

Industrial Control Systems Cybersecurity Initiative: Considerations for ICS/OT Monitoring Technologies with an Emphasis on Detection and Information Sharing

On July 28, 2021, President Biden issued [a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems](#). This memorandum formally announced the Industrial Control Systems (ICS) Cybersecurity Initiative and outlines U.S. policy to safeguard our critical infrastructure, with a particular focus on the cybersecurity and resilience of systems supporting the functions of government and the private sector so vital that their disruption would have a debilitating effect on our national or economic security or the public health and safety of the American people.

The Initiative is a voluntary, collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of vendor-neutral, and interoperable evaluation criteria for technologies and systems that provide users with asset and network visibility, indicators of compromise, threat detections, and warnings with actionable intelligence.

The highest priority for the ICS Cybersecurity Initiative is to defend the United States' critical infrastructure by urging critical infrastructure owners and operators to implement technologies that provide threat visibility, indications, detection, and warnings, and that facilitate response capabilities for cybersecurity in essential control system and operational technology networks.

Below are evaluation considerations that critical infrastructure organizations may leverage when assessing technologies that focus on detection of signatures and adversary techniques in ICS and operational technology (OT) environments. All organizations are encouraged to deploy technology that meets widely accepted cybersecurity standards—such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework core functions—to improve visibility on their systems. Each organization must assess and select the technologies or services that are best for its operational needs, architecture, and information sharing objectives.

The considerations listed below are recommendations, not requirements, and each organization should determine which of the considerations are applicable to its operating and business environment to select technologies that best fit its security and situational awareness needs.

The United States Government does not and will not select, endorse, or recommend any specific technology or provider as part of this Initiative. The government intends to work with critical infrastructure organizations and other private sector stakeholders to implement, to the maximum extent possible, information sharing with various ICS monitoring technology providers. Information shared with the government is aggregated and anonymized to prioritize threats with evidence from multiple sources to corroborate that prioritization and expedite a holistic response.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), in coordination with the National Security Council (NSC), interagency partners, and private industry partners, have developed the following criteria to help organizations evaluate ICS monitoring solution capabilities and features. While not exhaustive, these elements may be considered as a standard feature suite necessary for effective monitoring and defense.

Considerations for ICS/OT Cybersecurity Monitoring Technologies:

1. General Considerations

Critical infrastructure organizations may consider whether ICS/OT cybersecurity monitoring technologies include the following general considerations:

- 1.1. Technologies with capabilities built specifically for ICS assets that can analyze common ICS network traffic, data, and communications conforming to ICS protocols.
- 1.2. Technologies that support organizational adoption of practices outlined in established ICS frameworks and standards, such as [CIS CSC](#), [ISA/IEC 62443](#), [NIST SP 800-53](#), and [NIST SP 800-82](#).¹

2. Detection and Response Capabilities

Critical infrastructure organizations may consider whether ICS/OT cybersecurity monitoring technologies enable detection and response capabilities, including the ability to:

- 2.1. Discover and maintain an updated inventory of critical assets and systems that draw on industry-recognized and supported standards, including CIS CSC, ISA/IEC 62443, NIST SP 800-53, and NIST SP 800-82.¹
- 2.2. Develop ICS network traffic baselines for expected operations, compare monitored traffic to the developed baseline, and generate alerts for deviations from that baseline.
 - 2.2.1. These baselines may include ports, protocols, services, sending and receiving devices, volumetrics, and temporal aspects.
- 2.3. Detect and alert on:
 - 2.3.1. Indicators of known malicious activity
 - 2.3.2. Unauthorized or suspicious connections between an OT networks and any external network, including enterprise IT networks or the public internet
 - 2.3.3. Unauthorized or suspicious connections between network segments within the OT network, including non-Internet Protocol (IP) connections
 - 2.3.4. Configuration changes to OT assets
 - 2.3.5. Custom signatures deployed by the asset owners
 - 2.3.6. Other tactics, techniques, and procedures (TTPs) in the MITRE ATT&CK² framework.
 - 2.3.7. The installation or operation of new or unauthorized applications on ICS/OT assets
 - 2.3.8. The exposure and/or usage of ports, protocols, and services that are not necessary for the operation of ICS/OT assets
- 2.4. Ingest regularly updated feeds of threats, vulnerabilities, or other relevant intelligence focused on the access, exploitation, and protection of ICS and OT environments and assets. Tools should leverage commonly used frameworks and standards for information sharing, such as STIX/TAXII.

¹ Energy sector entities should also refer to DOE's [Cybersecurity for the Operational Technology Environment \(CyOTE\)](#) initiative.

² "MITRE ATT&CK for ICS" is in the process of being incorporated into [MITRE ATT&CK matrices](#).

- 2.5. Take corrective action in response to detected threats, such as isolating a device, stopping a connection, or leveraging allow lists and blocklists.
- 2.6. To the extent possible, technology leverages vulnerability data, including active exploit vulnerability data, such as CVSS version 3.1, as outlined by the National Vulnerability Database scoring methodology.
- 2.7. Maintain security mechanisms and controls sufficient to ensure that the technology itself cannot be used as a vector for adversaries to gain access into ICS networks or manipulate the physical process.

3. Integration and Interoperability

Critical infrastructure organizations may consider whether ICS/OT cybersecurity monitoring technologies are designed to be interoperable and integrate into a comprehensive security program, including the ability to:

- 3.1. Participate in a collective defense framework including data export capabilities enabling the sharing of insights, detections, and threat intelligence rapidly amongst the federal government, participants, and trusted organizations such as relevant information sharing and analysis centers (ISACs)/information sharing and analysis organizations (ISAOs).
- 3.2. Protect or anonymize the organization of participants in data/information sharing programs and ensure that risks and vulnerability information are not inadvertently disclosed between program participants unless explicitly authorized by the participating organization.
- 3.3. Allow for logs and/or alerts to be sent to centralized tools, such as those that aggregate and analyze logs and alerts, such as Security Information and Event Management (SIEM) systems.

4. Security Features

Critical infrastructure organizations should consider whether ICS/OT cybersecurity monitoring technologies have sufficient security features, such as:

- 4.1. Support for multi-factor authentication (MFA), especially hardware-based MFA or other phishing-resistant methods.
- 4.2. Cryptographic protection of data in transit, in use, and at rest (e.g., leverage NIST FIPS 140-3 approved cryptology to protect the data where feasible).
- 4.3. Prohibition of universal default passwords for initial installation.
- 4.4. Controls to minimize exposure of ports, protocols, or services to the network that are not necessary for the successful function of the technology.
- 4.5. Guaranteed communication standard references for communications protocols and use different cryptological keys for different devices.