A Standard Model for Threat Intelligence Practices
Agile Threat Intelligence

Lessons learned implementing threat intelligence practices in national security and large enterprise globally

– Joep Gommers, CEO EclecticIQ
Cyber threats
• Indicators of Compromise / Indicators of Attack
• Knows modus operandi – tools, techniques and procedures
• Who and why
• Hundreds of open-sources
• Dozens of communities
• Dozens of great intelligence companies like Group-IB

Threat intelligence Practice
• Turn information about cyber threats into value

Cyber security
• Cyber Operations
• Security operations
• IT Architecture
• IT Decision making
• Incident response
• Vulnerability Management
• Fraud Operations
• Business Risk
• Detection and Prevention
• Et cetera
(10 min)  target centric intelligence
(10 min)  standard models for cyber threat intelligence
(10 min)  example: agile threat intelligence
- Knowledge, tool and therefore capability proliferation of cyber threats is many factors faster than traditional domains. Therefore the cycle should speed up dramatically, leaving no time for repeated hand-over and translation of need.

- Expert knowledge can not be build up in time across all stakeholders. Keeping them in the loop keeps knowledge (somewhat) in sync. Collaborative approaches are necessary.
Long view planned
Short view planned
Immediate
Auto

Requirements and needs of stakeholders
Drive acquisition of new information
New information becomes available

Stakeholder
New needs arise
Actionable information or insights become available

http://eclectic.iq/resources
Long view planned

Short view planned

Immediate

Auto

New needs arise

Requirements and needs of stakeholders

Drive acquisition of new information

New information becomes available

Stakeholder

Actionable information or insights become available

http://eclectic.iq/resources
99f927f97838eb47c1d59500ee9155adb55b806a & & & & <p>http://eclectic.iq/resources
Bridging the gap
• There is a significant gap between use-cases for intelligence and the intelligence provided in the market
• Multi-vendor intelligence doesn’t consolidate well without technology and process

One knowledge base
• Build one knowledge base / repository of your cyber threat knowledge
• Make sure all stakeholders receive what they need from that, asynchronously

Build what you need
• Build only what you need to service your use-cases and stakeholders
• Don’t fall into the analysis-is-fun trap… even if its fun!

http://eclectic.iq/resources
standard models for threat intelligence

http://eclectic.iq/resources
MATURITY MODEL
How to get from A to B

CAPABILITY MODEL
What processes of management, steering, analysis, production and automation can you build?

PROCESS MODEL
How will it work day to day?

http://eclectic.iq/resources
Maturity model

https://www.eclecticiq.com/resources

• Plan for achievable and realistic steps towards full capability

• Alignment with business
  - stakeholder management
  - requirements management
  - awareness

• Ability to understand
  - source management
  - analysis
  - production
  - sharing and collaboration

• Ability to control / action
  - Dissemination
  - Integration
  - Specific use-cases
Capability model
Operational models
Realistic planning
• Take realistic steps from year to year. Prove value for budget.

Structure matters
• Analysts are the core of any intelligence capability, but as with any business capability – they need process, structure and technology enablement

Efficiency is HARD
• Efficiency is hard
• Estimating what you need to create certain outcome is HARD
• Measure
• Plan well
Finally! Agile

That little red thingy is our agile intel team
Example: EclecticIQ’s fusion center

Why: connecting 50 leading intelligence suppliers globally with the use-cases of our customers

Fusion Centers in Amsterdam, London, Brussels and Middle East (opening soon)

Mission:
- Data normalization
- Analytic consolidation
- Quality Assurance
- Knowledge base
- Analysis and Production
- Stakeholder management
- Dissemination and integration

http://eclectic.iq/resources
Three key teams that each fulfill a set of capabilities required for the entire intel team to work:

- Core cycle (short)
- Knowledge development (medium, ongoing)
- Investigations (long, ad-hoc)
Core cycle
• Short cycle
• Ongoing
• Quality Assurance
• Immediate action

Knowledge base
• Medium cycle
• Planned
• Institutionalize knowledge

Investigations
• Long cycle
• Planned
• Create new insights
<indicator id="id-1-indicator-61hec5e-38b-4e19-3d116a7f79150c" timestamp="2017-09-11T07:38:38.384374+00:00">
<indicator:Title>99f927f97838eb47c1d59500ee9155adb55b806a</indicator:Title>
<indicator:Type>File Hash Watchlist</indicator:Type>
<indicator:Descriptionstructuring_format="html"><p>99f927f97838eb47c1d59500ee9155adb55b806a &amp;nbsp; &amp;nbsp; &amp;nbsp; &lt;/p&gt;</indicator:Description>
<indicator:Indicated_TTP>
<stixCommon:TTP idref="id-1-ttp-29b16435-87dd-4686-93bf-ba53b7b3f4db" timestamp="2017-08-25T17:58:42.386214+00:00"/>
</indicator:Indicated_TTP>
<indicator:Likely_Impact><stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">U</stixCommon:Value></indicator:Likely_Impact>
</indicator>
T:1 Supplier sends indicators with associated TTPs
T:2 Core Cycle corrects tags
T:3 Other suppliers send new TTPs
T:4 Knowledge development team pick up story and find related indicators
T:5 Investigations writes report and discovers connections

T:1: detection is instrumented with indicators
T:2: prevention is instrumented with high confidence indicators
T:3-4: TTPs go to use-case development team for SIEM
T:5: Report is send to stakeholders
GET STARTED, WHILE YOU PLAN
Evaluate your access to information on a constant bases, determine the most appropriate action

- Assess quality
- Assess relevance
- Nominate for later attention, or
- Perform immediate action

IMPLEMENT FIRST PROCESSES
Start with the basics.

- Stakeholder Management: who need what and when?
- Prioritize: threshold / requirements
- Weekly spring planning
- Daily stand-up
- Knowledge management
- Investigations
- Disseminate / Export
Sprint planning
Daily standup

Last 24:
- Completed an investigation into Generic Rat
- Reviewed 3 reports

Next 24:
- I want to investigate strange malware sample

Blockers:
- A suppliers api update has broken my workflow, and I'm awaiting a fix from integrations
- My Antarctic Thunder APT report is in need of a reviewer before release.
Insights

• Work per person
• Work by category
  - questions from stakeholders
  - quality assurance / supplier management
  - stakeholder management
  - overhead
  - analysis and production: daily digest
  - analysis and production: reports, etc.
• Cycle times
• Bandwidth vs stakeholder requirements (budget justification)
• Predictability and performance of team
• Quality of suppliers based on time spend on quality assurance, knowledge management, technology integration, etc.
• Cost of stakeholder support
Asynchronous
• Agile intelligence allows many people or teams to work concurrently
• Some things need to go fast, some things need to go smart and planned

Tools
• Agile tools will get you started quickly and provide value insights
• Threat Intelligence Platforms will enable easy report export and IOC integration based on ONE knowledge base

Happy customers
• Your internal stakeholders are the customers of your intelligence practice
• Measure their awareness of cyber threats
• Understand their requirements
• Measure their happiness