

How can CYbersecurity Network TRaining Simulator (CYNTRS) benefit Department of Defense, Federal and Commercial agencies' information assurance programs?

By EADS NA Defense Security & Systems Solutions Inc.

An article in Federal Computer Weekly, 20 Aug 07, "Information assurance still a tough sell at DoD ex-official says," provides excellent information to answer this question. The article, written by Sebastian Sprenger, quotes Dr. Linton Wells II, former Principal Deputy Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer.

The article stresses the importance of defining the "playing field" as well as solutions, measuring the return on investment and guaranteeing results. The problem is exacerbated because IT requirements, attack methodologies, and defense technologies are a constantly moving target. Add the human factor into this equation and the difficulty increases exponentially.

According to Dr Wells, Senior officials have a difficult time funding programs without a solid foundation of return on investment metrics or distinguishable measures of merit with the increased statistics of computer network probes, attempts and attacks. Information assurance (IA) and computer defense programs only come into play during and after an incident or crisis.

IDENTIFYING THE PROBLEM AND THE SOLUTION

"It's a tough audience, because what they say is, 'Show me how this \$2 million you want to put on this is going to turn cell C17 from red to yellow to green in 2011'...and that's often a hard thing in information assurance."

Dr. Wells

The EADS NA Defense Security and Systems Solutions, Inc. (DS3) CYNTRS solution focus is to provide defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction at all operational levels within any enterprise. The lack of training and exercises in computer network defense can lead to unprotected and/or inadequately protected networks, loss of critical data and resources, and possible exploitation by adversarial elements. By using the CYNTRS solution, we are able to provide realistic network operations training without incurring any risk to operational networks.

Network professionals need to enforce IA controls and hold users accountable for their actions. CYNTRS will develop, train, maintain, and enhance the skills, techniques, and

experience needed to ensure computer network and security operators are capable of recognizing, combating, and mitigating harassing, aggressive, sophisticated, or destructive computer network attacks. CYNTRS is the tool and enabler for accomplishing this training. Through training exercises and labs with CYNTRS, your organization's computer network security posture and mindset will vastly improve. Malicious attempts will continue to grow with changing technology, but if we (all) hold the same vigilant security mindset in Information Assurance/Information Protection, successful events will be minimized. We do not just need IT security personnel to secure our computer networks; this is a job and standard operating procedure for all. With CYNTRS, incident response of these malicious attempts can be prevented, detected, and migrated before serious damage can affect the organization's network.

With CYNTRS, computer network and security operators can be educated to be aware of such security flaws or vulnerabilities in multiple tier networks as well as how to recognize and prevent malicious attacks. CYNTRS provides a near real-time, one-of-a-kind training and assessment of computer network and security operators responding to a simulated attack. Computer network and security operators can use CYNTRS to learn how to protect a network with the same "look and feel" as their own network environment, complete with routine data traffic, bottlenecks, outages and network attacks. CYNTRS has a unique, built-in capability to quickly "reset" the simulator to a baseline configuration for training or loading a new tool suite for test and evaluation prior to operational deployment.

By implementing CYNTRS into a information assurance and network security training program, personnel will be armed with the defensive techniques, instruction and experience needed to become competent and certified in managing and protecting enterprise networks. In addition, CYNTRS can be utilized to institute basic user IA and awareness programs. CYNTRS can be used to demonstrate the capabilities and effects of malicious activities and poor business practices to the end-user so they can better understand the importance of IA and awareness programs within any organization.

With CYNTRS and the proper training regimen, it is possible to turn an organization with a failing red rating to a passing green rating within 6 months to 2 years depending upon organizational size, area of responsibility, personnel competencies, processes/policies in place and accountability.

QUANTIFIABLE METRICS AND THE RETURN ON INVESTMENT

“Officials in charge of putting together the budget for the security of DOD's networks need better metrics for measuring return on investment for information assurance programs.”

Dr. Wells

Protection of critical data is the objective, but often metrics are needed to correctly interpret progress (return on investment) directly related to any solution that is

implemented within an enterprise. Metrics can be subjective and/or objective, but should be any kind of measurement to gauge some quantifiable component of performance. CYNTRS will provide the ability to measure the performance and response times of your network operators to repeatable, discrete events or complex scenarios. CYNTRS will enhance and streamline the gathering of these metrics, while developing competent and experienced computer network and security operators fully capable of defending your networks and data systems against exploitation and attack.

CYNTRS' top priority is to provide the most comprehensive network security training environment for today's Net-Centric world. CYNTRS' main concern within this network defense arena is to create net-savvy operators capable of quickly identifying, evaluating and responding to a plethora of ever-growing local and global computer network threats. CYNTRS will immerse network operators within various scenarios, to include: insider and outsider threat situations, situational analysis, and multi-tasking/prioritization drills. All these activities combine to provide a positive environment for learning, a definitive gain in experience, and well developed network defense skillsets.

Furthermore, CYNTRS can be used to test and evaluate new products prior to actual deployment on an enterprise network. This provides a significant return on investment by providing an environment to "work out the bugs" prior to operational use, saving "false starts", network downtime, etc., for a smooth initial roll-out.

GUARANTEEING RESULTS

"We have not done a good job in making the case that a dollar spent here is going to lead to a quantifiable increase there"

Dr Wells

Your network and data are valuable resources. You have a significant investment in infrastructure, security, and processes to protect those resources. In order to better your chances of protecting that investment, you should provide continuous training to "exercise" your personnel and processes. CYNTRS is your solution to help protect that investment. With CYNTRS, your personnel are better able to quickly identify, evaluate and respond to malicious events, network and computer problems, as well as catastrophic failure. The lack of continuous CYNTRS-based training may lead to unprotected and/or inadequately protected networks, loss of critical data or loss of operational control, and possible exploitation by malicious entities. Bottom line, CYNTRS helps to indirectly mitigate these threats and minimize potential revenue impact caused by loss of proprietary data, network outages and associated negative media coverage.

The CYNTRS solution provides the customer with a responsive training forum that focuses on information assurance and computer network defense. It provides your network professionals with the realistic training needed to respond to an ever growing

threat of data loss and system exploitation. What CYNTRS gives your operators that no other training provider can is an integrated training suite putting all your corporate tools at their disposal in order to manage and solve your most challenging IT issues. This solution can be readily expanded and customized for unique customer requirements as well as future application into different training environments such as training new personnel and testing new equipment and applications before implementation into the operational network. With CYNTRS, the benefits of continuous training in a realistic network environment will effectively and efficiently increase your organization's ability to protect your operational infrastructure and critical data.