Cyber Threat Intelligence and Incident Coordination Center (C³)

Protecting the Healthcare Industry from Cyber Attacks

July 2014
Vulnerabilities in Healthcare

The healthcare industry is not alone in facing increasingly sophisticated and targeted attacks by cyber criminals, but it faces unique risks to its infrastructure and ability to protect sensitive health, personal, and financial data. Organizations of all types, including health systems and plans, pharmacy benefit managers, and pharmaceutical manufacturers, are all at risk from cyber attacks by numerous individuals and groups seeking to gain unauthorized access to their information systems for financial gains or political reasons.

Compounding the issue for the healthcare industry is the lack of awareness, coordination, best practices, and education to address increasing cybersecurity threats and attacks. Healthcare information systems are inherently vulnerable to these attacks with their containment of consumer data, intellectual property and trade secrets, reliance on interconnectedness of industry participants, and advancements required to support new technology initiatives. The risk of disruption to business operations and chaos associated with attacks on electronic health record systems (EHRs) and medical devices necessitate a significant need to prioritize efforts and raise security awareness across the industry.

Healthcare organizations need support that includes anticipatory alerts of future cyber attacks, early identification of cybersecurity attacks that have occurred, coordination of response activities, and timely analysis of cyber threats and attacks specific to their industry and their unique business operations, specifically those vulnerabilities associated with EHRs and medical devices.

Community Defense and Proactive Alerting Approach

Created to provide this critical support and protect the U.S. healthcare industry from disruption by cyber attacks, the HITRUST Cyber Threat Intelligence and Incident Coordination Center (C³) relies upon a community defense and proactive alerting approach to enable the industry’s preparedness and response to cyber threats and attacks. It facilitates predictive intelligence, early identification, coordinated response and incident tracking, as well as knowledge sharing and enhanced preparedness for healthcare organizations challenged by cyber attacks.

An effective security posture requires anticipatory, predictive intelligence to enable an organization to stay ahead of these threats, assess risks, and take appropriate defensive actions. With the actionable threat intelligence provided through the HITRUST C³, healthcare organizations benefit from the avoidance of costs associated with post-event recovery and remediation, as well as the prevention of theft, destruction, and/or public release of critical data.
Cyber Threat Analysis and Intelligence Capabilities

The HITRUST C³ provides cyber threat warning and intelligence services to help healthcare organizations prioritize their cybersecurity efforts and raise security awareness by informing them of general and sector specific threats impacting the industry. This advanced level of healthcare-specific knowledge allows an organization to distill the noise of wider threats and focus on potential targeted threats. The service includes information from key government partners such as the Department of Homeland Security and U.S. Department of Health and Human Services (HHS) and is the result of a partnership between HITRUST and Booz Allen Hamilton, a global strategic consulting and cyber security firm servicing federal government, international and commercial companies across multiple industry sectors.

The center is focused on cybersecurity threats and events targeted at healthcare organizations in areas, including, but not limited to, networks, mobile devices, workstations, servers, applications, and medical devices. The center is also working with HHS to timely share various incident information and for participation in the Critical Infrastructure Information Sharing and Collaboration Program (CISCP).

With a subscription to the HITRUST C³, organizations have access to services in three key areas focused on improving cyber threat intelligence in the healthcare industry:

- **Anticipatory threat intelligence** provided through daily alerts and warnings of future attacks that may threaten a healthcare organization. The probability-based warnings of future cyber attacks make it possible for an organization to anticipate an attack, understand the chances of an attacker’s success, and take proactive action as needed.

- **Community situation awareness** provided with daily intelligence summary products that highlight key threats, incidents, and trends of global threat actors. These daily threat intelligence services will improve an organization’s ability to address risks and questions regarding global threats.

- **Customized alerting and warning service** tailored to the specific risks and threats for each subscriber, ensuring that the resulting threat intelligence is actionable and relevant to their organization.

New and Expanded Services

- More frequent anticipatory threat intelligence with probability-based warnings of future cyber attacks

- Improved community situation awareness with daily intelligence on key threats, incidents, and trends of global threat actors

- Increased customization of alerting and warning service tailored to the specific risks and threats of each subscriber
Organizations can also use the HITRUST C³ to submit potential malicious information found in their information technology environments so as to gain insight into threat sources and better prioritize their efforts to remediate, repair, and prepare for future attacks. Intended for multiple user groups—operations, investigators and chief information security officers—the center also facilitates access to industry-wide resources, enables instantaneous collaboration for support of suspicious incidents or ongoing attacks, and allows for automated notifications and escalations for cyber attacks and threats.

With a subscription to the HITRUST C³, organizations may choose from three tiers of pricing that package a combination of the following deliverables:

<table>
<thead>
<tr>
<th>Products &amp; Services</th>
<th>What You Get</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber Threat Alerts</strong></td>
<td>Anticipatory cyber threat alerts and warnings of future attacks across the healthcare industry based upon probabilities. Proactive hunting and monitoring of threat actor motivations, intentions, objectives, and capabilities (e.g., nation states and their proxies, hacktivist groups, crime syndicates, and rogue insiders).</td>
</tr>
<tr>
<td><strong>Cyber Threat Reports</strong></td>
<td>Periodic notification of cyber threats to healthcare organizations. Reports are produced for all standing intelligence analysis needs, based upon areas of interest.</td>
</tr>
<tr>
<td><strong>Cyber Threat Intelligence—Daily, Weekly and Monthly</strong></td>
<td>Global compendium of actionable cyber threat intelligence and critical developments of interest with a focus on the actions of nation states, known hacktivist groups and criminal syndicates. Detailed trend and behavioral pattern analysis linking cyber events to global economic and geopolitical events delivered through healthcare industry-specific executive summaries that provide concise insights on newly discovered or updated malicious software (malware), vulnerabilities or exploits.</td>
</tr>
<tr>
<td><strong>Intelligence Analyst Questions &amp; Answers</strong></td>
<td>Questions and answers clarifying any content in the reports and products on an as needed basis through the HITRUST C³ secure portal.</td>
</tr>
<tr>
<td><strong>Monthly Calls with Intelligence Analysts</strong></td>
<td>Threat intelligence analysts discuss key threats and trends, and forecast the most probable threats in the near-term. This call provides an opportunity for organizations to ask questions about the threat intelligence products, and includes an executive summary presentation.</td>
</tr>
</tbody>
</table>
Delivered via a Secure and Collaborative Platform

Enabling the delivery of the services through the HITRUST C³ is a unique, collaborative, and trusted platform for vulnerability reporting, knowledge sharing, and collaboration. The platform is the tool that supports the community defense model for the overall center and enables the input and output for the services provided.

Learn More and Subscribe

With the alerting and distribution of relevant and actionable information on cybersecurity threats and events, the HITRUST C³ is able to manage a major industry concern and move the industry forward through predictive alerts, early identification, and shared corrective actions and lessons learned.

Healthcare organizations of all types and sizes can subscribe to the HITRUST C³ for healthcare specific anticipatory alerts of future attacks and in-depth threat intelligence. Community-based pricing offers financial savings for subscribers to the service.

To learn more about the HITRUST C³ or subscribe, visit www.HITRUSTalliance.net/cyber-threat-intelligence.
For more information on HITRUST go to www.HITRUSTalliance.net