

## Threat Intelligence Sources (Cont'd)



### Technical Intelligence (TECHINT)

- Information is collected from an **adversary's equipment** or captured enemy material (CEM)
- TECHINT sources:
  - Foreign equipment
  - Foreign weapon systems
  - Satellites
  - Technical research papers
  - Foreign media
  - Human contacts

### Geo-spatial Intelligence (GEOINT)

- Information is collected by the exploitation and evaluation of **geo-spatial information** to assess human activities on earth
- GEOINT sources:
  - Satellite imagery
  - Unmanned Aerial Vehicles (UAV) imagery
  - Maps
  - GPS Waypoints
  - IMINT (Imagery Intelligence)
  - National Geospatial-Intelligence Agency (NGA)

### Imagery Intelligence (IMINT)

- Information is collected from objects that are used to reproduce the real scenario electronically by any **kind of electronic media** or device
- IMINT sources:
  - Visual photography
  - Infrared sensors
  - Synthetic Aperture Radar (SAR)
  - MASINT (Measurement and Signature Intelligence)
  - LASER
  - Electro-optics

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

## Threat Intelligence Sources (Cont'd)



### Measurement and Signature Intelligence (MASINT)

- Information is collected from the **sensors** that are intended to record distinctive characteristics (signatures) of fixed or dynamic targets.
- MASINT sources:
  - Electro-optical
  - Acoustic sensors like sonars
  - Infrared
  - Radar sensors
  - LASER
  - Spectroscopic sensors

### Covert Human Intelligence Sources (CHIS)

- Information is covertly collected from the target person by maintaining a **personal or other relationship** with the target person
- CHIS generally refers to a person or an agent under the Regulation of Investigatory Powers Act 2000 (RIPA), UK.
- CHIS sources are the persons targeted for information extraction

### Financial Intelligence (FININT)

- Information is collected about the **adversary's financial affairs** and transactions that may involve tax evasions, money laundering, or other practices. This in turn provides information about the nature, capabilities, and intentions of the adversary
- FININT sources:
  - Financial Intelligence Unit (FIU)
  - SWIFT
  - Banks
  - Informal value transfer systems (IVTS)

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

Notes: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## Threat Intelligence Sources (Cont'd)



### Social Media Intelligence (SOCMINT)

- Information is collected from **social networking sites** and other types of social media sources
- SOCINT sources:
  - Facebook
  - LinkedIn
  - Twitter
  - WhatsApp
  - Instagram
  - Telegram

### Cyber Counterintelligence (CCI)

- Information is collected from proactively established security infrastructure or by employing various **threat manipulation techniques** to lure and trap threats
- CCI Sources:
  - Honeypots
  - Passive DNS monitors
  - Online web trackers
  - Sock puppets (fake profiling) on online forums
  - Publishing false reports

### Indicators of Compromise (IoCs)

- Information is collected from **network security threats and breaches** and from the alerts generated by the security infrastructure, which likely indicate an intrusion
- IoCs Sources:
  - Commercial and industrial sources
  - Free IoC specific sources
  - Online security-related sources
  - Social media and news feeds
  - IoC buckets

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

## Threat Intelligence Sources (Cont'd)



### Industry Association and Vertical Communities

- Information is collected from various **threat intelligence sharing communities** where the participating organizations share intelligence information
- Vertical community sources:
  - Financial Services Information Sharing and Analysis Center (FS-ISAC)
  - MISP (Malware Information Sharing Platform)
  - Information Technology—Information Sharing and Analysis Center (IT-ISAC)

### Commercial Sources

- Information is collected from **commercial entities** and security vendors that provide threat information to various organizations
- Commercial sources:
  - Kaspersky Threat Intelligence
  - McAfee
  - Avast
  - FortiGuard
  - SecureWorks
  - Clisco

### Government and Law Enforcement Sources

- Information is collected from **government and law enforcement sources**
- Government sources:
  - US Computer Emergency Response Team (US-CERT)
  - European Union Agency for Network and Information Security (ENISA)
  - FBI Cyber Crime
  - StopThinkConnect
  - CERIAS Blog

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

Notes: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_