InfoSight
Bringing the Future into Focus
305-828-1003
info@infosightinc.com
www.infosightinc.com

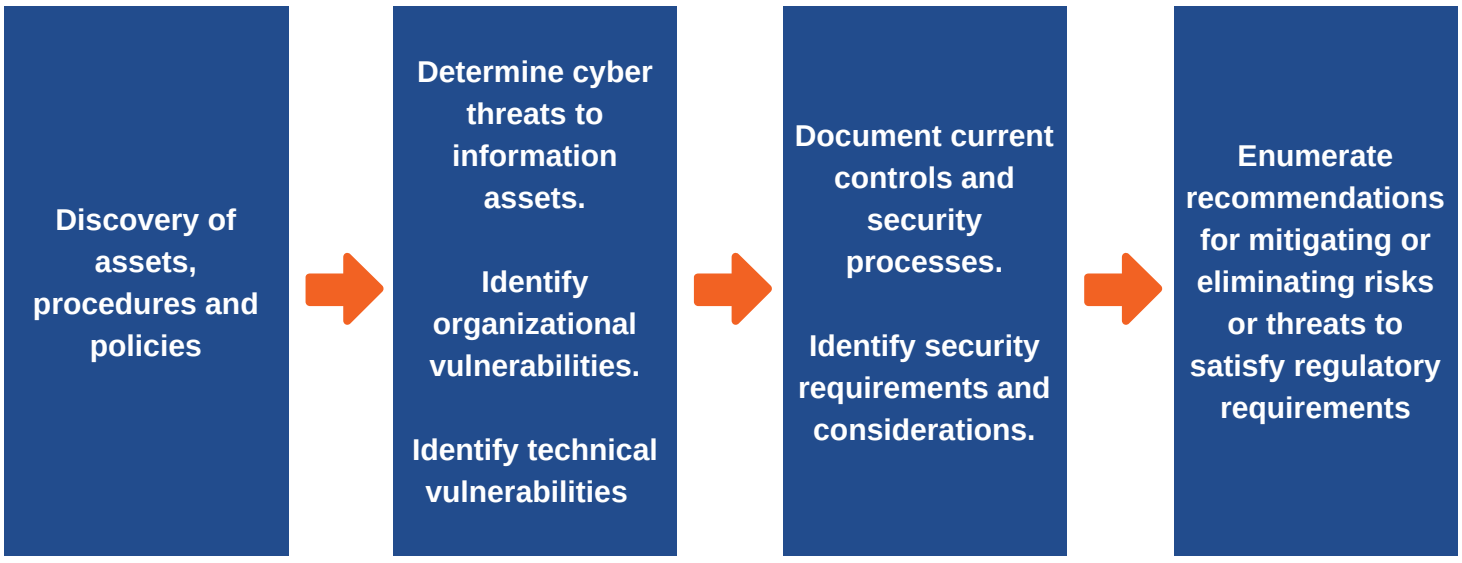
SCADA/ICS Risk & Vulnerability Assessments

The Challenge

Today all organizations face the risk of cyberattacks, but due to legacy SCADA and ICS technologies OT organizations have become a prime target. Being prepared prior to an attack is critical to minimize impact and allow quick recovery. When unprepared, hackers are nearly 100% successful. By regularly testing systems and controls an attacker's success rate plummets! This is where we come in.

Our Solution

InfoSight performs SCADA/ICS Risk and Vulnerability Assessments to provide a complete evaluation and holistic view of your organization's security posture. Our skilled security assessors conduct multi-disciplinary, multifaced reviews of your company's current OT ICS network and SCADA systems to identify vulnerabilities and control gaps that could be exploited by an attacker.
The NIST Cybersecurity Framework will serve as a baseline guided by the organization's overall risk management process or previous risk assessment activities. The assessment analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that an organization understands it's risks by identifying emerging risks and utilizing cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.



The Outcome

The main objective is to provide Management with information that outlines the organizations current risk exposures, including identified cybersecurity vulnerabilities and control weaknesses, along with recommendations designed to remediate and enhance the organizations cybersecurity posture.

InfoSight
Bringing the Future into Focus
305-828-1003
info@infosightinc.com
www.infosightinc.com

SCADA/ICS Risk & Vulnerability Assessments

Our Scope/Approach

In order to complete the SCADA/ICS Risk Assessment, InfoSight assessors will work with the organization to collect data and conduct interviews with key personnel. The following is an overview of our approach:

- **Determine Data Classification Categories:** In order to determine risk levels of data, InfoSight will assist in the development of a data classification matrix.
- **Inventory Systems:** Generate a list of all systems in use by the client that store, process, or transmit data. The inventory of systems will include hardware, software, and vendor provided services.
- **Classify Inventoried Systems:** From the results of interviews and risk analysis, the systems and/or vendors will be assigned to specific data classification categories.
- **Determine Initial Risk:** Various factors will be used to define the initial risk associated with each system/vendor. Vendor-provided services will be reviewed to determine risk ratings and associated vendor policies
- **Inventory Vulnerabilities and Threats:** Environment, physical, administrative, and technical concerns will be identified for each system/process. This process will include scans of network devices, external public facing devices and the evaluation of the effectiveness of existing security awareness efforts.
- **List Controls for Each Vulnerability or Threat:** An inventory will be created of the controls in place that help mitigate the identified vulnerabilities.
- **Classify Controls:** Controls will be classified as preventative, detective, corrective, or directive.
- **Determine Adequacy of Controls:** The adequacy of the controls will be defined as strong, adequate, or weak.
- **Determine Residual Risk:** Definitions will be created for residual risk based on the Initial Risks and Control Adequacy.
- **Generate Management and Technical Reports:** Once all data is analyzed and correlated, summary reports will be generated that list the characteristics of the systems, their vulnerabilities, corresponding controls, and the adequacy of those controls. A summary report will be generated to provide decision makers with a status of compliance and recommendations for changes to enhance the organizations cybersecurity posture.