RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **AIR-W01**

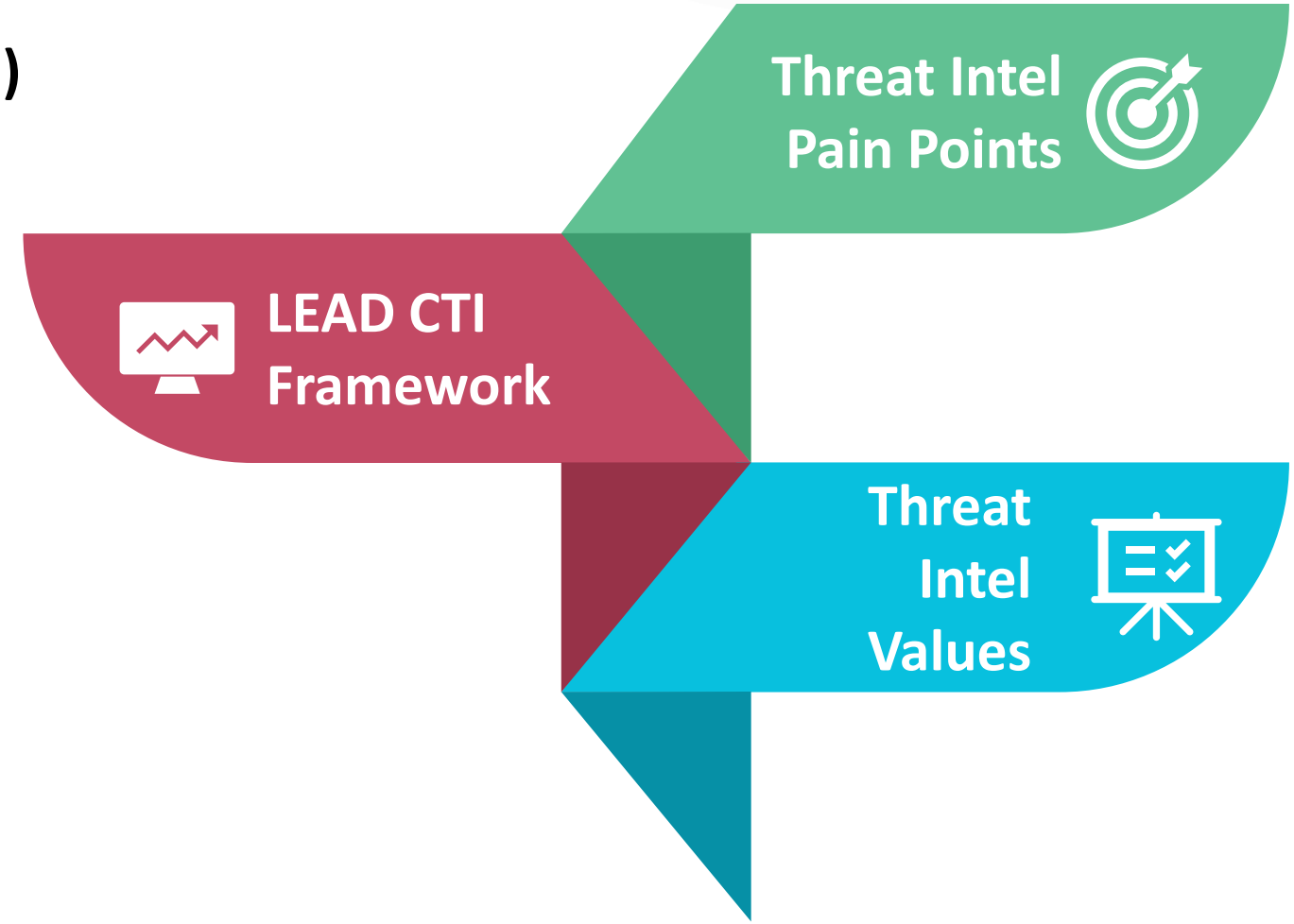
Intelligent Threat Intel 'LEAD' Framework

Filip Stojkovski

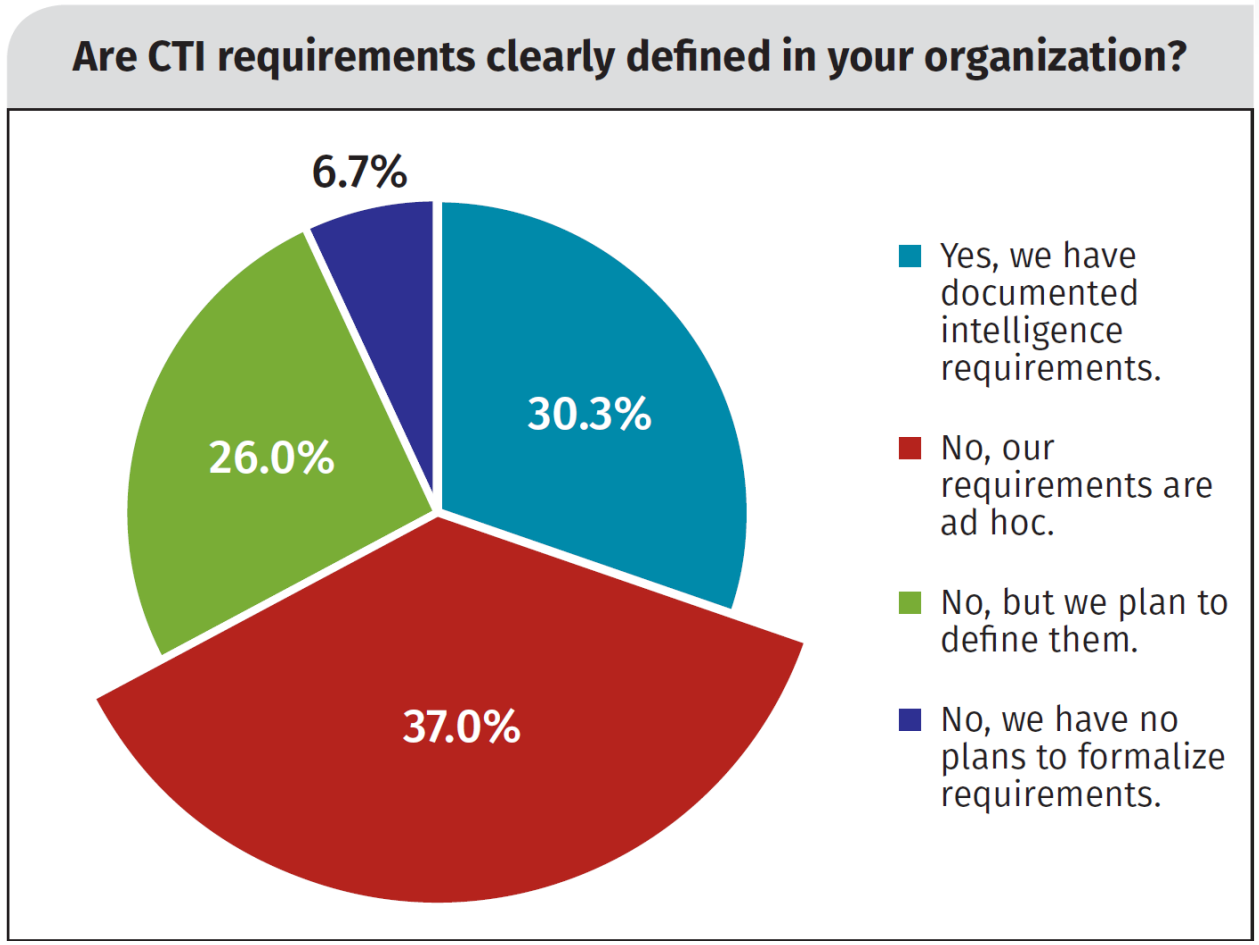
Threat Intel Manager
Adobe

Threat Intel - ‘LEAD’ Framework - 101

- **CTI (Cyber Threat Intelligence) pain points**
- **Efficiently and effectively solve the CTI problems.**
- **LEADing Threat Intelligence Program**



Threat Intel Pain Points - Requirements



Source Ref: https://www.sans.org/reading-room/whitepapers/threats/paper/38790

No clear CTI Requirements

=

Time Bomb

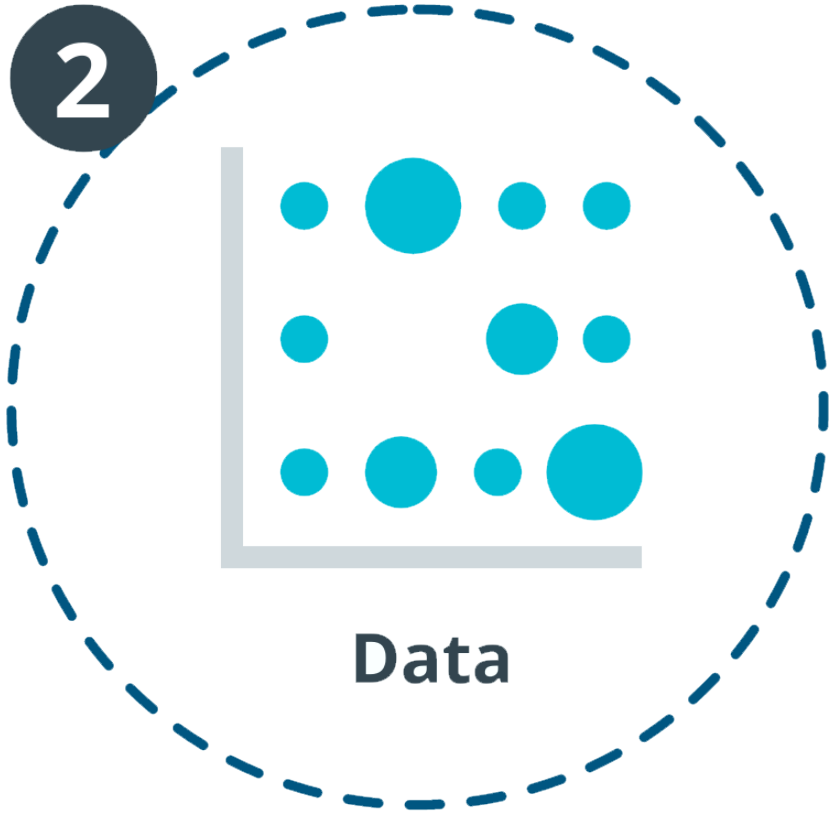
Threat Intel Pain Points - Data

Satisfaction with CTI	Not Satisfied
Analytics	34.3%
Cleanliness and quality of data	37.4%
Context	35.4%
Comprehensiveness of coverage	37.4%
Automation and integration of CTI information with detection and response systems	39.4%
Location-based visibility	**42.5%**
Identification and removal of expired indicators of compromise (IoCs) and other old data	**47.6%**
Machine learning	**55.9%**

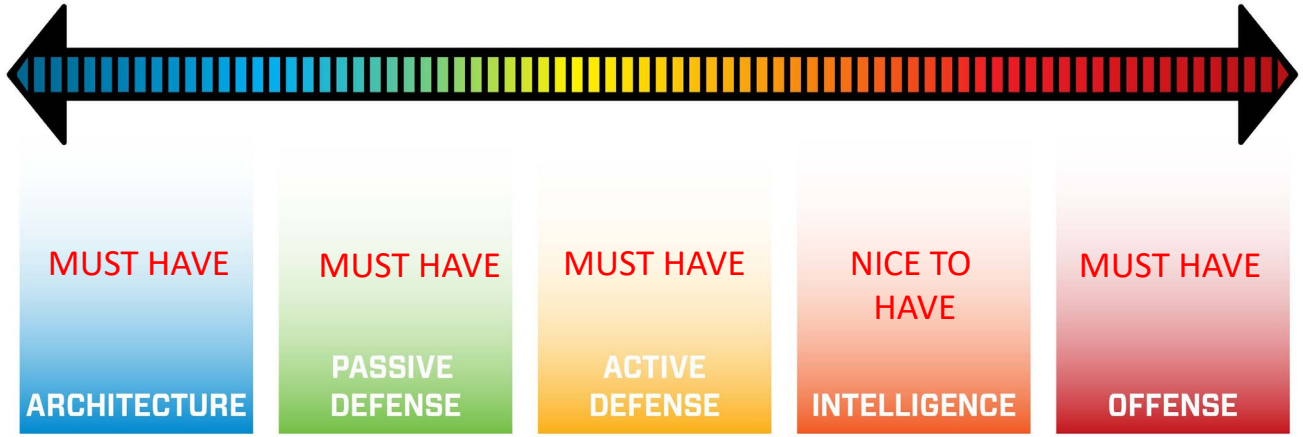
List of the biggest pain points for CTI

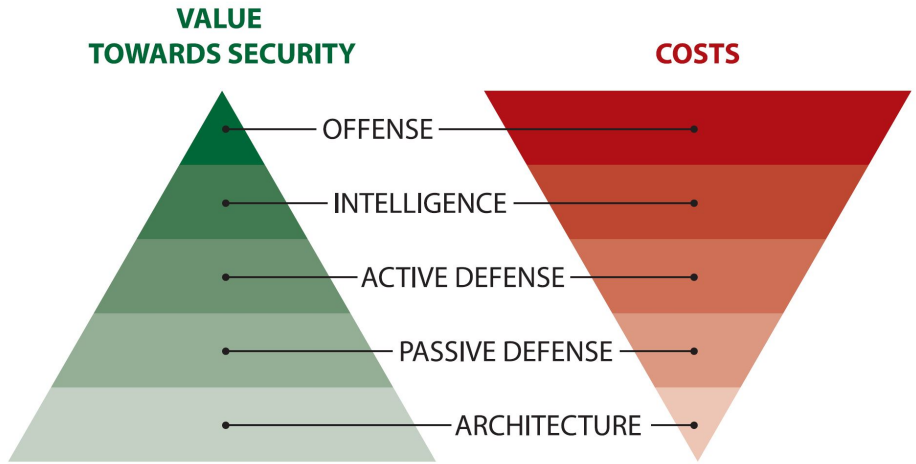
Source Ref: https://www.sans.org/reading-room/whitepapers/threats/paper/38790

The Threat Intel Problems



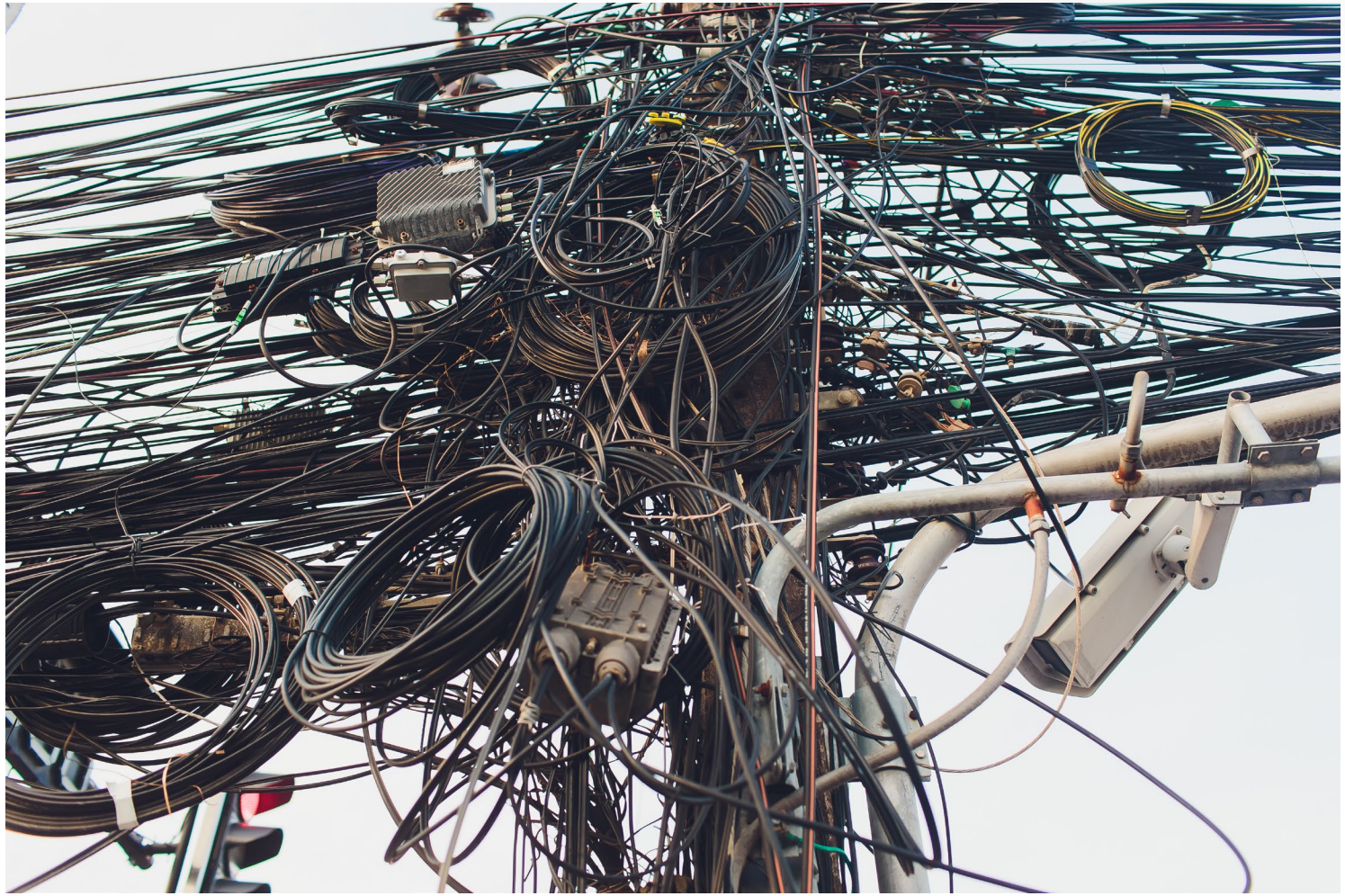
The Non-Essential Problem





Ref: https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

The Threat Intel Data

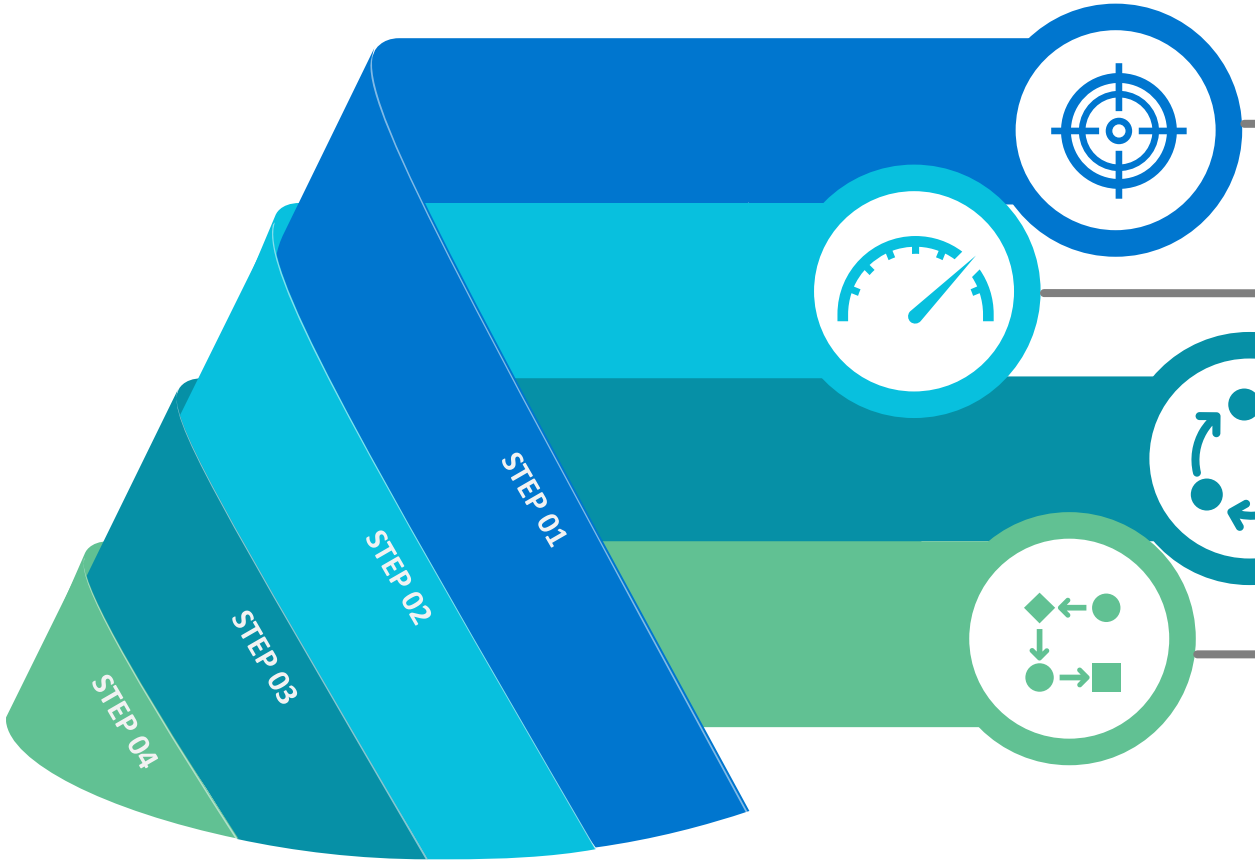


RSAConference2020

Solving the CTI Problem

How To Solve The TI Problem

‘LEAD’ Framework Structure



RELEVANT
Threat Profile + TI Program Requirements

EFFICIENT
TI Scoring + TI Categorization

ANALYST DRIVEN
Feedback Loop + Machine Learning

DELIVERABLE
Standardized TI Data + Metrics

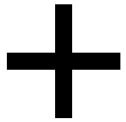
RELEVANT- Creating Threat Profile

From WHOM, you are trying to defend from?

Script Kiddies
Scammers

Organized Crime
Hacktivists

State-Sponsored
APT



WHAT, infrastructure you are trying to defend?

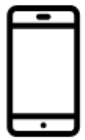
ICS

Servers

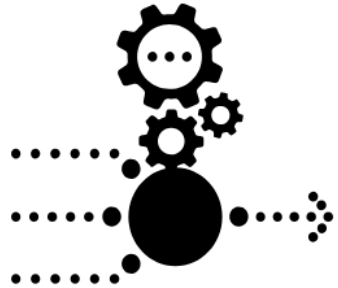
IOT

Payment
systems

Endpoints

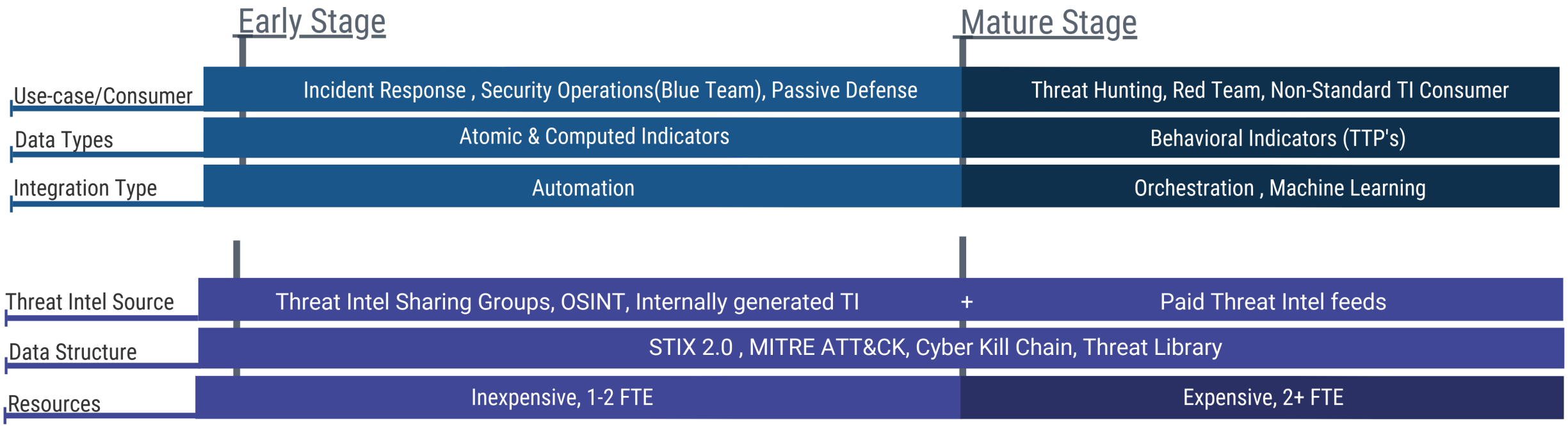


Mobile



RELEVANT - Threat Intel
TI - sources/feeds

RELEVANT – TI Program Requirements

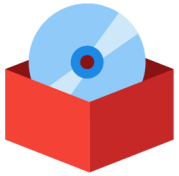


RELEVANT – Non-IR TI Consumers

E-commerce
(Fraudulent Payments)

Code repositories
(0-day exploits)

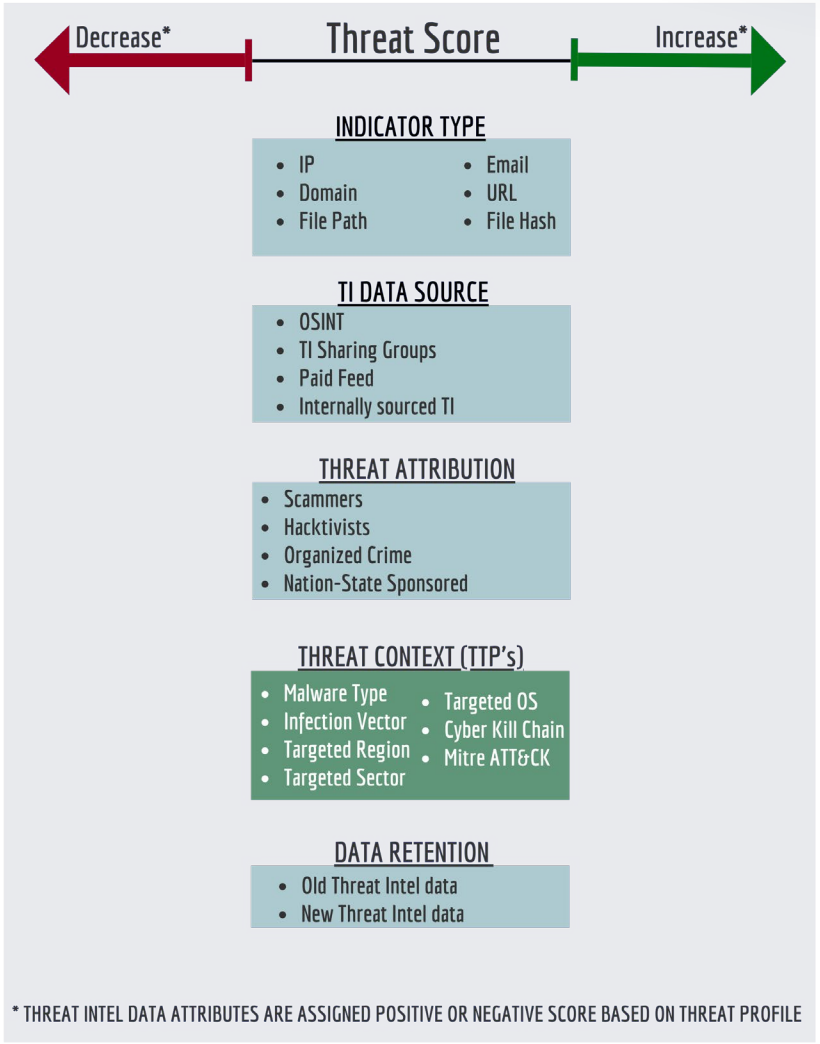
Customer Content
Moderation

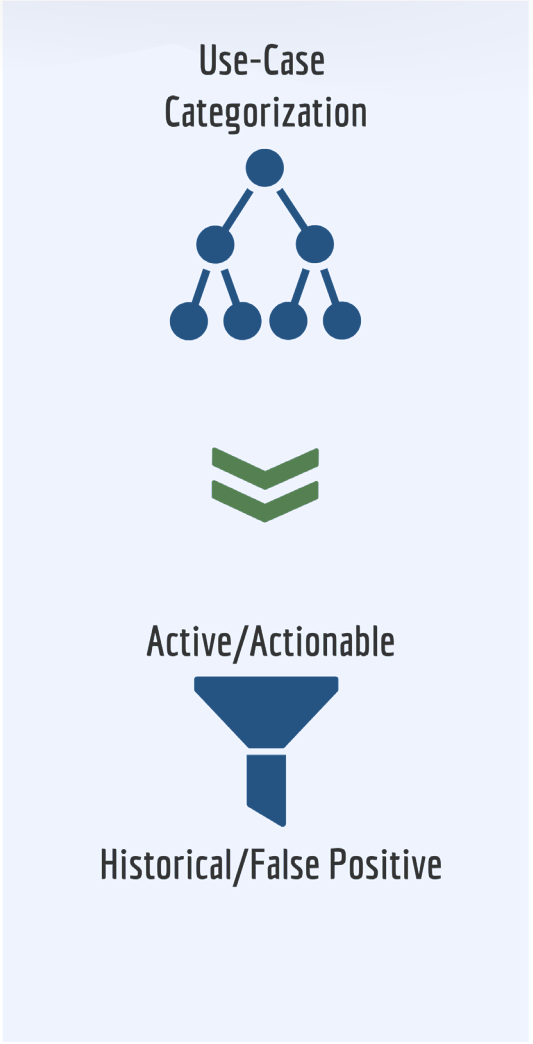


Piracy

EFFICIENT - TI Scoring & Categorization

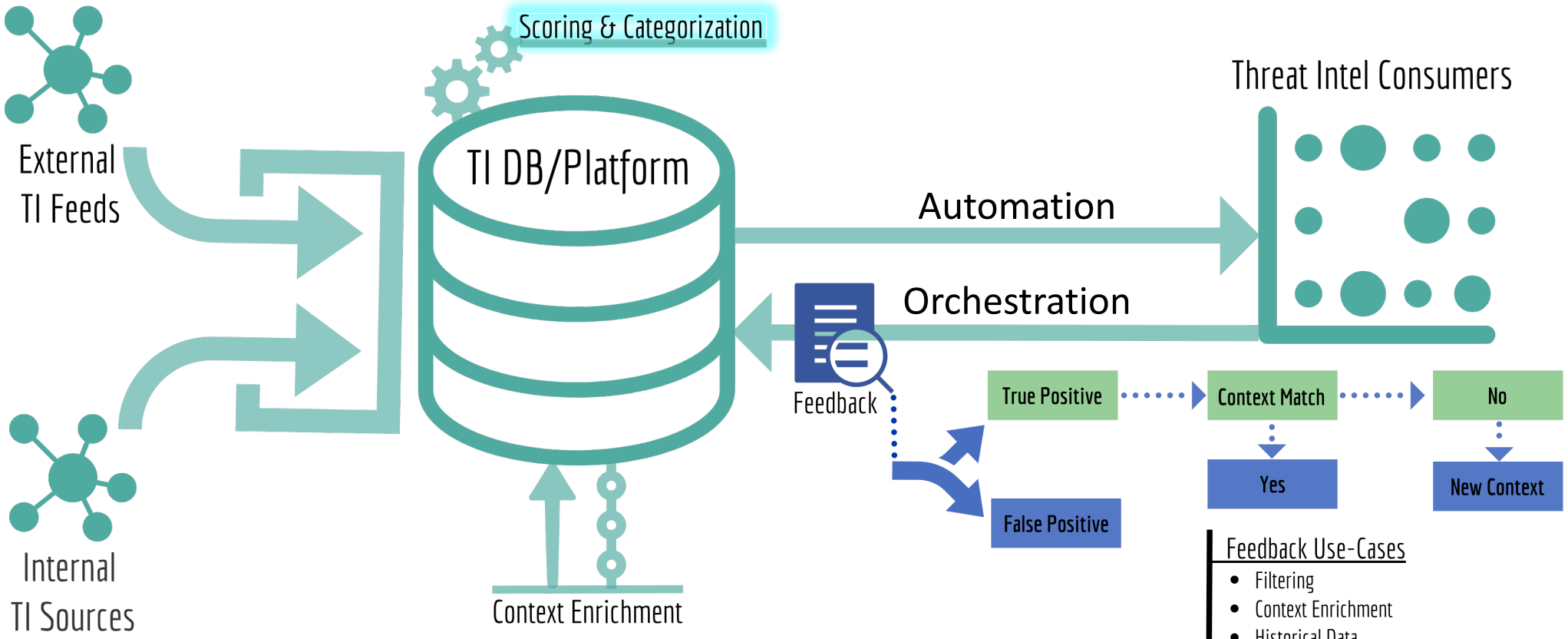
Scoring >>>



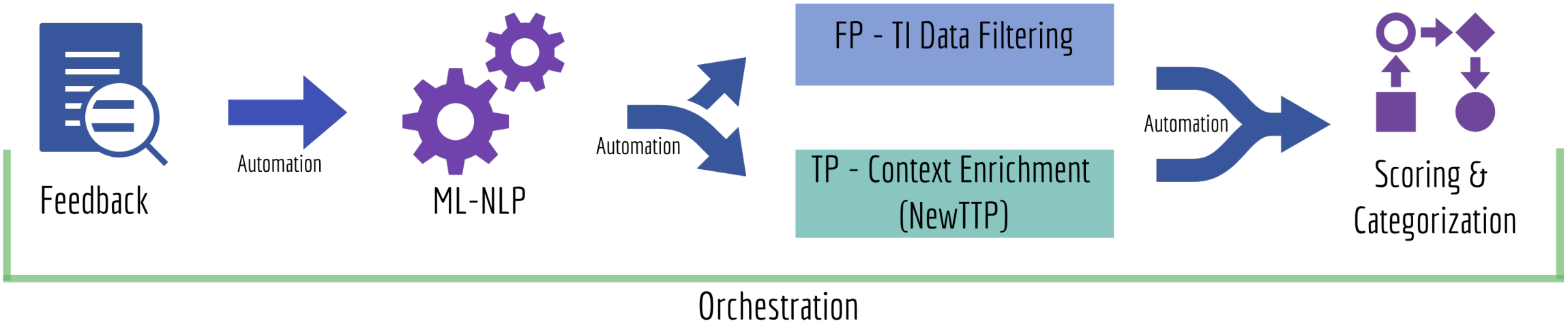


<<< Categorization

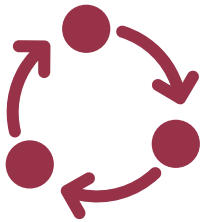
ANALYST DRIVEN - Feedback loop



ANALYST DRIVEN - Feedback loop & Machine Learning



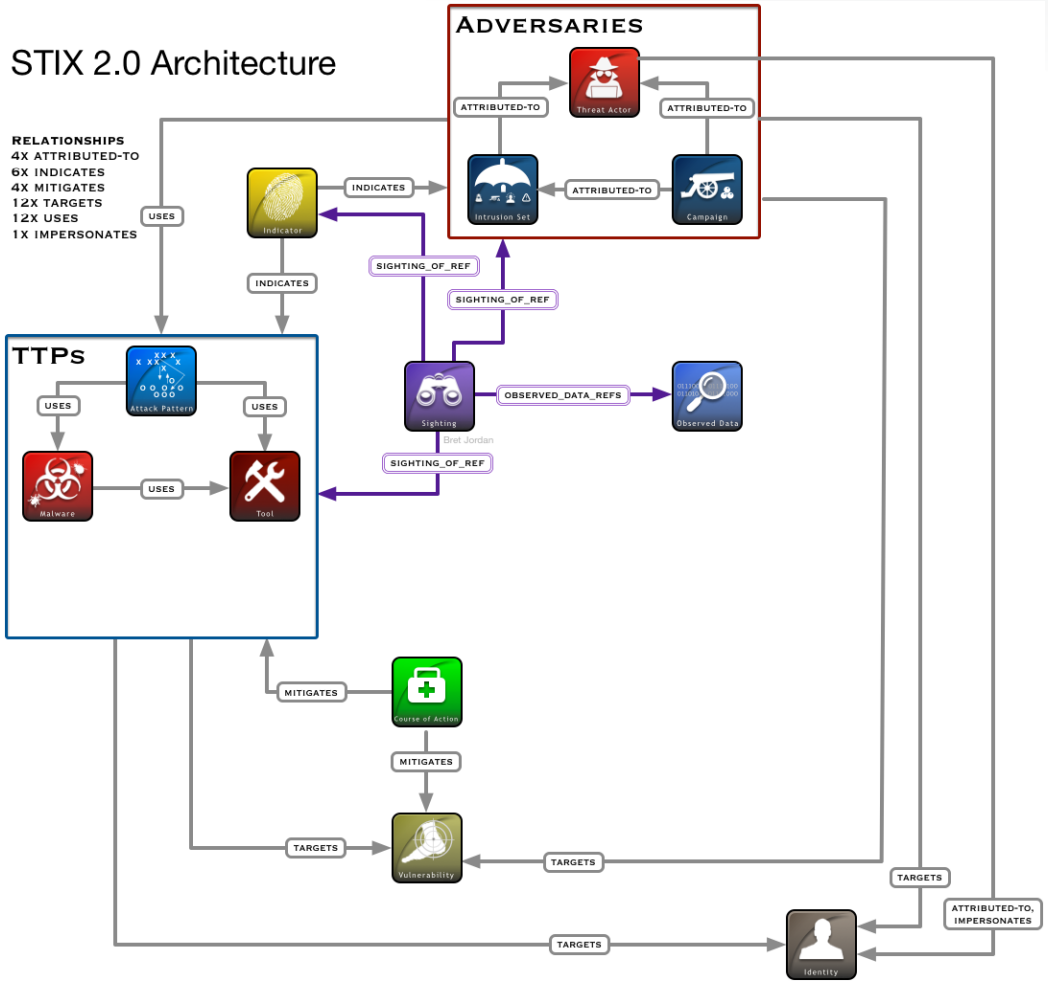
ANALYST DRIVEN - Machine Learning Use-cases

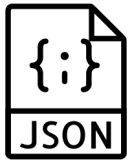


Dynamic TI
Apply ML on Feedback Loop
for automated scoring and categorization

Data Mining
Predict Adversary
TTPs and Infrastructure

DELIVERABLE - Standardized Threat Intel Format





DELIVERABLE - Metrics

~~Actor Driven~~

Actor Driven metrics will betray you on the long run.

How and Where

Start by how and where is used Threat Intelligence.

Audience

Tactical / Operational / Strategic

RSAConference2020

LEAD CTI Framework
Key Takeaways

“Apply”

- Next week you should:
  - Create Threat Profile and understand from **whom** and **what** you are trying to defend.
  - Promote CTI within your organization and find new stakeholders.
- In the first three months following this presentation you should:
  - Set Threat Intel Program Requirements and use LEAD maturity model to understand where you stand.
  - Try to make sense of your CTI data by applying scoring and categorization
  - Use Security Orchestration and Machine Learning to get the best of CTI
  - Use the results to create metrics that will justify and add value to your CTI Program

RSAConference2020

Q&A