U.S. DEPARTMENT OF
ENERGY

OFFICE OF
CYBERSECURITY, ENERGY SECURITY,
AND EMERGENCY RESPONSE

Cybersecurity Risk Information Sharing Program (CRISP)

Enhanced threat analysis with U.S. Intelligence insights for faster threat identification and mitigation

Background

CRISP is a public-private data sharing and analysis platform that facilitates the timely bi-directional sharing of unclassified and classified threat information among energy sector stakeholders.

Improving the speed and accuracy of data sharing enhances the ability to detect trends across the sector, identify fast-moving cyber attacks, and deploy effective mitigations before critical systems are affected.

Objectives

The U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) developed CRISP to combine state-of-the-art threat analysis capabilities with U.S. Intelligence insights to identify sophisticated attacks targeting critical U.S. energy systems.

CRISP leverages DOE's unique intelligence capabilities and expertise as part of the U.S. Intelligence Community, and advanced threat detection technologies developed by the DOE National Laboratories, to aggregate, analyze, and distribute actionable threat information to the energy sector. CRISP enhances the sector's ability to identify, prioritize, and rapidly mitigate threats.

Project Description

CRISP designed a platform for energy sector owners and operators to voluntarily share IT system traffic in near-real time by installing an information sharing device (ISD) at the border of their information technology (IT) systems, just outside the firewall.

Using the ISD, CRISP utilities passively share near-real-time network data, which undergoes classified analysis by DOE analysts and non-classified analysis using Pacific Northwest National Laboratory's advanced tools. This dual analysis is used to identify threat patterns and attack indicators across the energy industry. No other program shares cyber intelligence information fused with industry information in a collaborative sharing framework in the same way as CRISP.

CRISP analysis detects cyber attacks and threats, and delivers alerts and mitigations back to owners and operators through the Electricity Information Sharing and Analysis Center (E-ISAC).

CRISP is a voluntary, subscription-based program managed by the (E-ISAC) since 2014. Electric utilities participating in the program now account for about 75% of U.S. electric customers. Information sharing across a broad and diverse group of utilities is key to CRISP's approach.

Benefits

- Provides near-real-time alerts based on classified threat analyses
- Identifies malicious cyber traffic and offers rapid mitigations to energy utilities
- Improves the speed and security of data sharing among utilities
- Integrates U.S. Intelligence insights and advanced analytic capabilities with existing utility resources

Partners

- Pacific Northwest National Laboratory
- Electricity Information Sharing and Analysis Center (E-ISAC), operated by the North American Electric Reliability Corporation (NERC)

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber-attacks.

Contact Information:

Akhlesh Kaushiva, P.E.
Program Manager
DOE CESER
202-287-6062
Akhlesh.Kaushiva@Hq.Doe.Gov

For More Information:

https://www.energy.gov/ceser

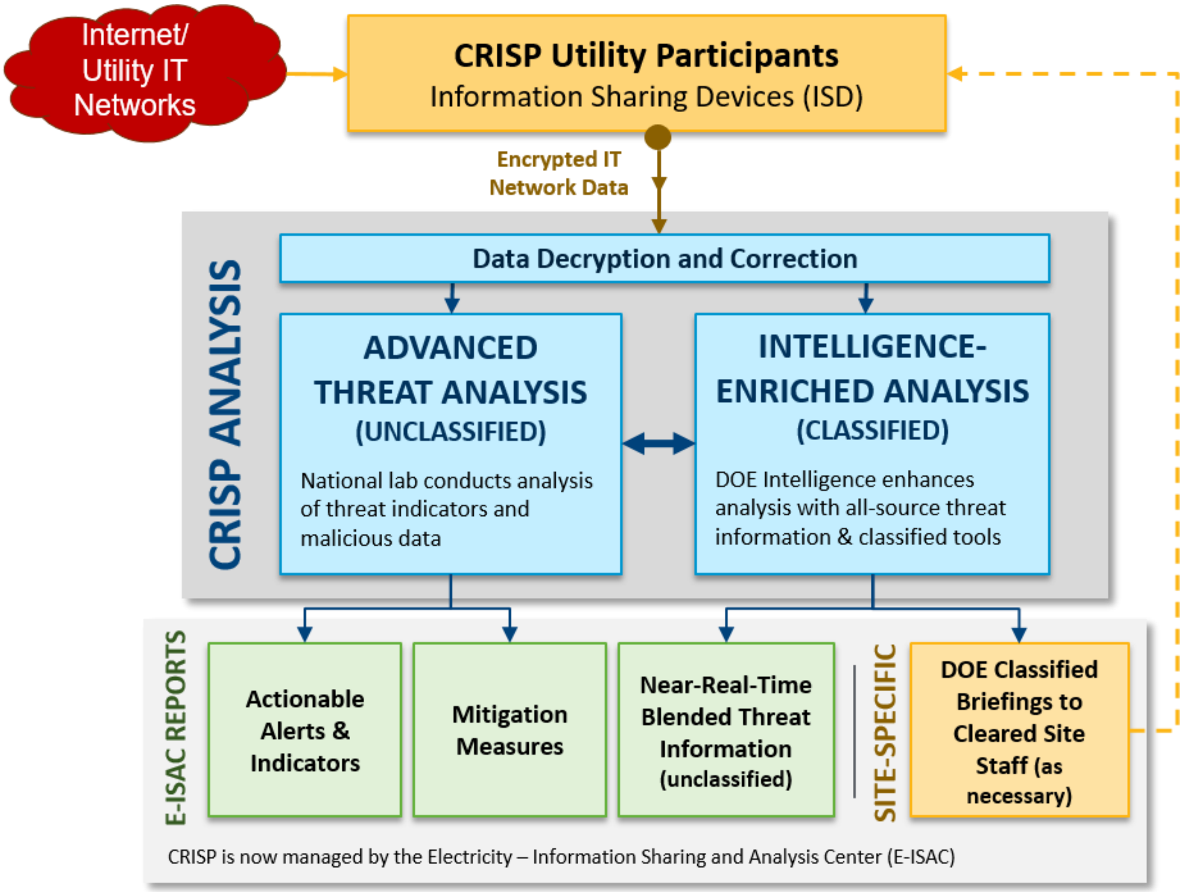
Internet/ Utility IT Networks
CRISP Utility Participants
Information Sharing Devices (ISD)
Encrypted IT Network Data
CRISP ANALYSIS
Data Decryption and Correction
ADVANCED THREAT ANALYSIS (UNCLASSIFIED)
National lab conducts analysis of threat indicators and malicious data
INTELLIGENCE-ENRICHED ANALYSIS (CLASSIFIED)
DOE Intelligence enhances analysis with all-source threat information & classified tools
E-ISAC REPORTS
Actionable Alerts & Indicators
Mitigation Measures
Near-Real-Time Blended Threat Information (unclassified)
SITE-SPECIFIC
DOE Classified Briefings to Cleared Site Staff (as necessary)
CRISP is now managed by the Electricity – Information Sharing and Analysis Center (E-ISAC)

Figure 1. CRISP Information Sharing and Analysis Process

CRISP Outcomes and Progress

Intelligence analysis of CRISP data has identified intrusions that would have gone undetected and alerted operators to threat indicators. In those cases, DOE notified victims and coordinated Federal onsite assistance teams—which in some cases found and mitigated other risk exposures.

Today, DOE provides classified threat analysis using all-source intelligence and classified tools to CRISP. This is complemented by advanced threat analysis in a non-classified environment—funded by utility participants—that identifies malicious traffic, directly alerts affected utilities, and supports risk mitigation.

The project team is currently working to grow industry participation in CRISP, improve performance, and reduce costs by leveraging the integrated platform of intelligence tools and information available via the Intelligence Community Information Technology Environment (ICITE). ICITE provides a common platform for the Intelligence Community to easily and securely share analytic tools and technologies, information, and resources. This is being conducted under DOE’s Cyber Analytic Tools and Techniques (CATT) project.

The team is also working closely with the E-ISAC to develop future evolutions of CRISP information-sharing technologies and devices.

Results

CRISP now delivers:

- Automated threat identification analytics and timely alerts based on classified threat analyses to partner companies
- Tools to identify malicious traffic, directly alert affected utilities, and mitigate risks
- CRISP reports supported the energy sector’s response to key attacks in 2017