

# Building blocks for CTI *(on a budget)*

---

Swetha Balla, April 2019

# Agenda



Lost in translation



A day in the life of an analyst



“why” FOSS?



Baselining



So what?



Benefits

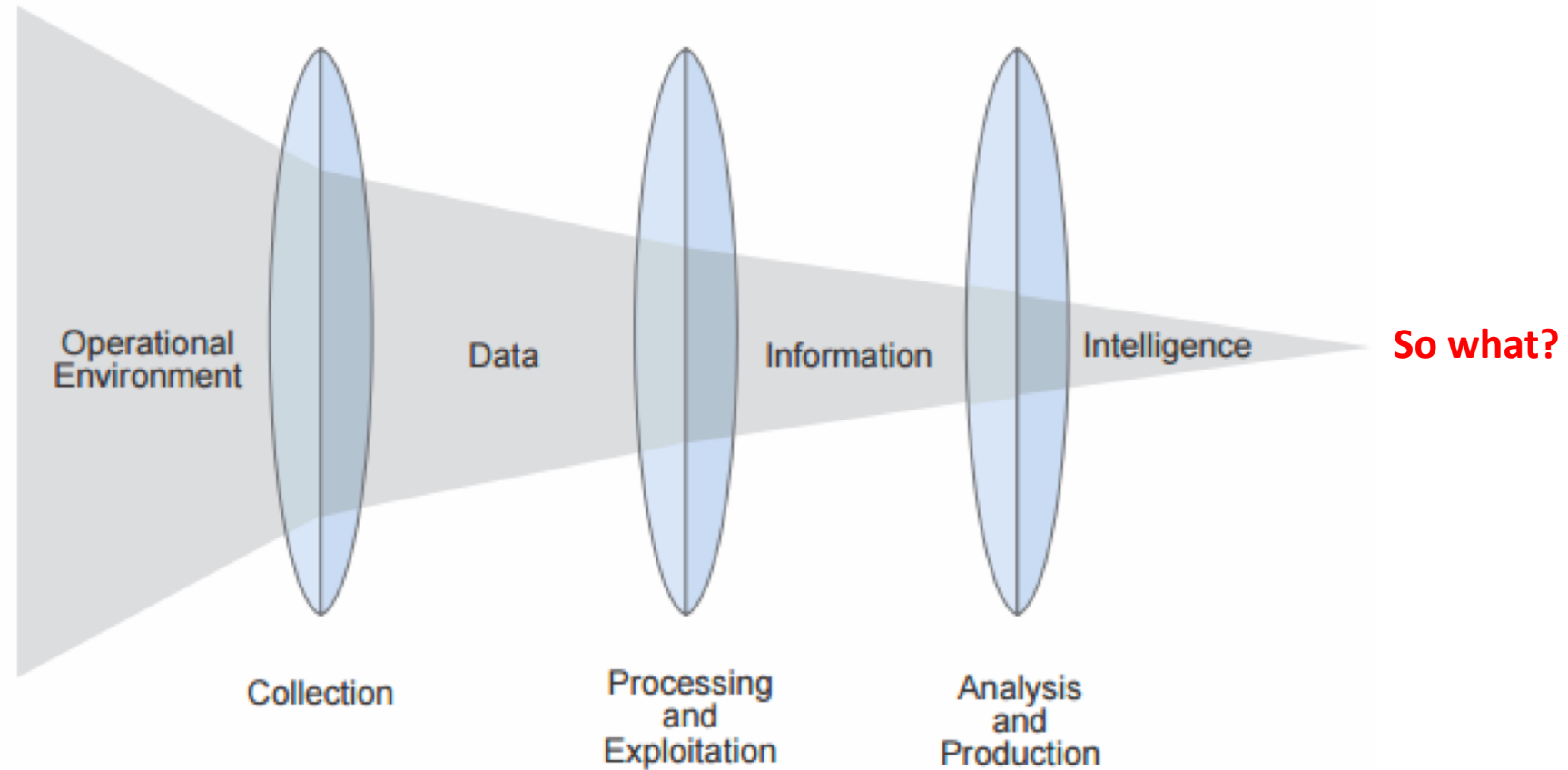


Learnings



TL;DR & Questions

Lost in  
translation



**Reference:** Recorded Future

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

# A day in the life of an analyst



DATA  
OVERLOAD



DATA  
MANAGEMENT



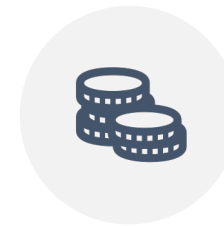
DATA ANALYSIS



DATA SHARING



NEW TEAM



LIMITED  
BUDGET

**Free and Open Source tools!**



"why" FOSS?

---

Why not?

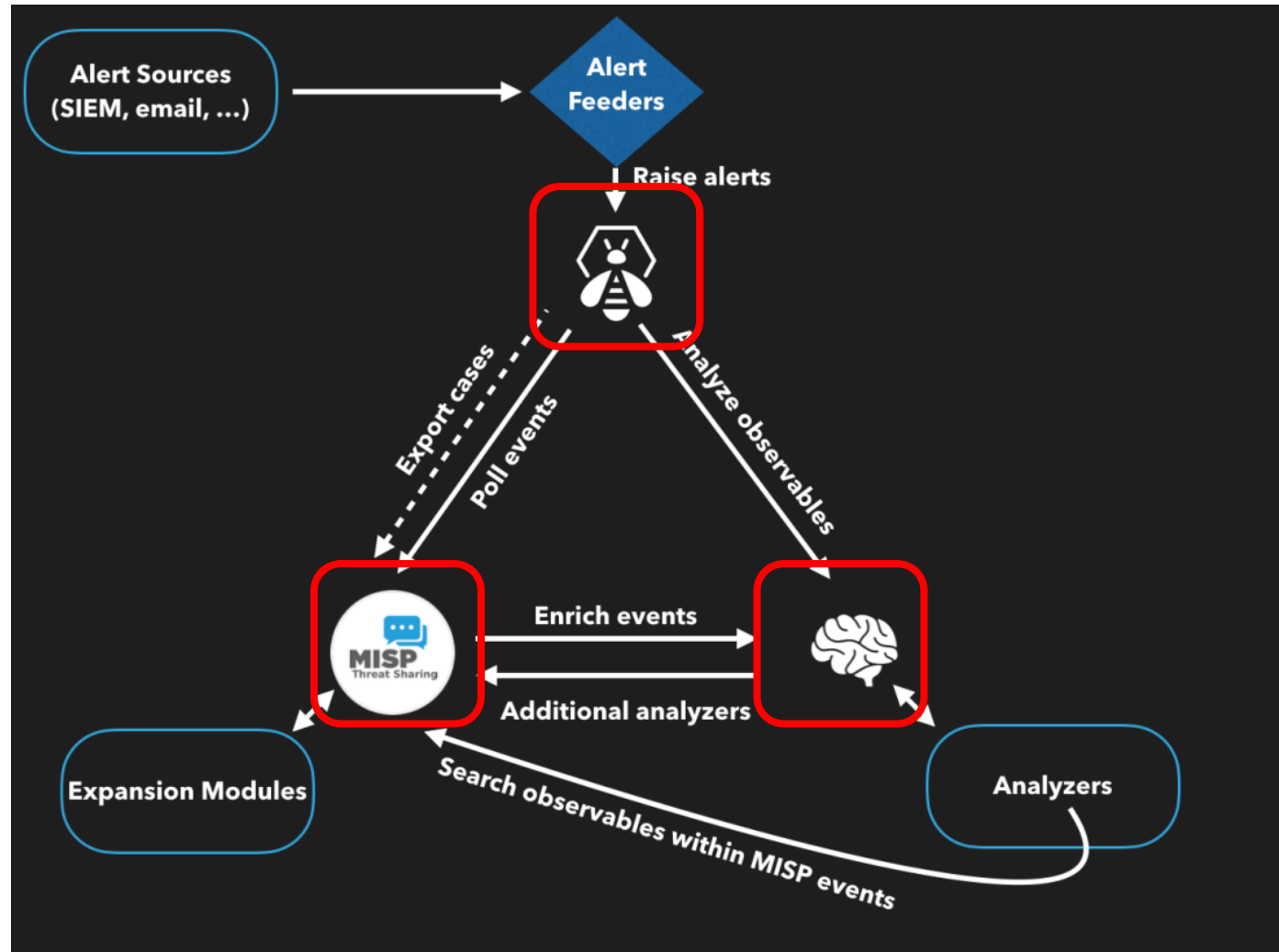
---

Quick starter

---

Shared & used by many mature security teams

# Baselining



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

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

So what?

TheHive interface showing a list of cases (11 of 26). The list includes cases like #19 - [MISP] #3150 OSINT - Sofacy's 'Komplex' OS X Trojan by Palo Alto networks, #24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement, #21 - [MISP] #4855 OSINT - Nemucod downloader spreading via Facebook, #20 - [MISP] #3107 OSINT - Turbo Twist: Two 64-bit Derusbi Strains Converge, and #17 - #3024 OSINT - In the Shadows: Vawtrak Aims to Get Stealthier by adding New Data Cloaking.

TheHive interface showing details for a specific case. The metadata section includes TLP (TLP-AMBER), Date added (Wed, Mar 20th, 2019 8:22 +08:00), Is IOC (star icon), Has been sighted (eye icon), Tags (LockerGoga), and Description (Not specified). The analysis section shows a table with columns for Analyzer, Last analysis, and Actions.

Analyzer	Last analysis	Actions
Hashdd_Status_1_0	None	[Icon]
URLhaus_1_1	None	[Icon]
Urlscan_io_Search_0_1_0	None	[Icon]

## OSINT - CVE-2015-2545: overview of current threats

TheHive interface showing details for a specific case. The event details include Event ID (3865), Juid (57460863-76dc-4272-8116-4ea302de0b81), Org (CIRCL), Owner org (CIRCL), Contributors (alexandre.dulaunoy@circl.lu), Email (alexandre.dulaunoy@circl.lu), Tags (ttp:white, circl:osint-feed, Type:OSINT, estimative-language:likelihood-probability="very-likely"), Threat Level (Medium), Analysis (Completed), Distribution (All communities), Info (OSINT - CVE-2015-2545: overview of current threats), Published (Yes), and Sightings (0 (0)).

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	[Icon]
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	[Icon]

TheHive interface showing details for a specific case. The related events section includes a table with columns for Date, Org, Date, and Info. The network diagram shows connections between various entities, including 212.7.217.10, webconcheck.myfw.us, be35b7882469ae4d9de233f75e7beb211fdde2c878694479a3e5872a4e78542, reg.finet.org, and Ever.

Date	Org	Date	Info
2016-05-27 (3883)	CIRCL	2016-05-23 (3844)	OSINT - Operation Ke3chang
2016-05-23 (3844)	CIRCL	2016-05-06 (3828)	Resurfaces With New TidePool Malware

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?