Incident Response –RS.RP

The steps to investigate suspicious activity and respond to a compromise support the recovery process. Understanding your organization's level of Incident Response (IR) maturity requires a review of the preparation measures already in place.

- **Roles and Responsibilities** – Who is in charge and which team members are responsible for information technology (IT), information security (InfoSec), and operational technology (OT) actions?
- **Key Team Member Contact List** – Is a call list maintained and does it include multiple contact methods and identify secondary points of contact?
- **War Room/Conference Line** – Is there a standard location and / or conference call setup for organizing the response team?
- **Vendor/Integrator/MSP Assistance** – Are there agreements with these parties to assist with the response efforts?
- **Third-Party Assistance** – Have teams (forensics, OT IR experts) that provide staff augmentation during IR events been identified, and are agreements in place?
- **Jump Bag** – Is the set of systems and tools (hardware, software, storage) necessary to interact with the different technologies in control network in place?
- **IR Triage Team** – Is there a dedicated team familiar with the control network and the tools and training needed to conduct information gathering and forensic analysis, and to provide actionable intelligence to IR team?
- **Table Top Scenarios (TTX)** - Have IR scenarios that include IT/InfoSec/OT/Physical Security team members been run to understand their reactions?

CRITICAL NOTE: Due to plant and public safety requirements, compromised control networks may stay operational for weeks or months, posing an ongoing threat in a contained and controlled state. Full eradication may occur only during the next scheduled plant maintenance window.

OT-specific IR plans and procedures are necessary to help organize and guide IT, InfoSec, and OT teams to success during these stressful events.

Incident Response – RS.RP (continued)

Example IR Table Top Scenarios (TTX) for IT/InfoSec/OT/Physical Security team members:

- **Ransomware** – An operator logs into the asset management server and sees a ransomware note on the desktop background and that all project files appear to be encrypted.
- **Maintenance or Compromise** – An administrator account was observed logging into all Windows servers and workstations across the control network.
- **Strange HMI Activity** - Operators notice mouse moving and clicking on different portions of HMI that is not consistent with normal operations.
- **Living off the Industrial Control Security (ICS) Land** – Operators troubleshooting network issues notice excessive ICS protocol traffic (OPC, IEC104, Modbus/TCP) from several systems.
- **Unauthorized Physical Access** – Physical security team notices a hole cut into the fence around the facility. The teams investigate and determine the physical access is a two-part attack. Physical access was gained to then access the facility where a cyber containment was introduced into the control network.

Security Awareness – PR.AT

Corporate security awareness programs cover the expectations of individuals accessing corporate assets. Control network security awareness programs are typically limited to covering safety training and requirements. In some control networks OT personnel do not have corporate accounts and, therefore, may not receive corporate security awareness training. IT, InfoSec, OT, and physical security personnel who have control network responsibilities should receive additional training to distribute knowledge about control network policies and their responsibilities. That training should also provide them with knowledge of how to identify suspicious activity and encourage them to report the activity as a part of their normal response and recovery steps.

SANS ICS

Security Program Maturity Quick Start Guide v0.1

SANS ICS
ics.sans.org

By Dean Parsons & Don C. Weber
dparsons@sans.org | don@cutawaysecurity.com

This guide covers the basics of using the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) (https://www.nist.gov/cyberframework) in order to understand the maturity of a security program implemented to protect control environments from any industrial control sector.

This guide concentrates on seven NIST CSF categories to help leadership, engineers, and administrators gauge the maturity of the current program and prioritize risk reduction.

How to Use This Sheet

This guide will use the following NIST CSF Domains and Categories to model and improve an organization's current program.

- **Policies** – ID.GV
- **Network Segmentation and Isolation** – PR.AC
- **Access Control** – PR.AC
- **Logging and Monitoring** – DE.AE
- **Asset Inventory Management** – ID.AM
- **Incident Response** – RS.RP
- **Security Awareness** – PR.AT

How to Evaluate Security Program Maturity

Consider the following steps to get started:

- Obtain executive leadership buy-in to conduct an internal security program maturity review.
- Identify key personnel from the information technology (IT), information security (InfoSec), and operational technology (OT) teams to conduct the maturity review.
- Review each section and the important topics outlined in each.
- Provide an honest grade for how well these topics are managed within the organization and control network.
- Use the grading to prioritize recommendations for executive leadership.
- Brief executive leadership and obtain guidance.
- Brief IT, InfoSec, and OT teams.

Policies – ID.GV

Standards, guidelines, and procedures built from corporate policies are not implementable within the control network. For example, the corporate approach to password management is too restrictive for the control network and is ignored. Other requirements, such as IR plans, will negatively impact safety. For example, removing systems from the network without warning due to malware infection will have unintended impacts on the process.

Organizations can develop control network policies by starting with and adapting current corporate policies. Control-network-specific policies will help the team understand the organization's business and operation requirements and allow them to build sound standards, guidelines, and procedures to ensure the availability, resiliency, and safety of the process.

Providing guidance for each of the NIST CSF functions and categories is a good beginning. The control network team can use this guidance to identify the standards, guidelines, and procedures for each area. More granular implementations will pull from other industry standards such as IEC 62443, ISO 27001, and NIST 800-82r2.

Network Segmentation and Isolation – PR.AC

- **Network Boundaries** – Network segmentation and isolation begin with network boundaries between the corporate network and the control network.
- **Remote Access** – Remote access for operators, engineers, integrators, vendors, managed service providers (MSP), and others cross these boundaries.
- **Internet Access** – There is always a path to the Internet, so understanding the restrictions applied to this path is critical.
- **Cloud Access** – Vendors and integrators are leveraging cloud access for maintenance and management.

Access Control – PR.AC

Access control manages authorization to assets within the control network. Control networks have unique requirements for management by company personnel and third-party partners.

- **Control Network Credentials** – Should be unique to the control environment. The control network Active Directory (AD) should not have a trust relationship or sync with corporate domains.
- **Multi-Factor Authentication** – MFA, like Windows AD, should not be shared with the corporate environment.
- **Vendors and Integrators** – Third-party accounts should be restricted to specific roles, responsibilities, and assets. MFA should be required. No direct access should be allowed from the Internet.
- **Managed Service Providers** – Many organizations share MSP services between the corporate and control networks. MFA should be required. No direct access should be allowed from the Internet.
- **Service Accounts** – Service accounts are used for many applications and should not share credentials between the corporate and control networks.

CRITICAL NOTE: Monitoring the use of credentials and MFA is the most important step to ensure that access control is an effective security control.

Logging and Monitoring – DE.AE

Organizing logging and monitoring within the control network is most effective when prioritized to address network events, then system events, and finally the consolidation, correlation, and evaluation of these events.

The following are several starting points for this discussion:

- Network Events
  - IP Flow Information Export (IPFIX)
  - Network Boundary Activity
  - Network Device Monitoring Configurations (Span port and physical taps)
  - Network Security Monitoring
- System Events
  - Windows Active Directory Events
  - DNS Events
  - Windows Event Logs
  - Syslog Events (*nix systems, PLCs, Field Devices)
- Managed Logging and Monitoring
  - Central Logging Windows
  - Central Logging Syslog
  - Security Operations Center Monitoring and Alerting

Asset Inventory Management – ID.AM

Asset Inventory Management is one of the most important and challenging categories for all organizations. Asset identification is accomplished using four methodologies: Physical, Passive Monitoring, Active Monitoring, and Configuration Analysis. Device categories include (but are not limited to):

- Control Hardware (PLCs, Field Devices)
- Network Devices
- Servers and workstations
- Process Control Software
- Other Software
- Transient Devices
- Removable Media