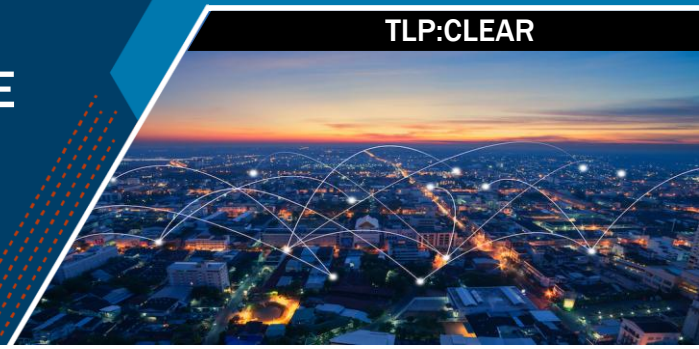
CRITICAL INFRASTRUCTURE CYBERSECURITY SHARED SERVICES PROGRAM



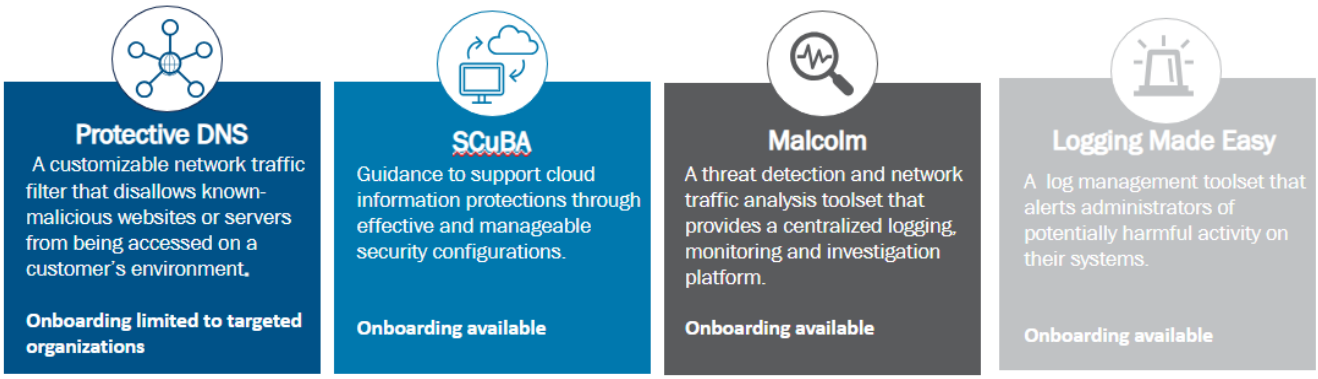
Background

Our Nation's critical Infrastructure (CI) organizations are facing increasing cyber threats from adversarial nation-states, lone wolf hackers, and other malicious cyber actors. In recent years, these attacks have intensified in both volume and impact affecting the day-to-day operations of our Nation's CI. CI organizations must adapt, improve, and obtain cybersecurity capabilities to combat these threats as they grow and intensify.

As a response, in FY 2023 U.S. Congress directed the Cybersecurity and Infrastructure Security Agency (CISA) to Program providing scalable commercial cybersecurity shared services that detect cybersecurity threats and mitigate vulnerabilities to CI organizations. To execute this effort, CISA established the Critical Infrastructure Cybersecurity Shared Services Program, which utilizes an evidenced based approach to inform service selection and delivery to the CI community.

CI Program Service Portfolio

The current service portfolio was selected to Program different value propositions and delivery models, each providing unique after-action insights and risk reduction capabilities for CI.



Graphic 1: Program Services

** The Program is funded on an annual basis and future delivery of services depends on congressional funding cycles.*

Who is Eligible to Participate?

Eligibility for CI Program service onboarding is evaluated on a service-to-service basis. Currently, the CI Program team is targeting high risk sectors and organizations for prioritized onboarding using risk-based criteria. SCuBA, Malcolm, and LME are open source tools free to download for any entity.

Targeted sectors eligible for participation currently include:

- Energy
- Water and Wastewater
- Communications
- Healthcare and Public Health
- Transportation System

Learn More

For more information on CISA's Critical Infrastructure Cybersecurity Shared Services Program, its portfolio of services, or participation eligibility, please email ServicesCOE@mail.cisa.dhs.gov

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.