Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

CYBER SECURITY EVALUATION TOOL

PERFORMING A SELF-ASSESSMENT

The Cyber Security Evaluation Tool (CSET®) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. It is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate their industrial control system (ICS) and information technology (IT) network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations. The Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) developed the CSET application, and offers it at no cost to end users.

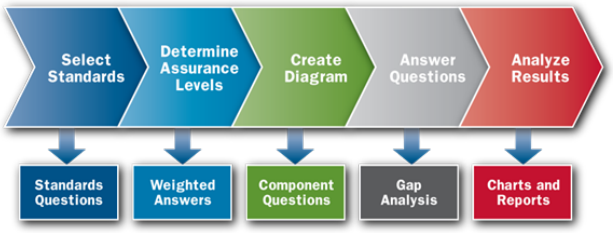
HOW IT WORKS

CSET helps asset owners assess their information and operational systems cybersecurity practices by asking a series of detailed questions about system components and architectures, as well as operational policies and procedures. These questions are derived from accepted industry cybersecurity standards.

When the questionnaires are completed, CSET provides a dashboard of charts showing areas of strength and weakness, as well as a prioritized list of recommendations for increasing the site's cybersecurity posture. CSET includes solutions, common practices, compensating actions, and component enhancements or additions. CSET supports the capability to compare multiple assessments, establish a baseline, and determine trends.

THE ASSESSMENT PROCESS

This assessment process can be used effectively by organizations in all sectors to evaluate ICS or IT networks.



1. Select Standards

Users select one or more government and industry recognized cybersecurity standards. CSET then generates questions that are specific to those requirements. Some sample standards include:

- DHS Catalog of Control Systems Security: Recommendations for Standards Developers
- NERC Critical Infrastructure Protection (CIP) Standards 002-009
- NIST Special Publication 800-82, Guide to Industrial Control Systems Security
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
- NIST Cybersecurity Framework
- NRC Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities
- Committee on National Security Systems Instruction (CNSSI) 1253
- *INGAA* Control Systems *Cyber Security Guidelines* for the Natural Gas Pipeline Industry
- NISTIR 7628 Guidelines for Smart Grid Cyber Security.

2. Determine Assurance Level

The security assurance level (SAL) is determined by responses to questions relating to the potential consequences of a successful cyber-attack on an ICS organization, facility, system, or subsystem. It can be selected or calculated and provides a recommended level of cybersecurity rigor necessary to protect against a worst-case event.

3. Create the Diagram

CSET contains a graphical user interface that allows users to diagram network topology and identify the "criticality" of the network components. Users can create a diagram from scratch, import a pre-built template diagram or import an existing MS Visio® diagram. Users are able to define cybersecurity zones, critical components, and

network communication paths. An icon palette featuring system and network components allows users to build and modify diagrams by simply dragging and dropping components into place.

4. Answer the Questions

CSET then generates questions using the network topology, selected security standards, and SAL as its basis. The assessment team can select the best answer to each question using the organization's actual network configuration and implemented security policies and procedures. Notes can be entered or files attached to individual questions, flagging them for further review or providing clarification. Each question has associated reference information that is provided for clarification. The system also displays the underlying requirements, any supplemental text, and additional resources to help address the problem identified.

5. Review Analysis and Reports

The Analysis dashboard provides interaction with graphs and tables that present the assessment results in both summary and detailed form. Users are easily able to filter content or "drill down" to look at more granular information. It also provides the top areas of concern that are prioritized based on current threat information. Professionally designed reports can be printed to facilitate communication with management and other staff members.

PREPARING FOR AN ASSESSMENT

To get the most out of a CSET assessment, ICS-CERT recommends selecting a cross-functional team from many areas of the organization. To adequately prepare for a CSET self-assessment, this team should review policies and procedures, network topology diagrams, inventory lists of critical assets and components, previous risk assessments, IT and ICS network policies and practices, and organizational roles and responsibilities. Staff should also understand their operational data flow.

GETTING STARTED

Get started by downloading CSET at https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET. To learn more about CSET or to request a physical copy of the software, contact cset@dhs.gov. For general program questions or comments, contact ics-cert@dhs.gov or visit https://ics-cert.us-cert.gov.

About ICS-CERT

ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

https://ics-cert.us-cert.gov

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center