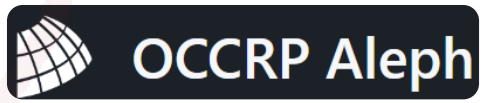
Collection / Processing / Analysis / Production

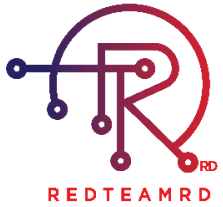



RANSOMWARE
.LIVE


HURRICANE ELECTRIC
INTERNET SERVICES


ID Ransomware


Recorded Future
Triage


REDTEAMRD


DNS-Dumpster


scam detector


FOFA


MX TOOLBOX®


GRAYHAT
WARFARE


VirusShare


DorkSearch
Faster Google Dorking


FULLHUNT


SCANNERO.IO


hunter


ONYPHE


//grep.app


ZoomEye

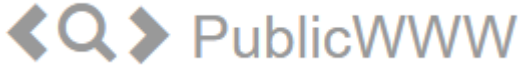

DNSCHECKER


VULNERS
.COM


IVRE


Netlas.io


WebCheck


PublicWWW


crt.sh


Binary
Edge


Pulsedive


WIGLE.NET


LeakIX.net

Abnormal Investigation

OSINT Framework

Others Tools

Collection / Dissemination (Sharing)

Collection / Processing / Analysis / Production / Dissemination

REDTEAMRD

Attack Surface Management Platforms (ASM)

Processing / Analysis / Production

x64dbg

Process Monitor

Collection / Processing / Dissemination

REDTEAMRD

Agencies issuing periodic threat bulletins

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

CISA Cybersecurity & Infrastructure Security Agency

Department of Justice Federal Bureau of Investigation

FIRST Improving Security Together

Cert-EU

ITU

KISA Korea Internet & Security Agency

INTERPOL

Federal Bureau of Investigation IC3 Internet Crime Complaint Center

incibe cert_

enisa European Union Agency for Cybersecurity

Agence Nationale de la Sécurité des Systèmes d'Information ANSSI

JPCERT CC

Collection / Dissemination (Sharing)

REDTEAMRD

GitHub

Sentinel LABS
SentinelOne

MANDIANT

SANS

Microsoft

AT&T

TREND MICRO

UNIT 42
BY PALO ALTO NETWORKS

eset

SONICWALL

verizon

FORTINET

wazuh.

elastic

Cloudforce One

Consider it!

- ✓ **Annoyance - Frustrate and Slow Down**
- ✓ **Attribution - Identify and Track**
- ✓ **Attack - Defenders go on the offensive**

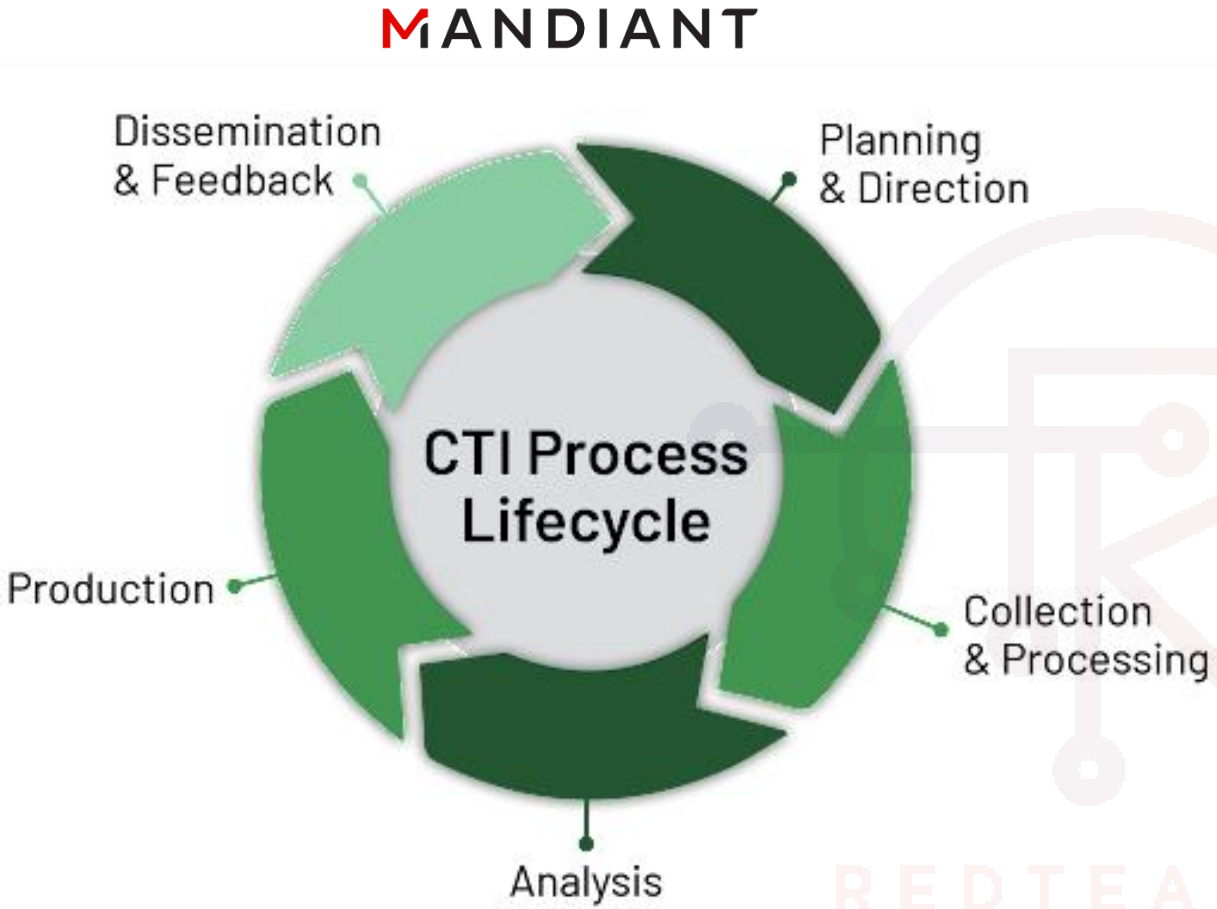
The Active Defense Harbinger Distribution (ADHD) framework

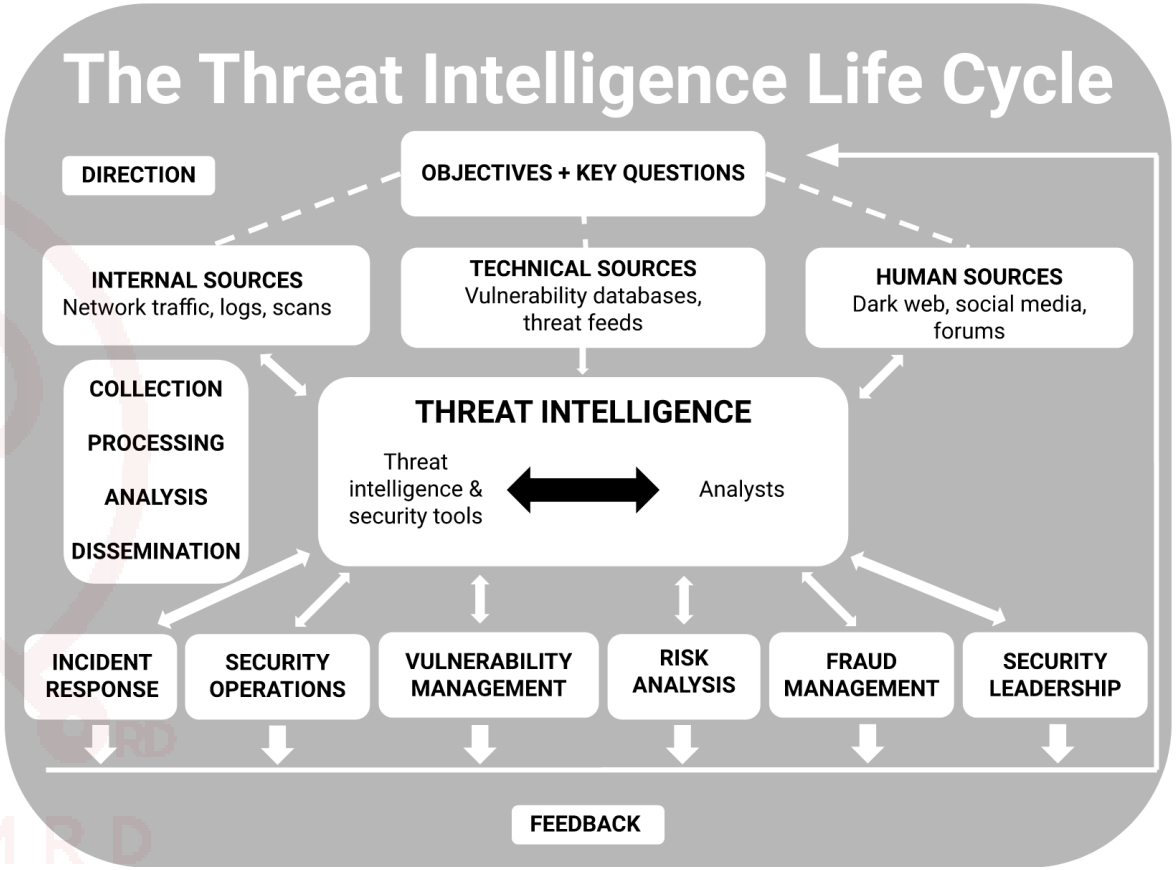
It can be a valuable addition to an organization's threat intelligence capabilities, providing proactive and advanced methods for detecting, analyzing, and mitigating threats.

ADHD includes tools to create decoys and honeypots that can trick attackers away from critical assets.

But above all, it helps to collect valuable intelligence from the adversary.

Threat Intelligence Cycle:





SentinelOne

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1