

Data Gathering

Table of Contents

Data Gathering.....	2
Data Gathering.....	3
Types of Intel Gather	4
Evaluating in Terms of Data Gathering	6
Notices	7

Data Gathering



Data Gathering

25

**025 Data gathering.

Data Gathering

- **Data Gathering:** Through automated and labor-intensive means, data and information is collected from multiple internal and external sources for analysts to analyze to answer organizational intelligence requirements
- **Internal Sources:** SIEM, NIDS, NIPS, HIDs DLPs, SOAR network and printer logs (Machine Data) and people, business units
- **External sources:** 3rd party intelligence providers, open source intelligence (social media), information sharing partnerships
- **Other sources?**



26


**026 When organizations know their environment, they can create the right intelligence requirements for data gathering. Data gathering means: through automated and labor-intensive means, data and information is collected from multiple internal and external sources for analysts to analyze to answer organization intelligence requirements. Data can come from multiple internal and external sources. So internal sources could be like your SIEM, your NIDS, your NIPS, your HIDs, your DLPs, your SOARs, your network and printer logs, people, business units. External sources could include third-party intelligence providers, open-source intelligence like social media or information sharing partnerships.

You want to get multiple sources when possible regarding a particular threat so that you have collaboration. Are there other types of sources? For those working in intelligence spaces, they might be familiar with the following.


Types of Intel Gather

Types of Intel Gather


Human Intelligence (HUMINT)




Signals Intelligence (SIGINT)



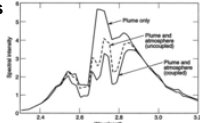
Open Source Intelligence (OSINT)




Imagery Intelligence (IMINT)




Measurement and Signatures Intelligence (MASINT)



Geospatial Intelligence (GEOINT)





<https://www.dni.gov/index.php/what-we-do/what-is-intelligence>
https://www.youtube.com/watch?v=EDtzX_VXr8A

https://www.satcen.europa.eu/page/introduction_to_imagery_intelligence_imint
<https://pentestworld.com/2018/07/10/raven-linked-in-information-gathering-tool/>
https://www.youtube.com/watch?v=EDtzX_VXr8A
<http://www.usmagazine.com/articles/1724/vstar-systems-brings-signals-intelligence-to-the-civilian-world>
http://www.projectrho.com/public_html/rocket/spacewardetect.php

27

****027 HUMINT.** HUMINT is the collection of information from human sources. SIGINT, or signals intelligence, is derived from signal intercepts comprising, however transmitted, either individually or in a combination all communications intelligence, electronic intelligence, foreign instrument signals intelligence, and the National Security Agency is responsible for the collection, processing and reporting of SIGINT.

There's also imaging intelligence or IMINT, which is representations of objects produced electronically or by optical means on film or electronic display, devices or other media. Imagery can be derived from visual photography, radar sensors, and electro-optics.

There's also geospatial intelligence. Here this is the analysis and visual representation of security-related activities on earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information. There's also OSINT or open-source intelligence that's publicly available information regarding--excuse me--appearing in print or electronic forms such as newspapers, journals, the internet, social media, commercial databases, videos, graphics, drawings, and then lastly, there's MASINT, measurement and signals intelligence, and that's technically derived intelligence data or other imagery that's different than imagery and SIGINT, excuse me.

MASINT data is usually intelligence that locates, identifies or describes distinctive characteristic of targets. It employs a broad group of disciplines such as nuclear, optical, radio frequency, acoustics, seismic, and material sciences.

Evaluating in Terms of Data Gathering

- In evaluating the state of the practice of cyber intelligence in terms of Data Gathering, we considered the following factors:

1. Intelligence Requirement Process
2. Intelligence Requirement and Data Source Alignment
3. Organization Information Sharing Process
4. Technology for Data Gathering
5. Data Source Validation



28

**028 In evaluating a state of practice of cyber intelligence in terms of data gathering, we considered the following factors for assessing organizations. Does the organization have an intelligence requirement process? An intelligence requirement is basically a question or need your organization has about something. For example, what threats is my organization facing now and in the future? Does your organization have a process for generating these types of requirements? Does your organization have an intelligence requirement and data source alignment process? In other words, based on these requirements, do you have the right data sources to go answer those requirements? Does your organization have an organization information sharing process? What is that process? Is it

able to share information both internally and externally effectively?
What kind of technology does your organization have for data gathering?
Is it outdated? Are there redundancies in technology and is there new data out there that could help your organization collect data?

And lastly, data source validation.
How does your organization validate the data that it is receiving?

Notices

Notices

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM20-0262

