ENISA Threat Landscape:  
Current and Emerging Threat Assessment  

Louis Marinos  
18 June 2015
Why ENISA Threat Landscape?

• ... raising awareness of potential threats in cyberspace ...(mandate)

• Use available expertise to support Stakeholders in UNDERSTANDING the real threat

• Help developing protection according to the real threats
ENISA Threat Analysis Process

- Collect
  - Vendor 1 Report
  - Vendor 2 Report
  - Vendor n Report
  - Agency Study
  - R&D NGO Analysis
  - CERT Advisories
  - Feed Services

- Collate

- Analyse
  - Top Threats
  - Emerging Trends
  - Structure Data

- Set Context
  - Thematic Landscapes
  - Asset Types
  - Protective Controls
  - Threat Agents

- Disseminate
  - Information Dissemination

ETL

Flash Note

ETL State of play
Content and quality

- **Strategic (S):** the highest level information about threats.
  - Created by humans, consumed by humans
  - Lifespan months

- **Tactical (T):** at this level, stakeholders obtain aggregated information about threats, TTPs and their elements.
  - Created and consumed by humans and machines
  - Lifespan weeks, months

- **Operational (O):** technical information about incidents, etc.
  - Created by machines, consumed by machines/humans
  - Lifespan days, weeks
ENISA Threat Analysis Process

- Collect
  - Vendor 1 Report
  - Vendor 2 Report
  - R&D NGO Analysis
  - CERT Advisories
  - Feed Services

- Collate
- Analyse
  - Top Threats
  - Emerging Trends
  - Structure Data

- Set Context
  - Thematic Landscapes
  - Asset Types
  - Information Dissemination

- Disseminate
  - ETL

Facilitate input processing
Better management of input/output..
### ENISA Threat Analysis Process

<table>
<thead>
<tr>
<th>Collect</th>
<th>Collate</th>
<th>Analyse</th>
<th>Set Context</th>
<th>Disseminate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor 1 Report</td>
<td>Vendor 2 Report</td>
<td>Vendor n Report</td>
<td>Agency Study</td>
<td>R&amp;D NGO Analysis</td>
</tr>
<tr>
<td>ENISA Processing</td>
<td>Structure Data</td>
<td>Emerging Technologies</td>
<td>Current Threats</td>
<td>Thematic Landscapes (Sector)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Information Dissemination</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ETL</td>
</tr>
</tbody>
</table>

**Fast path..**

**Recent data modelling**
Understanding used structures.

Thematic Landscape

Attributes - Collection:
- Threat classification
- Affected Asset Type
- Affected Business Sector
- Emerging technology area
- Threat Agents
- Relevant Reference
- Trend
- Relevant URL

Attributes Current Threats:
- Description of threat
- Issues related to threat
- Overall trend
- Threat Agents
- Related threats
- Position in kill chain

Attributes Emerging Technology Area:
- Relevance of Emerging Area
- Possible Vulnerabilities/Weaknesses
- Top 10 threats (from current)
- Foreseen Trend
- Threat Agents
- Issues related to threat/area
- References

Attributes Sector:
- Asset Inventory
- Relevant Threats
- Possible Vulnerabilities/Weaknesses
- Assessed particular sector threats (from incidents)
- Threat Agents
- Threat mitigation practices/controls
- References

Attributes Threat Agents:
- Description
- Motives
- Capabilities
- References
ENISA Threat Analysis Process

<table>
<thead>
<tr>
<th>Collect</th>
<th>Collate</th>
<th>Analyse</th>
<th>Set Context</th>
<th>Disseminate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor 1 Report</td>
<td>Vendor 2 Report</td>
<td>Vendor n Report</td>
<td>Agency Study</td>
<td>R&amp;D NGO Analysis</td>
</tr>
<tr>
<td>CERT Advisories</td>
<td>Feed Services</td>
<td>ENISA Processing</td>
<td>Top Threats</td>
<td>Emerging Trends</td>
</tr>
<tr>
<td>Thematic Landscapes</td>
<td>ETL</td>
<td>Information Dissemination</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

People are asking...
Requirements, requirements... (mostly presentation, but also content)

- Provide hooks to risk assessment, based on this information develop a use case
- Develop landscapes for types of organizations (e.g. prosumers/freelancers, SMEs, and government agencies)
- Look at main asset types – infrastructure (power+ network+ housing), mobile/fixed endpoints, cloud/web servers, cloud/web applications
- Do a risk assessment for each of the above – pointing out the main threats to navigate
- Consolidate internal information
- Create various views.
### ENISA Threat Analysis Process

<table>
<thead>
<tr>
<th>Collect</th>
<th>Collate</th>
<th>Analyse</th>
<th>Set Context</th>
<th>Disseminate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor 1 Report</td>
<td></td>
<td></td>
<td></td>
<td>ETL</td>
</tr>
<tr>
<td>Vendor 2 Report</td>
<td></td>
<td></td>
<td></td>
<td>Information Dissemination</td>
</tr>
<tr>
<td>Vendor n Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency Study</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R&amp;D NGO Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERT Advisories</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feed Services</td>
<td></td>
<td>Top Threats</td>
<td>Threat Agents</td>
<td>Flash Note</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emerging Trends</td>
<td>Protective Controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Asset Types</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Structure Data</td>
<td>Information Dissemination</td>
<td></td>
</tr>
<tr>
<td>ENISA Processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The nasty matter with presentation
• Presentation/Visualization of results increases use/re-use and efficacy

• It is expected that quite some approaches for presentation of TI will emerge soon.

• Current:
  – Good practices are: Verizon-DBIR, Hackmageddon, Kill-Chain...
  – STIX data format as presentation tool?
  – An interesting/novel approach is project Sinfonier
Develop realistic use cases
What to do with Threat Information?

User Domain (National, Industry, Organizations)

- Assessments (Risk / Threat)
- Security Policy Recommendations
- Management Investment Decisions
- Planning of Security Controls
- Operation of Security Controls
- Auditing / Security Testing

Threat Assessment
- Collect
- Collate
- Analyse
- Set Context

Dissemination
Why this landscape the painting?...

<table>
<thead>
<tr>
<th>Risk oriented</th>
<th>Threat oriented</th>
<th>Prevention oriented</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Threat</td>
<td>- Threat Agents</td>
<td>- Patterns</td>
</tr>
<tr>
<td>- Weakness</td>
<td>- Attack vectors</td>
<td>- Big data</td>
</tr>
<tr>
<td>- Impact</td>
<td>- Kill chains</td>
<td>- Triage</td>
</tr>
<tr>
<td>- Acceptance levels</td>
<td>- Trends</td>
<td>- Actions</td>
</tr>
<tr>
<td>- Controls</td>
<td></td>
<td>- Controls</td>
</tr>
</tbody>
</table>

... is based on ↑...

<table>
<thead>
<tr>
<th>Risk/Business Intelligence</th>
<th>Threat Intelligence</th>
<th>Operational Intelligence</th>
</tr>
</thead>
</table>

We need to *increase* reaction speed at all levels!
Takeaways: Great work just released
Takeaways...

• For users:
  – Understand the scope of your assessments
  – Identify threat exposure and understand what you can afford
  – Build TI tool usage models according to points above
  – Increase agility of assessments and ISMS
  – Think that current state of TI is still initial BUT has a great potential

• For providers:
  – Establish usable information according to requirements
  – Increase structuring / follow user needs
  – Facilitate visualization, data re-use, historical data
  – Interconnect with ISMS / increase agility

• For ENISA:
  – Cooperation
  – Create data
  – Check the hook to ISMS
..thank you for your attention..

L. Marinos
louis.marinos@enisa.europa.eu
# CATER Threat Intelligence Checklist

<table>
<thead>
<tr>
<th>Coverage</th>
<th>Source</th>
<th>Data types</th>
<th>Social media</th>
<th>Closed web sources</th>
<th>Language support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Internally-generated</td>
<td>Raw technical (IP Address)</td>
<td>Number of sites (domains) covered.</td>
<td>Active access</td>
<td>Western only?</td>
</tr>
<tr>
<td></td>
<td>Shared feed inclusion</td>
<td>Domain Intelligence (DNS)</td>
<td>Depth of sources.</td>
<td>TOR Hidden Services</td>
<td>Non Roman Character sets?</td>
</tr>
<tr>
<td></td>
<td>Third party supplied</td>
<td>Passive information</td>
<td>Whole firehoses? (Twitter)</td>
<td>I2P/ Freenet</td>
<td>Full Unicode support?</td>
</tr>
<tr>
<td></td>
<td>Forensic intelligence</td>
<td>File hashes</td>
<td>Non-English sites (e.g. Sine Weibo, VKontakte)</td>
<td>Internet Relay chat (public)</td>
<td>Trained analysts?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Indicators of compromise</td>
<td></td>
<td>Internet Relay Chat (closed)</td>
<td>Machine only translation?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enhanced technical</td>
<td></td>
<td>Walled Garden Sites</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Geopolitical analysis</td>
<td></td>
<td>Forums (Deep Web)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Report-based intelligence (many to one)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tailored intelligence (one to one)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accuracy</th>
<th>Filtering and prioritization</th>
<th>Cognitive bias removal</th>
<th>Interpretation required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Does the source filter the results?</td>
<td>Has intelligence ‘trade craft’ been applied to the outputs to ensure a consistent representation of the quality of the intelligence?</td>
<td>Raw data: machine only based feed, requiring application of rules Enriched: interpreted feed providing enriched information to permit easier correlation Enhanced: feed is interpreted by a skilled resource prior to publication</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timeliness</th>
<th>Ingestion and discovery</th>
<th>Reporting speed</th>
<th>Access to historical data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Seconds</td>
<td>Seconds</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Minutes</td>
<td>Minutes</td>
<td>Weeks</td>
</tr>
<tr>
<td></td>
<td>Hours</td>
<td>Hours</td>
<td>Months</td>
</tr>
<tr>
<td></td>
<td>Days</td>
<td>Days</td>
<td>Years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ease of integration</th>
<th>Integrations</th>
<th>API available</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>STIX/TAXII/IODEF</td>
<td>Is it RESTful?</td>
</tr>
<tr>
<td></td>
<td>Maltego</td>
<td>Does it support open standards?</td>
</tr>
<tr>
<td></td>
<td>SIEM integration</td>
<td>What level of bespoke engineering is required?</td>
</tr>
<tr>
<td></td>
<td>Incident Management</td>
<td>Does it conform with a Service Level Agreement?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relevance</th>
<th>Specificity</th>
<th>Prioritization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>General</td>
<td>Alerted by severity</td>
</tr>
<tr>
<td></td>
<td>Geography</td>
<td>Use of meta tags</td>
</tr>
<tr>
<td></td>
<td>Industry</td>
<td>Accuracy of analysis reflected?</td>
</tr>
<tr>
<td></td>
<td>Company</td>
<td>Management report for multiple stakeholders?</td>
</tr>
</tbody>
</table>
What do others do?

• Excellent positioning of threat intelligence
  • Content types
  • Life-cycles
  • Flows of information

• Very good analysis of various parts
  • Types of threat intelligence (detailed)
  • Criteria for external TI providers
  • Checklist
Landscape painting tools...

Content and quality