USE CASE

SITUATIONAL AWARENESS

Securing Networked Infrastructure for the Energy Sector

V.2
Formerly *Data Aggregation and Monitoring*
November 15, 2013
energy_nccoe@nist.gov

This revision incorporates comments from the public.

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices.

This document is a detailed description of a particular problem that is relevant across the energy sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the energy sector and vendors of cybersecurity solutions. The solutions proposed by this effort will not be the only ones available in the fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at energy_nccoe@nist.gov.

1. DESCRIPTION

Goal

To improve the security of operational technology, energy companies need mechanisms to capture, transmit, analyze and store real-time or near-real-time data from industrial control systems (ICS) and related networking equipment. With such mechanisms in place, electric utility owners and operators can more readily detect anomalous conditions, take appropriate actions to remediate them, investigate the chain of events that led to the anomalies, and share findings with other energy companies. Obtaining real-time and near-real-time data from networks also has the benefit of helping to demonstrate compliance with information security standards.

Motivation

Energy utilities rely on networked operational technology (OT) to control the generation, transmission and distribution of power. While there are a number of useful products on the market for monitoring enterprise networks for possible security events, these products tend to be imperfect fits for the unusual requirements of control system networks. A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots.

Illustrative Scenario

A dispatcher at an operations center sees that a relay has tripped at a substation and begins to investigate the cause. The dispatcher uses a single software interface that monitors system buses, displays an outage map, maps operational network connections to the bus and outage maps, and indexes logs from operational network devices and physical security devices. The dispatcher begins her investigation by querying network logs to determine whether any ICS devices received commands that might have caused the trip. If the answer is yes, then, using the same interface, she can automatically see logs of the most recent commands and network traffic sent to the relevant devices,

allowing her to easily extend the investigation to internal systems and users who communicated with the suspect devices. The system may also be able to alert her to incidents of similar network traffic that were flagged as suspicious and shared by analysts at other power companies.

If she finds that network traffic did not cause the trip, the dispatcher can check to see if there were any alerts from physical security devices that would imply a breach. This helps the dispatcher determine whether to send physical security personnel or a field technician to further investigate.

2. Desired Solution Characteristics

- data visualization and analysis capabilities that help dispatchers and security analysts view control system behavior, network security events and physical security events as a cohesive whole
- analysis and correlation capabilities that help dispatchers and security analysts understand and identify security events and predict how those events might affect control system operation
- scalability sufficient to meet the needs of a large metropolitan utility
- mechanisms that ensure the accuracy and integrity of data collected from remote facilities
- ability to collect logs, traffic and operational data from a variety of sources including servers, ICS equipment, networking equipment, security appliances, issue tracking systems and mobile devices
- ability to allow dispatchers and security analysts to easily automate common, repetitive investigative tasks
- built-in information sharing capabilities that allow dispatchers and security analysts to easily share and acquire new threat indicators, correlation rules, mitigations and investigative techniques
- customizable interfaces that allow users to tailor the system to meet specific business needs
- automated report generation to aid utilities in demonstrating compliance with relevant standards
- intuitive user interfaces that are appropriate for utility dispatchers with limited network security expertise or security analysts with limited expertise in electric power

3. Business Value

- improves a company's 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
- increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions
- improves accountability and traceability, leading to valuable operational lessons learned
- simplifies regulatory compliance by automating generation and collection of a variety of operational log data

4. Relevant Standards and Regulations

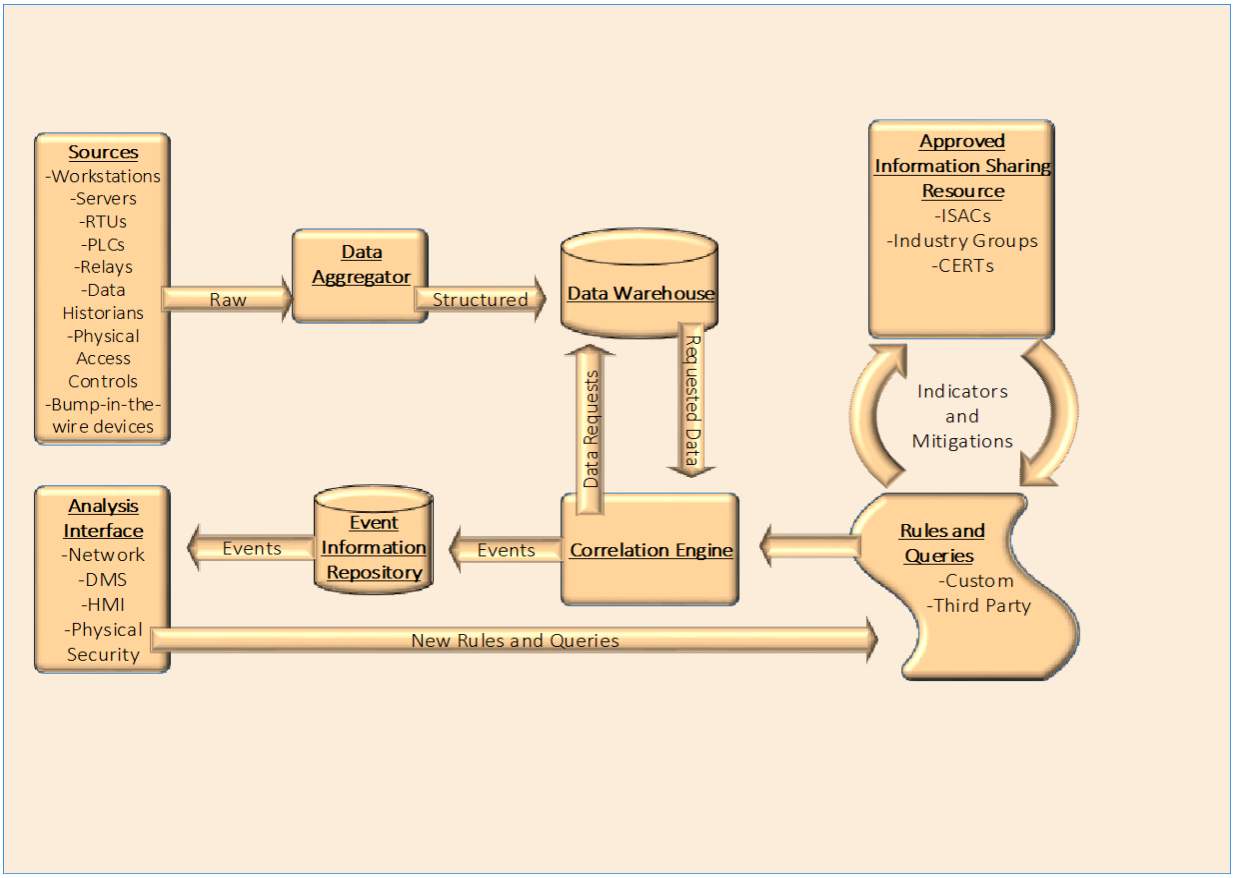
- ISA 99, Industrial Automation and Control Systems Security
  http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
- IEC 62351: Security
  http://www.iec.ch/smartgrid/standards/
- NERC Critical Infrastructure Protection Plans v.3 and v.5
  http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- NRC 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks
  http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
- NRC Regulatory Guide 1.152, Rev. 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
  http://pbadupws.nrc.gov/docs/ML1028/ML102870022.pdf
- NIST IR 7628, Guidelines for Smart Grid Cyber Security
  http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
- NIST SP 800-82, Guide to Industrial Control Systems Security
  http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
  http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2

5. Example Component List

- security incident and event management (SIEM) or log analysis software
- ICS equipment, such as RTUs, programmable logic controllers (PLC), and relays, along with associated software and communications equipment (e.g., radios, encryptors)

- “bump-in-the-wire” devices for augmenting OT 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

6. High-Level Architecture



7. Approach to Comments

We received more than 130 comments from 40 reviewers regarding the two draft use cases. Comments were grouped according to their commonalities, then we distilled those grouped comments into these brief statements. We have provided a response to each statement and revised the use cases accordingly.

8. General Comments

1. There were many comments identifying products of potential interest, or indicating interest in getting involved.

   Response: We welcome inquiries from companies that are interested in participating in our use cases. In the next few weeks, we will publish a Federal Register notice for each use case with instructions for companies that hope to get involved. To receive announcements about the publication of the Federal Register notices, send an email to nccoe@nist.gov.

2. The (new) capabilities envisioned in each use case can themselves introduce new vulnerabilities or become targets of attack.

   Response: This is a legitimate concern for any new feature added to any system, but it should not prevent us from seeking out new capabilities that improve security, efficiency and function. The NCCoE's mission is to help American companies become more secure, so we take seriously the security of our example solutions. Unfortunately, because the field of cybersecurity currently cannot measure security, no solution can be proven to be free of vulnerability, and so there is no way to guarantee the security of a solution. The NCCoE will analyze the solutions to gain reasonable assurance that they are appropriate for the security of critical infrastructure like the energy industry.

3. Operational availability trumps security. In particular, offline operation of systems or endpoint devices needs to be addressed.

   Response: This comment is true of many critical infrastructure sectors, including electric power. The use case descriptions have been modified to reflect the need for disconnected operation.

4. Some comments conjectured that the capabilities are going to be expensive to procure and time-consuming to deploy. What near-term business value will justify that investment? Conversely, several additions to the Business Value sections were suggested.

Response: These comments resulted in some modifications to the Business Value sections in the use cases. The NCCoE has found many private sector companies developing unexpected solutions that are not well publicized. Therefore, we are hopeful that if we clearly state wished-for capabilities without assuming they are impractical to achieve, these use cases will result in a variety of solutions for utilities with a wide range of security needs and budgets.

5. The component lists are an inconsistent mix of technology, objectives and environmental factors.

   Response: The component lists have been modified for better consistency.

6. Several comments advocated making compliance to the NIST Federal Information Processing Standards and other federal security guidelines a requirement for the use cases.

   Response: Federal standards and guidelines are not mandatory for non-governmental use unless adopted by a relevant regulator. Furthermore, the solution sets that result from these use cases will not have any specific government or regulatory approval, certification, or accreditation. Nevertheless, the NCCoE will seek to be consistent with or improve upon the best available security practices in a manner that will be practical for all members of the affected sector.

9. Comments on this Use Case

1. Isn't this about situational awareness? Data aggregation and monitoring are just components of that.

   Response: We agree that the primary goal of this use case is to increase situational awareness, and have therefore decided to retitle the use case.

2. Finding patterns in the data is the hard part.

   Response: We welcome products that will help analysts understand data and prioritize security and reliability events. We encourage companies that market such products to respond to our upcoming Federal Register notices.

3. Open telemetry and logging interfaces for endpoint integration will be critical. Existing systems have none, and are not likely to be replaced en masse.

   Response: The product replacement lifecycle for industrial control systems is extremely long, and that is not likely to change soon. Therefore, we are

interested in operational products that are capable of supporting telemetry and logging features as well as “bump-in-the-wire” devices that are meant to augment endpoint devices with the necessary functions.

4. In other communities, non-real-time analytics have been more flexible and powerful; a goal of real-time analysis is not necessarily desirable.

   Response: This use case discusses real-time data, not real-time data analysis. We may have unintentionally implied, however, that analysis should be real-time as well. In fact, analysis can be post-event, in the same time frame as the event(s), or even predictive. The NCCoE is interested in making detection and remediation of network-related security and reliability events faster and more effective. That begins with better and faster access to data, whatever the timeframe required for analysis.

5. Consuming threat information is as much a challenge as consuming situational information.

   Response: Threat information is a valuable subset of situational information, and the NCCoE is interested in products that help integrate threat information into the overall situational awareness picture.

Appendix: Security Control Map

This table maps the preliminary list of desired characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF) and other NIST activities. This is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Example Characteristic		Cybersecurity Standards and Best Practices						Sector-Specifc Standards and Best Practices
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27001**	**SANS CAG20**	**NERC CIP v3/5**
device inventory	identification of all IT devices	Identify	Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2	CSC 1-1, CSC 1-4	CIP-002-5 R1, CIP-010-5 R1
vulnerability management	mechanisms for Identification of vulnerabilities and information sharing	Identify	Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16	ISO/IEC 27001:2013 A.6.1.4, A.12.6.1, A.18.2.3	CSC 4-1, CSC 4-4	CIP-003-5 R1, CIP-004-5 R1, CIP-007-5 R1, CIP-007-5 R2, CIP-007-5 R3, CIP-007-5 R4, CIP-008-5 R1, CIP-010-5 R2, CIP-010-5 R3
threat identification	mechanisms for Identification of threat and Information sharing	Identify	Risk Assessment	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources ID.RA-3: Threats, both internal and external, are identified and documented	NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5, RA-3, PM-12, PM-16	ISO/IEC 27001:2013 A.6.1.4	CSC 4-1, CSC 4-4	CIP-004-5 R1, CIP-007-5 R2, CIP-008-5 R1, CIP-010-5 R3
logging and auditing	logging and auditing mechanisms	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	NIST SP 800-53 Rev. 4 AU Family	ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	CSC 4-2, CSC 4-6	CIP-003-5 R1, CIP-004-5 R4, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R4, CIP-007-5 R5, CIP-011-5 R2
security monitoring	mechanisms to monitor networks for security events	Detect	Security Continuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events DE.CM-2: The physical environment is monitored to detect potential cybersecurity events DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events DE.CM-4: Malicious code is detected DE.CM-5: Unauthorized mobile code is detected DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed DE.CM-8: Vulnerability scans are performed	NIST SP 800-53 Rev. 4 AC-2, AU-12,AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, SC-5, SC-7, SC-18, SC-44, PE-3, PE-6,PS-7, PE-20, SI-3, SI-4, SA-4, SA-9, PE-3, RA-5	ISO/IEC 27001:2013 A.12.2.1, A.12.4.1, A.12.5.1, A.12.6.1, A.14.2.7, A.15.2.1	CSC 5-1, CSC 5-8	CIP-002-5 R1, CIP-003-5 R1, CIP-004-5 R2, CIP-004-5 R3, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-005-5 R4, CIP-005-5 R5, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R1, CIP-007-5 R2, CIP-007-5 R3, CIP-007-5 R4, CIP-007-5 R5, CIP-010-5 R1, CIP-010-5 R2, CIP-010-5 R3
security events and anomalies	mechanisms to ensure security events are detected in a timely manner	Detect	Anomalies and events	DE.AE-2: Detected events are analyzed to understand attack targets and methods DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors DE.AE-5: Incident alert thresholds are established	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4,	ISO/IEC 27001:2013 A.16.1.1, A.16.1.4	CSC 5-1, CSC 5-8	CIP-003-5 R1, CIP-006-5 R1, CIP-007-5 R2, CIP-007-5 R4, CIP-007-5 R5, CIP-008-5 R1, CIP-008-5 R2, CIP-008-5 R3, CIP-010-5 R2
security event analysis	mechanisms to ensure events are investigated	Respond	Analysis	RS.AN-1: Notifications from detection systems are investigated	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5	CSC 5-10, CSC 18-1	CIP-003-5 R1, CIP-004-5 R2, CIP-004-5 R4, CIP-004-5 R5, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R2, CIP-007-5 R4, CIP-007-5 R5, CIP-008-5 R1, CIP-008-5 R2, CIP-010-5 R2
security incident containment	mechanisms to ensure security incidents are contained	Respond	Mitigate	RS.MI-1: Incidents are contained RS.MI-2: Incidents are mitigated RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	NIST SP 800-53 Rev. 4 IR-4 , CA-7, RA-3, RA-5	ISO/IEC 27001:2013 A.12.2.1, A.12.6.1, A.16.1.5	CSC 18-4, CSC 18-6, CSC 18-7	CIP-003-5 R1, CIP-007-5 R2, CIP-007-5 R5, CIP-008-5 R2, CIP-010-5 R2, CIP-010-5 R3
information protection	mechanisms to encrypt data	Protect	Data Security	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected	NIST SP 800-53 Rev. SC-8, SC-28	ISO/IEC 27001:2013: A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	CSC 16-16, CSC 17-7	CIP-011-5 R1