


## Module 4 Working with Information Sources

[Presenter Name]  
[Date]



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

### Agenda

By the end of this module, you will be able to:

- Categorize levels of information sources
- Establish how to work with open-source and proprietary intelligence
- Identify methods for gathering and handling critical information
- Define processes that allow information sharing and exchange
- Practice gathering information from various sources

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

## Section 1: Categorizing Information Sources

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

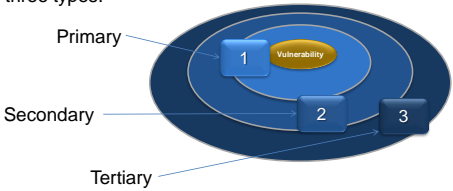
---

---

---

Information Sources and Types

- Information sources provide critical data for CSIRTs that can be used to identify, analyze, and resolve vulnerabilities
- Information sources are then categorized into three types:



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

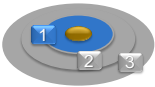
---

---

---

Primary Information Source

A primary information source is, generally, the first person to discover a vulnerability or report it to the CSIRT



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

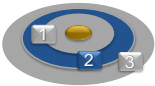
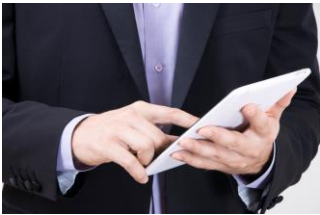
---

---

---

Secondary Information Source

A secondary information source is a security database, article, or journal whose data can be used to analyze and/or resolve the vulnerability



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

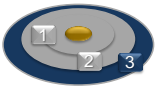
---

---

---

Tertiary Information Source

A tertiary information source is a report that synthesizes data from secondary sources or from your own analysis of similar incidents or vulnerabilities



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

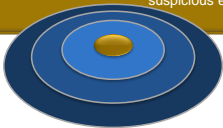
---

---

---

Information Sources in Use

**Vulnerability**  
One of your users finds a URL that asks for a login and password and sends the suspicious email to the CSIRT immediately



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Information Sources in Use

**Vulnerability**  
One of your users finds a URL that asks for a login and password and sends the suspicious email to the CSIRT immediately



**Primary Information Source**  
The CSIRT reads the email from the user and checks the URL in question

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

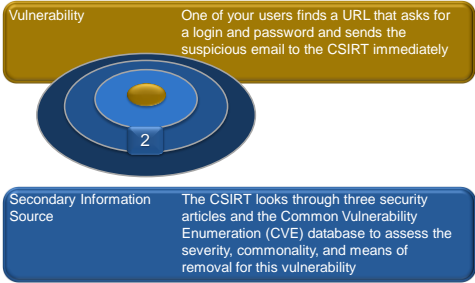
---

---

---

---

Information Sources in Use



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

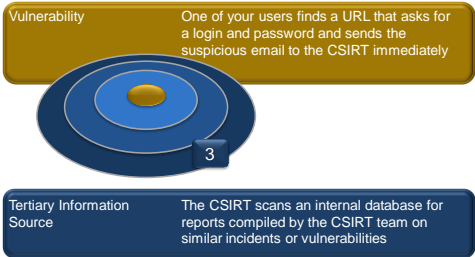
---

---

---

---

Information Sources in Use



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

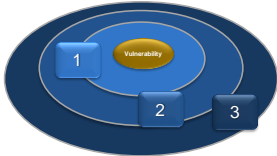
---

---

---

Phishing Example

- Your organization is being targeted by a phishing attack
- You need to gather as much information as possible to resolve the incident
- Classify information as primary, secondary, and tertiary



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Phishing Example: Primary Information

- Who was the intended target of the attack?
- What is the URL and hostname of the attacker?
- What was the social engineering method?



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

---

Phishing Example: Secondary Information

- Who is the owner of the URL and what is his or her location?
- What is the sender's name and location?
- Has anyone already been phished inside organization?
- What type of data has been compromised?
- How was the system initially accessed?
- Which passwords were used to access the system?



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

---

Phishing Example: Tertiary Information

- Are there reports about similar phishing incidents in the past?
- What other attacks, if any, have been documented online on this URL or domain?



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

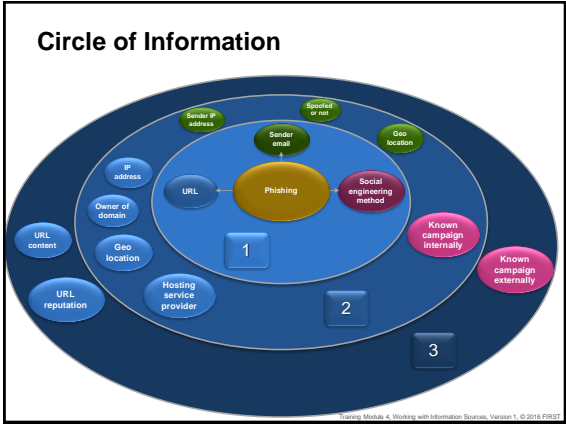
---

---

---

---

---



---

---

---

---

---

---

---

### Learning Check

If the primary, secondary, and tertiary information sources about an incident differ from each other, what do you do?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

### Questions?

What questions do you have about this lesson?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Section 2:  
Types of Information

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---


---

---

Types of Information

Types of common information you might need to gather:

- IP address (source and destination)
- Domain name
- Internet service provider (ISP)
- Email address
- System logs



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---


---

---

---

Open-Source Intelligence

- Open-source intelligence is information made available for public consumption that can be accessed over the Internet by anyone at any time
- Types of open-source intelligence:
  - nslookup
  - ht://Dig
  - Google
  - Social media



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Proprietary Intelligence

- Proprietary intelligence describes a technology owned exclusively by a single company that carefully guards knowledge about the technology or the product's inner workings
- Types of proprietary intelligence:
  - Maltego
  - Deep Magic
  - Cuckoo Sandbox



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Learning Check

What are the protocols in your organization for the types of information that can or cannot be shared, and how the information will be distributed?



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Questions?

What questions do you have about this lesson?



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Section 3:  
Information Gathering Process

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Information Gathering Process



- When researching a vulnerability, the information you collect is your weapon against it, so it is imperative that you be thorough
- When a vulnerability is detected, a CSIRT will need to accumulate all relevant information to identify the threat

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Information Gathering Process



- When researching a vulnerability, the information you collect is your weapon against it, so it is imperative that you be thorough
- When a vulnerability is detected, a CSIRT will need to accumulate all relevant information to identify the threat

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Gathering and Handling Information

- There are two forms of information gathering:  
**proactive** and **reactive**.
- Proactive information gathering is forecasting the possibility of a threat and taking the necessary precautions to avert it
  - Reactive information gathering is waiting for a threat to happen and reacting appropriately to that particular type of threat



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Gathering and Handling Information:  
Proactive

- Proactive information gathering example: Signing up for RSS feeds
- Other forms of proactive information gathering:
  - Regular system checks
  - Periodic CSIRT team drills
  - Subscribing to email lists
  - Setting the appropriate level of logging and checking periodically
  - Developing a background script for analysis



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Gathering and Handling Information:  
Reactive

- Reactive information gathering example: Using Google to research the threat, its effects, and how to properly eradicate the vulnerability
- Reactive information gathering is any attempt at gathering information made after a threat is detected



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Information Gathering Process



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---


---

---

---

Verifying and Scoring  
Collected Information

The verification process begins with your information source

- If you have a primary information source, your verification is as easy as speaking with that source
- 
- If you have only secondary information sources, additional research might be required for proper verification
- Apply a score to information once it is verified

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Information Gathering Process



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Saving Information for Analysis

- All information collected should be saved and stored for analysis
- This becomes **proactive information** and is beneficial for:
  - Training and tools for future CSIRT members
  - Possible information sharing for other CSIRTs and organizations
  - Future analysis of the effectiveness of the CSIRT
- Use a file system or Incident Management system



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Information Gathering Process



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Importance of Sharing Information

- Sharing information is reciprocal in its benefits
- Without the sharing of information, open-source intelligence would be far less beneficial and vulnerabilities would be more difficult to identify



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Establishing and Maintaining  
Sharing Relationships

- Creating and maintaining relationships is crucial to the success of a CSIRT
- CSIRTs commonly establish relationships with:
  - Other CSIRTs at neighboring/like organizations
  - ISPs
  - Social media outlets



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Learning Check

In which situations are differences in the way team members gather information helpful to your team? In which cases is varying from the norm not helpful?



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---

Questions?

What questions do you have about this lesson?



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

---

---

---

---

---

---

---



---

---

---

---

---

---

---