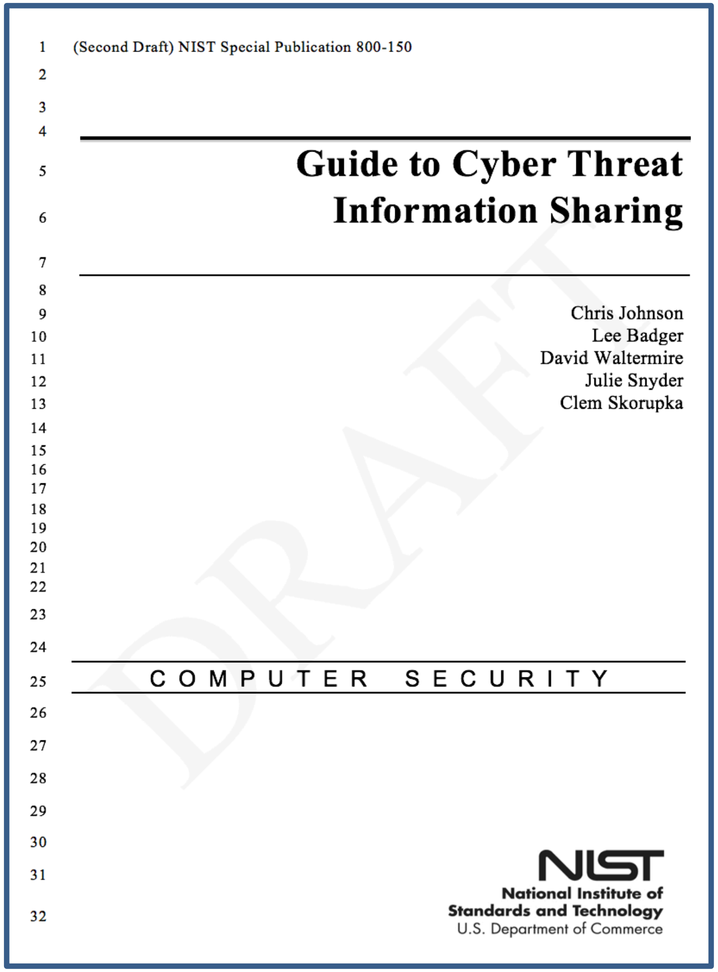
NIST SP 800-150: Guide to Cyber Threat Information Sharing

Chris Johnson, NIST

August 16, 2016

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-150 2nd DRAFT



(Second Draft) NIST Special Publication 800-150

Guide to Cyber Threat Information Sharing

Chris Johnson
Lee Badger
David Waltermire
Julie Snyder
Clem Skorupka

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Why Share?

- Collective defense
- Improved security posture
- Knowledge enrichment through collaboration
- Enhanced situational awareness
- Augment internal collection with external sources
- Greater defensive agility
- Enhanced decision-making

What are some of the Challenges?

- Establishing trust
- Interoperability and automation
- Protecting sensitive information
- Integrating threat information into decision-making processes
- Complying with legal and regulatory requirements
- Limiting attribution
- Infrastructure and personnel

Sources of Cyber Threat Information (CTI)

Internal

- Sensors (e.g., IDS, AV)
- Systems (System, Network, and Application logs)
- Tools (e.g., Forensic toolkits, network diagnostics)
- Repositories (e.g., SIEM, Ticket Management Systems)
- Personnel

External

- Open, public sharing communities and resources
- Government sources
- Sector peers and business partners
- Vendor alerts and advisories
- Commercial Services

Uses of CTI

- Prioritize the implementation of security controls
- Develop user training and awareness campaigns
- Capital planning and investment
- Enhance detection capabilities
- Inform response and recovery operations

Types of CTI

Types of cyber threat information include**:**

- **Indicators**
- **Tactics, Techniques, and Procedures**
- **Threat Actors**
- **Vulnerabilities**
- **Cybersecurity Best Practices**
- **Courses of Action**
- **Tools and Analysis Techniques**

Types of CTI Indicators

“A technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred.”

Examples:

- **IP addresses**
- **Domain names**
- **File names, sizes**
- **Hashes of file contents**
- **Service names**
- **Altered configuration parameters**

Types of CTI
Tactics, Techniques, and Procedures

The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

Examples**:**

- **Spear phishing email**
- **Social engineering**
- **Website (drive-by attack)**
- **Exploit operating system or application vulnerability**
- **Removable media**
- **Obfuscation techniques**

Types of CTI
Threat Actors

Information regarding the individual or a group posing a threat.

Examples:

- **Affiliation**
- **Identity**
- **Motivation**
- **Relationships**

Types of CTI
Vulnerabilities

A vulnerability is a software flaw that can be used by a threat actor to gain access to a system or network.

- **Overview**
- **Impact**
- **Technical Details**
- **Affected systems, platforms, and versions**
- **References**
- **Mitigations**

Types of CTI
Cybersecurity Best Practices

Commonly used cybersecurity methods that have demonstrated effectiveness in addressing classes of cyber threats.

Examples:

- **Response actions (e.g., patch, configuration change)**
- **Recovery operations**
- **Detection strategies**
- **Protective measures**

Types of CTI
Courses of Action

Recommended actions that help to reduce the impact of a threat**:**

- **Detect (e.g., add or modify an IDS signature)**
- **Protect (e.g., implement multi-factor authentication)**
- **Respond (e.g., block network traffic to C&C server)**
- **Recover (e.g., restore base system image)**

Types of CTI
Tools and Analysis Techniques

Recommended tools (e.g., log extraction/parsing/analysis, editor)

Useful tool configurations (e.g., capture filter for network protocol analyzer)

Signatures (e.g., custom or ”tuned” signatures)

Extensions (e.g., connectors or modules)

Code (e.g., algorithms, analysis libraries)

Visualization techniques

Desirable Characteristics of CTI

Timely – allow sufficient time for the recipient to act

Relevant – applicable to the recipient’s operational environment

Accurate – correct, complete, and unambiguous

Specific – provide sufficient level of detail and context

Actionable – provides or suggests an effective course of action

Establishing a CTI Sharing Capability

- Set Goals and Objectives
- Identify Internal Sources of CTI
- Define Scope
- Establish Sharing Rules
- Join a Sharing Community
- Plan for Ongoing Support

Establishing a CTI Sharing Capability: Set Goals and Objectives

CTI Sharing is not the objective

Needs to align with mission, business, and security needs

Talk with organizational stakeholders

Secure approval and buy-in from leadership, legal team and privacy officials

Address specific problems

Reduce risk

Enhance cybersecurity practices

Requires prioritization

Goals need to be revisited over time

Establishing a CTI Sharing Capability: Identify Internal Sources of CTI

Where does CTI "live"?

- **Operating system, service, and application logs**
- **Router, Wi-Fi, remote services logs**
- **System and application configuration settings and states**
- **Firewall, IDS, and Antivirus logs and alerts**
- **Web browsers history, cookies, and cache**
- **Security Information and Event Management (SIEM)**
- **Email systems**
- **Help desk ticketing systems, incident management/tracking system, and people**
- **Forensic toolkits and dynamic and/or virtual execution environments**
- **Diagnostic and monitoring tools (PCAP & protocol analysis)**

Establishing a CTI Sharing Capability: Define Scope

Establish the scope of information sharing based on:

Current capabilities

Information availability

Information needs

Available resources

Degree of automation

Establishing a CTI Sharing Capability: Sharing Agreements

Sharing agreements should describe the rules regarding:

- **Types of information that can be shared**
- **Conditions and circumstances when sharing is permitted**
- **Distribution to approved recipients**
- **Identification and redaction of PII and other sensitive information**
- **Use of automated information exchange mechanisms**
- **Non-attributed information exchange**
- **Information handling requirements and designations**

Establishing a CTI Sharing Capability: Sharing Agreements

Sharing rules are expressed in:

- **Memorandums of Understanding**
- **Service Level Agreements**
- **Nondisclosure Agreements**
- **Framework Agreements**
- **Informal Arrangement**

Established sharing communities often have templates

Establishing a CTI Sharing Capability: Sharing Agreements

- Talk with your organization's legal and privacy officials
- Have them review the types of information you plan to share and point out potential risks.
- Determine appropriate handling designations
- Reevaluate when:
  - Regulatory or legal requirements change
  - Organizational policy is updated
  - New information sources are introduced
  - Operating/threat environment or risk tolerance changes
  - Organizational mergers, realignments, and acquisitions occur

Establishing a CTI Sharing Capability: Join a Sharing Community:

Potential sharing partners and resources:

- **Government (e.g., US-CERT, NVD, CSRC)**
- **Industry sector peers (e.g., ISACs)**
- **Threat intelligence vendors**
- **Supply chain partners (PSIRTs)**
- **Regional/Local Sharing Orgs**
- **Vendor consortiums**
- **Open source intelligence repositories**

Establishing a CTI Sharing Capability: Join a Sharing Community:

Some Considerations:

- Membership fee structures
- Eligibility requirements
- Types of CTI that the community exchanges
- Delivery mechanisms, formats, and protocols used
- Frequency and volume of information provided
- Quality and timeliness of the information provided
- Terms of use and other restrictions
- Security and privacy controls provided

Establishing a CTI Sharing Capability: Ongoing Support

Implement a support plan that addresses personnel, funding, infrastructure, training, and processes needed for:

- **Collecting and analyzing CTI from internal and external sources**
- **Implementing and maintaining protective measures**
- **Supporting monitoring and threat detection capabilities**
- **Membership or service fees**

NIST CTI Programs and Resources

Standards, Specifications, and Guidelines

- NIST SP 800-61
- NIST SP 800-150
- NIST IR 8057
- Others

Data Repositories and Reference Data Sets

- National Vulnerability Database (NVD)
- NVD and National Software Reference Library Integration
- National Checklist Program
- United States Government Configuration Baselines

Product Conformance Testing and Testing Tools

- SCAP 1.2 Product Test Suite Content
- SCAP Content Validation Tool (SCAPVal)
- SCAP 1.2 Validation Program

Research

- Multidimensional Cybersecurity Analytics
- Automated Generation of Indicators Using OVAL

Other Federal CTI Programs and Resources

- DHS Enhanced Cybersecurity Services (ECS) Program
- DoD Defense Industrial Base (DIB) Cybersecurity Program
- DHS Cyber Information Sharing and Collaboration Program (CISCP)
- National Cyber Investigative Joint Task Force (NCIJTF)
- DHS National Cybersecurity and Communications Integration Center (NCCIC)
- FBI Private Industry Notifications (PINs) and FBI Liaison Alert System (FLASH) Reports
- DoE Cybersecurity Risk Information Sharing Programs (CRISP)
- DHS Automated Indicator Sharing Initiative (AIS)
- DoE Cyber Fed Model (CFM) Program
- Department of the Treasury’s Financial Sector Cyber Intelligence Group (CIG)

Other Federal CTI Programs and Resources

CTI Programs include**:**

- **DoD Defense Cyber Crime Center (DC3)**
- **Department of Commerce, National Institute of Standards and Technology, Computer Security Resource Center (CSRC)**
- **DHS Critical Infrastructure Cyber Community (C^3) Voluntary Program**
- **National Security Agency (NSA) Information Assurance (IA) Guidance**
- **Small Business Administration (SBA) cybersecurity best practices**

Information Sharing and Analysis Centers (ISACs)

- Automotive
- Aviation
- Communications
- Defense Industrial Base
- Defense Security Information Exchange
- Downstream Natural Gas
- Electricity
- Emergency Management and Response
- Financial Services
- Healthcare Ready
- Information Technology

Source: National Council of ISACs
https://www.nationalisacs.org

"an ISAC is a trusted, sector specific entity which … collects, analyzes, and disseminates alerts and incident reports to … provide analytical support to government and other ISACs" *

Information Sharing and Analysis Centers (ISACs)

- Maritime
- Multi-State
- National Health
- Oil and Natural Gas
- Real Estate
- Research and Education
- Retail Cyber Intelligence
- Supply Chain
- Surface Transportation, Public Transportation and Over-the-Road Bus
- Water

Source: National Council of ISACs https://www.nationalisacs.org

- Public/private sector security cooperation
- Daily Information Exchange
- Weekly Meetings
- Threat Response & Reporting Guidelines

ISAO Standards Organization

Mission:

"To improve the Nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices."

Working Groups:

- ISAO Creation
- ISAO Capabilities
- Information Sharing
- Privacy and Security
- ISAO Support
- Government Relations

Source: ISAO Standards Organization
https://www.isao.org

Participating in CTI Sharing Relationships

Participating in CTI Sharing Relationships Ongoing Communication

Meet regularly with trusted sharing partners to:

- **Discuss current threats**
- **Share or develop mitigation strategies**
- **Provide training and develop skills**
- **Mentor new community members**
- **Develop key practices and resources**
- **Build rapport and foster trust**
- **Share technical insights**

Participating in CTI Sharing Relationships Consume and Respond to Alerts

Upon receipt of a security alert, advisory, or bulletin organizations should have procedures in place for:

- **Establishing that the alert is from a trusted, reliable source**
- **Seeking confirmation from an independent source (if necessary)**
- **Determining if the alert affects systems, applications, or hardware that the organization owns or operates**
- **Characterizing the potential impact of the alert**
- **Prioritizing the alert**
- **Determining a suitable course of action**
- **Taking action (e.g., changing configurations, installing patches, notifying staff of threats)**

Participating in CTI Sharing Relationships Consume and Use Indicators

The ingest and use of indicators from external sources is often a multi-step process that includes, if not all, of the following activities:

- **Validation – verifying the content's quality, integrity, and provenance**
- **Decryption – transforming encrypted files or data streams back to their original format**
- **Decompression – unpacking compressed content**
- **Extraction – parsing, identifying, and extracting indicators of interest**
- **Prioritization – processing indicators based on relative importance**
- **Categorization – reviewing indicator metadata to determine security designations and handling requirements**

Participating in CTI Sharing Relationships
Indicator Enrichment

What feedback mechanisms exist for:

- **Correcting errors**
- **Making clarifications**
- **Providing supplemental information**
- **Requesting additional information**
- **Suggesting alternate interpretations**
- **Exchanging analysis techniques or results**

Participating in CTI Sharing Relationships Common Data Formats and Automation

- Exchange of information at greater speed through automation
- Less need for human intervention
- Structural and semantic agreement fosters interoperability
- Talk with your security tool vendors
  - Support the use cases you care about
  - Demonstrate interoperability with the tools and repositories you currently use or plan to use
  - Where are they in the ”adoption curve”
  - Formal validation vs. self-assertion
  - Success stories
- Actively participate in standards/specification development efforts

Status and Next Steps

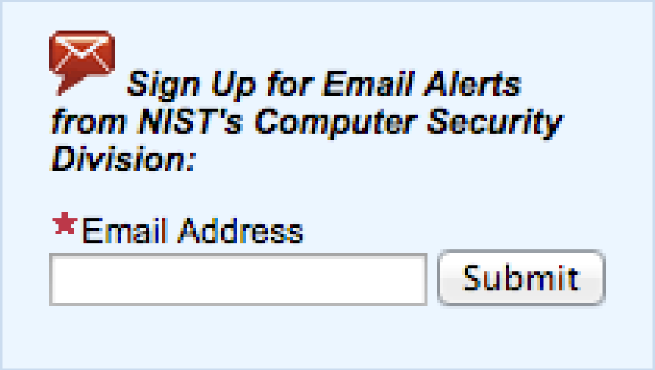
- Completed the review and adjudication of public comments received on the 2nd DRAFT NIST SP-800-150
- Updated the publication based on the comments we received
- Prepared a Final version of SP 800-150 that is entering the NIST publication review and approval process
- Release NIST SP800-150 (Final) and post to the NIST Computer Security Resource Center (CSRC) http://csrc.nist.gov/

A Few Take-Aways

- Use CTI to support all **cybersecurity and risk management functions** (not just incident response)
- Use **automation** to increase **operational tempo**
- **Scope sharing activities** according to organizational capabilities
- Help improve the **quality** of CTI **content, tools and standards**
- Use CTI to better protect **what is important** to your organization
- **Know and understand** the CTI you collect now
- Augment internal collection with **external sources**
- Look for information that is **easier to share** (e.g. threats vs. incidents)
- **Join** a Sharing Community (and get/stay involved)

NIST Computer Security Division Mailing List

Visit the Computer Security Resource Center online at:
http://csrc.nist.gov/



Sign Up for Email Alerts from NIST's Computer Security Division:

*Email Address

Questions?

Chris Johnson

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

chris.johnson@nist.gov