SECURITY INTELLIGENCE

Delivery of timely and relevant security intelligence from NH-ISAC's Global Situational Awareness Center. Security intelligence partners include US DHS, HHS, FBI, the National Council of ISACs (representing all critical infrastructure ISACs), and Dell SecureWorks.

INFORMATION SHARING

Soltra Edge - Industry-leading automated, and systematic two-way intelligence information sharing platform compliant to STIX™ and TAXII™.

Vorstack Automation and Collaboration Platform (ACP) - Automated intelligence into actionable intelligence supporting incident response.

COORDINATED RESPONSE

National Health Cybersecurity Communications and Control (NH-CCC) - Unified and secure communications platform planning, managing, exercising and directing response activities (cell, landline, text, e-mail, secure voice, secure video, radio).

LEADING PRACTICE

Access to leading practice and supporting technologies via NH-ISAC trusted partners.

UNIQUE CAPABILITIES

Enable NH-ISAC member firms to advance their information security practices while effectively leveraging scarce resources, thereby significantly improving health sector cyber resilience.

National Health ISAC

Membership Services

Securing the resilience of the nation's healthcare and public health critical infrastructure depends upon advancing the ability to prepare for and respond to threats and vulnerabilities. Moving from a 'reactive' to a 'proactive' security stance requires a full spectrum of capabilities enabled through a trusted community to share vital cybersecurity information, significantly improving critical decisions and resiliencing of systems essential for the health sector. As the nationally recognized ISAC for the nation's health sector by US HHS, US DHS, and the National Council of ISACs; NH-ISAC is entrusted to meet these challenges via a member-driven culture of shared trust supporting security intelligence exchange, coordinated response, and security leading practice availability.

NH-ISAC members receive the following industry-leading services/capabilities as part of their membership agreement:

- **License to Soltra Edge** - The leading automated threat intelligence sharing management platform developed in a strategic venture (Soltra) between the Financial Services ISAC (FS-ISAC) and The Deposit Trust & Clearing Corporation (DTCC). Soltra's mission is to design and deliver solutions that increase resilience to cyber and physical risks and threats for critical sector entities worldwide. Soltra Edge champions the use of standards- based cyber threat intelligence (STIX™ + TAXII™) repositories for critical infrastructure entities, including ISACs, CERTs, etc, each acting as hubs, creating secure trusted environments where members can securely share cyber threat intelligence. Soltra-Edge can be utilized as a stand-alone or connect to third-party SIEMs.

  STIX™ (Structured Threat Information eXchange) - Led by MITRE and US DHS, community-driven cyber threat intelligence standardized language (Language Constructs - Observable, Indicator, TTPs, Incident, Exploit Target, Campaign, Threat Actor, Course of Action)

  TAXII™ (Trusted Automated eXchange of Indicator Information) - Secure and automated cybersecurity intelligence transport mechanism for STIX™ formatted information.

- **License to the Vorstack Automation and Collaboration Platform (ACP)** - Cybersecurity intelligence sharing capability and threat management platform leveraging STIX™ and TAXII™. ACP automates turning threat data into actionable intelligence and into incident response - reducing discovery and response time, automating manual tasks, organizing relevant information, providing alerts/early warnings, and building "Neighborhood Watch" environments among Trusted Partners. ACP connects to third-party SIEMs and security log management tools (automating ingestion, querying and reporting).

- **Sonatype Application Health Checker** - Utility enabling members to run a scan of commercial software products to determine the bill of materials of open source frameworks used in the development of software. Enables member organizations to understand the risk of the use of open source components.

- **BSIMM (Building Security into Maturity Model)** - Software Security Maturity Assessment - Discounted price offered by Cigital. BSIMM was built entirely from observations made studying sixty-seven real software security initiatives. BSIMM does not tell you what you should do; instead, it tells you what everyone else is actually doing. BSIMM-V describes 112 activities organized in twelve practices organized into 4 domains (Governance, Intelligence, SDL Touchpoints, Deployment). Each activity is given an objective, a description, and one or more real examples.

National Health
Information Sharing & Analysis Center
(NH-ISAC)

Global Situational Awareness Center
AMF Building, NASA Causeway West
NASA/Kennedy Space Center
Kennedy Space Center, FL 32899