churches, government entities, and the military). Since the RGI provides the global Internet without the need for access to the operational network, special access program and coalition enclaves can be built and secured, or cross-communication with allies during an exercise without the risk of accidental exposure to non-exercise information.

The out-of-the-box RGI solution provides the true-IP global routing infrastructure and various location types for populating the subnets around the world. Utilizing SLAM-R's site builder capability, architecture planners and engineers build out the gray-space location based on the requirements for exercise, training, and testing scenarios. The site builder function permits customers to add sites to their gray space utilizing templates for the asset they wish to add. There are 16 physical interfaces for connecting physical devices to the RGI, including control/Supervisory Control and Data Acquisition (SCADA) system interfaces. The physical interfaces can be expanded by adding physical switches to the out-of-band network. Physical devices (to include representative LAN solutions) can then be networked to a specific location. Locations have full domain services, defense in depth construction, and network traffic communication between sites and machines.

3.3 VIRTUALIZED CYBER CLASSROOM ENVIRONMENT (VCCE®)

The VCCE provides the core networking environment of the blue space. The VCCE's virtualized LANs provide the environment for teaching multiple students network defense and attack in individualized workspaces and for exercises, experiments, and wargames. This solution is optimal for a training and testing environment with shared core services (DNS, NTP, Web), but an isolated network environment for each student/team or experiment where the changes made by one student/team do not impact the environment of another. The VCCE is multiple LANs referred to as pods, all interconnected through a single virtualized Internet (gray) space. Each platform will contain seven (7) virtualized, fully functioning HOTSIMs (hereafter referred to as pods); each with four (4) student seats supporting up to 28 students at any given time. Each pod will be populated with simulated users with ambient and attack traffic being generated from/to user bots on the blue space network and the gray space Internet. The pods can be configured the same or differently to

support the specific function of a particular team, testing event, or network build-out. Multiple baselines for the pods can be created and snapshotted for use based on need. Since each pod is a fully functioning network, students will need to take on different roles (similar to those in a security operations center) to administer and defend the network. The pod configuration permits instructors to train individuals as well as small and large teams. Baseline workstation images include tools/applications to manage, monitor, and secure the network such as: the tools to manage a Microsoft network (sys admin tools), putty, Wireshark, WinSCP, Pidgin, Chrome, and Firefox. As the workstations are full-stack virtualized workstation, whether Windows or Khali (or other operating system) additional applications can be added to virtual machine image

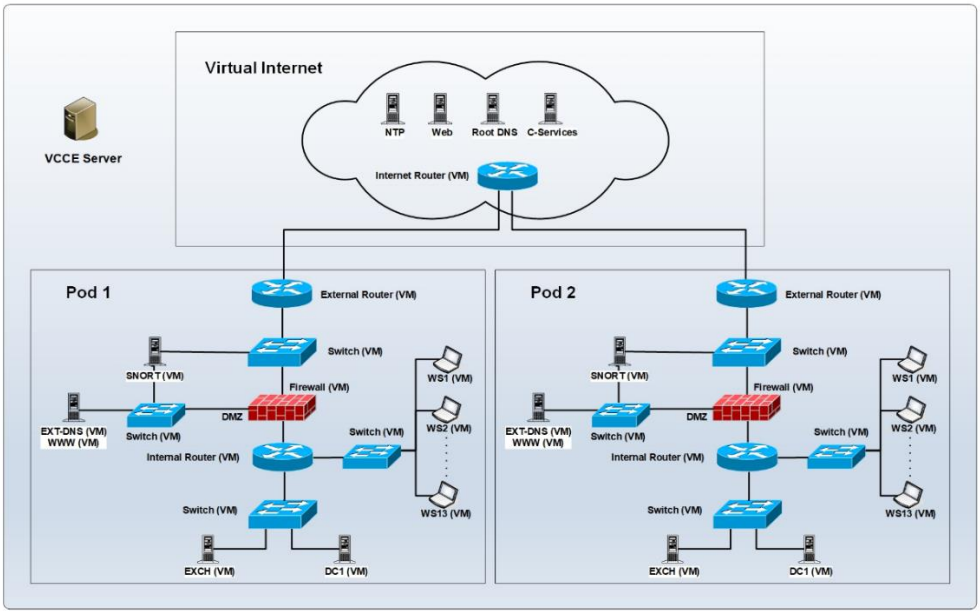

Figure 16: VCCE Representative Architecture

4 MOBILE CYBER RANGE SOLUTIONS

Metova CyberCENTS has delivered transitized versions of each of our CENTS solutions (CYNTRS, HOTSIM, RGI). Each transit case weighted for a 2-man lift and each case includes casters. Shock absorbency rating is based on customer requirement (Figure 8).

Figure 17: Transitized CYNTRS

5 INTEGRATION WITH OTHER SYSTEMS AND EXPANSION

The CENTS platform solutions are built on an open systems architecture permitting the integration of new hardware or software based on customer need. The CENTS architecture is vendor-independent/agnostic, and the virtualization technology is an open standard, Linux KVM. The systems devices are also vendor agnostic and can be updated or changed at will. The open architecture also permits the integration of other vendor products into the range for testing of capabilities. The SLAM-R APIs allow vendors to create add-on products that increase a system's flexibility, functionality, interoperability, potential use, and useful life. Since SLAM-R allocates resources dynamically, a CENTS solution's ability to scale upward is done through the adding of "compute nodes" providing additional processing power, memory, and storage.

5.1 INTEGRATION WITH LVC M&S ENVIRONMENTS

Metova has developed innovative methods and software tools to generate cyber-attack and defense effects for both live and simulated actors within the Live, Virtual, Constructive training environment. The data exchange broker performs discovery, role player assignment, targeting, and denial of service (DoS) attacks against battlefield simulations that can be used for training within multi-domain battle.

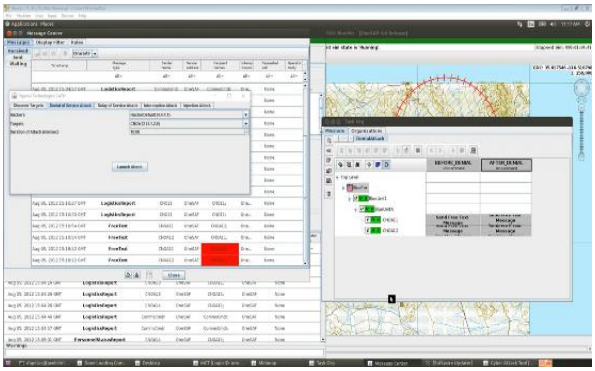

Figure 18: Sample LVC Interface

5.2 INTEGRATION WITH ICS/SCADA ENVIRONMENTS

Our learning platform provides high-fidelity emulation of Industrial Control Systems and Supervisory Control and Data Acquisition systems that leverages physical devices, emulation and simulation technologies. The trainer enables users to create ICS/SCADA environments of varying levels of fidelity for vulnerability identification, cybersecurity implementation and vulnerability mitigation. This trainer includes all hardware, software, realistic plant operations simulation and the interface between plant networks and corporate networks, as well as the integration of IT and OT networks. This trainer has the ability to simulate multiple variations of OT environments, application configuration, cyber red/blue team capability, vulnerability assessment capability and testbed capability for the application of cybersecurity measures. The picture to the right displays the Metova CyberCENTS Portable ICS Module which simulates the functions of a nuclear power facility using an Allen Bradley PLC/HMI and a display of lights for critical infrastructure within the facility.

Figure 19: AB ICS Module

Our simulated OT environments consist of VMs running within the cyber trainer segmented into an OT network segment. The virtual HMI/PLC devices utilize the ModbusTCP protocol.

Simulated Building, EMS, Power, Transit and Water Environments

Figure 20: Metova ICS/SCADA Virtual Machines

6 LEARNING MANAGEMENT SYSTEM

The CyberCENTS LMS is a learning platform is designed to provide instructors, curriculum managers, and students with a robust centralized, integrated, and secure platform where they create, manage, and consume tailored learning experiences. The LMS enables you to do what you do best; educating and training your people by providing rich and empowering learning content.

Key LMS Features:

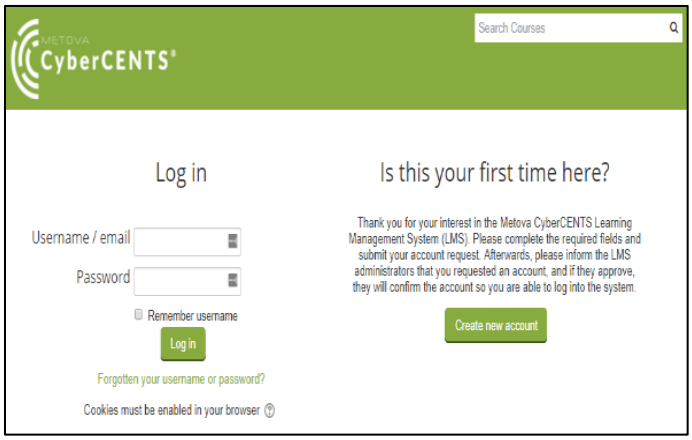

Figure 21: Learning Management System

- Flexible platform permits course content development (e.g. lessons, assignments, quizzes)
- Supports standard learning material, such as documents, presentations, and video
- BigBlueButton interface providing real-time audio, video, slides, chat, and screen sharing
- System designed to scale to support organizational growth
- Operates on open and closed networks
- Tailorable Role-Based Access Control
- Course and Category Management for logical organization of courses
- Custom Learning Plans and Lessons facilitating custom course flow
- Feedback Loop
- Fosters collaboration via chat, forums, and direct messaging
- Learning validation and grading
- Shareable content between CyberCENTS Learning Management Systems

The LMS consists of a Linux-based platform running a customized installation of the Moodle extensible learning platform and course management system. Moodle is an open-source, collaborative software platform released under the GNU General Public License used by thousands

of learning providers with a large developer, support and user-base that is constantly being advanced to support evolving learning requirements. CyberCENTS uses existing community plugins along with our custom-developed plugins to support the needs of a highly integrated, learning environment providing a seamless "single pane of glass" experience for the training environment. The LMS supports standardized components, and is designed to provide instructors, content developers, and students with a robust, secure, and integrated system to create customized learning environments. Additional plugins supporting a variety of capabilities can be added to the extensible platform to enhance the overall learning environment.

Figure 22: LMS Student View

The CyberCENTS LMS provides the training organization with the following capabilities:

- Student(s) enroll, select and complete instructor-led and self-paced courses
- Student(s) access syllabi, lessons, wikis/blogs, documents, multimedia and other course materials
- Instructor(s) access/edit lesson plans, trainee guides, presentations, and course control documents
- Event creation, resource scheduling and content repository for assigned training
- A gradebook for tracking the progress of students throughout their learning experience
- Instructor/student, student/student interaction via a communication platform

The LMS web portal is a single-pane dashboard for student interaction with course content and instructors/peers through collaboration tools, such as voice and video. The gateway is used for processing enrollment as a student in an instructor-driven classroom course, on-site or online, and workforce development training. The LMS provides a mechanism for instructor communication, sending/receiving documentation, and storing community documents to aid in course delivery.

The LMS includes core Application Programming Interfaces (APIs) allowing third parties to integrate with the system. These functions enable the completion of key tasks, such as user and course creation, retrieving and updating course progress and grades for individual learners, and system interaction by course participants. Integrators can develop custom plugins and web service clients to execute remote function calls by external applications using industry standard protocols (i.e. REST, SOAP, XLM-RPC, and AMF), further enhancing interoperability between the system and custom environments and applications.

Integration is readily available. The LMS, although hosted within the Cyber Range architecture, has a publicly accessible network address if permitted by the organization. This not only provides seamless access by the learner, but also allows course content developers to redirect them to various open and closed environments and content sources, such as cyber ranges, media sources like Google Drive, YouTube, and Vimeo, and other online websites.

7 CENTS DIFFERENTIATORS

Open Architecture – Proven ability to integrate with other technologies and systems; hardware-in-the-loop or other virtual machines.

Configurable – Support different missions including training, T&E, target development/ mission rehearsal, proof of concept

Site Builder/Add Device Capability – Wizard menus provide the capability to create the interfaces for new sites or add devices for expansion.

Accessible – Remote access or on-site (garrison and deployed)

Multi-mode and Re-roll Capability – Automatic or manual mode; reconstitution allows event replay with repeatable results

Threat/Target Emulation – Site builder and open architecture permit incorporation of virtualized or physical devices.

Flexible and Scalable – Platforms and configurations can reflect a flat network or be intricate and multi-layer supporting a tiered reporting and management network.

Self-Contained Environment – Simulated Internet and root DNS removes the need for an Internet connection. Permits incorporation of collateral/SAP level activities on a single range

Traffic Generation – IETF RFC compliant dynamic traffic flows; service thresholds based on customer defined profiles

Simulated Internet and Root DNS – Realistic multi-hop routing using dynamic routing protocols, multi-layer websites; all IP addresses and websites resolve in DNS

True-Life System Response - Drill-down to the OSI Layer 2; user-configurable devices; real-time event execution; events run until mitigation steps are taken or terminated by the operator

Industrial Control Systems – ICS modules with events targeted as SCADA systems

Social Media – Social networking and blog capabilities (Facebook/Twitter like services) provide depth, bring realism, and facilitate team intra-system communication, and intelligence training

Authority to Operate – CENTS/SLAM-R has been issued an ATO by the HAF/A3 under the NIST Risk Management Framework as instantiated in the Virtual Interconnected Training Environment (VITE) program of record.

Simulator Certification – CENTS/SLAM-R as configured for VITE has been issued a SIMCERT by AFSPC/A3 certifying VITE as an Air Force Cyber Simulator meeting the requirement to mission qualify Cyber Mission Forces.

Commercial Product – Stable baseline, software development life cycle and sustainment trail, available maintenance packages, and software updates/new features backed by corporate funding.