METOVA CyberCENTS®

SLAM-R©
RANGE AUTOMATION ENGINE

Sentinel-Legion-Autobuild-Myrmidon-Reconstitution (SLAM-R©)

The SLAM-R appliance is Metova's range automation engine providing network monitoring with Sentinel – traffic generation, user emulation, simulated internet, and root Domain Name System (DNS) through Legion – rapid simulator duplication through AutoBuild – scenario building and network attacks through Myrmidon – and rapid system baselining through Reconstitution. A management console is used to manage the SLAM-R hardware.

Real threats executing in a safe and authentic environment for training, testing and exercises

SLAM-R®

ENVIRONMENTS

SLAM-R provides a complete and detailed simulated network integrated into each CENTS® platform or your existing environment.

TRAFFIC

With SLAM-R, customer configurable network traffic is generated through simulated users who browse websites, send e-mail, use social media sites, retrieve files, etc.

ATTACK

At the push of a button, SLAM-R supplies current and real traceable and attributable attacks. Attack status and feedback are provided continuously for controller observation.

INTERNET

SLAM-R has realistic Internet supporting an authentic user experience.

CONTACT: 1+ 618.624.7800, cybercents.sales@metova.com | **VISIT:** www.cybercents.com

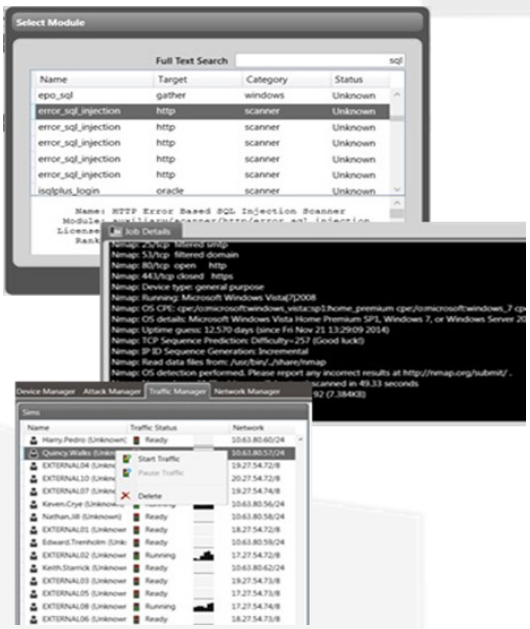
METOVA CyberCENTS®

SLAM-R®

SLAM-R©

MORE THAN JUST ANOTHER CYBER RANGE COMPONENT
SLAM-R RUNS ALL CENTS® CYBER RANGES

SLAM-R© powers every CENTS® platform. It provides an immersive training, testing and exercise environment requiring no third-party add-ons. In a single solution SLAM-R provides virtualization of, and immersion into an emulated network with the same look and feel as your real-world operations center, with capabilities to create and execute complex scenario-based network events. The SLAM-R tool suite operates as a single node or as part of a vast distributed cyber range network, while still providing the range operator with a unified interface. SLAM-R includes a virtual population of clients, users, and servers, all interoperating within a virtual Internet. The SLAM-R attack engine is populated with thousands of cyber events and scenarios experienced by operators worldwide. All traffic and attacks flowing through the cyber range are fully attributable.



POINT AND CLICK ATTACK GENERATION

The attack framework provides the controller the ability to quickly and easily create, configure, schedule attacks, and create scenarios based on real-world events.

INSTANT ATTACK FEEDBACK

As attacks execute, the controller is provided immediate and continuous feedback from the perspective of the adversary.

REAL USER NETWORK TRAFFIC

Data traffic emulates standard user operations such as web surfing, email, and file server access, along with other data traffic to and from the Local Area Network and the Internet.