NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SITUATIONAL AWARENESS

For Electric Utilities

The National Cybersecurity Center of Excellence (NCCoE) addressed the challenge of situational awareness for electric utilities through collaborative efforts with members of the energy sector and vendors of cybersecurity solutions. The example solution is detailed in NIST Cybersecurity Practice Guide, SP 1800-7. The NCCoE solution may not be the only one available in the fast-moving cybersecurity technology market. Please contact us at energy_nccoe@nist.gov with suggestions and comments.

CHALLENGE

Energy companies rely on operational technology to control the generation, transmission, and distribution of power. While there are a number of useful products available to monitor enterprise networks for possible security events, these products tend to be imperfect fits for the unusual requirements of industrial control system (ICS) networks.

A network monitoring solution that is tailored to the unique needs of utility sector control systems would reduce security blind spots. To improve the security of information and operational technology, energy companies need mechanisms to capture, transmit, analyze and store real-time or near real-time data from across both IT and ICS networks and systems.

SOLUTION

The NCCoE's implementation augments existing and disparate physical, operational, and information technology situational awareness efforts by using commercial and open-source products to collect and converge monitored 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 work and development of this example implementation is documented in NIST Cybersecurity Practice Guide 1800-7: *Situational Awareness for Electric Utilities*. Energy sector organizations can use some or all of the guide to implement a converged situational awareness platform using NIST and industry standards. Commercial, standards-based products, such as the ones used in this example are readily available and interoperable with commonly used operational and information technology infrastructure and investments.

BENEFITS

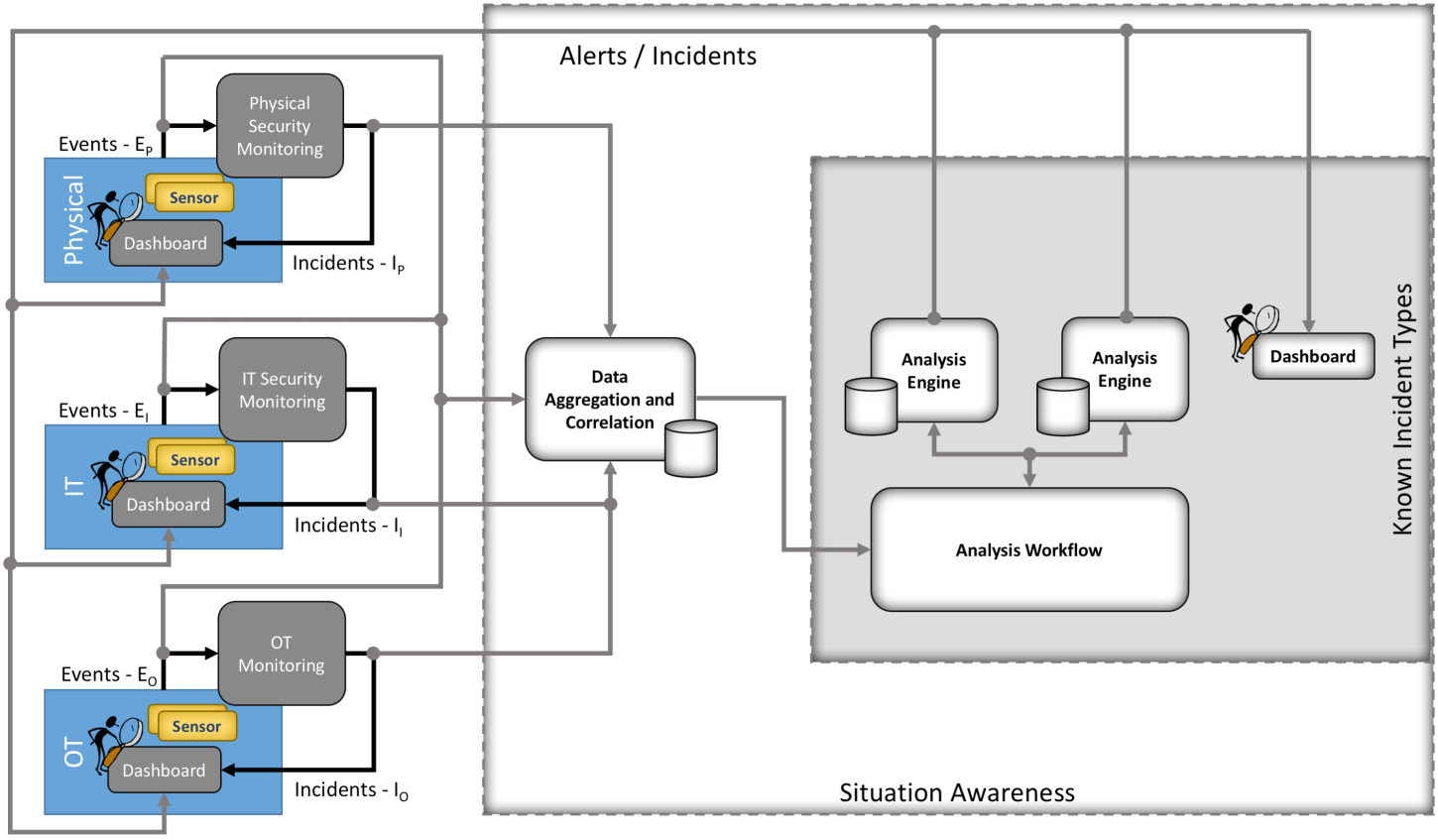
The potential business benefits of the situational awareness solution developed in this project include:

- 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

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
energy_nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE



COMPONENTS

Situational awareness solutions for energy companies include but are not limited to the following components:

- 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.

TECHNOLOGY PARTNERS/COLLABORATORS

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. Technology collaborators on this project include:

DRAGOS, Hewlett Packard Enterprise, ICS², OSIsoft., radiflow Secure your Assets, PAS Technologies, RSA, Schneider Electric, SIEMENS, tdi technologies, waratek, WATERFALL Stronger Than Firewalls

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.

DOWNLOAD THE PROJECT DESCRIPTION

For more information on this project, visit: https://nccoe.nist.gov/projects/use_cases/situational_awareness

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email energy_nccoe@nist.gov.