Building blocks for CTI
(on a budget)

Swetha Balla, April 2019

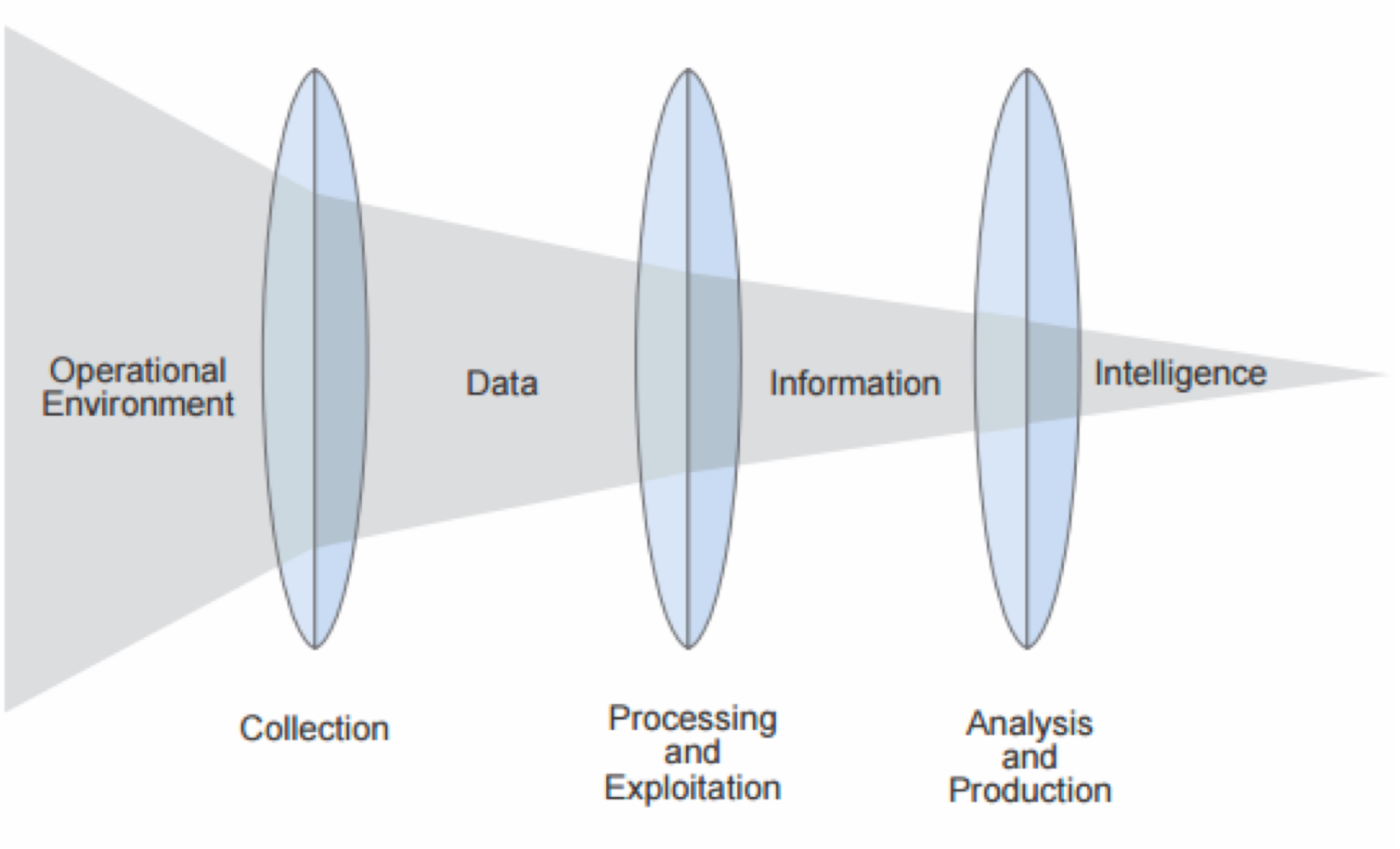
Opinions are my own and not the views of my employer.

Agenda

- Lost in translation
- A day in the life of an analyst
- “why” FOSS?
- Baselining
- So what?
- Benefits
- Learnings
- TL;DR & Questions

Opinions are my own and not the views of my employer.

Lost in translation



Reference: Recorded Future

A day in the life of an analyst

DATA OVERLOAD

DATA MANAGEMENT

DATA ANALYSIS

DATA SHARING

NEW TEAM

LIMITED BUDGET

Free and Open Source tools!

Opinions are my own and not the views of my employer.

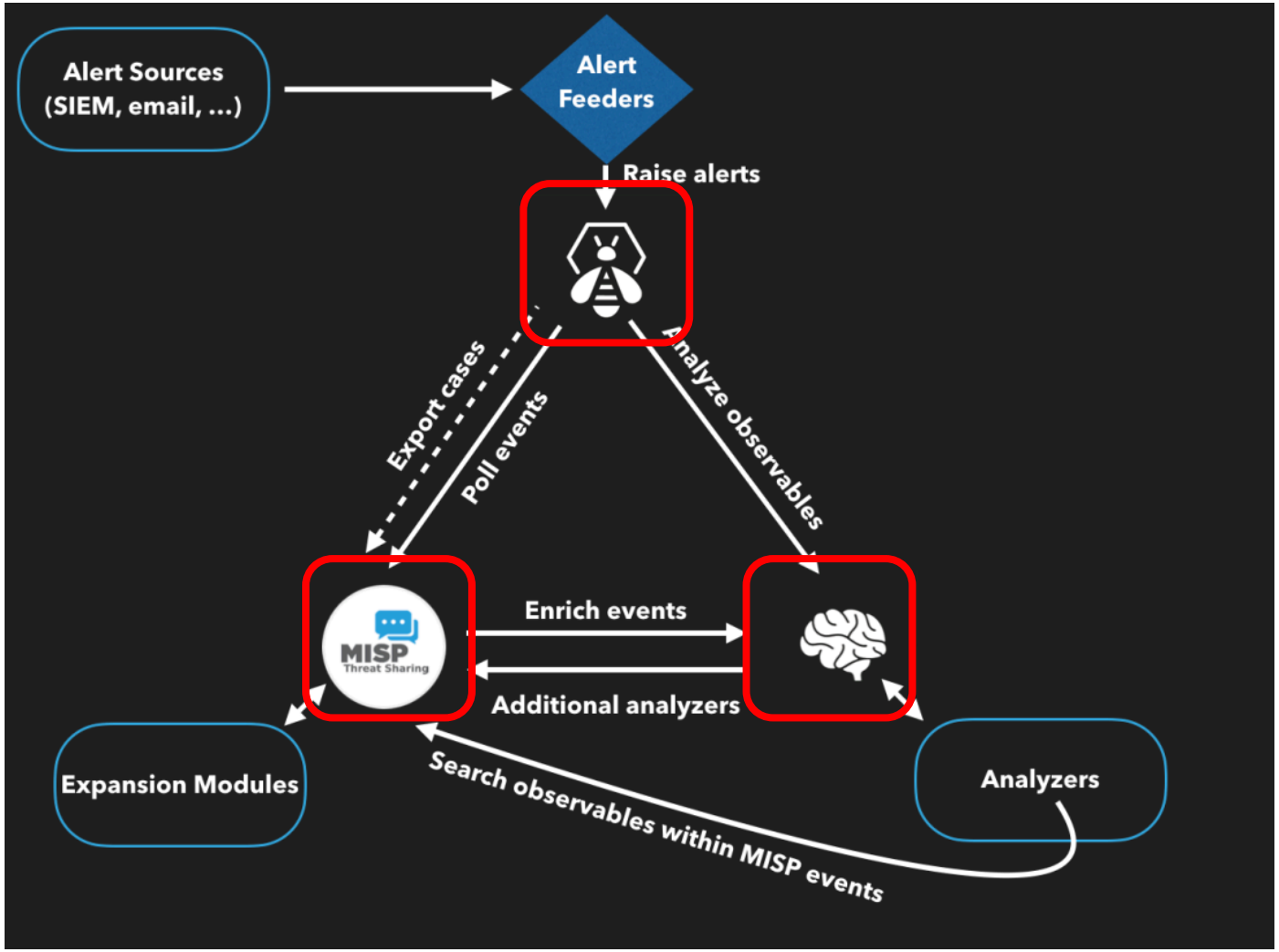
Why not?

Quick starter

Shared & used by many mature security teams

Opinions are my own and not the views of my employer.

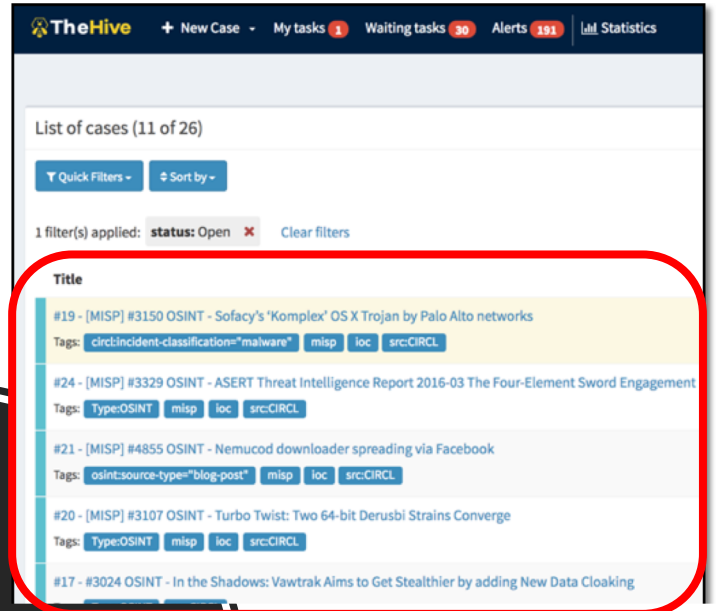
Baselining

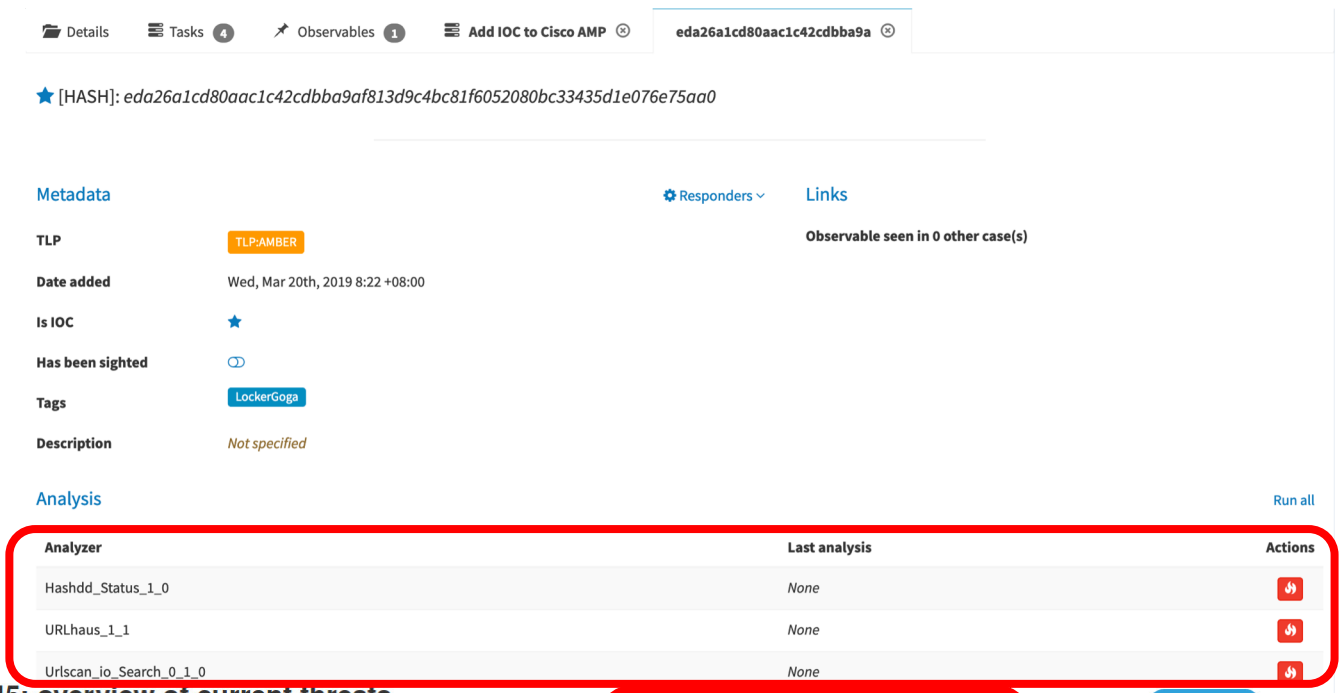


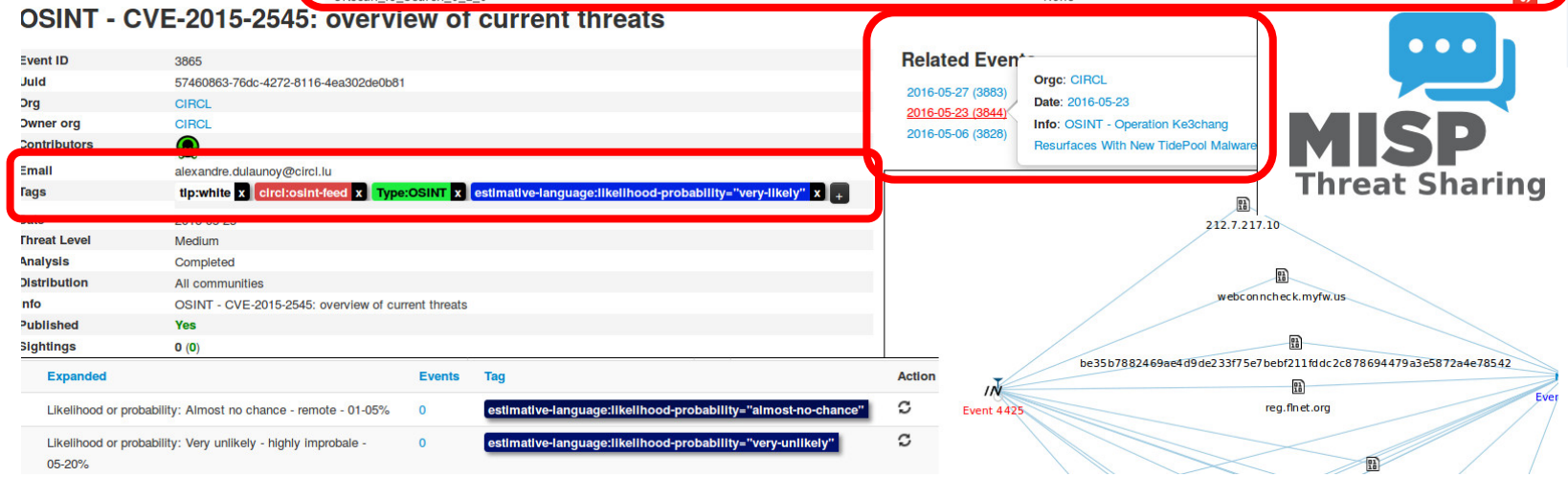
Gather (TheHive), Analyze (Cortex), Process & Collaborate (MISP)

Opinions are my own and not the views of my employer.

So what?







TheHive -> MISP: Internal Observables -> Enrichment & (maybe) sharing
TheHive -> Cortex: Internal Observables -> Enrichment
MISP -> TheHive: External Observables -> Alerts -> Incidents

Opinions are my own and not the views of my employer.

Benefits

GATHERING

COLLECTION

ENRICHMENT

Kick-started the ability to build an internal threat database

Learnings

TLC

TheHive doesn't have RBAC and this would require spinning up multiple instances

Security testing

The tools have to be tested by a Penetration Testing team to ensure that there are no critical vulnerabilities

One isn't enough

MISP on its own might not work; need to complement with other technologies like STAXX

Active community helps with lack of vendor support

TL;DR

Lay the building blocks

Planning and requirements

Data collection and processing

Processes: Analysis, Production

Crawl, walk, run

Implement the building blocks using FOSS tool

Identify potential gaps in using FOSS tools

Contribute to the community (key *tenet* of CTI)

Continuous evolution

New technologies & tools

Constant change

Questions?

Opinions are my own and not the views of my employer.