



Build a Resilient Operational Technology (OT) Cybersecurity Program with the SANS ICS Five Critical Controls

The 5 Critical Controls can be implemented together to create an OT cybersecurity program tailored to your organization’s specific risks.



ICS Incident Response Plan



Defensible Architecture



Network Visibility & Monitoring



Secure Remote Access



Risk-based Vulnerability Management



Smaller, less mature organizations should use the 5 Critical Controls as a framework for building efficient and effective cybersecurity programs



Larger, more mature organizations should use the 5 Critical Controls to measure and improve resiliency

Build a strong foundation



Alignment on the risk/threat scenarios that can impact your mission
What will your attack look like?



Identification of the most important sites (health, safety, business, environment, national security, etc.)
Know yourself



Vendor partnerships are essential to ICS environments
Identify needs and overlapping interests

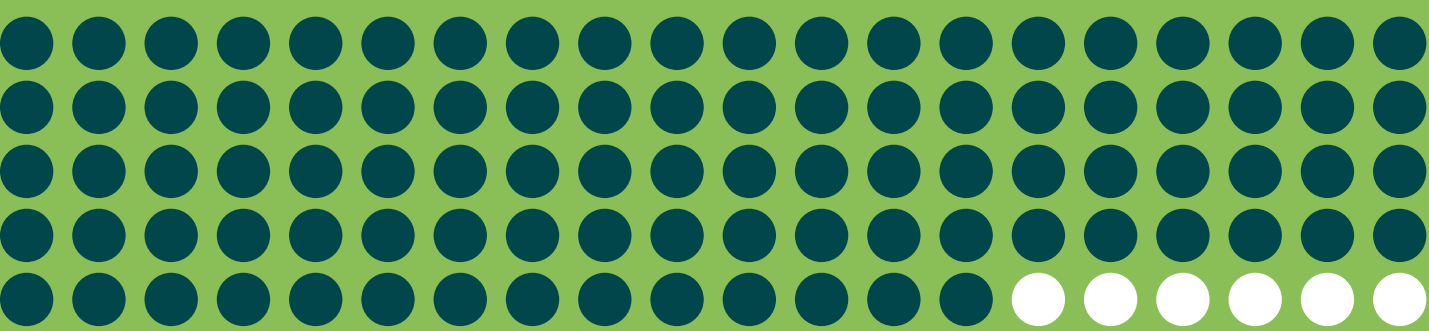


Prioritized tactical and strategic plan aligned with operations
What is needed and when to operate through an attack?



Staffing levels and training to provide the necessary tools, technology and capabilities to your practitioners
People will save the day

Benchmark Your Maturity and Prioritize Your Next Steps



94 percent of Dragos engagements in 2023 uncovered a significant deficiency in one or more controls

Work with your operations team and OT security experts to start putting these controls into practice, ensuring they are fully operational and can efficiently handle key scenarios. Dragos offers a Benchmarking Guide to help you assess your level of maturity in each control.



Chart a Path Forward – Starting with the Dragos Platform

The Dragos Platform is the most effective OT-native cybersecurity monitoring and visibility solution. Integrating Asset Visibility, Vulnerability Management, Threat Detection, and Response, the platform enables organizations to align to SANS 5 Critical Controls to deliver an all-encompassing approach to securing ICS/OT systems against the sophisticated threat landscape.

ICS Incident Response Plan	Defensible Architecture	Network Visibility & Monitoring	Secure Remote Access	Risk-based Vulnerability Management
DRAGOS PLATFORM				
<ul style="list-style-type: none">• Detect & contextualize threats• Forensic data & timelines for investigations• Response playbooks	<ul style="list-style-type: none">• View asset groups & communications• Validate security controls• Audit & compliance	<ul style="list-style-type: none">• Asset discovery• Protocol analysis• Activity logging• Threat detection• Response playbooks• Vulnerability management	<ul style="list-style-type: none">• Monitor 3rd-party remote access sessions• Validate SRA controls for internal and 3rd party	<ul style="list-style-type: none">• Match vulnerabilities to asset inventory• Now, next, never priorities & alt mitigation• Track status to completion

The Dragos Platform is the primary control for ICS Network Visibility and Monitoring, but the technology also delivers value across the other critical controls.