NCCIC ICS ICS PRIVATE SECTOR CRITICAL INFRASTRUCTURE ASSESSMENTS

Who We Are

As a core part of its mission, the National Cybersecurity and Communications Integration Center (NCCIC) provides cybersecurity assessments in partnership with CI owners and operators to strengthen the cybersecurity posture of their industrial control systems (ICS).

These voluntary assessments are based on standards, guidelines, and best practices and are performed at the request of the asset owner/operator. The assessment methodology provides a structured approach that asset owners and operators can leverage to evaluate and validate the cybersecurity of their ICS environments. The information gained from these assessments provides owner and operators with the understanding necessary to build effective defense-in-depth strategies for enhancing their cybersecurity posture.

What We Do

NCCIC's private sector cybersecurity assessment services include

- evaluation of ICS architecture,

- analysis of network traffic, and

- systems log review and analysis.

First, a high-level preliminary evaluation of the organization's security posture is conducted utilizing the Cyber Security Evaluation Tool (CSET®). This is followed by an in-depth review and evaluation of the ICS network design, configuration, and inter-connectivity to internal and external systems. This system analysis provides the asset owner with a comprehensive cybersecurity evaluation focusing on defensive strategies associated with their specific control systems network.

Following the system analysis, the assessment team analyzes the network data traffic to identify anomalous and potentially suspicious communications sourced from, or destined for, control system assets. This offering provides a sophisticated analysis of the asset owner's network traffic, collected by the asset owner, from within their control system network environment. NCCIC SMEs analyze the captured network traffic using a combination of open source and commercially available tools to develop a detailed representation of the communications, flows, and relationships between devices.

Because NCCIC's private sector assessment services are based on Congressional funding, they are offered as either a facilitated onsite or remote assessment at no cost to the CI asset owner.

Lastly, the systems log analysis provides an in-depth evaluation of system log data. Asset owners submit system or event logs which provide a sampling of the central control system elements being assessed, such as an ICS server, a Historian/Database collector, or a remotely connected human-machine interface system.

These assessment services are completely hands-off with no direct access to the ICS network needed. The only information NCCIC will have access to is the information provided by the asset owner.

Outcomes

Upon completion of the assessment, NCCIC compiles an in-depth report that includes an analysis of key discoveries and practical mitigations for enhancing the organization's cybersecurity posture. The report is provided to the asset owner in approximately six weeks after the completion of the assessment.

Data Protection

All information shared with NCCIC during the assessment process is confidential to the asset owner and protected under the Protected Critical Infrastructure Information (PCII) program. To learn more about these protections, visit the PCII website: https://www.dhs.gov/pcii-program, or email PCII-Assist@hq.dhs.gov.

To Request an Assessment:

Contact us at: ICS-Assessments@hq.dhs.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