Agency Priority Goal Action Plan

Energy Sector Cybersecurity

Goal Leader(s):

Nicholas Andersen, Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

Sean Plankey, Principal Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

David Harvilicz, Senior Advisor and Director of Strategic Initiatives, Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

Overview

Goal Statement

Identify, contain, and defeat cyber threats to our Nation's energy delivery systems through a shared understanding between industry and government of adversarial techniques to mitigate energy sector cyber-attacks. DOE will have dramatically improved our National energy sector's ability to identify, contain, and defeat cybersecurity threats. Out of 47 commonly known types of Industrial Control Systems (ICS) cyber-attack techniques, our partnership with the energy sector will improve sharing of operational and information technology data and will be capable to detect and mitigate at least 24 of the commonly known techniques of cyber-attacks by September 30, 2021 as compared to 4 in FY 2019.

Challenge

- The frequency, scale, and sophistication of cyber threats continue to increase.
- Ensuring that operational technology (OT) data is shared across appropriate communication channels in a timely and effective manner.
- Adversaries seek to disrupt energy services, damage highly specialized equipment, and even threaten human health and safety as well as our national security.

Opportunity

- Trusted mechanisms for sharing and analyzing OT data.
- Process to deliver timely and actionable information from multiple analysis teams.

Leadership & Implementation Team

Senior Advisor in the Office of Policy for Cybersecurity, Energy Security, and Emergency Response
Alexander Gates

Principal Deputy Assistant Secretary
Sean Plankey

Deputy Assistant Secretary
Nicholas Andersen

Senior Advisor and Director of Strategic Initiatives
David Harvilicz

Goal Structure & Strategies

Long-Term Vision for OT analysis capability

Create an industry-wide capability to:

- Validate supply chain of critical components to reduce threat vectors.
- Share near-real-time OT network data between industry and government and leverage U.S. intelligence capabilities to detect sophisticated cyber threats.
- Deliver actionable cyber threat information to utilities to better protect U.S. electric power infrastructure against cyber attacks.

Near-Term Goals for OT analysis capability

- Increase internal detection capability or industry's detection capability for tactics, techniques and procedures (TTPs) associated with OT networks.
- Adopt government-formed testing and reporting strategies to mitigate supply chain vulnerabilities.
- Leverage known frameworks for TTP discovery.
- Introduce a paradigm shift in information sharing to event driven sharing where events can be any anomalous activity (network traffic, physical operations/processes, logical events, i.e. login attempts) as defined by the owners and operators providing possible Indicators of Attack (IOA).
- Share actionable cyber threat information and intelligence-informed cyber expertise to advise projects within industry to help reconfigure critical devices to reduce threat vectors.

Summary of Progress – FY 20 Q1

Use cases have been developed with industry teams to determine what data sources are available for sharing information for analysis. Each use case has been analyzed to identify which data sources the utility can collect to enable a more effective analysis for IOAs as well as applicability to existing TTPs. The use cases are also being evaluated for data source availability across the sector, analysis capability with available data and legal/regulatory constraints with sharing data. The three use cases are Alarm Logs, Human Machine Interface (HMI), and Remote Logins:

1. Alarm Logs – This encompasses any alarm from an Incident Command System (ICS) with the accompanying data and alarm messages. It is proposed to pull these from alarm logs on systems and devices for which such logs are accessible through automation. Where automation is not possible, such logs may be collected and provided manually when an anomaly is detected.
2. HMI – Logs of suspicious activity surrounding the HMI environment, including (1) when someone operates part of the system not using the HMI, (2) when someone obtains unauthorized access to the HMI or its infrastructure, and (3) when there's something flowing on the environment that's never been seen before and can't be explained.
3. Remote Login – Logins to any ICS system which occur remotely, with priority on those logins from unexpected hosts or with unexpected timing.

Summary of Progress – FY 20 Q2

During the second quarter of 2020 CESER began the work to refine use cases and develop and operationalize pilot concepts and structures for data receipt and analysis. The following milestones were completed in the second quarter:

1. Identify data sources from industry for each of the Alarm Logs, HMI, and Remote Logins use cases.
   a) Out of 120+ data fields identified in the MITRE ATT&CK Framework tactics, techniques and procedures (TTPs) of an intruder, CESER worked with participants in each of the use cases to identify relevant subsets of data fields within their use~~s~~ cases.
   b) CESER is collaborating with partners to analyze the subsets of data fields for (1) availability of data, (2) suitability of data, and (3) viability of information sharing agreements and concerns.

2. Conduct pilot activity to share data from at least 1 use case.
   a) CESER-funded, pilot activity is underway at Idaho National Laboratory (INL) and is being expanded into Q3.
   b) CESER, INL, and other partners are working to develop an understanding of the real-world data within the data field subsets of each use case, analyzing variations in the data, and developing tools to group data from disparate entities into a common format/baseline. This work is funded by CESER.
   c) CESER, INL, and other partners are working to develop tools based on triggering events defined by the use case companies.

Summary of Progress – FY 20 Q3

During the third quarter of 2020 CESER continued to work on pilot activities to receive and analyze use case data. The following milestones were completed in the third quarter:

1. Identified multiple companies willing to share data with CESER for each of the Alarm Logs, HMI, and Remote Logins use cases.
   a) The alarm log use case participants signed their agreements first and this use case will be the focus for the first pilot activity.
   b) Shared with the sector the processes and plans for receiving the data from triggered events (events were previously defined in the use case groups in Q1), distilling the data into TTPs and developing tools for the sector to use to internally identify these TTPs for sector trend analysis.
   c) The initial pilot for Alarm Logs data will be completed in Q4.

2. Conduct pilot activity to share data from at least 1 use case.
   a) Pilot activity is underway and will be concluded in Q4.
   b) CESER is working to develop an understanding of the real-world data within the data field subsets of the alarm log use case, analyzing variations in the data, and developing tools to group data from disparate entities into a common format/baseline.
   c) CESER is working to develop tools based on triggering events defined by the use case companies to identify TTPS. The tools will be made available for distribution to the sector.

Summary of Progress – FY 20 Q4

During the fourth quarter of 2020 CESER continued to work on pilot activities to receive and analyze use case data. The following milestones were completed in the fourth quarter:

1. Completed tool development in each of the 3 use cases.
   a) Alarm log: 5 tools created*.
   b) Human Machine Interface: 7 tools created*.
   c) Remote Login: 9 tools created*.

   * N.B. some tools are applicable to multiple use cases

2. Conduct pilot activity to share data from at least 1 use case.
   a) The initial pilot for Alarm Logs data completed.
   b) CESER is working to develop a broader understanding of the real-world data within the data field subsets of all use cases, developing approaches to extend the tool beyond the pilot companies.
   c) CESER is working to develop tools based on triggering events defined by the use case companies to identify TTPs. The tools will be made available for distribution to the sector.

Key Milestones

- Increase detection capability for tactics, techniques and procedures (TTPs) associated with operational technology (OT) networks.
- Produce analytic tools to detect common TTPs
  - 12 additional tools by end of FY20
  - 12 additional tools by end of FY21

Milestone Summary					
Key Milestone	**Milestone Due Date**	**Milestone Status**	**Change from last quarter**	**Owner**	**Comments**
Analyze use cases for applicable TTPs	Q1, FY2020	Completed	N/A	CESER	
Identify data sources from industry for each use case	Q2, FY2020	Completed	N/A	CESER	
Conduct pilot activity to share data from at least 1 use case	Q2,FY2020	Completed	N/A	CESER	
Develop analysis capability for TTPs in 1 use case, at least 6 TTPs	Q3, FY2020	Completed	yes	CESER	Completed behind schedule in Q4 FY 2020
Conduct pilot activities for remaining 2 use cases	Q3, FY2020	Completed	yes	CESER	Completed behind schedule in Q4 FY 2020
Develop analysis capability for TTPs in the remaining 2 use cases, at least 3 additional TTPs per use case	Q4, FY2020	Completed	yes	CESER	
Conduct additional pilot activities for 3 use cases	Q1, FY2021		N/A	CESER	
Develop analysis capability for TTPs, at least an additional 4 TTPs per use case	Q2, FY2021		N/A	CESER	
Provide strategy for industry to participate in new sharing model for OT analysis	Q3, FY2021		N/A	CESER	
Provide capability for the Energy Sector covering new information sharing paradigm and TTP coverage	Q4FY2021		N/A	CESER	

Data Accuracy and Reliability

All data will be provided by Energy Sector asset owners and operators and the Intelligence Community. Regarding the shared data, the department will rely on the owners and operators to identify and appropriately mark the data for analysis and data protection. Sample data fields to be shared will potentially include, but not be limited to:

- Source Internet Protocol Address
- Date
- Time
- User Name
- Host Name
- Process Name
- Process Setting
- User/Operator
- Control Action
- Alarm Name
- Alarm Message
- Login Attempts failed
- Login Attempts successful

Additional Information

Contributing Programs

Organizations:

- CESER

Program Activities:

- Cybersecurity for the Operational Technology Environments (CyOTE™)
- Cyber Analytic Tools and Techniques (CATT™ 2.0)

President's Management Agenda

- CAP Goal 1: Modernize IT to Increase Productivity and Security.
- CAP Goal 2: Leveraging Data as a Strategic Asset.
- CAP Goal 4: Improving Customer Experience with Federal Services

Regulations:

- North American Electric Reliability Corporation critical infrastructure protection

Tax Expenditures:

- N/A

Policies:

- Executive Order 13636—Improving Critical Infrastructure Cybersecurity
- Presidential Policy Directive 21 (PPD-21)—Critical Infrastructure Security and Resilience
- Presidential Policy Directive 41 (PPD-41)—United States Cyber Incident Coordination
- The FAST Act
- Executive Order 13920- Securing U.S. Bulk Power Systems

Other Federal Activities:

- DHS Automated Indicator Sharing, DOE is extending this to include Operational Technology indicators

Stakeholder / Congressional Consultations

CESER is engaging with the Electric Sub-Sector Coordinating Council and the Oil and Natural Gas Sub-Sector Coordinating Council with regular monthly calls as well as specific workshops for technical and legal topics. CESER is also engaging with multiple cross government working groups; Control Systems Interagency Working Group and the Technical Working Group on Cyber Threat Information Sharing.