NIST SPECIAL PUBLICATION 1800-7A

Situational Awareness

For Electric Utilities

Volume A:
Executive Summary

Jim McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Otis Alexander
Sallie Edwards
Don Faatz
Chris Peloquin
Susan Symington
Andre Thibault
John Wiltberger
Karen Viani
The MITRE Corporation
McLean, VA

August 2019

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP1800-7

The first draft of this publication is available free of charge from:
https://nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf

Executive Summary

Situational awareness, in the context of this guide, is the understanding of one's environment and the ability to predict how it might change due to various factors.

As part of their current cybersecurity efforts, some electric utilities monitor physical, operational, and information technology (IT) separately. According to energy sector stakeholders, many utilities are currently assessing a more comprehensive approach to situational awareness, which, through increased real-time or near real-time cybersecurity monitoring, can enhance the resilience of their operations.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore an example solution that can be used by energy sector companies to alert their staff to potential or actual cyber attacks directed at the grid.

The security characteristics in our situational awareness platform are informed by guidance and best practices from standards organizations, including the NIST Cybersecurity Framework and North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Version 5 standards.

This NIST Cybersecurity Practice Guide demonstrates how organizations can use commercially available products that can be integrated with an organization's existing infrastructure. The combination of these products provides a converged view of all sensor data within the utility's network systems, including IT, operational, cyber, and physical access control systems, which often exists in separate "silos."

The example solution is packaged as a "how to" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world and based on risk management. The guide may help inform electric utilities in their efforts to gain situational awareness efficiencies. Doing so may enable faster monitoring, identification, and response to incidents while also saving research and proof-of-concept costs for the sector and its ratepayers and customers.

CHALLENGE

As part of the agenda to address the U.S. critical infrastructure, the energy sector, along with healthcare, finance, transportation, water, and communications sectors, has reported significant cyber incidents. As an integral component to the energy sector, industrial control systems (ICS) are increasingly vulnerable to cybersecurity threats, whether intentional or unintentional. In December 2015, the energy sector realized the potential effect of a combined attack on an electric utility's IT and ICS. In this instance, a Ukraine power grid was attacked, resulting in an electricity disruption that left approximately 225,000 people without electric power. The malicious actors then inundated the company's customer service center with calls, which slowed the response time to the electricity outage by causing internal challenges.

The monitoring model used by some electric utilities includes separate physical, operational, and IT silos, a practice that lacks efficiency and can negatively impact response time to incidents, according to the NCCoE's energy sector stakeholders. However, a number of useful products are commercially available for monitoring enterprise networks for myriad security events; yet, these products can have limited effectiveness when considering the specific ICS infrastructure requirements. A converged network monitoring solution that is tailored to the ICS cybersecurity nuances could reduce blind spots for electric

utilities, resulting in comprehensive situational awareness across enterprise business system and operational ICS environments.

SOLUTION

The NCCoE has developed *Situational Awareness for Electric Utilities* to augment existing and disparate physical, operational, and IT situational awareness efforts by using commercial and open-source products to collect and converge monitoring information across these silos. The aggregated and correlated information is analyzed, and relevant alerts are provided to each domain's monitoring capabilities, improving the situational awareness of security analysts. The converged data can facilitate a more effective, efficient, and appropriate response to an event, compared with a response that relies on isolated data.

The NCCoE sought existing technologies that provided the following capabilities:

- Security information and event management (SIEM) or log analysis software
- ICS equipment (e.g., remote terminal units, programmable logic controllers and relays) along with associated software and communications equipment (e.g., radios and encryptors)
- "bump-in-the-wire" devices for augmenting operational technology with encrypted communication and logging capabilities
- software for collecting, analyzing, visualizing, and storing operational control data (e.g., historians, outage management systems, distribution management systems, human-machine interfaces)
- products that ensure the integrity and accuracy of data collected from remote facilities

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 system 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 to *Situational Awareness for Electric Utilities* can help your organization:

- improve ability to detect cyber-related security breaches or anomalous behavior, likely resulting in early detection and having less impact on energy delivery, thereby lowering overall business risk while supporting enhanced resilience and reliability performance outcomes
- increase probability that investigations of attacks or anomalous system behavior will realize successful output, which in turn can inform risk management and mitigation
- improve accountability and traceability, resulting in lessons-learned use cases
- simplify regulatory compliance via automating generation and collection of disparate operational log data

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/situational-awareness . 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.

Please note: Hewlett Packard Enterprise in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.

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