

LO#08: Explain Cyber Threat Intelligence

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

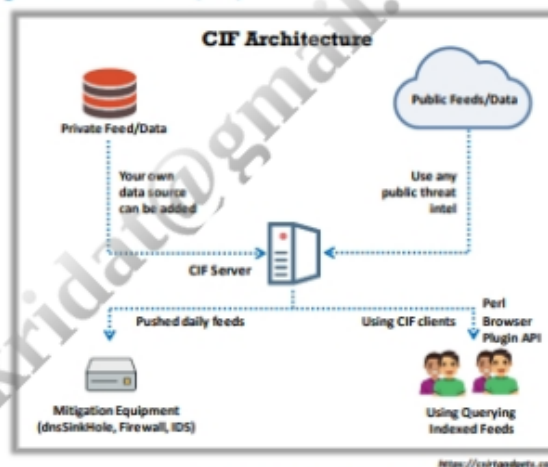
Threat Intelligence Frameworks



Collective Intelligence Framework (CIF)

Collective Intelligence Framework (CIF) is a cyber threat intelligence management system that allows you to **combine known malicious threat information** from many sources and use that information for incident detection, response, and mitigation.

CIF helps to parse, normalize, store, post-process, query, share, and **produce data sets of threat intelligence**.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notes: _____

Threat Intelligence Data Collection



- Threat Intelligence Data Collection is a collection of **relevant and reliable data** for analysis. It is the key to achieving better threat intelligence output
- Data can be gathered from **multiple sources and feeds** including Human Intelligence (HUMINT), Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Open Source Intelligence (OSINT), Social Media Intelligence (SOCMINT), and others
- Analysts can collect threat data either from multiple security teams in an organization or by **manually conducting** the threat **data collection**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threat Intelligence Sources



Open-Source Intelligence (OSINT)

- Information is collected from the **publicly available sources** and analyzed to obtain a rich useful form of intelligence
- OSINT sources:
 - Media
 - Internet
 - Public government data
 - Corporate and academic publishing
 - Literature

Human Intelligence (HUMINT)

- Information is collected from **interpersonal contacts**
- HUMINT sources:
 - Foreign defense personnel and advisors
 - Accredited diplomats
 - NGOs
 - Prisoners of War (POWs)
 - Refugees
 - Traveler interview or debriefing

Signals Intelligence (SIGINT)

- Information is collected by **intercepting signals**
- Signal intelligence comprises of:
 - Communication Intelligence (COMINT)**: Obtained from the interception of communication signals
 - Electronic Intelligence (ELINT)**: Obtained from electronic sensors like radar and lidar
 - Foreign Instrumentation Signals Intelligence (FISINT)**: Signals detected from non-human communication systems

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notes: _____

