MANDIANT
NOW PART OF Google Cloud

THREAT INTELLIGENCE
WHITE PAPER

Activating Cyber Defense Around CISA's Cross-Sector Cybersecurity Performance Goals

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 3.

Nation-state threat actors continue to pursue critical infrastructure technologies. Last year Mandiant reported findings of custom-made tools that enable attackers to scan for, compromise and control certain industrial control systems (ICS) or supervisory control and data acquisition (SCADA) devices once they have established access in an operational technology (OT) network[1]. As industrial and critical infrastructures become increasingly network-connected, this heightened threat sophistication enhances the need for updated cybersecurity guidance for critical infrastructure. The Cybersecurity and Infrastructure Agency (CISA), National Institutes of Standards and Technology (NIST) and the interagency community developed cybersecurity goals consistent across all critical infrastructure sectors.

In October 2022, CISA released the Cross-Sector Cybersecurity Performance Goals (CPGs)[2] as a guide to help organizations identify and prioritize the most important cybersecurity practices. CISA CPGs are meant to be a baseline to address cybersecurity challenges organizations face daily. They aim to make progress on the shared goal of reducing cyber risk to better defend our nation's critical infrastructure such as hospitals, energy suppliers, transportation systems and major manufacturing.

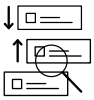
Mandiant embraces CISA CPGs guidelines to create a starting point to reduce risk. The CPGs serve as a first iteration of goals to National Security Memorandum (NSM-5): Improving Cybersecurity for Critical Infrastructure Control Systems. They are an important step, not an all-encompassing cybersecurity program, to get started on the path toward a stronger cybersecurity practice.

1. Mandiant, INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems, April 13, 2022
2. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022

CPGs are intended to be a floor, not a ceiling, to reduce cyber risk. Key characteristic highlights include:

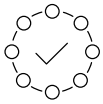
Mapped subset of cybersecurity practices

Relevant guidelines specific for IT and OT



Prioritized risk reduction practices

Informed by threats observed by CISA and its government and industry partners



Applicable across all CI (critical infrastructure) sectors

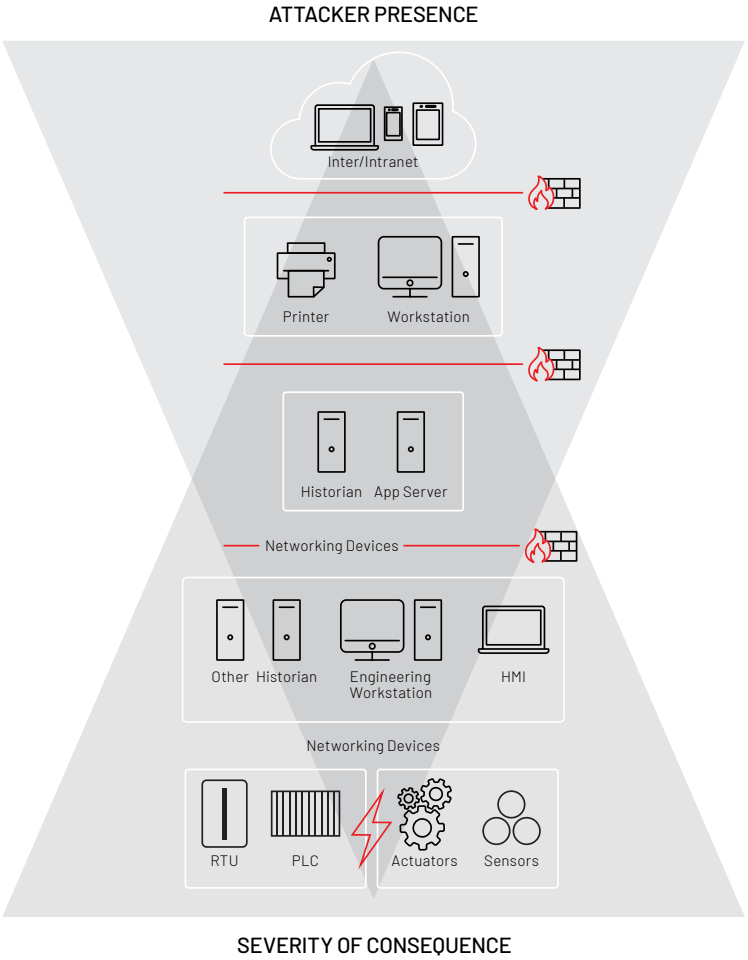
The CPGs call out specific actions and items related to OT and ICS as a way to help these organizations better defend their critical infrastructure.

Regardless of the size of an organization, protecting critical infrastructure requires an understanding of relevant cyber threats, rigorous security testing, and threat detection and response conducted across the entire enterprise. The CPGs help organizations think about how to focus investment toward the most impactful security outcomes while taking into account budget, staffing and expertise. The investment in practices to implement the CPGs will "help meaningfully address serious risks to the safety, health and livelihoods of the American people[3]."

3. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022.

Understanding of Relevant Cyber Threats

The CPGs guide organizations to maintain awareness of relevant threats and leverage attacker tactics, techniques, and procedures (TTPs) to detect ongoing attacks. Understanding relevant cyber threats is paramount in Mandiant's approach to OT security in which we guide customers to enhance threat detection capabilities of both IT and OT networks, with full situational awareness[4]. We believe that defenders and incident responders should focus much more attention on intrusion methods, or TTPs, across the attack lifecycle, most of which are present on what we call "intermediary systems"—predominantly systems that cross the network boundaries of IT and OT or those networked workstations and servers within the OT network that use operating systems and protocols that are similar to (or the same as) those used in IT. Narrowing the focus to intrusion methods is effective because the majority of sophisticated OT attacks leverage these intermediary systems as stepping-stones to their ultimate target.



4. Mandiant, The Mandiant Approach to Operational Technology Security, December 2019

The greatest opportunity for detecting a targeted OT attacker is in the intersection between the two triangles in Figure 1[5]. It is here that the balance between attacker presence and operational consequence of an intrusion makes it easier and more meaningful for security organizations to identify threat activity. Defenders should understand attacker intrusion methods and leverage that knowledge to hunt for and detect advanced threats. Threat hunting close to the OT DMZ and the Distributed Control System (DCS) can be most efficient as the intrusion's detectable features are still present and the severity of potential consequences of the intrusion is high, but still not critical.

5. Mandiant, The Mandiant Approach to Operational Technology Security, December 2019

2022

In 2022, Mandiant reported sensitive OT and network documentation being exposed in ransomware extortion attacks[6]. The exposure of sensitive OT data from ransomware-related or any type of data leak provides sophisticated actors with information on targets, specifically about the victim's infrastructure, assets, security weaknesses, and processes. Reconnaissance data of this kind is used by threat actors to create more significant and precise attacks.

TABLE 1: Documentation Exposed in Ransomware Extortion Attacks

Victim (Names Redacted)	Leak Contents
Manufacturer of industrial and passenger trains	Password administration credentials for an OEM, requirements for control architecture and communication channels for European tram vehicle, backups of Siemens TIA Portal PLC project files, etc.
Two oil and gas organizations	In-depth network and process documentation, including diagrams, HMIs, spreadsheets, etc.
Control systems integrator	Engineering documentation from customer projects (Some files were password protected, which we did not attempt to bypass).
Hydroelectric energy producer	Most data was financial and accounting related, however we identified a list of names, emails, user privileges, and some passwords from IT, plant maintenance, and operations employees.
Satellite vehicle tracking service provider	Product diagrams, visualizations, and source code from a proprietary platform used to track automobile fleets via Global Positioning System (GPS).
Renewable energy producer	Legal agreements between the victim and customers stating the conditions for maintenance and supply of renewable energy infrastructure. The contracts stated that the service provider had full access to the third party's SCADA system via public internet IP addresses.

- Enforce robust data handling policies for employees and subcontractors that touch data from all segments of the network to ensure that internal documentation is protected.
- Avoid storing highly sensitive operational data in less-secure networks.
- Place special attention on selecting subcontractors that implement comprehensive security programs to safeguard operational data.
- Victims of ransomware intrusions should assess the value of any leaked data to determine what compensatory controls can help decrease the risk of further intrusions.
- Change any leaked credentials and API keys. Consider changing exposed IP addresses for critical systems and OT jump servers.
- Periodically conduct red team exercises to identify externally exposed and insecure internal information.

6. Mandiant, 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information, January 2022

Rigorous Security Testing

One key to confidently improving the security posture of OT networks is safely testing security controls at each layer of the OT network against the most prevalent attacks and malware families targeting critical assets. CISA CPGs recommend regular third-party validation of the effectiveness and coverage of an organization's cyber defenses.

Mandiant advises a tailored program to fit the assessment needs of the organization. A comprehensive testing program for OT is most effective when it is conducted from the attackers perspective, leverages simulation and emulation to alleviate impact to real-time operations, and incorporates an appropriate mix of red team, purple team, penetration testing and network and component security testing. Where proactive testing is not acceptable, due to the operational uptime requirements of production OT environments, Mandiant recommends technical assessments that evaluate the effectiveness of network segmentation, access controls, network monitoring systems, transient device policies, and incident response capabilities. Continuous testing not only evaluates the effectiveness of security controls at a point in time, but also helps to identify complex security issues across integrated networks (IT to OT) before an attacker exploits them. Ongoing validation can also prepare the organization's team to monitor, detect and respond to cyber incidents. From these programs organizations should expect: tactical recommendations for mitigation of critical findings, strategic recommendations for long-term improvement, and identification of gaps in the staff's ability to monitor and respond to OT incidents.

Open Platform Communications servers enable similar and manufacturer-independent data exchange among machines, devices and systems within the industrial environment.

Response and Recovery

In section 7, CISA CPGs outline the need for organizations to maintain, practice and update cyber security incident response plans for relevant threat scenarios. Mandiant's experience on the frontlines of response for high profile OT incidents, such as TRITON and INCONTROLLER and have led to a deeper understanding of the difference between IT and OT incident response and the tools and procedures required to carry out an OT response.

While the goals of remediation and containment (to remove the threat from the environment and restore systems to normal operational conditions) are the same in IT and OT environments, the tools can be vastly different. IT responders routinely use endpoint detection and response technology to aid in investigation, containment and recovery / remediation. These tools are not typically installed on servers or components of OT networks.

Containment in IT is relatively simple and often much less impactful than it can be in complex OT environments. For example, stopping and starting specific functions or even removing an entire system on the IT network is common practice. These actions can be more impactful when taken on an OT component. A comprehensive understanding of the underlying processes must be taken into account before starting or stopping processes or pulling a component offline without impacting operations which can cause significant downtime or potential risk of life safety. Open Platform Communication (OPC) servers, for example, can impact the entire manufacturing line for weeks if haphazardly taken offline. Detailed planning — outside of an active incident response — helps system owners make risk-based decisions based on potential downtime, production loss or life safety risks. The organization's ability to understand the goals and objectives of potential attackers can help guide the system owner into making safer, less risky decisions.

Lastly, OT networks are composed of many vendor-run subnetworks that the organization does not have direct access to. Mandiant recommends response plans and playbooks be developed to incorporate third-party systems and tested in conjunction with those vendors. The importance of having a plan, and practicing it, to resolve cyber security incidents quickly, efficiently, and at scale can not be overstated.

Mandiant maps OT security offerings to the NIST Cybersecurity Framework's Five Functions[7], which CISA CPGs are meant to supplement, matching services to the lifecycle of an organization's cyber security risk management.

7. NIST, Cybersecurity Framework, The Five Functions, May 2021

		IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Intelligence	Intelligence Subscription					
	Dedicated Intelligence Analyst					
	Vulnerability Assessment Service					
	Custom Analysis and Blackbox Assessment					
Consulting	Healthcheck					
	Security Program Assessment					
	Attack and Penetration Testing					
	Incident Response Planning					
	Incident Response					
	Security Training					
	Dedicated Consultant					
Managed Defense for OT	Jumpstart					
	Ongoing Monitoring					
3rd Party Technology	OT Network Protocol Monitoring					

Figure 2. Mandiant OT-specific Offerings

Mandiant offers frontline cybersecurity insights with a deep functional knowledge of industrial control systems gained through decades of hands-on work in ICS and OT environments. Mandiant OT experts conduct advanced security testing to help industrial organizations improve mitigation and detection capabilities across end-to-end OT networks. Let us help your organization map CISA CPGs for a more secure OT environment and increased cyber readiness.

Read more articles from **The Defender's Advantage Cyber Snapshot**.

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud

©2023 Mandiant, Inc. All rights reserved. Mandiant is a registered trademark of Mandiant, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. I-EXT-WP-US-EN-000502-01