NIST Special Publication 1800-7A

SITUATIONAL AWARENESS

For Electric Utilities

Volume A:
Executive Summary

Jim McCarthy
National Cybersecurity Center of Excellence
Information Technology Laboratory

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

February 2017

DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/use_cases/situational_awareness

Situational Awareness for Electric Utilities

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) developed an example solution that can be used by electric 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.
- The NCCoE's approach uses commercially available products that can be integrated with an organization's existing infrastructure. The combination of these commercially available products provides a converged view of all sensor data within the utility's network systems, including IT, operational, 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 analysis. 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 rate payers and customers.

CHALLENGE

As part of the U.S. critical infrastructure, the energy industry, along with healthcare, finance, transportation, water, and communications sectors, has reported significant cyber incidents. As an important component to the energy sector, industrial control systems (ICS) may be increasingly vulnerable to cybersecurity threats, whether intentional or unintentional. In December 2015, electric companies saw the potential effect of a combined attack on an electric utility's IT and ICS systems. In this instance, a Ukraine power grid was attacked, and electricity knocked out for 225,000 people. 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 model used by some electric utility companies of monitoring separate physical, operational, and information technology "silos" is a practice that lacks efficiency and can negatively impact response time to incidents, according to the NCCoE's energy sector stakeholders. A number of useful products are commercially available for monitoring enterprise networks for possible security events; however, these products can have limited effectiveness when considering the specific requirements of ICS networks. A converged network monitoring solution that is tailored to the cybersecurity nuances of ICS would reduce blind spots for electric utilities, resulting in more comprehensive situational awareness across both 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 information technology situational awareness efforts by using commercial and open-source products to collect and converge monitoring information across these silos. The converged information is analyzed and relevant alerts are provided back to each domain's monitoring capabilities, improving the situational awareness of security analysts in each silo. The converged data can facilitate a more efficient and appropriate response to an incident compared to an incident response that relies on isolated data from within a single silo.

The NCCoE sought existing technologies that provided the following capabilities:

- security incident 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, and human-machine interfaces)
- products that ensure the integrity and accuracy of data collected from remote facilities.

BENEFITS

The potential business benefits of this situational awareness reference design developed in our project include:

- improved ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk, while supporting enhanced resilience and reliability performance outcomes
- increased probability that investigations of attacks or anomalous system behavior will reach successful conclusions which can inform risk management and mitigation following incidents
- improved accountability and traceability, leading to valuable operational lessons learned
- simplified regulatory compliance by automating generation and collection of a variety of operational log data

SHARE YOUR FEEDBACK

You can view or download the guide at https://nccoe.nist.gov/projects/use_cases/situational_awareness. Help us make it 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 business processes associated with implementing it.

To provide comments or to learn more by arranging a demonstration of this reference solution, contact us at energy_nccoe@nist.gov.

TECHNOLOGY PARTNERS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor 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 applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology.

LEARN MORE

http://nccoe.nist.gov
nccoe@nist.gov
301-975-0200