CYBERSENTRY PROGRAM

OVERVIEW

Successful cyberattacks—such as ransomware and distributed-denial-of-service attacks—on our nation's critical infrastructure can have severe consequences for the National Critical Functions (NCFs) that underpin our national security, public safety, and economic prosperity.

Many organizations have deployed detection capabilities and industry-standard controls to safeguard their enterprises against cyber threats. However, more can be done to help protect the nation's most critical infrastructure from malicious activity—coming from advanced persistent threats (APTs) and other highly sophisticated threat actors—that could result in acute impacts to these NCFs.

CISA's CyberSentry program provides unique visibility into cyber threats targeting critical infrastructure entities that are highly targeted and highly consequential, enabling a true partnership between CISA and each participating organization to provide an added layer of detection and response using sensitive operational information.

CyberSentry is a CISA-managed threat detection and monitoring capability that provides operational visibility into information technology and operational technology (IT/OT) networks within participating critical infrastructure entities. CyberSentry monitors for malicious activity affecting critical infrastructure participants' IT and OT networks, in many cases using sensitive information derived from government or international partners. Obtaining and effectively leveraging this visibility is a core component of CISA's Strategic Plan Objective 1.2 to improve our ability to actively detect cyber threats targeting U.S. critical infrastructure.

HOW DOES IT WORK?

CyberSentry is comprised of integrated hardware and software capabilities that CISA strategically positions at critical infrastructure partner facilities to achieve visibility into internal IT/OT networks. After deploying these capabilities, CISA analysts use their unique insights from national cybersecurity missions to analyze critical infrastructure partner networks for potential threats. If CISA analysts find any cybersecurity concerns, CISA: (1) notifies the critical infrastructure partner, (2) works with them to help resolve the concern, and (3) if necessary, and if requested, can deploy resources to provide additional support. Participation in the CyberSentry program is voluntary and is provided without fees or equipment costs to partners.

WHO CAN PARTNER?

CISA is currently seeking a limited set of critical infrastructure participants who own and operate IT and OT systems that align with associated NCFs and are facing unique risk from sophisticated threat actors. CISA is working with critical stakeholders, such as the National Risk Management Center within CISA and various Sector Risk Management Agencies (SRMAs), on a rigorous and flexible methodology that will assist with the CyberSentry onboarding approach.

It is important to note that each CyberSentry partner must be willing to provide access to in-depth network traffic and other telemetry for the program to effectively provide its unique support. Interested organizations should contact the CISA CyberSentry Program Management Office at CyberSentry.PMO@cisa.dhs.gov.

BENEFITS OF CYBERSENTRY

Becoming a CyberSentry partner offers a critical infrastructure organization an unparalleled opportunity to leverage whole-of-government analytics and response insights for proactive threat detection that augments—but does not replace—existing cybersecurity tools and/or security operations centers.

Participation in CyberSentry will better position an organization to detect and respond to threats across their enterprise and, consequently, reduce risk to their assets. Through CyberSentry, CISA has been able to work closely with its critical infrastructure partners to identify and mitigate multiple cyber threats and incidents that may have gone undetected. These threats have ranged from advanced cyberattacks to inadvertent insider threats. All cyber threats and mitigation efforts learned through CyberSentry are anonymized and shared more broadly across the critical infrastructure community through CISA's reporting publications and alerts.

- The SolarWinds supply chain compromise resulted in significant compromise across the SolarWinds customer base. Due to CyberSentry's unique partnerships, the program was able to analyze data from all partners and identify which partners were at risk within just a few hours. All impacted partners were notified, and the program worked closely and quickly with these partners to confirm remediation of the threat.

- On multiple occasions CISA analysts identified possible malicious activity at partners sites and worked with its partners to identify the root causes of the activity. Through this collaborative partnership, CISA and its partners were able to better understand these malicious activities and were able to identify and stop unauthorized insider actions.

- In one instance, a laptop infected with malware was attached to a CyberSentry partner's IT network. CISA's tools quickly discovered and identified the malware and reported where the laptop had been attached. 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.

- In another instance, a malware signature was detected and CyberSentry discovered that an attacker was actively exfiltrating information. The attacker was also downloading and executing additional tools to expand access on the system. CISA worked with its partner to identify and recover information that had been captured. Within a few hours of the attacker's initial access, CyberSentry delivered a report to its partner detailing the data that had been exposed and provided a preliminary analysis of the malicious tools that had been added to the network. After conferring with CISA analysts, the partner was able to isolate infected systems within hours, eliminating the threat.

Through effective and efficient lines of communication, trust, and collaboration, CISA and critical infrastructure entities are enabled and empowered to build a more robust and collective cyber defense for the nation.