Health Industry Cyber Threat Information Sharing and Analysis

Annual Review of HITRUST Cyber Threat XChange (CTX)
Summary of Findings and Recommendations

Public Discussion Document
In 2012, in response to an increase in cyber threats and cyberattacks targeted at healthcare organizations and a general lack of awareness, coordination, best practices and education for addressing such threats and attacks, the Health Information Trust Alliance (HITRUST) established a Cybersecurity Incident Response and Coordination Center to provide crucial support for the healthcare industry. This support includes facilitating the early identification, analysis and distribution of cybersecurity threat and attack information, and industry coordination of response activities.

In 2015, HITRUST updated its Cybersecurity Incident Response and Coordination Center by deploying a more robust and sophisticated infrastructure to support automated collection, comprehensive analysis, detailed alerting, and standards-based distribution, known as the HITRUST Cyber Threat XChange (CTX).

On a routine basis, HITRUST reviews the performance of its programs and services compared to stated objectives, assumptions, user satisfaction, and other metrics established for its programs to evaluate effectiveness. This Summary of Findings represents a recent review of the HITRUST Cyber Threat XChange (CTX), which includes the following:

1. **Current requirements and guidance regarding the submission of indicators of compromise (IOC) to the HITRUST CTX is deficient and contributes to under-reporting or inconsistent reporting of IOCs**

2. **Current level of IOC collection is not representative of the level of cyber threats being perpetrated against the healthcare industry – nor are complete and timely IOCs available through existing government and other readily available commercial cyber threat sources**

**Additional Recommendations:**

1. Establish detailed requirements for IOC sharing

2. Commence an enhanced IOC sharing pilot to quantify the benefits and identify any issues

3. Evaluate methods to incentivize organizations to participate in cyber threat information sharing
What are the Key Functions to Support Cyber Information Sharing and Analysis?

It is important to understand the various components required for effective cyber information sharing and analysis, including technical, operational and policy.

The diagram identifies the key components:

1. Collection
2. Analytics
3. Threat Modeling, Correlation and Alerting
4. Distribution and Integration
5. Collaboration
What are the Key Functions to Support Cyber Information Sharing and Analysis?

1. **Collection**
   In order to aggregate cyber threat indicators, organizations must have the ability to efficiently and securely submit them in a variety of formats and using many different methods including STIX, TAXII, Custom APIs and online portal.

2. **Analytics**
   Analytics takes the threat indicators submitted and reviews them for completeness and other criteria to evaluate the probability of the threat, whereby providing highly reliable IOCs. This enables a high quality data set to be maintained and allows for easy of prioritization when it comes to assessing which threats need to be handled first. Without applying analytics to the data set, a high false positive rate will be experienced. In order to fully understand the magnitude of the threat, and streamline the analyst workflow, third party context is added to the intelligence ensuring an analyst has as much information as possible regarding the threat and that the IOCs are actionable.

3. **Threat Modeling, Correlation, and Alerting**
   Threat modeling provides users insights into the adversaries behind ongoing campaigns along with the general tactics they used for compromising targets. The usage of threat correlation permits vision into data relationships between threat model components. The alerting functionality assists the SOC team with a warning that an adversary is targeting, attempting to access, or has accessed an organization’s infrastructure.

4. **Distribution and Integration**
   The timely and effective consumption of information into an organization’s existing security infrastructure that can be acted upon is vital. At a minimum, STIX, TAXII and SIEM integration should be supported.

5. **Collaboration**
   The ability to securely collaborate with peers and share strategies, approaches, and experiences on a specific threat or related experiences is an important component in support of knowledge transfer and education.
Cyber Threat Intelligence and Why We Share It

To effectively defend against cyber attacks, an organization needs timely access to relevant, actionable cyber threat intelligence that is provided in a format they can consume. This threat intelligence includes IOCs (i.e., an artifact or observable that suggests that an attack is likely, underway, or that a compromise may have already occurred); the tactics, techniques and procedures (TTPs) of an adversary; the systems and information that they target; and any other threat-related information that provides greater situational awareness to those responsible for defending and responding to threats and incidents.

Cyber threat intelligence is a vital part of cyber defense and incident response. It allows organizations to gather intelligence about the active threats to their environment and implement targeted defensive measures – at both the tactical and strategic level.

The premise behind cyber threat intelligence sharing, sometimes referred to as “cyber community defense,” is the notion that one organization’s “cyber threats and attacks” will be another’s “cyber defense”. More specifically, when one organization detects and shares timely and complete indicators with an information sharing and analysis organization, which in turn is able to quickly evaluate and distribute, it enables others to appropriately defend their environment, by allowing them to adequately prepare in advance of being attacked or, in certain instances, assess their own environment to determine if the threat is already present.

Threat information exchanged within an industry or community of interest can be particularly beneficial because the participating organizations often face adversaries that use common TTPs and target the same types of systems and information.

Benefits of cyber threat intelligence sharing include:

- Improved cyber situational awareness
- Enhanced cyber threat understanding
- Cyber threat correlation
- Greater defensive agility
NIST defines three basic types of indicators:

**Atomic indicators** are simple data elements that cannot be further decomposed (e.g., IP address).

**Computed indicators** are derived from other incident data (e.g., hash value).

**Behavioral indicators** are composite indicators, consisting of atomic and computed indicators joined through combinatorial logic and perhaps enhanced through the inclusion of contextual information.

Organizations with basic network monitoring capabilities should be able to produce atomic indicators and perhaps simple computed indicators from existing data sources. The generation of sophisticated computed indicators or behavioral indicators often requires more advanced tools and analytical processes, and greater technical expertise.

IOCs are a key component to cyber defense, cyber intelligence and cyber sharing, but requirements need to be established and met to realize the potential. IOC, is a shared object that should provide a high degree of confidence that an intrusion may have taken place or that a threat actor is operating within a target environment.

When producing and publishing or sharing indicators, it is important to include metadata that provides context for the indicator by describing how it is to be used and interpreted, how it was observed, and how it relates to other indicators. Metadata may also include handling instructions, sensitivity designations, and provenance information (e.g., what tool was used to acquire the data, how the data was processed). Publishers of indicators should also consider assigning a confidence level to the information that it intends to share. The confidence level represents the degree of certainty that the publisher asserts for a specific data element, relationship, or data set. Users of the information may take this confidence level into consideration when using this information as basis for decisions. As indicators are created, aggregated or enriched, their sensitivity and classification should be reevaluated; in some cases it may be necessary to sanitize the data or place restrictions on its use or dissemination.

The challenge when sharing IOCs is that not all indicators are created equal – as mentioned above. In many cases today, only atomic indicators without the corresponding metadata are shared. For example, many indicators are hashes of malicious files detected within an organization. But research has found that 90% of malicious files today are only detected on a single device. This means the majority of malicious hashes would not significantly improve protection outside of the original victim’s network. Also, many of these indicators may be days, weeks, and even months old due to the lack of trained personnel and processes available to most organizations to detect and share. Research has also shown that over 60% of malicious domains are only alive for one hour or less, which means sharing must occur in less than an hour to be effective related to malicious domains and associated threats.

For cyber threat intelligence sharing to be most effective the IOCs must include the following characteristics:

**Specificity:** At a level of detail that addresses the salient facts about the threat, allows the recipient to understand if and how the threat may affect them and, if appropriate, implement defenses or counter measures.

**Timely:** Provide ample opportunity for the recipient to anticipate the threat and prepare a suitable response. The timeliness of intelligence is context-dependent (i.e., cyber-relevant) and needs to take into account the volatility of the threat, the speed of attack, and the capabilities of the adversary.

When these two characteristics are met, recipients can develop a suitable response to the threat. Cyber threat actors often use similar approaches and tools against multiple organizations supporting the value of timely information sharing with other organizations.
What Level of Cyber Threat Sharing is Occurring With HITRUST CTX?

The information below highlights the desire by organizations to access cyber threat information in the HITRUST CTX (either through SIEM integration, STIX/TAXII server or portal). What is also highlighted is that only a small percentage of organizations are sharing information back with the HITRUST CTX, and that less than half of those shared IOCs are considered actionable:

![Bar Chart]

Month of August 2015

Of the IOCs contributed to CTX during the sampling period, only 50% were considered actionable, making the other 50% unactionable*

*Unactionable is defined as an IOC that “as is” does not provide a sufficient confidence for a preventative or defensive action to be taken without a significant risk of a false positive. Often these indicators lack relevant metadata or, if correlated with other indicators, can provide sufficient confidence for actions to be taken, but only with the combined context. As such, there is not enough information to form a high basis for blocking.
What is Impacting the Ability for Organizations to Share IOCs with the HITRUST CTX? (1 of 2)

Through interviews and surveys with participants and evaluation of other approaches, a number of findings and recommendations have been identified(1).

It is hard to share what you don't know. Many organizations were unaware of the cyber threats and attacks being perpetrated against their environment.

This aligns with ongoing concerns about the level of maturity and available resources within organizations across the healthcare industry to effectively detect and defend against cyber threats. It also supports the value that cyber threat information sharing can address if the information is timely, actionable and consumable in helping organizations better detect cyber threats and defend their environments.

As part of the evaluation, a number of Breach Detection Systems where deployed – specifically, the Trend Micro Deep Discovery Appliances (DDA)(2) at CTX participating organizations that collected data over the month of August 2015. These breach detection appliances from Trend Micro and similar devices in this market category are designed to identify malicious activity based on evaluations of suspicious content, communication and behavior. Information collected by these appliances was compared with information that these same organizations reported to HITRUST CTX.

During the reporting period, the collection devices identified 286 times more unique file hashes, of which 24% were identified as not being seen previously by CTX(3) (including from industry, government, and third party feeds).

Accuracy, timeliness, and completeness of an IOC directly relates to making an indicator actionable. IOCs become less valuable over time and need to contain a minimum dataset in order for them to deliver optimum value.

The detection and reporting of an IOC needs to focus on speed – and that comes from automation, which is not the current model for most participating organizations.

Reporting more than just a single IOC data point, including other metadata associated with the IOC, allows the correlation of additional threat data to be done. Leveraging automation for the reporting of IOC data to the other shared organizations can also improve the protection against identical or similar threats affecting them. This automation also removes any potential mistakes or non-sharing of critical IOC data. Ultimately, the objective of an effective threat intelligence sharing model would be one in which the collection, detection, and reporting of new IOCs is automated and seamless to the participating organizations and provides them actionable intelligence to minimize their risks of being compromised.

During the evaluation, the DDA’s were able to provide a complete set of IOCs within 5 minutes of detection – without any human intervention.

A number of factors impact the ability of an organization to share complete and timely IOCs, the most common being technology infrastructure and availability of personnel.

---

(1) It should be noted that HITRUST previous analysis identified issues and recommendations relating to alerting, reporting, and distribution with the HITRUST CTX. Follow-up discussions indicate that these issues where adequately addressed through recent updates and enhancements.

(2) DDA uses advanced threat technologies like custom sandboxes, heuristic scanning rules, exploit code analysis, and Command & Control (C&C) communications which are typically not part of a traditional security suite.

(3) It should be noted that participating organizations did not limit their submission of IOCs due to liability or other concerns that would have reduced what IOCs where shared. Although we had heard this concern previously, we have worked to ensure appropriate liability protections are in place through participation agreements, and anonymization techniques.
Correlating IOCs across multiple sites created additional observations such as:

- The attacker seems to have compromised web servers hosted within the United States, staging them for future downloads.
- The attacker favors PHP-based backdoor web shells.
- Their operational time matches US-local time coinciding with active business hours for time zones within the United States – geo-IP location of the affected healthcare institution indicates Central Time Zone, (UTC-06:00).

An example of an IOC that includes more companion data is as follows:

- Timestamp: 2015/06/15 12:59:12 PM
- Region: US
- IP address: 143[redacted]53
- Industry: Healthcare
- Product: DDI 3.8
- Detection: HKTL_MADSHELL
- SHA1: 3f86bd230c01c54d356d910c5ba161b2857ee5fb
- File type: Script
- Protocol: HTTP
- URL: http://www.em[redacted]m/prophoto/thumb/mad.jpg
- Domain rating: Education
- Web server location: Florida, United States
Key Findings and Recommendations (1 of 2)

Finding

Current requirements and guidance regarding the submission of IOCs to the HITRUST CTX is deficient and contributes to under-reporting or inconsistent reporting of IOCs.

Recommendation

Define specifications and requirements relating to the submission of IOCs needs to be published by HITRUST for use by the HITRUST CTX.

Specifications and guidance should include at a minimum:

- **Level of Detection and Reporting**: Organizations participating should possess the technical and operations capabilities to detect and report (some level of ) IOCs

- **Duration from Detection to Submission**: Duration from detection that organizations should submit IOCs

- **Completeness of IOC**: IOCs submitted should contain a defined set of metadata based on the IOC type

Recommendations may not apply universally, and considerations should be given on how to best apply, based on various factors.

This guidance is crucial in supporting more actionable indicators, cyber threat correlation, greater defense agility, and the value in helping an organization mitigate cyber risks. Additionally, analysis should be performed to determine if the data can support predictive modeling, such as potential industry-specific attacks or the next phase of an attack campaign by a known threat actor or group.

The data clearly demonstrates that participants in a sharing community are today primarily consumers of threat intelligence rather than producers of information. Incentives should be identified to encourage organizations to engage in more active information sharing.
Finding

Current level of IOC collection is not representative of the level of cyber threats being perpetrated against the healthcare industry – nor are complete and timely IOCs available through existing government and other readily available commercial cyber threat sources.

Recommendation

1. Explore leveraging advances in information security technology, specifically breach detection technology, to address some of the current gaps in more efficient and effective IOC collection in support of cyber threat information sharing
2. The HITRUST CTX platform should be updated to allow automated collection of IOCs from Breach Detection systems meeting a defined requirement
3. HITRUST should evaluate seeding the healthcare industry with Breach Detection Systems distributed across various segments of the industry to enable IOC collection spanning major segments
4. Risks and liability concerns with automated sharing need to be appropriately addressed for organizations to embrace the technology for this purpose
5. Costs and other resource requirements need to be fully understood

Notes:

- Although augmenting the sharing process with technology will benefit the IOC collection and an organization’s cyber awareness, it does not address other cyber preparedness and response maturity aspects.
- HITRUST CTX has already been updated to support collection from Trend Micro Deep Discovery Appliance
**Next Steps and Action Items**

**Establish Requirements for IOC Sharing**

A comprehensive set of requirements need to be developed that define specifics and expectations for IOC sharing. They include the ability of an organization to detect cyber threat activity, the time it takes to share IOCs, and the level of detail associated with the IOCs.

1. **Organizational Cyber Security Detection Effectiveness:** Organizations should deploy technology capable of a security effectiveness, as defined by NSS Labs Breach Detection Systems (BDS) Testing, over 90%. The technology should be deployed to evaluate at least 50% of an organization’s inbound and outbound SMTP, HTTP, HTTPS, FTP, and IM traffic. Cyber Security Detection Effectiveness is defined as the ability to accurately detect and log IOCs, and attempted breaches with a high level of confidence to avoid false positives. Detection must include accurately and effectively identifying exploits, malware, and offline infections. HITRUST CTX is leveraging the methodology developed by NSS Labs for their Breach Detection Systems (BDS) evaluation. More information can be found [here](#).

2. **Timeliness of Submission:** Organizations should be capable of submitting IOCs to HITRUST CTX within 10 minutes of detection. Submission can occur through a API or Threat Stream Optic Link.

3. **Required IOC Attributes:** For cyber threat intelligence sharing to be most effective the IOCS must include a certain level of detail that addresses the salient facts about the threat; allows the recipient to understand if and how the threat may affect them; and, if appropriate, implement defenses or counter measures. It is expected that IOCs submitted will not contain any submitting entity information other than the organizational type submitting. The proposed IOC dataset is attached as Addendum “A”.

Next Steps and Action Items

Enhanced IOC Sharing Pilot

- Commence a pilot to validate the effectiveness, quantify the benefits, and identify any impediments or risks associated
  - Identify pilot structure, approach, and success measures
  - Determine any legal or liability protections that need to be implemented or addressed prior to commencing
  - Confirm pilot group participants—limited to 10 organizations
  - If requested, Pilot group to be provided with Trend Micro Deep Discovery Appliances and engineering support
- Pilot should evaluate methods to incentivize organizations to participate in cyber threat information sharing
- Pilot steering committee:
  - Pilot committee chair: Dave Kaercher, Chief Information Officer, Blue Cross Blue Shield Kansas City
  - Pilot should commence in November 2015
About CTX

The HITRUST Cyber Threat XChange (CTX) was created to significantly accelerate the detection and response to cyber threats targeted at the healthcare industry. HITRUST CTX automates the process of collecting and analyzing cyber threats and distributing actionable indicators in electronically consumable formats that organizations of varying sizes and cyber security maturity can utilize to improve their cyber defenses.

Designed to optimize the way organizations defend against cyber-attacks, by complementing traditional signature and anomaly based technologies, CTX delivers a data driven security approach that enables your existing security investments to function more effectively.

Advanced intelligence specific to the healthcare industry includes: intelligence of the top threat actors observed targeting the healthcare sector; suspicious domain registrations associated with your organizations domain; key word alerting for compromised credentials; indicators of compromise (IOCs) specific to healthcare industry; integrated sandboxing for malware analysis; access to threat intelligence circles; collaboration, and SIEM integration.
Other HITRUST Cybersecurity Programs

**HITRUST Cyber Threat Intelligence and Incident Coordination Center**: The Cyber Threat Intelligence and Incident Coordination Center provides cyber threat warning and threat 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.

**Cyber Threat Briefings**: As the number of cyber-attacks targeted at the healthcare industry rises, HITRUST is partnering with the U.S. Department of Health and Human Services to conduct monthly cyber threat briefings to aid organizations in better understanding current and probable cyber threats relevant to the healthcare industry and to share best practices for cyber threat defense and response.

More Info: [https://hitrustalliance.net/cyber-threat-briefings/](https://hitrustalliance.net/cyber-threat-briefings/)

**CyberRX**: CyberRX is a series of no cost, industry-wide exercises coordinated by HITRUST, in conjunction with the U.S. Department of Health and Human Services, with the mission to mobilize healthcare organizations and explore innovative ways of improving preparedness and response against cyber attacks intended to disrupt the nation’s healthcare operations.

More Info: [https://hitrustalliance.net/cyberrx/](https://hitrustalliance.net/cyberrx/)

**Cyber Discovery Study**: HITRUST is undertaking the first empirical and comprehensive study to analyze the methods, severity, and pervasiveness of cyber threats targeting a variety of healthcare organizations. The study will enable a better understanding of the actual magnitude, complexity, relations of cyber-attacks, commonalities of target organizations and data, and degree of cyber threats persisting within organizations. The goal is to accurately identify attack patterns and persistence, as well as the magnitude and sophistication of specific threats across enterprises.

More Info: [https://hitrustalliance.net/cyber-discovery/](https://hitrustalliance.net/cyber-discovery/)
Addendum “A”: IOC Collection Schema

**Confidence**: Numerical value representing indicator confidence (0-100)

**Type**: Type of indicator (URL, IP, Domain, File, Email Address, etc.)

**Classification**: Classification level of the indicator (Public, Private)

**Severity**: Severity of the associated threat (Low, Medium, High, Very High)

**Metadata**: Contextual information associated with the indicator (Threat Name, Source, Threat Type, etc.)

**Value**: The indicator value

**CTX Trust Circles**: Areas within CTX the IOC should be shared

**Threat Score**: Calculated value based on confidence and severity
Addendum “B”: Screenshot

Screenshot showing IOCs received directly from a Trend Micro Deep Discovery Appliance
About HITRUST

Founded in 2007, the Health Information Trust Alliance (HITRUST) was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with public and private healthcare technology, privacy and information security leaders, has championed programs instrumental in safeguarding health information systems and exchanges while ensuring consumer confidence in their use.

HITRUST programs include the establishment of a common risk and compliance management framework (CSF); an assessment and assurance methodology; educational and career development; advocacy and awareness; and a federally recognized cyber Information Sharing and Analysis Organization (ISAO) and supporting initiatives.

www.HITRUSTalliance.net