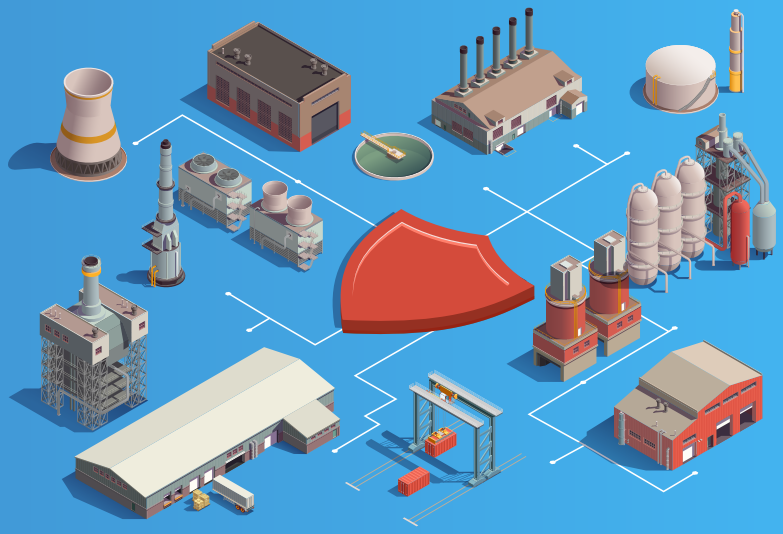
enhanced information solutions

How to Best Defend Your ICS Processes



The US Cybersecurity & Infrastructure Security Agency (CISA), in partnership with the US Department of Energy (DOE) and the UK's National Cyber Security Centre (NCSC), has released its "Recommended Cybersecurity Practices for Industrial Control Systems" guide, revised for 2020.

Implement a risk-based defense-in-depth approach to securing ICS hosts and networks

EIS Cyber is OT-focused, meaning our interests are the ICS processes first. We help you identify and classify your assets and properly segment networks to best protect your most critical assets.

Identify, minimize, and secure all network connections to ICS

EIS Cyber seeks out and identifies all points of ingress and egress to the ICS then then helps replace or reinforce the necessary points and eliminate those that are unnecessary.

Disable unnecessary services ports and protocols

EIS Cyber identifies high risk and unnecessary applications then shuts them down or offers more secure alternatives, often through simple configuration changes that require no additional products whatsoever.

Check, prioritize, test, and implement ICS security patches

EIS Cyber helps you construct a tiered patch management system that flows to the lowest level of the control system and coordinates with your organization's overall cyber security plan.

Backup system data and configurations

EIS Cyber installs, configures and either maintains or trains site personnel on the use of industry standard, OEM supported backup and recovery solutions, applicable to physical, virtual or hybrid configurations.

Leverage both application whitelisting and antivirus software

EIS Cyber offers multiple solutions for antivirus, antimalware, and whitelisting. Solutions supported by your ICS vendor and designed to minimize the likelihood of threats making it to your system then ensure if an incident occurs, it is quickly detected, identified and eliminated.

Continually monitor and assess the security of ICS, networks, and interconnections

EIS Cyber offers a variety of online and offline assessment services, ranging from simple passive network detection to full on penetration testing.

Enable available security features and implement robust configuration management practices

EIS Cyber is aware of ICS vendor and OEM security offerings, when they are disabled by default for ease of implementation and understands how they fit into your organization's overall cyber security plan.

Provide ICS cybersecurity training for all operators and administrators

EIS Cyber has multiple layers of offerings to ensure your people understand the threats they face and how to deal with them. Ranging from simple email alerts on credible threats to periodic webinars for awareness, onsite custom training for your cyber plan and referrals to certificate issuing training centers.

Maintain and test an incident response plan

EIS Cyber will develop, test, and periodically refine your incident response plan – including layers of isolation all the way down to the mission critical systems for site operations.

EIS Cyber recognizes that implementing and maintaining an industrial cyber security program can be a daunting task. We will work with you to identify your most critical needs and establish a phased program that works within your resource constraints. Realizing every site has different levels of expertise, EIS Cyber is comfortable serving in many different capacities, be it a purely advisory or consultancy capacity all the way to full implementation.

Talk to one of our expert consultants today. We are here to provide assistance, regardless of where you are on your ICS journey.

eiscyber@eisinc.com **+1 (440) 725-2220**