NCYTE CENTER

National Cybersecurity Training & Education Center

How To Deploy The Cybersecurity Evaluation Tool (CSET)

Stephen Miller Professor Emeritus
Leadership Consultant NCyTE

8/16/2024

Topics Covered

- Overview of CSET Tool
- Performing a Self-Assessment
- How it Works
- The Assessment Process
- Preparing for an Assessment
- Getting Started
- Using CSET for RISK Assessment
- Common Challenge Using CSET for Assessments
- CSET Curriculum Modules
- CSET Tool Demo
- Q&A

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Overview of CSET Tool

What is CSET tool?

- The Cyber Security Evaluation Tool (CSET®) is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating Operational Technology and Information Technology.

Overview of CSET Tool

The Cyber Security Evaluation Tool (CSET®) provides the following:

1. A framework for analyzing cybersecurity vulnerabilities associated with an organization's overall industrial control system (ICS) and information technology (IT) architecture.

2. A consistent and technically sound methodology to identify, analyze, and communicate to security professionals the various vulnerabilities and consequences that may be exploited by cyber means.

3. The ability for the user to document a process for identifying cybersecurity vulnerabilities.

4. Suggested methods to evaluate options for improvement based on existing Standards and recommended practices.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Performing a Self-Assessment

- 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) National Cybersecurity and Communications Integration Center (NCCIC) developed the CSET application and offers it at no cost to end users.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

How it Works

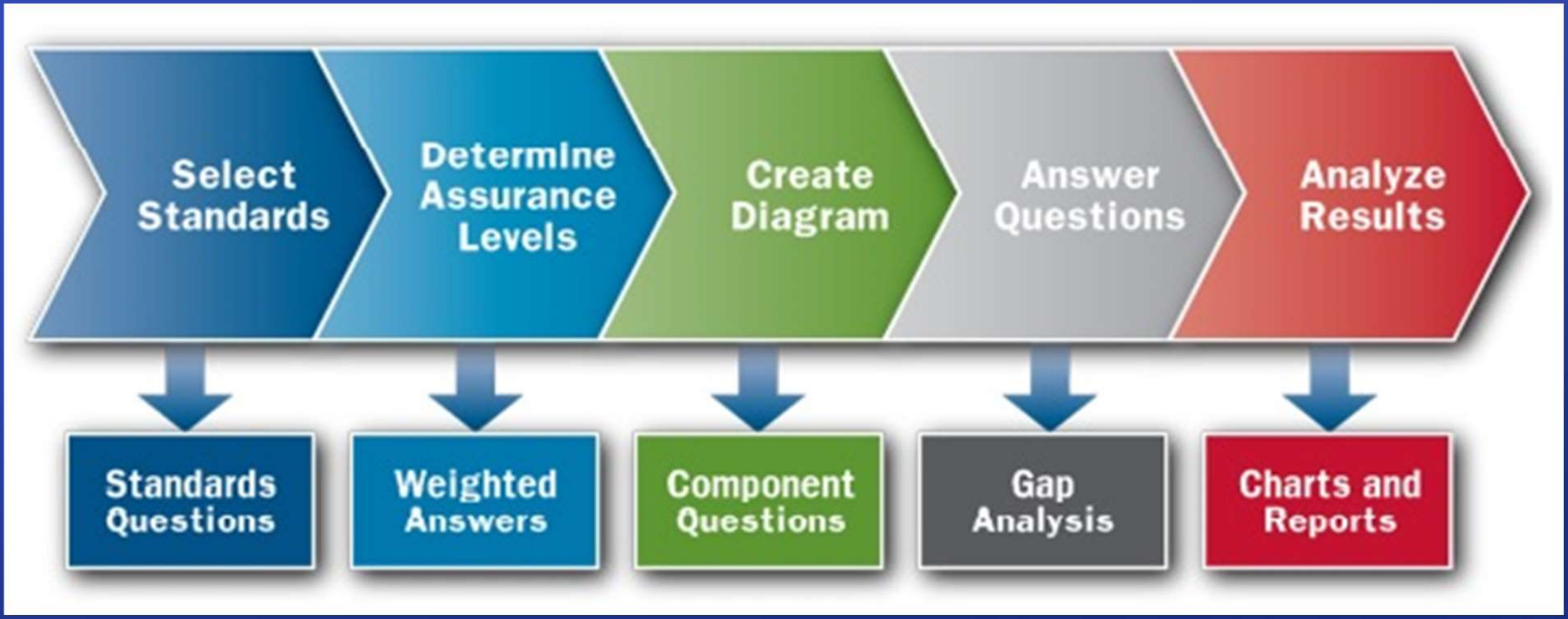
NCyTE CENTER
National Cybersecurity Training & Education Center

- 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,
  - 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.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

The Assessment Process

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



* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

1. Select Standards

NCYTE CENTER
National Cybersecurity Training & Education Center

- 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 Critical Infrastructure Framework

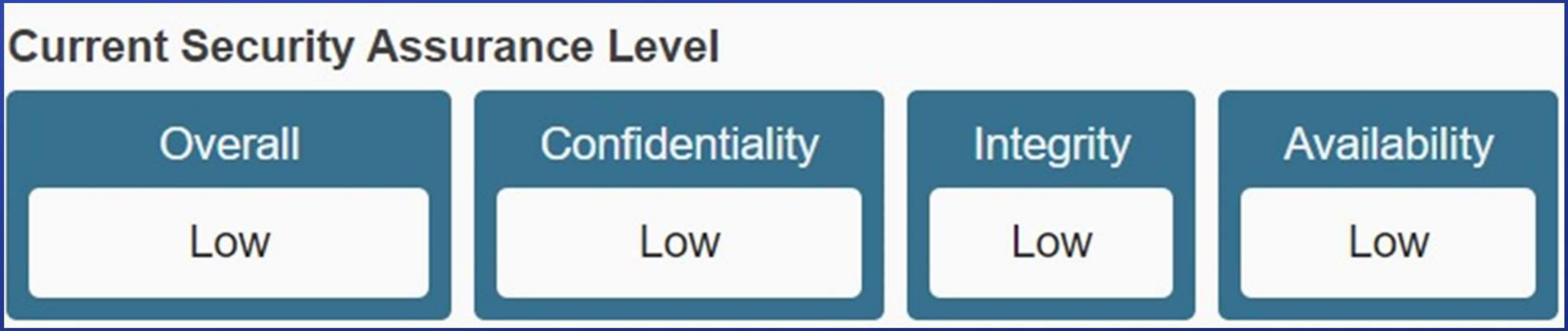
* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Whatcom
COMMUNITY COLLEGE
BELLINGHAM, WA

2. Determine Assurance Level

NCYTE CENTER
National Cybersecurity Training & Education Center

- The Security Assurance Level or SAL determines the number of questions to be answered and the level of rigor of the assessment.
- For example, a typical high SAL will contain 350-1000 questions where a low SAL will typically contain 30-350 questions, depending on the selected standard.

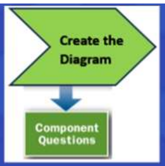


Current Security Assurance Level

Overall	Confidentiality	Integrity	Availability
Low	Low	Low	Low

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Whatcom
COMMUNITY COLLEGE
BELLINGHAM, WA

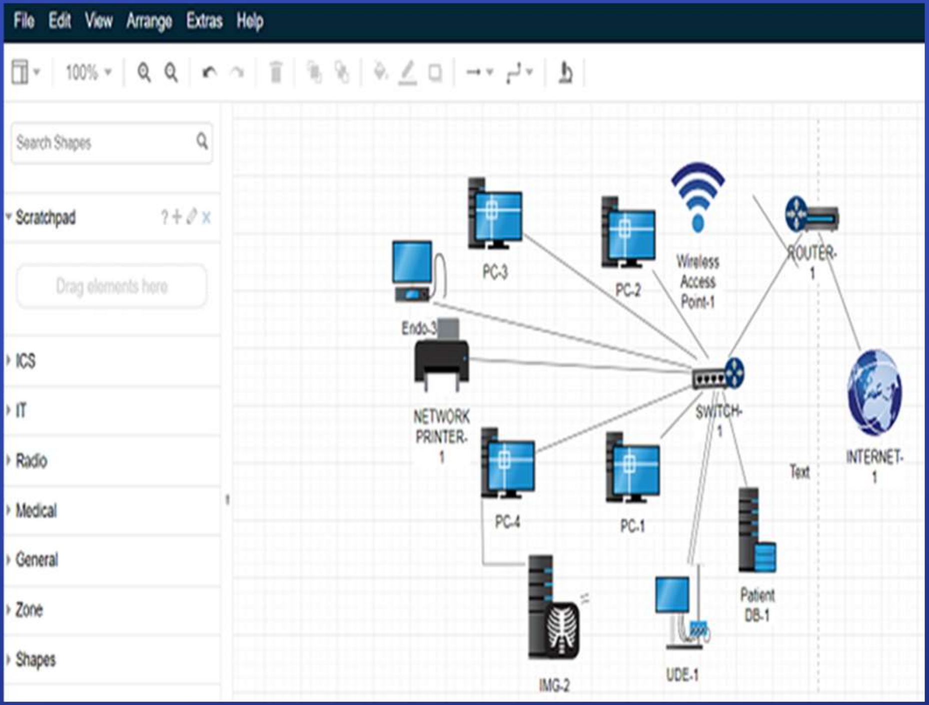

Create the Diagram

Component Questions

NCYTE CENTER

National Cybersecurity Training & Education Center

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.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Whatcom COMMUNITY COLLEGE

BELLINGHAM, WA

NCYTE CENTER
National Cybersecurity Training & Education Center

4. Answer the Questions

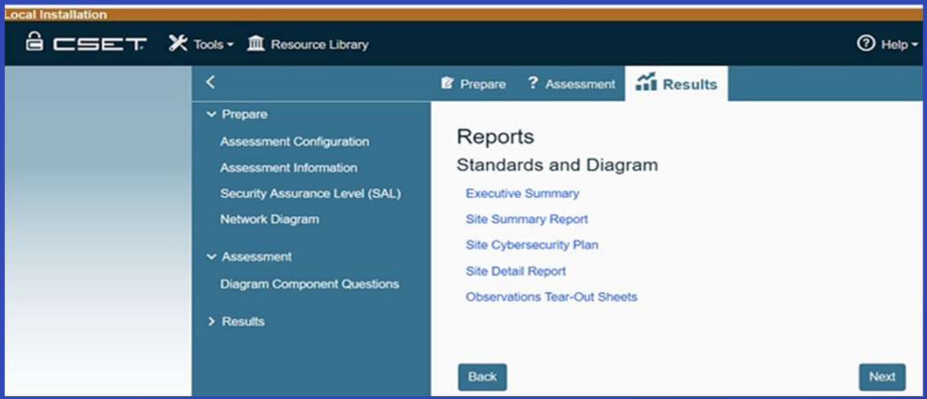
- CSET then generates questions using the network topology, selected security standards, and SAL as its basis.
- The assessment team can select the best answer to each question using the organization’s actual network configuration and implemented security policies and procedures.
- Notes can be entered, 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.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Whatcom
COMMUNITY COLLEGE
BELLINGHAM, WA

5.Review Analysis and Reports

NCyTE CENTER
National Cybersecurity Training & Education Center



Local Installation

CSET Tools Resource Library Help

Prepare | Assessment | Results

- Prepare
  - Assessment Configuration
  - Assessment Information
  - Security Assurance Level (SAL)
  - Network Diagram
- Assessment
  - Diagram Component Questions
- Results

Reports

Standards and Diagram

- Executive Summary
- Site Summary Report
- Site Cybersecurity Plan
- Site Detail Report
- Observations Tear-Out Sheets

Back Next

EXECUTIVE SUMMARY

CYBER SECURITY EVALUATION TOOL

CSET

- 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.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Whatcom
COMMUNITY COLLEGE
BELLINGHAM, WA

Preparing for an Assessment

- To get the most out of a CSET assessment, NCCIC (US-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
  - ✓Organizational roles and responsibilities
- Staff should also understand their operational data flow.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Getting Started

- Get started by downloading CSET V11.5 at https://www.cisa.gov/uscert/ics
- Downloading-and-Installing-CSET.
- Get started by downloading CSET at
- https://www.cisa.gov/downloading-and-installing-cset
- https/github.com/cisagov/cset
- Downloading-and-Installing-CSET.
  - Two options Local PC and Enterprise

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Using CSET for RISK Assessment

- The CSET tool guides the facility through a systematic evaluation process:

- **Data Collection:**
  - Gather information on hardware, software, administrative policies, and user obligations.
  - Document network architecture and critical assets.
- **Standards and Regulations:**
  - Compare collected data against relevant security standards (e.g., NIST SP 800-53, ISO/IEC 27001).
  - Identify compliance gaps and areas needing improvement.
- **Vulnerability Assessment:**
  - Analyze vulnerabilities in the control systems and IT infrastructure.
  - Use CSET to simulate potential attack scenarios and their impact.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

NCYTE CENTER
National Cybersecurity Training & Education Center

Using CSET for RISK Assessment Cont.

- **Risk Analysis:**
  - Assess the likelihood and impact of identified threats.
  - Prioritize risks based on their potential to disrupt operations.
- **Recommendations:**
  - Implement multi-factor authentication (MFA) for access control.
  - Regularly update and patch systems to mitigate vulnerabilities.
  - Conduct employee training on cybersecurity best practices.
  - Enhance physical security measures (e.g., surveillance, access controls).
- **Reporting:**
  - Generate a comprehensive report detailing findings, risks, and recommended actions.
  - Use the report to inform stakeholders and guide decision-making.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Common Challenge Using CSET for Assessments

NCYTE CENTER
National Cybersecurity Training & Education Center

- Using the Cyber Security Evaluation Tool (CSET) for assessments can present several challenges:
- **1.** Complexity and Learning Curve
- **Understanding the Tool:** CSET can be complex, especially for users who are not familiar with cybersecurity frameworks and standards.
- **Training Requirements:** Adequate training is necessary to effectively use the tool and interpret its results.
- **2.** Data Collection and Documentation
- **Comprehensive Data Gathering:** Collecting detailed information about all assets, systems, and processes can be time-consuming and challenging.
- **Documentation Gaps:** Incomplete or outdated documentation can hinder the assessment process.
- **3.** Resource Intensive
- **Time and Effort:** Conducting a thorough assessment requires significant time and effort from the organization.
- **Dedicated Personnel:** Assigning dedicated personnel to manage the assessment process can be challenging, especially for smaller organizations.

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Common Challenge Using CSET for Assessments

NCYTE CENTER
National Cybersecurity Training & Education Center

- **4.** Customization and Relevance
  - **Tailoring Assessments:** Customizing the assessment to fit the specific needs and context of the organization can be difficult.
  - **Relevance of Standards:** Ensuring that the selected standards and frameworks are relevant to the organization’s specific industry and threat landscape.
- **5.** Interpreting Results
  - **Complex Reports:** The reports generated by CSET can be detailed and complex, making it challenging to extract actionable insights.
  - **Prioritizing Recommendations:** Determining which recommendations to prioritize and implement first can be difficult.
- **6.** Continuous Improvement
  - **Regular Updates:** Keeping the assessment up-to-date with evolving threats and changes in the organization’s infrastructure requires ongoing effort.
  - **Feedback Integration:** Incorporating feedback from previous assessments and drills into the current assessment process.

NSF

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Whatcom
COMMUNITY COLLEGE
BELLINGHAM, WA

PC platform System Requirements Local Installation:

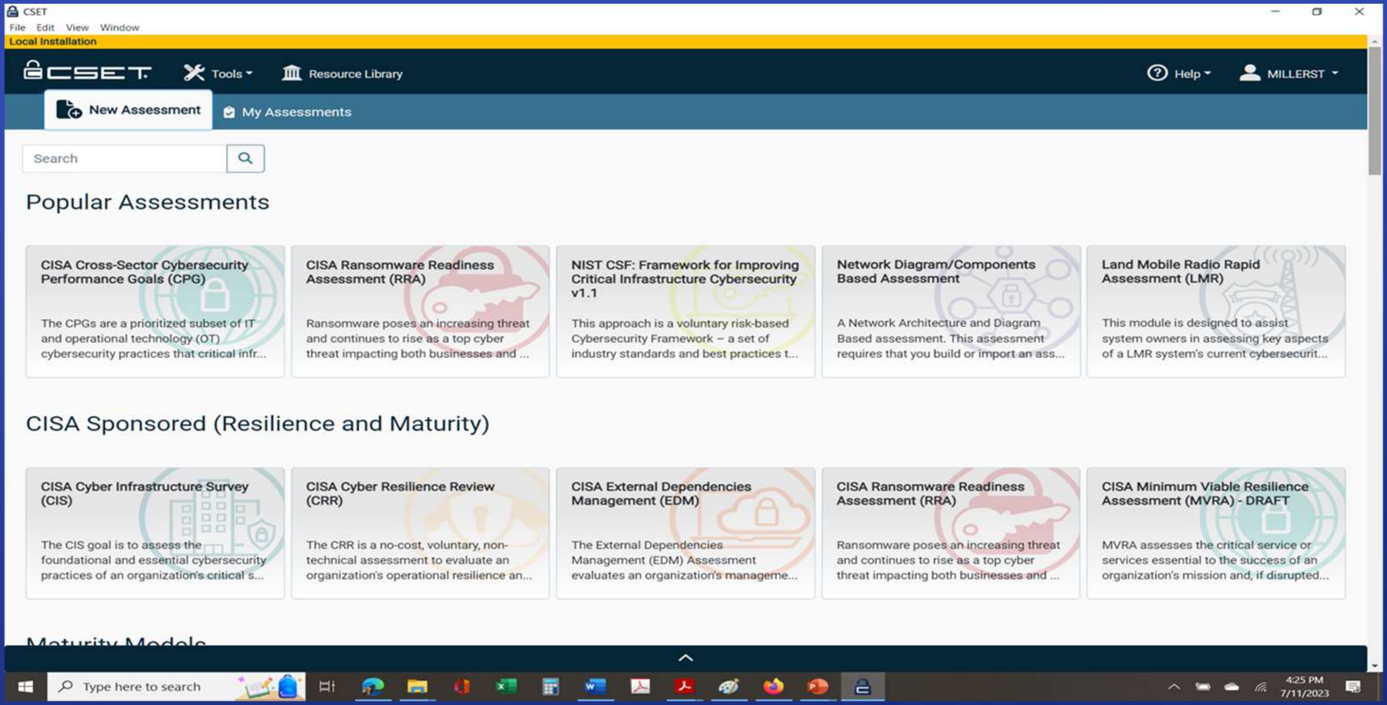
- It is recommended that users meet the minimum system hardware and software requirements prior to installing CSET.
- This includes:
  - Pentium dual core 2.2 GHz processor (Intel x86 compatible)
  - 6 GB free disk space
  - 4 GB of RAM
  - Microsoft Windows 10 or higher
  - Microsoft .NET 7 Runtime (included in CSET installation)
  - Microsoft ASP.NET Core 7 Runtime (included in CSET installation)
  - Microsoft SQL Server 2022 LocalDB (included in CSET installation)
- MAC Not Supported

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

CSET v12.0.3.2

- **What's New:**
- CSET version 12 includes the Incident Management Review (IMR) module. The IMR is based on the principle that a resilient incident management function can improve an organization's overall cyber resilience. The IMR consists of a series of questions, the answers to which provide insights into how an organization can improve its ability to identify, analyze, and respond to incidents in a repeatable manner.

CSET Tool Demo



Popular Assessments

CISA Cross-Sector Cybersecurity Performance Goals (CPG)
The CPGs are a prioritized subset of IT and operational technology (OT) cybersecurity practices that critical infr...

CISA Ransomware Readiness Assessment (RRA)
Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and ...

NIST CSF: Framework for Improving Critical Infrastructure Cybersecurity v1.1
This approach is a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices t...

Network Diagram/Components Based Assessment
A Network Architecture and Diagram Based assessment. This assessment requires that you build or import an ass...

Land Mobile Radio Rapid Assessment (LMR)
This module is designed to assist system owners in assessing key aspects of a LMR system's current cybersecurit...

CISA Sponsored (Resilience and Maturity)

CISA Cyber Infrastructure Survey (CIS)
The CIS goal is to assess the foundational and essential cybersecurity practices of an organization's critical s...

CISA Cyber Resilience Review (CRR)
The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience an...

CISA External Dependencies Management (EDM)
The External Dependencies Management (EDM) Assessment evaluates an organization's manageme...

CISA Ransomware Readiness Assessment (RRA)
Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and ...

CISA Minimum Viable Resilience Assessment (MVRA) - DRAFT
MVRA assesses the critical service or services essential to the success of an organization's mission and, if disrupted...

Maturity Models

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

What's Coming from NCyTE CSET Modules Across Sectors

- CSET Modules covering most frameworks and standards
- Module will include a scenario based on a critical infrastructure sector
- Module will have students use AI in simulating answers to CSET tool questions based on sector scenario.
- Module will be available on NCyTE and Clark.Center
- Timeline development and publishing based on demand
  - Starting with Network Diagram, IT, SCADA, Medical…
  - Currently on Clark.Center – Network for Medical DRP/BCP
  - IT & SCADA 4QTR 2024

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Q&A

NCYTE CENTER
National Cybersecurity Training & Education Center

- QUESTIONS?
- Contact Information:
- sdmillertx@gmail.com
- https://www.ncyte.net/home
- https://www.cisa.gov/downloading-and-installing-cset

* Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.