



# Cyber Threat Intelligence Management



# Agenda for the next 13:37 minutes





# Where does this talk fit?

Intermediate

Expert



Intro



Advanced

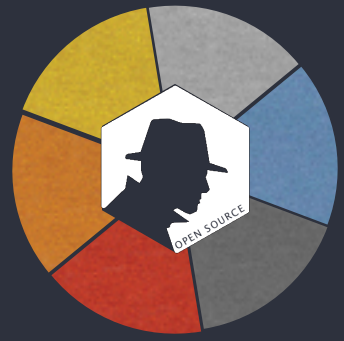


1337 Tier



Was that a fat joke?





You aren't my manager pal!

Proactive

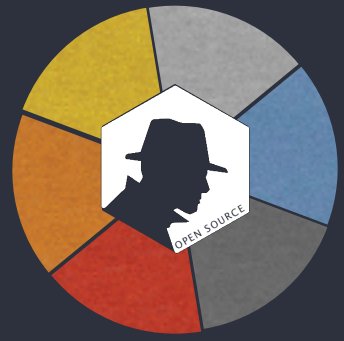
Context



Contribute

Response times





# Cyber Threat Intelligence Common Language

01

Observable

02

Threat Actor

03

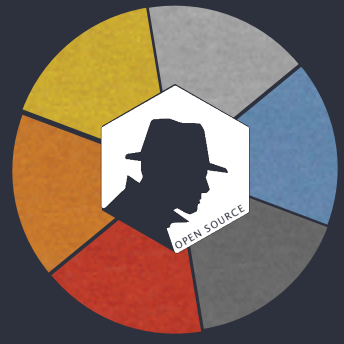
Tactics, Techniques and Procedures

04

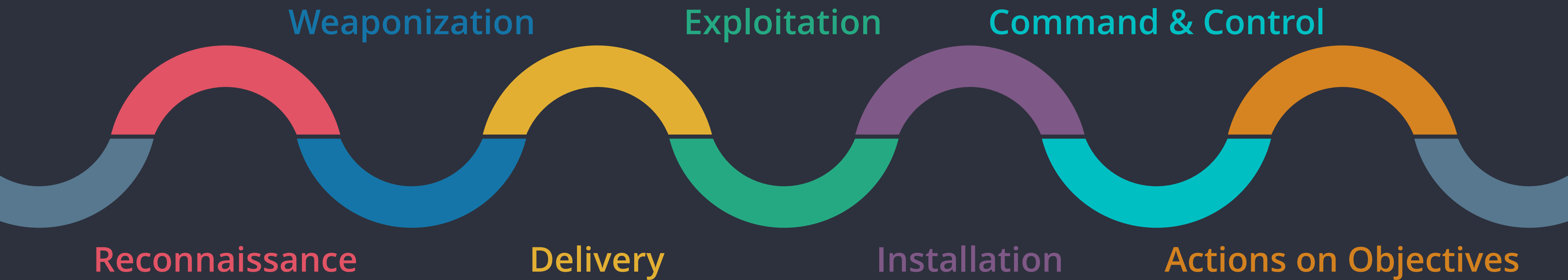
Indicator

05

Campaign



# Lockheed Martin Cyber Kill Chain ®





# Cyber Threat Intelligence Common Language

06

Lockheed Martin Cyber Kill Chain®

07

Traffic Light Protocol

08

Intelligence Disciplines (\*INT)

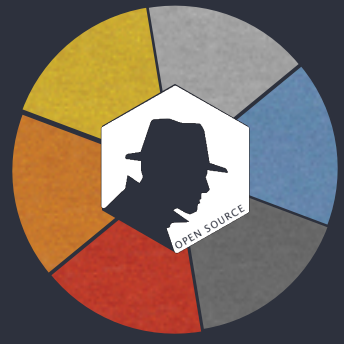
09

STIX, TAXII, CybOX & OASIS

10

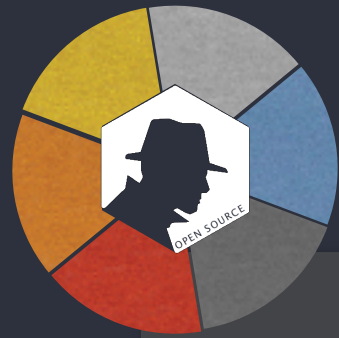
F3EAD Framework





# F3EAD Framework





## F3EAD Framework related to IR

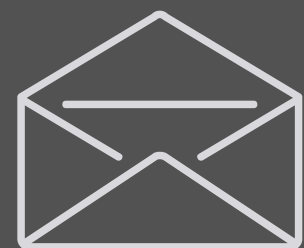
# Operations

# Intelligence

Find

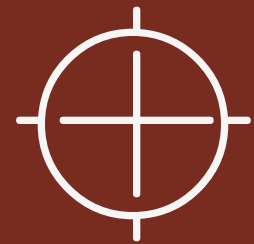


**SIEM**



01

Fix

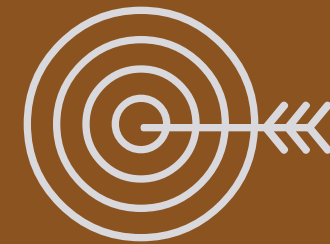


**SIEM**



02

Finish



**IR**

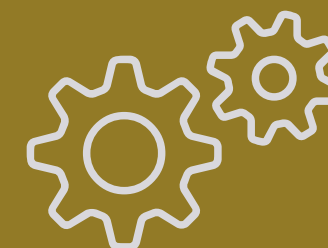


03

Exploit

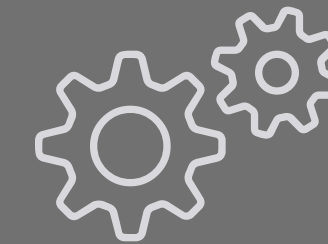


**TIC**



04

Analyze



**MAS**



05

Disseminate



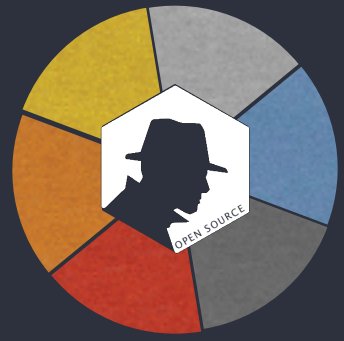
**SIEM**



**TIC**

06





# How to build a Threat Intelligence Center (TIC)

  
Plan

  
Documentation

  
Internal Tools

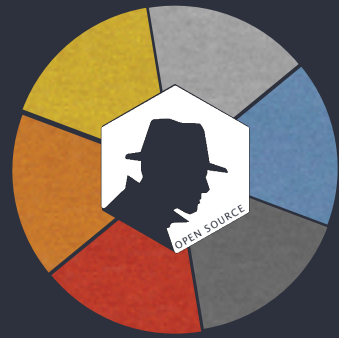
  
Internal Development

  
Internal Relationships

  
External Relationships

 50%

 50%



## The tools to build an Open Source Threat Intelligence Center (TIC)



STIX

# CRITs

STIX friendly

Mongo

Python Friendly

Over 30 Services

CTI repository

Campaign Tracking

[crits.github.io](https://crits.github.io)

TAXII

# SOLTRA

CRITs friendly

Eats whatever you feed it

TAXII Gateway for partners

FS-ISAC

Utilizes TLP

Notifications

[soltra.com](https://soltra.com)

Development

# GitLab

Developer friendly

Local Version Control

Track Issues

Locally crowdsource dev

Integrates with Slack

For teams of 1 - 30K

[gitlab.com](https://gitlab.com)



Malware

# Cuckoo

CRITs friendly

STIX Friendly

Python Friendly

Automated Malware Analysis

Win/OSX/Linux Analysis

Volatility

[cuckoosandbox.org](https://cuckoosandbox.org)



# TIC.SeckKC..org:443

Powered By: Threat Note

cory@seckc.org