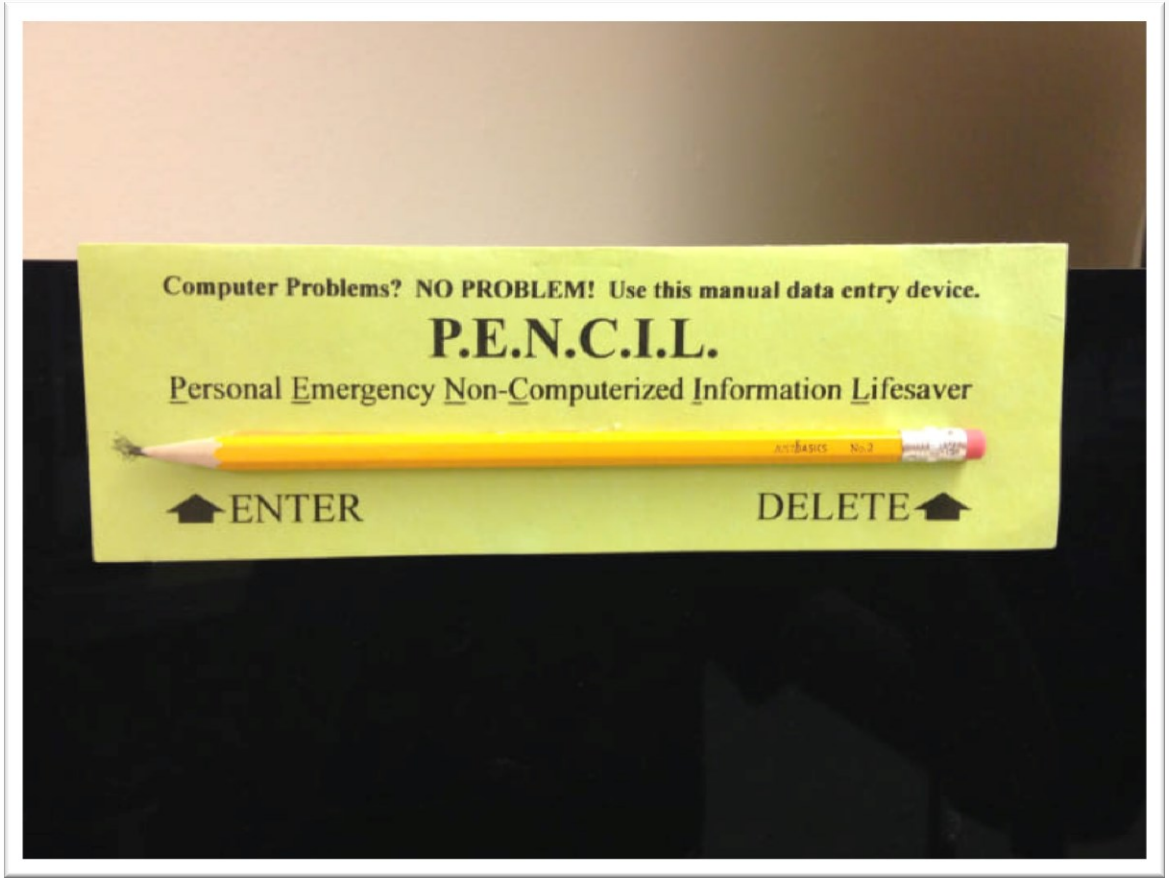
SCALING INTELLIGENCE FOR COMMUNITIES

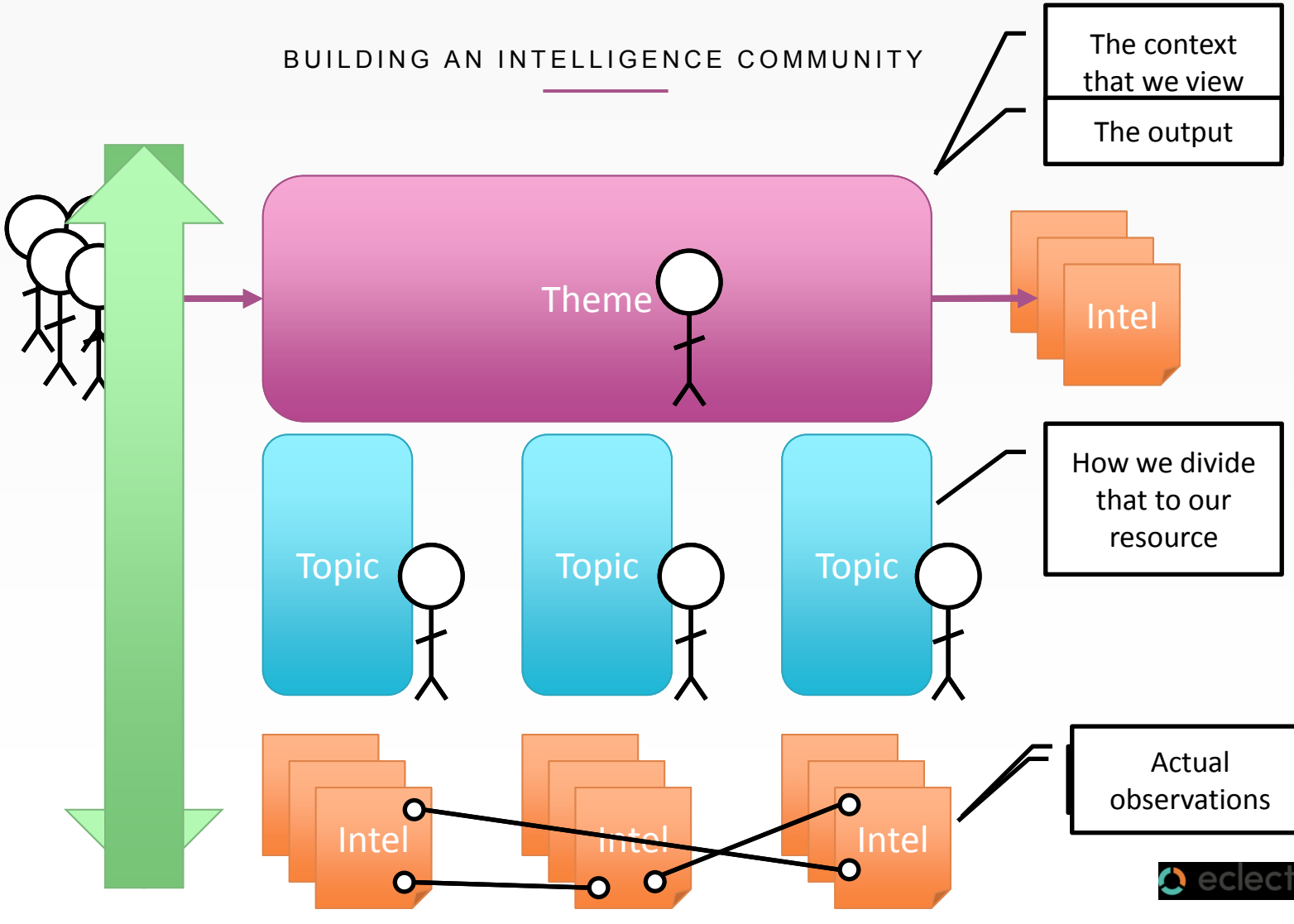
ENISA – 31 Oct 17

HUMANS DON'T SCALE (WELL)



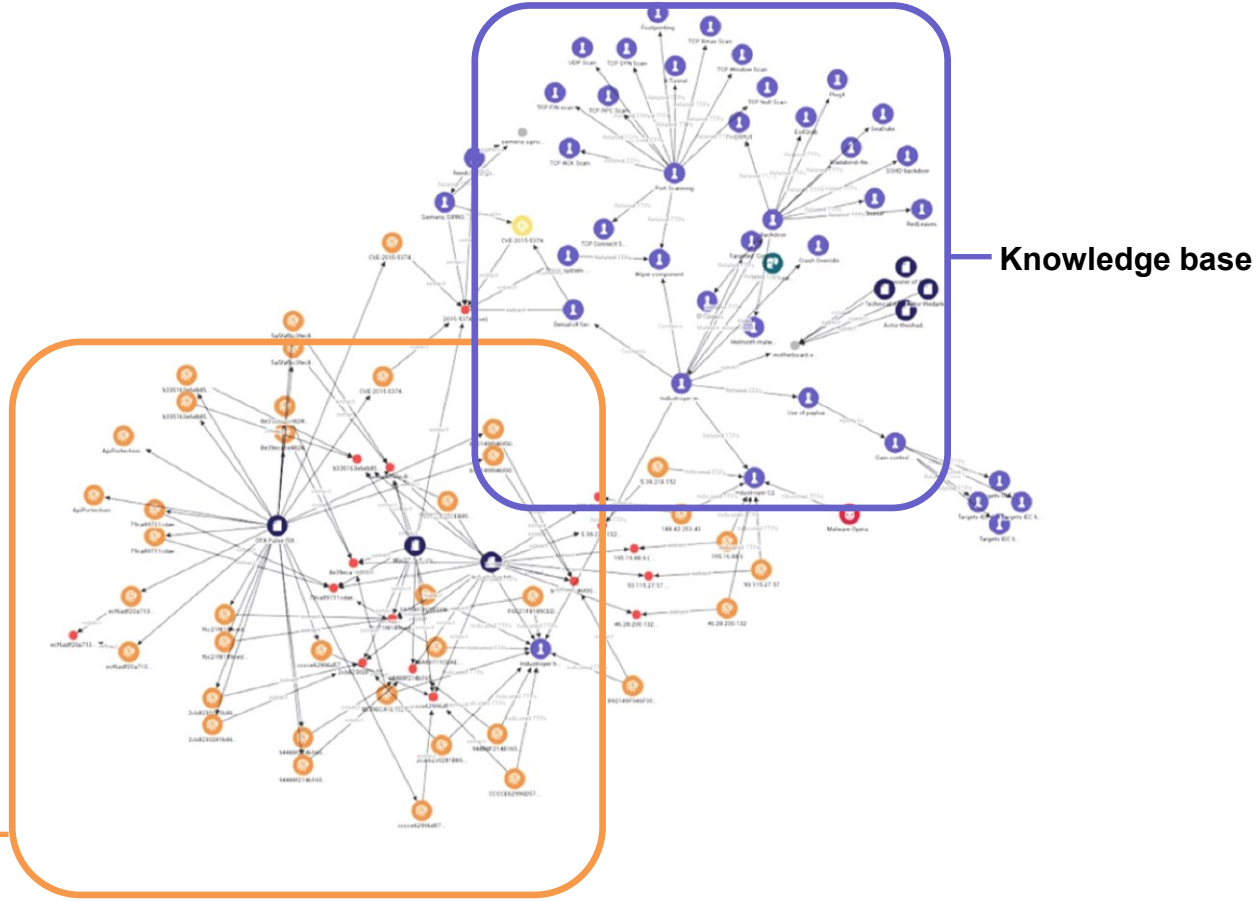
https://img.devrant.io/devrant/rant/r_819863_VPVHo.jpg

BUILDING AN INTELLIGENCE COMMUNITY

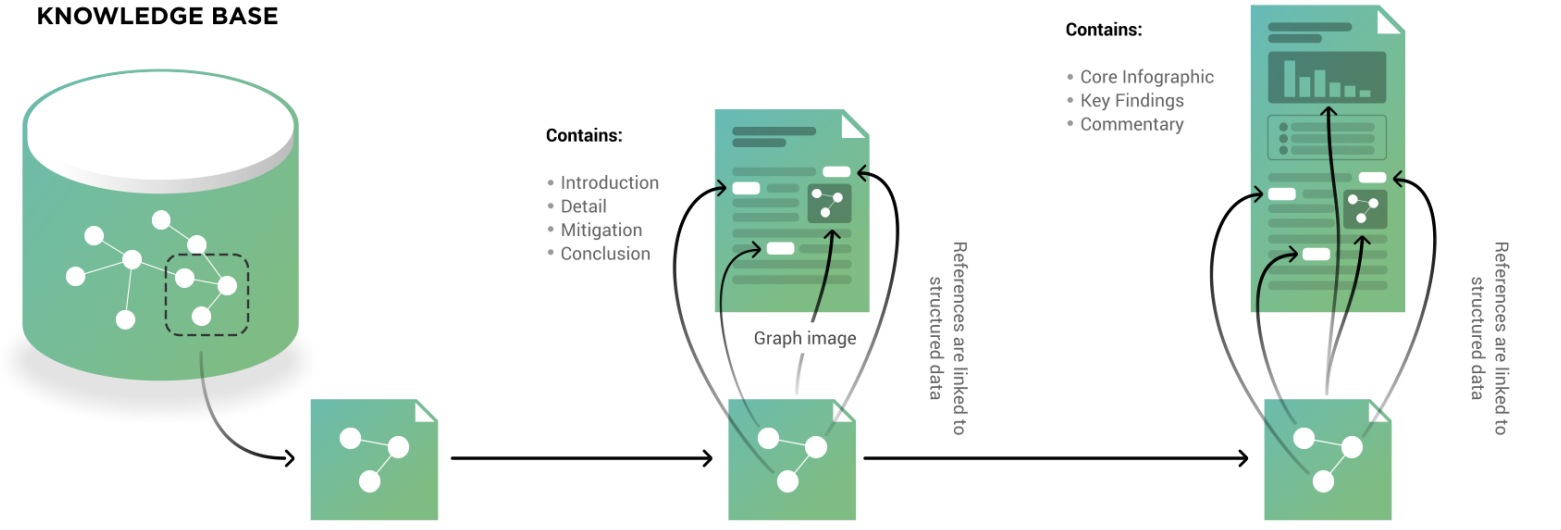


THREAT INTEL APPROACH

- STIX, MISP, OpenIOC, <insert structured language here>
- Clustering a knowledge base for topics/themes
- Automate the process of ingestion, analytics, enrichment and notification
- Pivot for interesting overlaps and produce a report _*from*_ the data



STRUCTURED PRODUCTS



OPERATIONAL

- Indicator Watchlists
- EDR and/or SIEM Feeds
- Threat Profile / Structured Library sharing

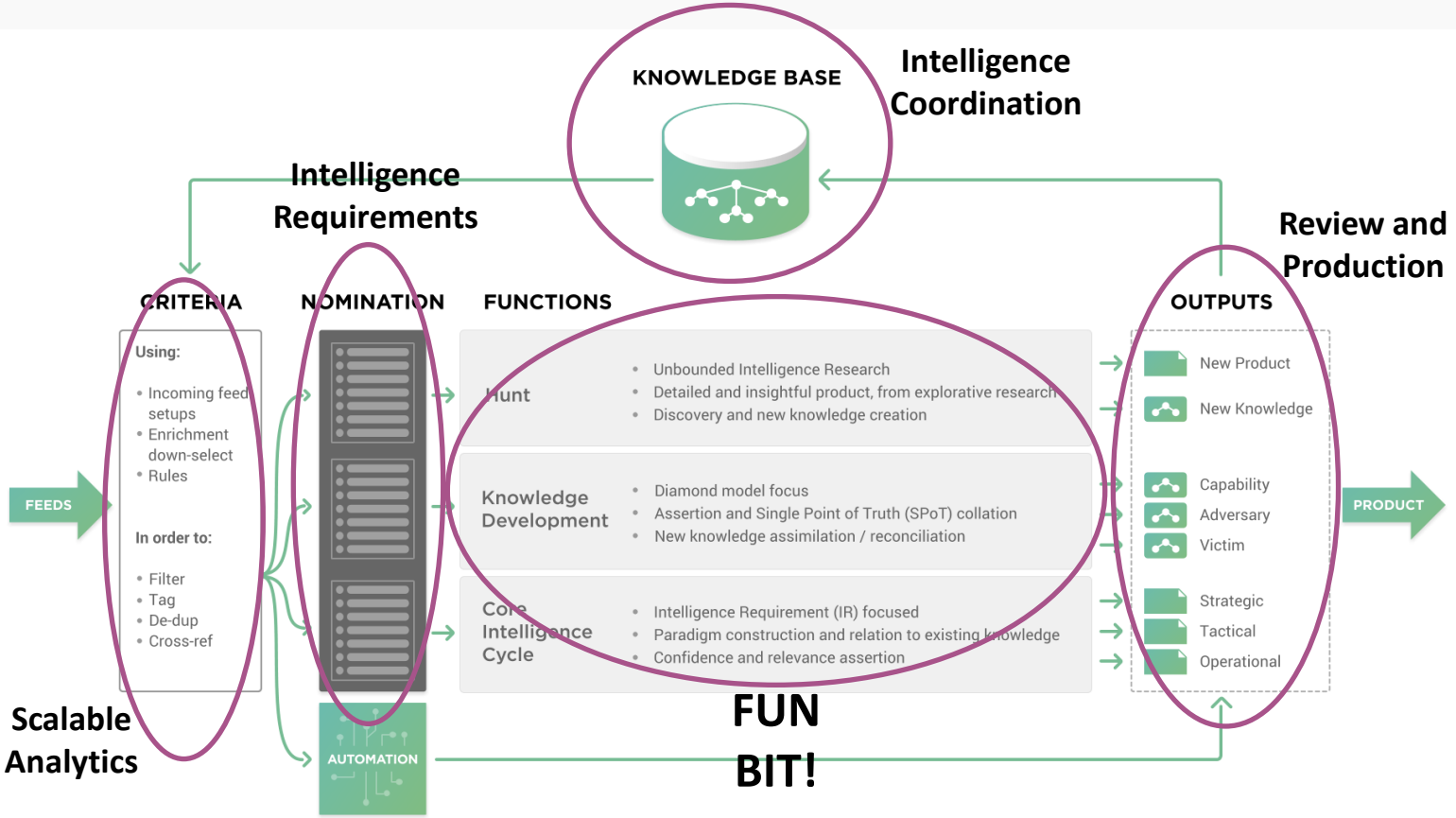
TACTICAL

- Paradigm-oriented Digests
- Thematic Reporting
- Ad-hoc and responsive analysis

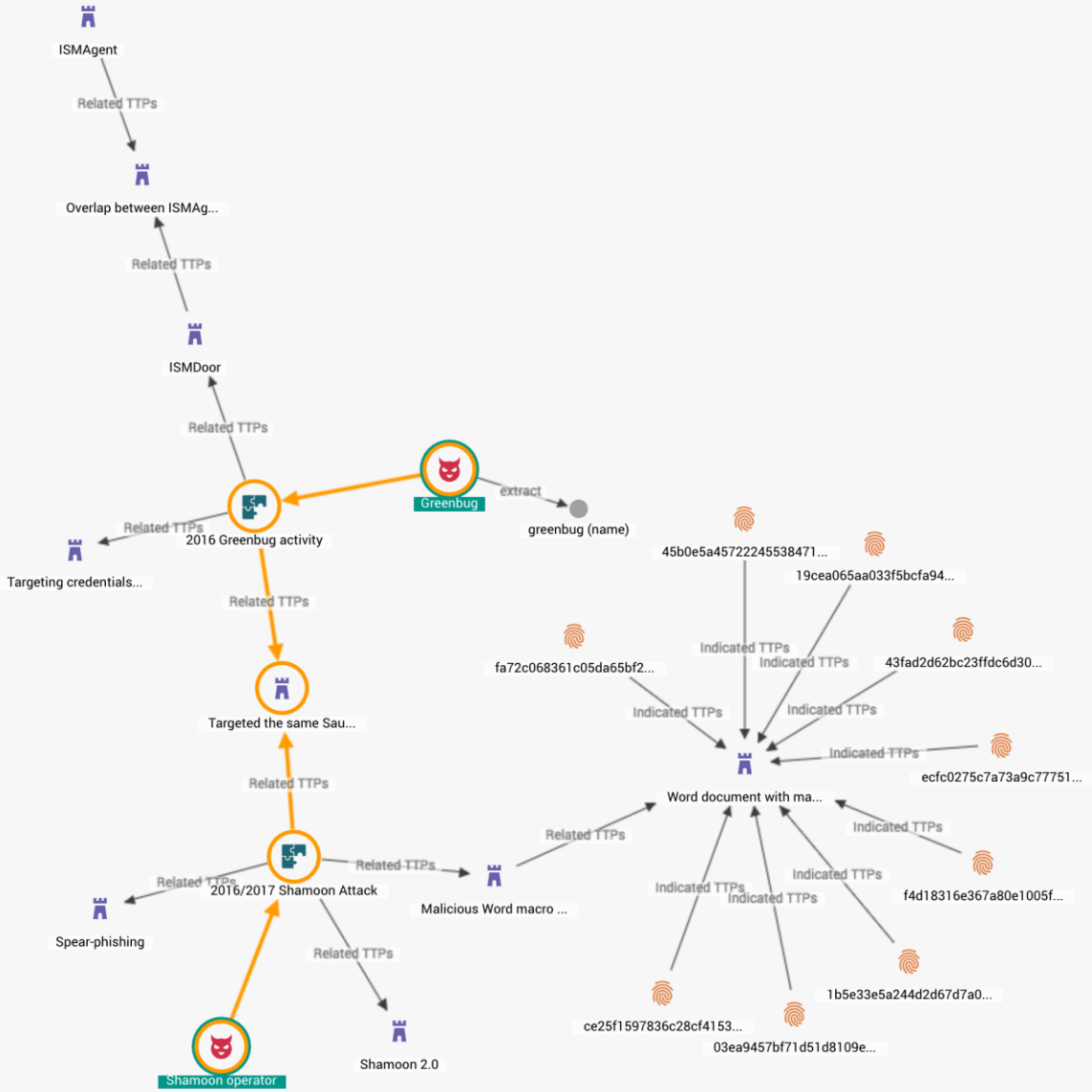
STRATEGIC

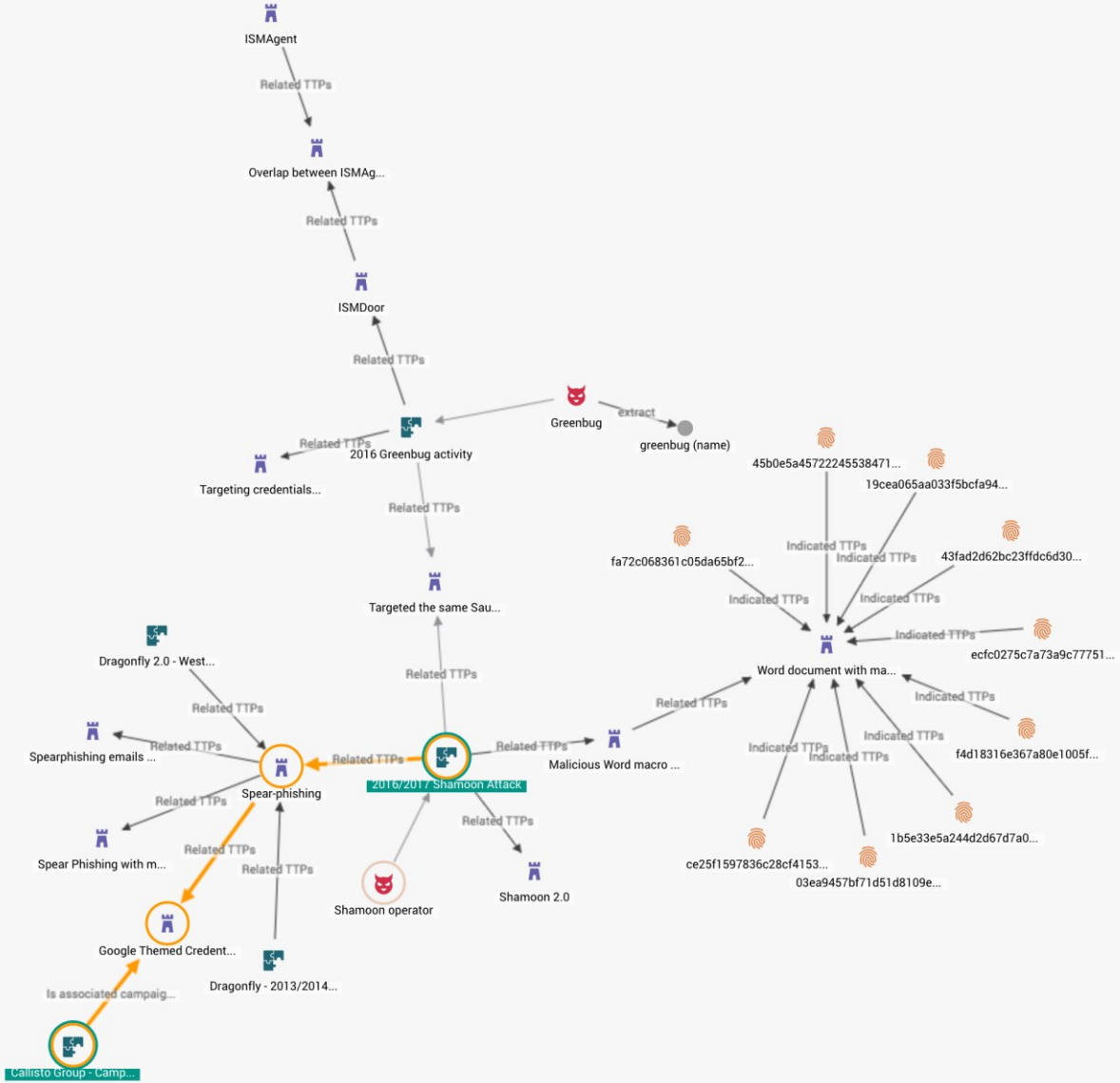
- Trend reporting
- Core messages as statistics
- Summarization and unstructured commentary

HUMANS WORKING ON DATA



eclectic iq


ISMAgent
Related TTPs
Overlap between ISMAg...
Related TTPs
ISMDoor
Related TTPs
Greenbug
extract
greenbug (name)
2016 Greenbug activity
Related TTPs
Targeting credentials...
Related TTPs
Targeted the same Sau...
Related TTPs
2016/2017 Shamoon Attack
Related TTPs
Spear-phishing
Related TTPs
Malicious Word macro ...
Related TTPs
Shamoon operator
Related TTPs
Shamoon 2.0
45b0e5a45722245538471...
19cea065aa033f5bcfa94...
fa72c068361c05da65bf2...
43fad2d62bc23ffdc6d30...
Indicated TTPs
Indicated TTPs
Indicated TTPs
Indicated TTPs
Indicated TTPs
ecfc0275c7a73a9c77751...
Word document with ma...
Indicated TTPs
f4d18316e367a80e1005f...
Indicated TTPs
Indicated TTPs
Indicated TTPs
1b5e33e5a244d2d67d7a0...
ce25f1597836c28cf4153...
03ea9457bf71d51d8109e...


ISMAgent
Related TTPs
Overlap between ISMAg...
Related TTPs
ISMDoor
Related TTPs
Greenbug
extract
greenbug (name)
Related TTPs
2016 Greenbug activity
Targeting credentials...
Related TTPs
Targeted the same Sau...
45b0e5a45722245538471...
19cea065aa033f5bcfa94...
fa72c068361c05da65bf2...
43fad2d62bc23ffdc6d30...
Indicated TTPs
Indicated TTPs
Indicated TTPs
Indicated TTPs
Indicated TTPs
ecfc0275c7a73a9c77751...
Word document with ma...
Related TTPs
Indicated TTPs
Indicated TTPs
Indicated TTPs
f4d18316e367a80e1005f...
Malicious Word macro ...
Related TTPs
Related TTPs
Related TTPs
Dragonfly 2.0 - West...
Related TTPs
Spearphishing emails ...
Related TTPs
Related TTPs
Spear-phishing
2016/2017 Shamoon Attack
Related TTPs
Related TTPs
Spear Phishing with m...
Related TTPs
Related TTPs
Related TTPs
Shamoon operator
Shamoon 2.0
ce25f1597836c28cf4153...
03ea9457bf71d51d8109e...
1b5e33e5a244d2d67d7a0...
Google Themed Credent...
Dragonfly - 2013/2014...
Is associated campaig...
Callisto Group - Camp...

SUMMARY

- Humans don’t scale (well)
  - Orient around structured objects (data)
  - Automate ingest, analytics, enrichment
  - Data-driven reporting

- Have scalable processes
  - Identify bottlenecks – decide threshold for ‘quality vs timeliness’
  - Let the analysts analyse
  - Don’t forget to sense check the big picture!