Cybersecurity Risk Information Sharing Program (CRISP)

Introduction

The Cybersecurity Risk Information Sharing Program (CRISP) and associated information sharing pilots comprise the leading information sharing and energy sector cyber situational awareness platforms for the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER). CRISP is a public-private partnership that delivers relevant and actionable cybersecurity information to participants from United States electricity industry. Collaboration between government and private industry is essential to combat cyber threats to United States critical electric infrastructure. By leveraging the open-source cyber threat intelligence and government-informed reporting provided by the Pacific Northwest National Laboratory (PNNL), the Electricity Information Sharing and Analysis Center (E-ISAC) provides CRISP participants with information related to advanced threat actors, custom automated analytics to identify anomalies, event and incident trending statistics and other information relevant for operators of critical electric infrastructure.

Partners in Situational Awareness

E-ISAC CRISP CYBERSECURITY RISK INFORMATION SHARING PROGRAM

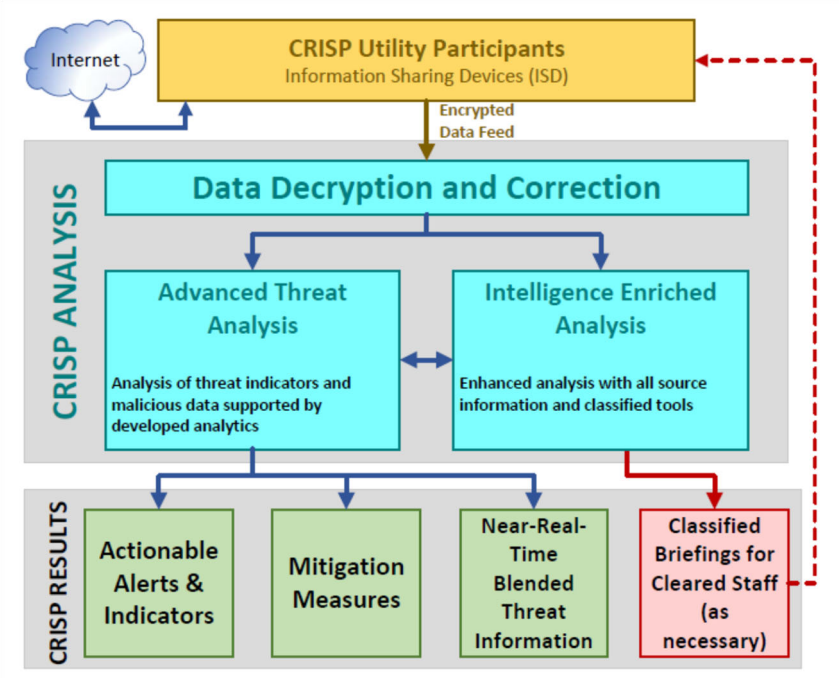
Pacific Northwest NATIONAL LABORATORY

How CRISP Works

CRISP receives data related to network traffic at or near the Internet perimeter that is voluntarily shared by electric power participants, collates technical analysis, and identifies indicators of compromise (IOCs). CRISP participants and their information are anonymized and kept confidential. The program also leverages subject matter experts and resources from the E-ISAC, PNNL and the Argonne National Laboratory (ANL).

Together, this team of experts works with the participants to do the following:

- Install a passive information sharing device (ISD) on participant networks outside their firewalls to collect data relating to Internet traffic
- Analyze voluntarily shared data against a catalogue of threats, tactics, and known actors
- Identify and share appropriate steps that industry may take to mitigate any identified threats
- Provide opportunity for additional resources and support from DOE CESER



CRISP Participation

The CRISP partnership was originally launched by the DOE Office of Electricity and E-ISAC in 2014 as a member-financed endeavor. Today, CRISP is managed by the E-ISAC, advised by CESER, and supported with DOE cyber threat intelligence and DOE analytics through PNNL. CRISP uses a shared-cost model with a standardized master services agreement. After entering the agreement, participants receive and install the ISD on their networks which analyzes network traffic, packages the results of sensing, and encrypts it for transfer. Data flows from the participants' ISDs to the E-ISAC and PNNL for unclassified analysis and to the government for classified analysis. Through CRISP, the DOE/E-ISAC partnership supports the mission to enable a greater level of information sharing by the government on potential risks to the security, reliability, and resiliency of the electric power grid.

Quality Intelligence

CRISP analysts compare high-value, and not publicly available, threat indicators to data received from CRISP participants. Using these indicators, reports are produced that identify potentially suspicious activity. Reporting includes both periodic national level energy sector cyber analyses and incident driven site specific alerts. CRISP participants may also investigate further based upon information provided in these reports to correlate internal cyber activity with reported IOC's. This public-private partnership has provided a detailed understanding of the intrusion methods, aspirations, and technical proficiency that threat actors employ to evade detection and conduct computer network exploitation and attacks.

CRISP also fosters collaboration among participants on the sharing of IOCs by generating reports based on information shared by CRISP participants. These cases include targeted spear phishing campaigns, redirects to suspicious web pages, and other IOCs. This increased information sharing has resulted in enhanced awareness and security for CRISP participants.

CRISP Expansion and R&D

CESER additionally sponsors pilot programs to expand CRISP to specific critical electric infrastructure entities and to the Oil and Natural Gas subsector. CESER operates pilot programs in these areas to increase data available for analysis, providing a benefit to all CRISP members, and to provide for collective defense through broad situational awareness of the electric and oil and natural gas subsectors.

CESER also sponsors R&D efforts through the Cybersecurity for Energy Delivery Systems (CEDS) research cooperative agreements to enhance industry's capability to share data from operational technology (OT) systems. CESER leverages the CRISP model for a pilot program involving CESER CEDS R&D and CRISP for correlation of IT and OT threat data.

For More Information on CRISP and Participation in the Program

Contact DOE CESER at ceser.infoshare@hq.doe.gov or the E-ISAC at crisp@eisac.com.