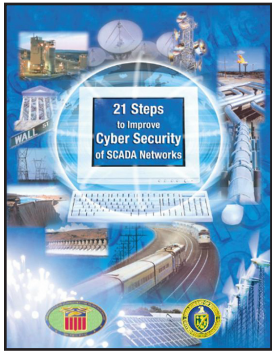




21 Steps Security Metrics Tool

Overview of the 21 Steps Tool



The **21 Steps Security Metrics Tool** (beta-test version) has been developed by the I3P to provide organizations with a simple and easy-to-use tool for quickly assessing and displaying the general cyber security status of process control system (PCS) networks. The tool is based on “21 Steps to Improve Cyber Security of SCADA Networks,” a guidance document published in

2002 by the Department of Energy Office of Energy Assurance for the President’s Critical Infrastructure Protection Board. (see http://www.oenergy.gov/DocumentsandMedia/21_Steps_-_SCADA.pdf).

The *21 Steps Tool* can be used as provided, or it can be customized by the user to assess different security steps and use different performance evaluation criteria as required. The same software framework and principles employed in this tool can also be used to develop other tools that can evaluate security based on a more comprehensive and detailed set of security guidelines or standards.

21 Steps to Improve Cyber Security

The *21 Steps Tool* evaluates cyber security performance in 21 different performance areas. The first 11 steps focus on the specific actions that can be taken to increase the security of control systems and PCS networks. Among the areas assessed are the:

- performance of audits and physical security surveys of PCS devices and networks and connected networks
- identification and disconnection of unnecessary connections to the network
- evaluation and strengthening of the security of remaining connections

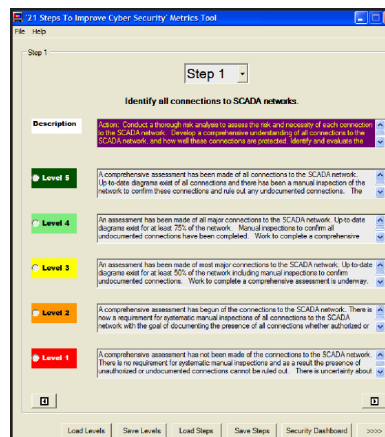
- efforts to harden networks by removing or disabling unnecessary services
- implementation of security features provided by device vendors
- implementation of internal and external intrusion detection systems.

The last 10 steps focus on management actions that are pertinent to establishing an effective cyber security program. These include:

- documentation of network architecture and identification of systems that serve critical functions
- establishment of a rigorous risk management process
- establishment of a defense-in-depth network protection strategy
- establishment of cyber security requirements and policies and an associated accountability system
- establishment of an effective configuration management processes, backup systems, and disaster recovery plans.

Running the 21 Steps Tool

When the tool is first started, the cover page of the “21 Steps to Improve Cyber Security of SCADA Networks” is briefly displayed. The tool then displays a written description of the starting screen for the tool.



The tool displays a written description of Step 1 and the five levels of performance for this step. Level 1 represents a low level of security performance, Levels 2 through 4 represent intermediate levels of performance, and Level 5 represents the highest level of security for this step.

Researcher Contact Information

Pacific Northwest National Laboratory
 Operated by Battelle for the U.S. Department of Energy

Cliff Glantz
cliff.glantz@pnl.gov
 509.375.2166

Lori Ross O’Neil
lro@pnl.gov
 509.375.6702

About Pacific Northwest National Laboratory

Researchers at Pacific Northwest National Laboratory are advancing the frontiers of scientific knowledge and rapidly translating their discoveries into innovative technologies. State-of-the-art facilities combined with innovation and creativity help Pacific Northwest’s scientists and engineers resolve critical challenges in energy, the environment, and national security for government and industry clients. Pacific Northwest also strives to move scientific gains from the laboratory to the marketplace through various programs and partnerships.

This work was supported under Award number 2003-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

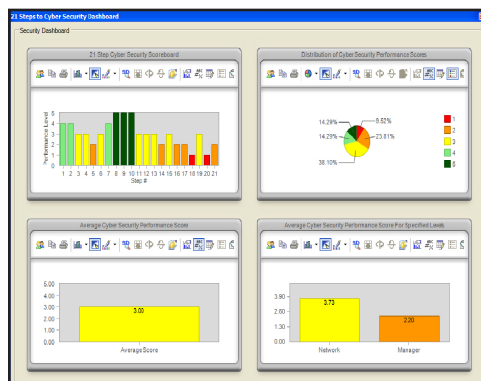
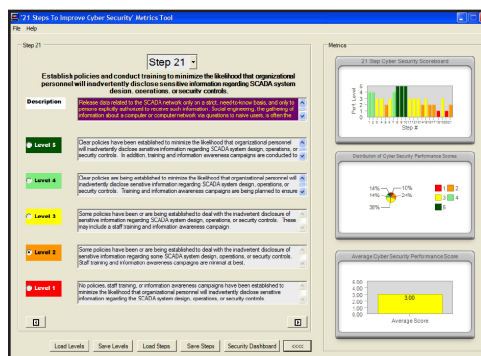
After reading these descriptions the user determines which performance level best captures the status of the PCS network that they are evaluating. The user then clicks the corresponding performance level indicator. This assigns the indicated performance level to Step 1. The user can then proceed to Step 2, accessed using the drop down Step menu or clicking the advance button (>>>>) at the bottom of the screen, to evaluate performance for this step.

Someone knowledgeable with the security practices for the PCS network being assessed can complete the entire 21 Step assessment in less than 10 minutes. While performing the assessment, a dashboard indicator can be displayed to graphically indicate interim security performance results.

Alternatively, a full security dashboard can be displayed to give a larger view of the security status assessment for the network.

In the upper left quadrant of the dashboard display, performance levels are shown for each of the 21 steps. The better the performance, the taller is the column indicator.

To further emphasize the performance level, the color of each column may vary from red (for the lowest performance level) to green (for the highest performance level). In the upper right quadrant hand corner of the display, a pie chart shows the distribution of performance levels for the 21 steps. The colors used in the pie chart mirror the colors used in the column display. In the lower left quadrant of the display, the average performance level overall all of the 21 steps are indicated. In the lower right quadrant of the display, the average performance level is separately given for the network security steps (Steps 1-11) and for management actions to enhance security (Steps 12 -21). These results can be used to indicate if there is an imbalance between network administrative and management security levels.

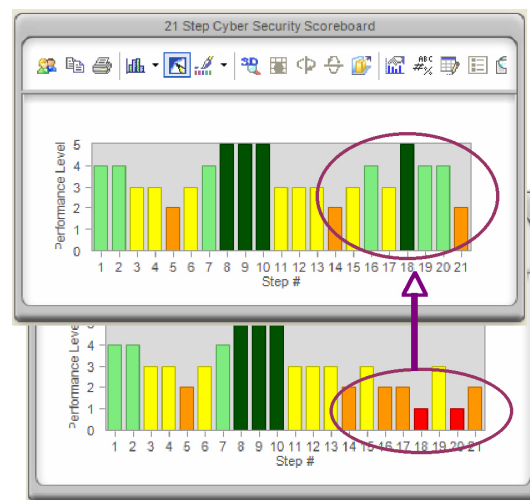


Saving and Retrieving Information

The 21 Step tool allows for saving assessment results and reloading these results for future examination and reassessment. In addition, the descriptions for the Steps and individual performance levels can also be edited, saved, and re-loaded to allow the user to customize the assessment to best address their organization's security assessment needs. These options are accessed through buttons at the bottom of the tool's display or from a drop down menu. A user's guide and a copy of the original 21 Steps Report is also available for display by clicking the Help button on the main toolbar.

Assessing Security Options

The 21 Step Tool can be used to assess various security options by looking at how security enhancements may change the security levels and average scores. When coupled with cost information, this can provide decision makers with guidance as to how best to deploy their security resources.



Installing the 21 Steps Tool

All of the software needed to run the tool on a Windows XP- or Vista-based personal computer is provided in the tool's installation package. Memory and performance requirements for installing and running the software are minimal -- the program was designed to run on the most basic of laptops and workstations. The 21 Steps Tool was created using Microsoft Visual Basic© and the ChartFx© software.

Acquiring the 21 Steps Tool

The current beta-test version of the 21 Steps Tool is available for testing by interested organizations. We welcome your feedback to help us improve the tool. For further information, please contact Cliff Glantz (cliff.glantz@pnl.gov; 509.375.2166).