NIST SPECIAL PUBLICATION 1800-23A

Energy Sector Asset Management

For Electric Utilities, Oil & Gas Industry

Volume A:
Executive Summary

James McCarthy
Glen Joy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Lauren Acierto
Jason Kuruvilla
Titilayo Ogunyale
Nikolas Urlaub
John Wiltberger
Devin Wynne
The MITRE Corporation
McLean, Virginia

May 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-23

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/library/energy-sector-asset-management-nist-sp-1800-23-practice-guide

Executive Summary

- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to demonstrate how energy organizations can strengthen their operational technology (OT) asset management practices by leveraging capabilities that may already exist within their operating environment or by implementing new capabilities.
- As electric utilities and the oil and gas industry are some of the nation's critical infrastructures, the incapacitation or destruction of assets, systems, and networks in the energy sector could have serious negative effects on the economy, public health, and safety.
- As industrial control systems (ICS) in the energy sector become more interconnected, vulnerabilities within OT assets and processes are targets for malicious actors.
- A challenge for energy organizations is maintaining an updated asset inventory. It is difficult to protect what is not seen or is not known. Without an effective asset management solution, organizations that are unaware of assets in their infrastructure may unnecessarily expose themselves to cybersecurity risks.
- This NIST Cybersecurity Practice Guide provides detailed steps on how energy organizations can identify and manage OT assets and detect cybersecurity risks associated with them.

CHALLENGE

Energy organizations may be a prime target of growing and evolving cybersecurity threats, given the criticality of their infrastructure to our nation. A cyber attack that disrupts OT processes or equipment can result in safety issues and the loss of power, as well as in significant productivity costs. Currently, many energy organizations rely on manual processes to manage their OT assets, which makes it challenging to quickly identify and respond to potential threats. Existing asset inventories may be static, one-time, or point-in-time snapshots of auditing activities conducted previously without a way to see the current status of those assets. As OT systems become interconnected and integrated with other information technology (IT) systems, organizations looking to modernize OT processes will have to find automated methods to strengthen their OT asset management capabilities.

SOLUTION

The NCCoE, in collaboration with experts from the energy sector and technology vendors, developed an asset management example solution that includes managing, monitoring, and baselining OT assets to reduce the risk of cybersecurity incidents. This practice guide outlines practical steps on how organizations can implement new asset management capabilities or leverage existing asset management capabilities, to enhance the security of OT assets.

The NCCoE sought existing technologies that provided the following capabilities:

- OT/ICS asset inventory (including devices using serial connections)
- high-speed communication mechanisms for remote asset management
- reliable/secure/encrypted communications

- continuous asset monitoring
- log analysis and correlation
- cybersecurity event/attack detection
- patch-level information
- vulnerability awareness

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT/OT infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide on Energy Sector Asset Management can help your energy organization:

- reduce cybersecurity risk and potentially reduce the impact of safety and operational risks such as power disruption
- develop and execute a strategy that provides continuous OT asset management and monitoring
- respond faster to security alerts through automated cybersecurity-event capabilities
- implement current cybersecurity standards and best practices, while maintaining the performance of energy infrastructures

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at energy_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200