



LIFE AFTER THREAT INTELLIGENCE EXCHANGE

# THREAT MANAGEMENT AND OUR TECHNICAL LEARNINGS IMPLEMENTING CTI

Joep Gommers @joepgommers  
Marko Dragoljevic @chipi\_nbgd

[Download whitepaper](http://bit.do/threatintel)  
<http://bit.do/threatintel>

*15min*

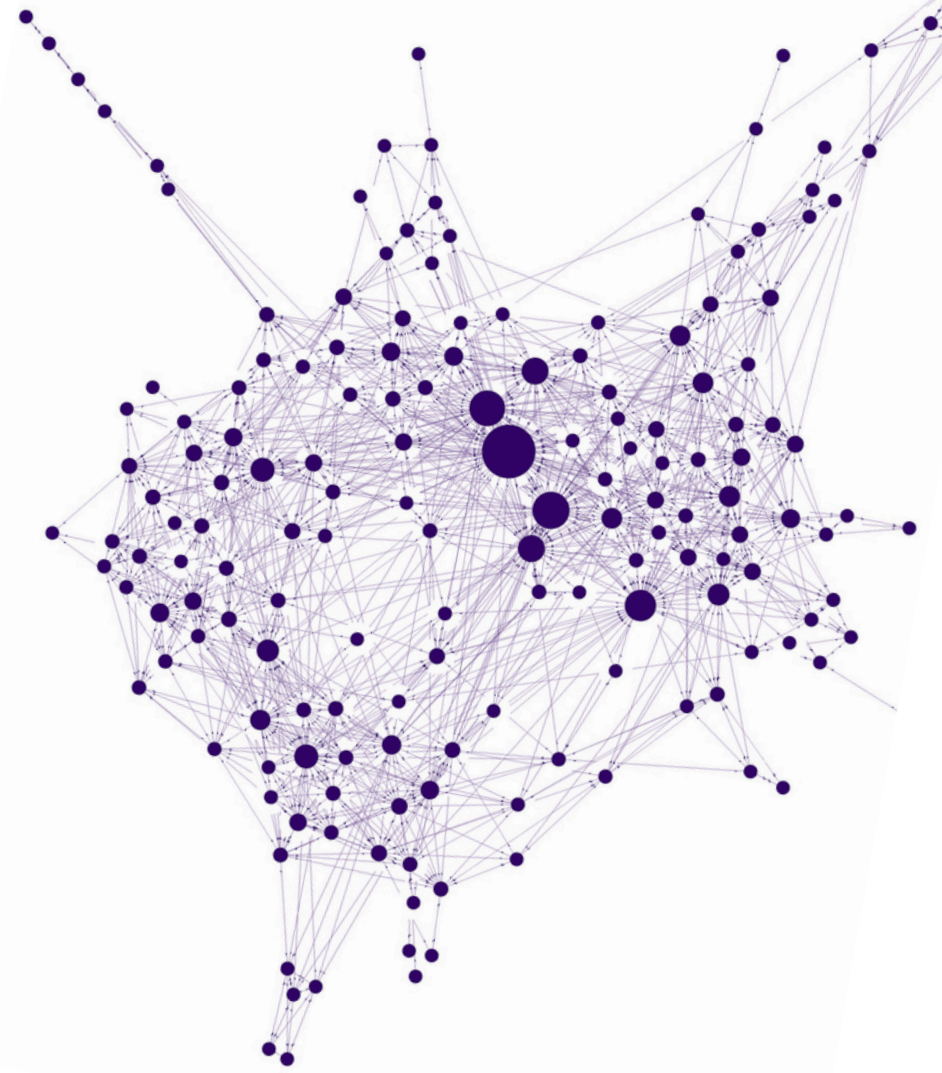
threat management (people, process)

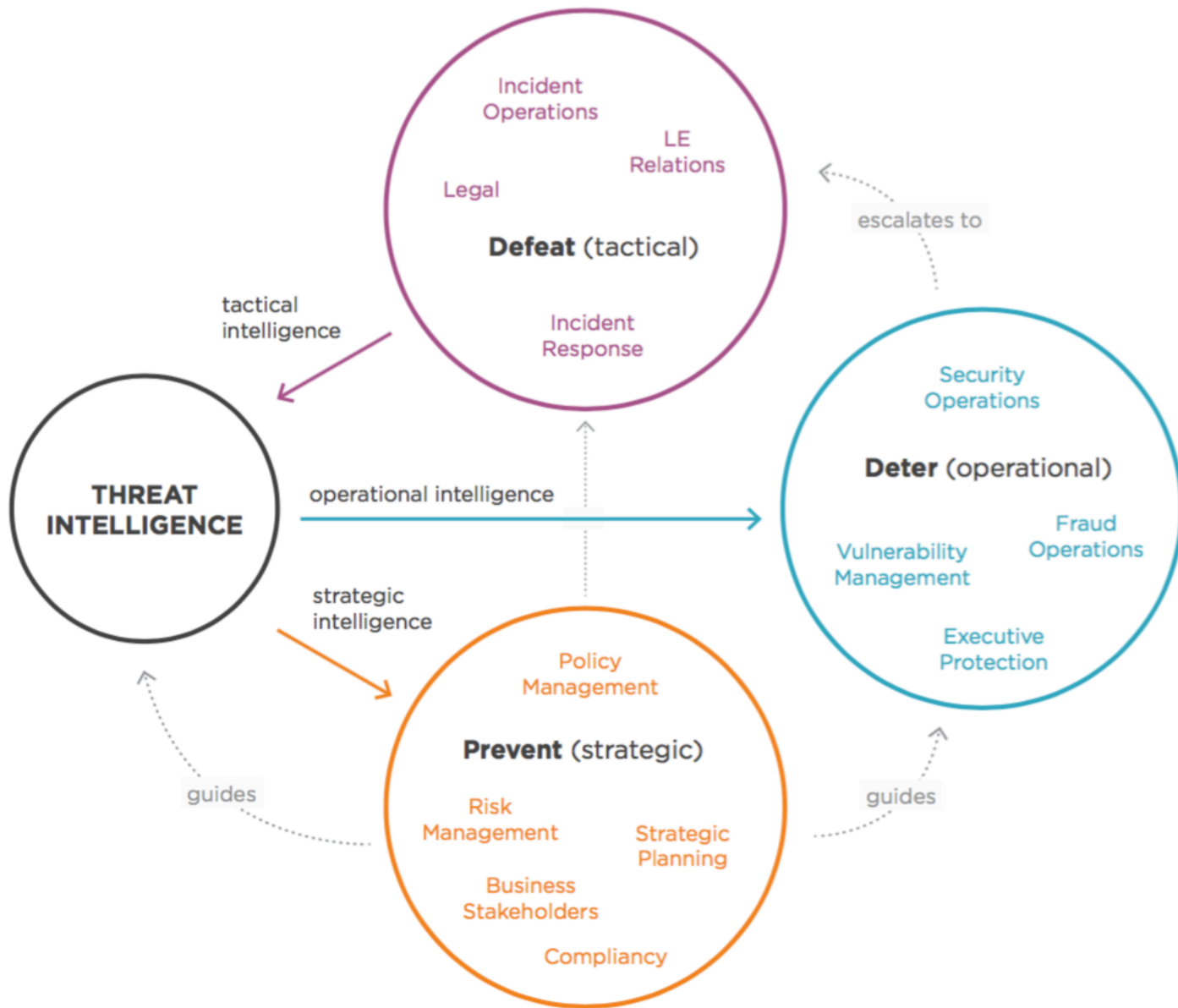
*10min*

practical technology learnings implementing CTI (technology)

*5min*

Q&A







# COMMON CHALLENGES AND PROBLEMS

## *Intelligence relevancy*

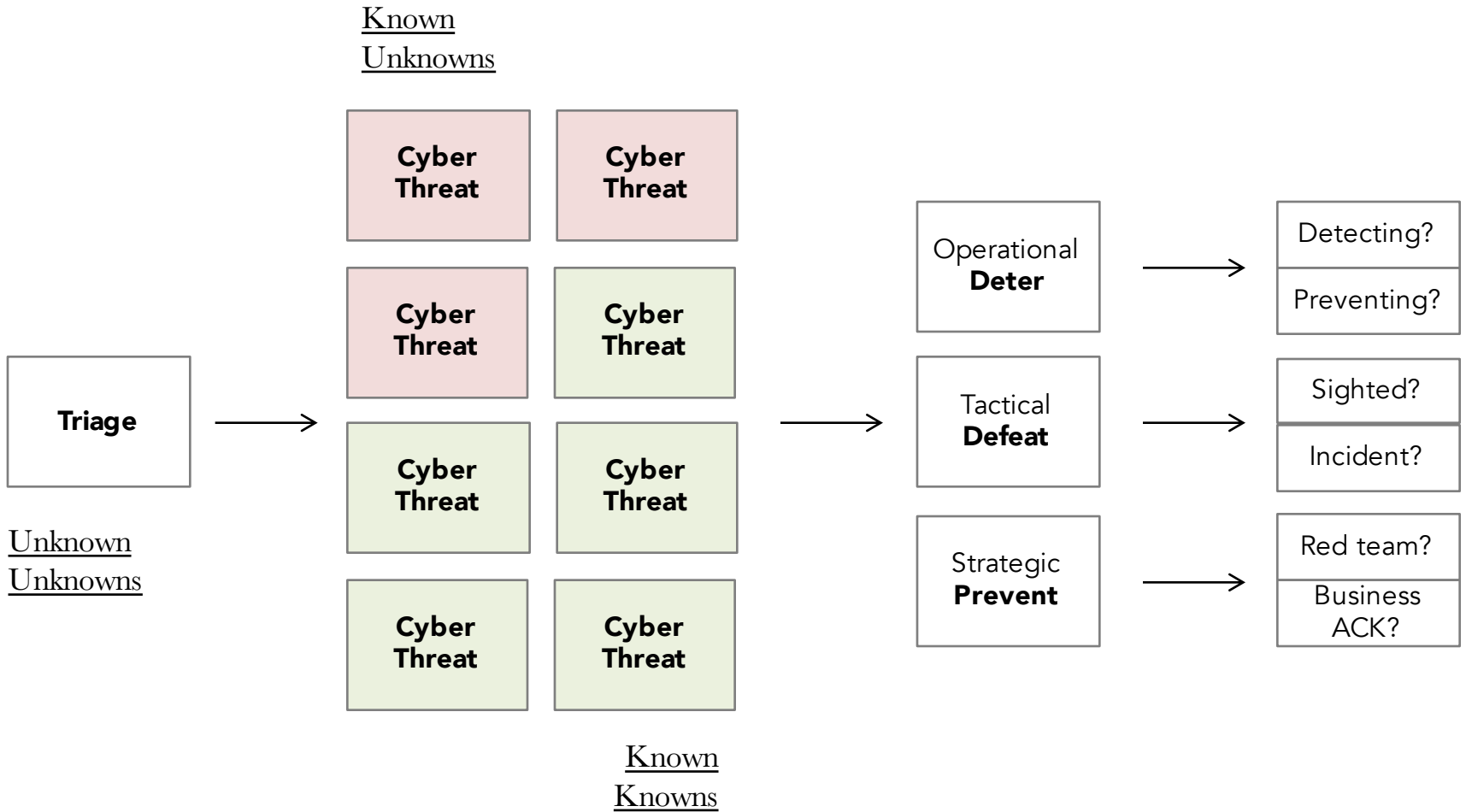
Cyber defences rely upon relevant threat intelligence, real-time collaboration and suitably configured responses. EclecticIQ provides actionable intelligence by normalizing and consolidating threat intelligence from a range of sources.

## *Process efficiency*

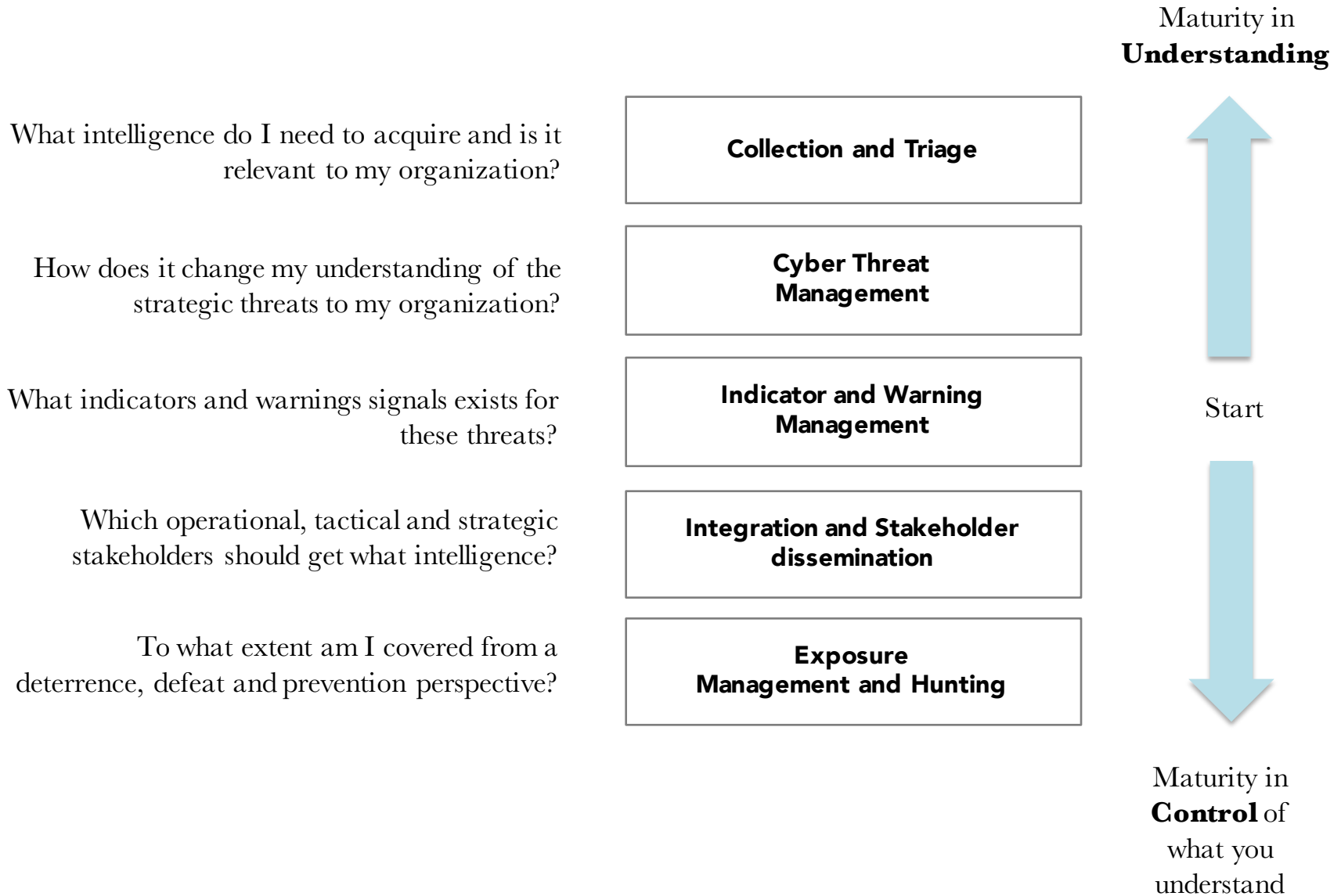
We solve the problems of repetitive work and complex analysis involved in enabling security staff to harness the power of intelligence in incident response, intelligence analysis, revenue assurance, security operations and security leadership.

## *Enterprise Integration*

Evolving threats need live integration of actionable threat indicators and intel from detection, prevention and response technologies. Forget repetitive work and custom engineering. Turn cyber intel into business value and correct your defenses.



# THREAT MANAGEMENT PRACTICE





# WE'VE LEARNED TOGETHER WITH OUR CUSTOMERS

- Intelligence is a practice, not just an artefact
- Intelligence related to the entire ecosystem from Red to Blue concepts
- Build for real stakeholders
- Balance people, process with **TECHNOLOGY** (stay tuned for @marko)
- Maturity is really just business need, build for reality not perception
- Maturity in understanding; beyond IOC/IOA into threat management
- Maturity in control; beyond integration and exposure management

# A STAKEHOLDER-CENTRIC APPROACH TO BUILDING A CYBER THREAT INTELLIGENCE (CTI) PRACTICE

how to make cyber threats relevant to executives, business stakeholders, security operations and incident responders

---



[Download whitepaper](http://bit.do/threatintel)  
<http://bit.do/threatintel>

# THREAT INTELLIGENCE PLATFORM

Threat Intelligence Platforms have emerged to facilitate technology needs for CTI / Threat Management practices and/or if you're building your self consider core functionality:

- **Collection and Exchange**
- **Normalization, Fusion and Enrichment**
- **Relevancy and Triage**
- **Complex Analysis**
- Concern Management (Cases, Campaigns, Threats, Topics, etc.)
- IOC Management
- Exposure Management
- Human dissemination
- **Machine integration (security controls, workflow systems, etc.)**

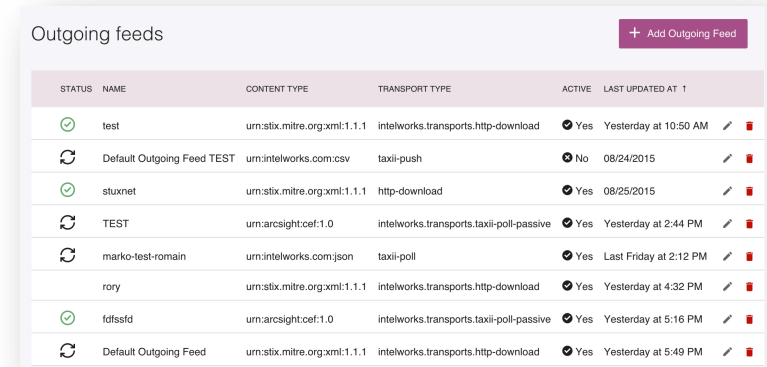
# MOTIVATION AND OBSERVATION

- Share technology perspective on the CTI space as an engineer-invader
- Share challenges we have encountered building EclecticIQ TIP solution
- Share best-practices to get started if you're building or buying
- Common terminology
- Adopt processes that work well in other areas for CTI
  - Agile Software Development
  - DevOps
- Focus on off-the-shelf technologies and investment into problem-solution solving
- CTI is not a big data space, unless
  - you're into raw collection yourself
  - you consider security ops as CTI, which it is not

# COLLECTION, EXCHANGE AND INTEGRATION

Automate everything you can with  
HUMAN supervision and THEN focus on  
HUMAN itself

- Get data in
  - Process data
  - Enrich data
  - Process: correlate, group, tag -
  - Get data out
- In/Out flows should be standards based
  - Structural and functional deepening
  - Content formats and transport mechanisms



STATUS	NAME	CONTENT TYPE	TRANSPORT TYPE	ACTIVE	LAST UPDATED AT		
✔	test	urn:stix.mitre.org:xml:1.1.1	intelworks.transports.http-download	✔ Yes	Yesterday at 10:50 AM	↻	✖
⌛	Default Outgoing Feed TEST	urn:intelworks.com:csv	taxii-push	⊘ No	08/24/2015	↻	✖
✔	stuxnet	urn:stix.mitre.org:xml:1.1.1	http-download	✔ Yes	08/25/2015	↻	✖
⌛	TEST	urn:arcsight:cef:1.0	intelworks.transports.taxii-poll-passive	✔ Yes	Yesterday at 2:44 PM	↻	✖
⌛	marko-test-remain	urn:intelworks.com:json	taxii-poll	✔ Yes	Last Friday at 2:12 PM	↻	✖
	rory	urn:stix.mitre.org:xml:1.1.1	intelworks.transports.http-download	✔ Yes	Yesterday at 4:32 PM	↻	✖
✔	fdfsfd	urn:arcsight:cef:1.0	intelworks.transports.taxii-poll-passive	✔ Yes	Yesterday at 5:16 PM	↻	✖
⌛	Default Outgoing Feed	urn:stix.mitre.org:xml:1.1.1	intelworks.transports.http-download	✔ Yes	Yesterday at 5:49 PM	↻	✖

*EclecticIQ Platform*

Transport

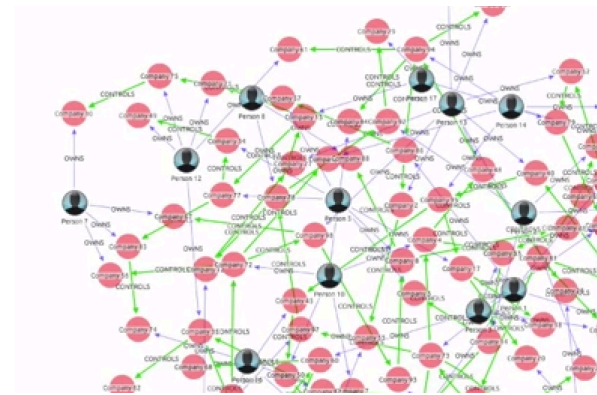
- TAXII, HTTP, FTP, Disk, etc.

Content

- STIX, OpenIOC, IODEF
- YAML, JSON, CSV
- SNORT, YARA

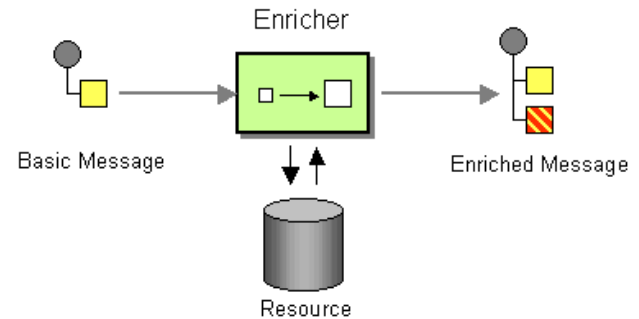
# NORMALIZATION AND FUSION

- One internal format to rule them all
- Flexible for being future proof
- This is area where to invest and try to absorb complexity
- Don't think about how to make it easy, think about how to be flexible and be able to catch up
- Data Fusion
- Semantical Fusion



# ENRICHMENT

- Asynchronous collection
- Many APIs available; open and commercial. Use them!
- SIGINT
- Enterprise Integration Patterns
- Supports data fusion
- Supports data clustering
- Support data classification



# RELEVANCY AND TRIAGE

- Automated vs Machine assisted (human)
- Evaluation on a variety of axis related to threshold and relevancy criteria
- Reliability
- Credibility
- Relevancy
  - Content
  - Time
- Many more..

The screenshot displays the EclecticIQ Platform interface. On the left, a 'Discovery' table lists various entities and rules. The table has columns for 'TYPE', 'TITLE', and 'RULE NAME'. The 'URI: securetargeting.com/' row is highlighted. On the right, a 'NEIGHBOURHOOD' graph shows a central node 'securetargeting.com' connected to several other nodes, including 'http://secure...', 'URI: secureta...', 'C2C Site: sec...', 'Domain: secur...', and 'C2C Site: sec...'. The graph is labeled 'DIRECTLY RELATED ENTITIES'.

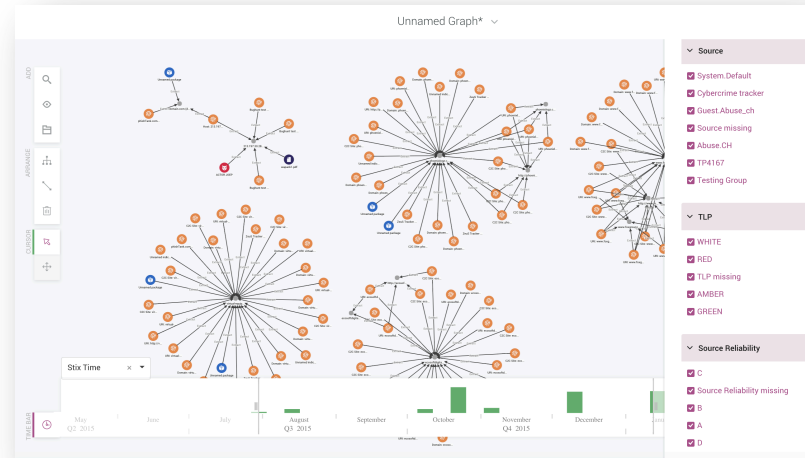
TYPE	TITLE	RULE NAME
Host	213.197.30.28	Example
URI	securetargeting.com/	Example
WebInject		Example
C2C Site	www.coldworld.c	Example
Domain	vogel-no0t.com	Example
C2C Site	originfiness.fa	Example

*EclecticIQ Platform*



# COMPLEX ANALYSIS

- Multi views optimized for specific use-cases
- Don't be afraid to create specific data views
- Each class of problems deserved specific solutions
- Polygot persistence
  - Graph
  - Search
  - Document
  - Etc.



TITLE	SOURCE	TLP
<input type="checkbox"/> Malicious E-mail Subject Line	TAXII Stand Samples	
<input type="checkbox"/> untitled	TAXII Stand Samples	Red
<input type="checkbox"/> Malicious file	TAXII Stand Samples	
<input type="checkbox"/> Detected Poison Ivy beaconing through perimeter firewall	TAXII Stand Samples	
<input type="checkbox"/> Victim Targeting: Customer PII and Financial Data	TAXII Stand Samples	
<input type="checkbox"/> Victim Targeting: Customer PII and Financial Data	TAXII Stand Samples	
<input type="checkbox"/> ZBot	TAXII Stand Samples	
<input type="checkbox"/> 192.168.1.1	TAXII Stand Samples	
<input type="checkbox"/> untitled	TAXII Stand Samples	
<input type="checkbox"/> Block traffic to PIVY C2 Server (10.10.10.10)	TAXII Stand Samples	