NCCIC

National Cybersecurity and Communications Integration Center

NCCIC ICS FEDERAL 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).

The Industrial Control Systems Federal Critical Infrastructure Assessments (ICS-FCIA) is a comprehensive cybersecurity evaluation focused on identifying the health of the control systems within the Federal Government against advanced persistent threats. These assessments provide an in-depth evaluation from open source public information, to include

- attack paths,
- indicators of compromise,
- mitigation techniques to eradicate and secure environments, and
- monitoring/exercise capabilities to review and maintain secured system(s).

What We Do

These assessments include the following services:

State of Security

Open Source research is conducted to determine the footprint of information that is publically available for aggressors to leverage to develop attack paths and techniques to target the facility/systems.

Maturity Level Evaluation (MLE) using the CSET®

A high level preliminary evaluation of the ICS security posture leveraging the NCCIC Cyber Security Evaluation Tool (CSET®) is performed based on maturity model standards. This MLE aids in the scope and focus of the assessment activities to assist system owners on what is needed to increase their level of maturity.

Indicators of Compromise

Evaluations are performed on the system(s)/network(s) to identify indicators of compromise. This supports the assessment activities mitigation techniques and aids the owner in eradicating and securing the system(s)/network(s) environments. Network traffic capture/analysis is performed to identify attack vectors.

Evaluation of ICS Architecture

Provides ICS owners and operators with a comprehensive technical review and cyber evaluation of the architecture and components that comprise their ICS operations; including an in-depth review and evaluation of the control system's network design, configuration, interdependencies, process mapping, and the supporting applications and technologies. This analysis provides ICS asset owners with a comprehensive cybersecurity evaluation focusing on defensive strategies associated with their specific control systems network.

NCCIC

National Cybersecurity and Communications Integration Center

Analysis of Network Traffic

Network data traffic analysis provides asset owners with information to identify anomalous and potentially suspicious communications sourced from, or destined for, control systems assets. This service offering provides a sophisticated analysis of the asset owner's network traffic using a combination of both open-source and commercially available tools. ICS-FCIA is able to strategically visualize and present the network traffic and device-to-device communications that are occurring within various ICS.

Log Review & Analysis

The system log analysis provides evaluation of system log data for central control system elements being assessed, such as an ICS server, a Historian/Database collector, or a remotely connected human-machine interface (HMI) system to identify access controls and potential malicious activities.

Operational Sustainability Exercise

Based on the assessment activities, the assessment team develops a table top exercise to evaluate the effectiveness of continuity of operations, sustainability, and incident response plans to address key issues of compromised events, attacks, and failures of system components.

Outcomes

ICS-FCIA will compile an in-depth and detailed report upon completion of all assessment activities. All information shared with NCCIC during the assessment and analysis including the report are confidential to the asset owner and protected as FOUO.

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