

2023  
**CHEMICAL  
SECURITY  
SUMMIT**

---

August 29-31, 2023

#ChemicalSecurity



# CHEMICAL SECURITY SUMMIT

---

August 30, 2023

## Cyber Threats Facing the Chemical Sector

**Amy Thomas**

Cyber Risk Analyst

Vulnerability Management, Cybersecurity Division, CISA

**Carole Kelliher**

Deputy Program Manager, CyberSentry

Cybersecurity Division, CISA

**Moderator: Kelly Murray**

Associate Director

CISA Chemical Security



**#ChemicalSecurity**

# CYBERSENTRY 101

## CHEMICAL SECTOR SECURITY PANEL



# Agenda



## Overview

- What is CyberSentry & Benefits



## Partnerships and Benefits



## Participation



## Discussion





# Overview

## OVERVIEW

CyberSentry (CS) is a CISA-managed threat detection and monitoring capability, governed by an agreement between CISA and voluntarily participating critical infrastructure (CI) partners that operate significant networks supporting National Critical Functions (NCFs).







## MISSION NEED

CyberSentry is a core component of CISA's strategic goal to gain operational visibility into critical Information Technology and Operational Technology networks within critical infrastructure sectors to identify and defend against cyber attacks. CyberSentry analysts continually monitor alerts and analyze data at partner sites, and insights gained from one partner benefit other partners that may have similar behavior on their networks.



## STRATEGIC PARTNERSHIPS

CS is a **partnership-enabled program** with partners across six critical infrastructure sectors:

-  Communications
-  Energy
-  Healthcare and Public Health
-  Nuclear Reactors, Materials, and Waste
-  Transportation Systems
-  Water and Wastewater Systems

 *Actively looking for  
Chemical Sector Partnerships*

For more information:  
[CyberSentry.PMO@cisa.dhs.gov](mailto:CyberSentry.PMO@cisa.dhs.gov)

# CyberSentry Program Partnerships

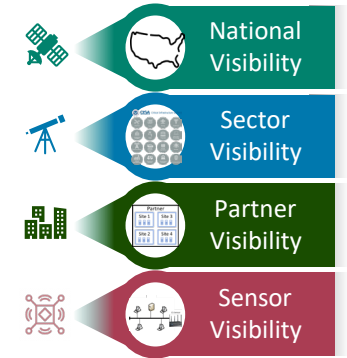
## COLLECTIVE VALUE OF PARTNERSHIP

Collaboration with CS partners is an important component of the program. Malicious activity found on one partner's site is used to validate and inform all partners and the broader CI community.

- CS is a voluntary bi-directional relationship.
- CS is provided without fees or equipment costs to partners.
- CS capabilities leverage CISA analysts and unique government insights.
- Additional analysts monitoring for known and unknown threats
- CS partnerships provide valuable information sharing across multiple critical infrastructure sectors.
- CS does not replace an organization's cybersecurity team or cybersecurity products.

## APPROACH TO VISIBILITY & RISK

Partnerships provide CS with valuable visibility that is used to hunt for and disseminate findings to all partners and to CISA's public information sharing channels. The CS program is developing a risk-based framework for selecting future CI partners to maximize visibility into the national risk picture.



## PROGRAM ADVANTAGES

- Enables analysis of incidents across CI sectors to identify commonalities and trends
- Provides operational insights that inform the protection of the larger CI community and Federal assets
- Offers greater historical and current cyber situational awareness into Information Technology and Operational Technology (IT/OT) networks



# CyberSentry Program Benefits

## BENEFITS TO PARTNERS

CISA leverages its unique government data and analysts to monitor for known and unknown threats and proactively hunt CS participant networks. CISA analysts can identify malicious activity within hours of receiving intelligence. Partnerships enable quick notification after discovery, and follow-on incident response coordination efforts can be initiated within 24 hours.

- ✓ **Threat Analysis:** CISA-conducted additional analysis
- ✓ **Visibility:** Improved visibility and swift threat detection
- ✓ **Incident Response:** Reduction in incident response reaction time
- ✓ **Cyber Preparedness:** Enhanced preparedness against nation-state actors and threats
- ✓ **Critical Infrastructure Defense:** Improved collective defense



## EXAMPLE SUCCESS STORIES

**MOVEit Response:** CS data helped quickly identify partners affected by the MOVEit file transfer software breach. All impacted partners were notified, and the program worked closely and quickly with these partners to confirm remediation of the threat.

**Malicious Activity Identified on High-Risk Devices:** CS analysts identified high-risk devices at several partner sites that were susceptible to observed threat activity. CS worked with affected partners to mitigate the risk.

**Malware Discovery:** CS tools quickly discovered and identified malware in a partner's IT network. Working with the partner, CISA analysts were able to locate the infected device so the partner could remove it from the network and verify that the threat was contained.

**Attacker Exfiltration Detected:** CS discovered that an attacker was actively exfiltrating information. CS worked with the partner to identify and recover information. After conferring with CS analysts, the partner was able to isolate infected systems, eliminating the threat.

# Participation Discussion

## Target Partner Characteristics

CISA would like to partner with select companies across critical infrastructure sectors. The CS Program is intended to protect against threats to National Critical Functions (NCFs) – functions so vital to the US that their disruption would have a debilitating impact on the nation.







*Actively looking for  
Chemical Sector  
Partnerships*

For more information:

[CyberSentry.PMO@cisa.dhs.gov](mailto:CyberSentry.PMO@cisa.dhs.gov)

## Key Partner Characteristics

CISA is aiming to partner with select critical infrastructure entities that:

-  Operate networked operational technology systems
-  Have dedicated cybersecurity personnel and cybersecurity monitoring capabilities
-  Produce, distribute, or maintain products or services that are essential to the operation of national critical functions
-  Provide data that supports visibility objectives







For more information:  
[CyberSentry.PMO@cisa.dhs.gov](mailto:CyberSentry.PMO@cisa.dhs.gov)