ENISA Threat Landscape:

Current and Emerging Threat Assessment

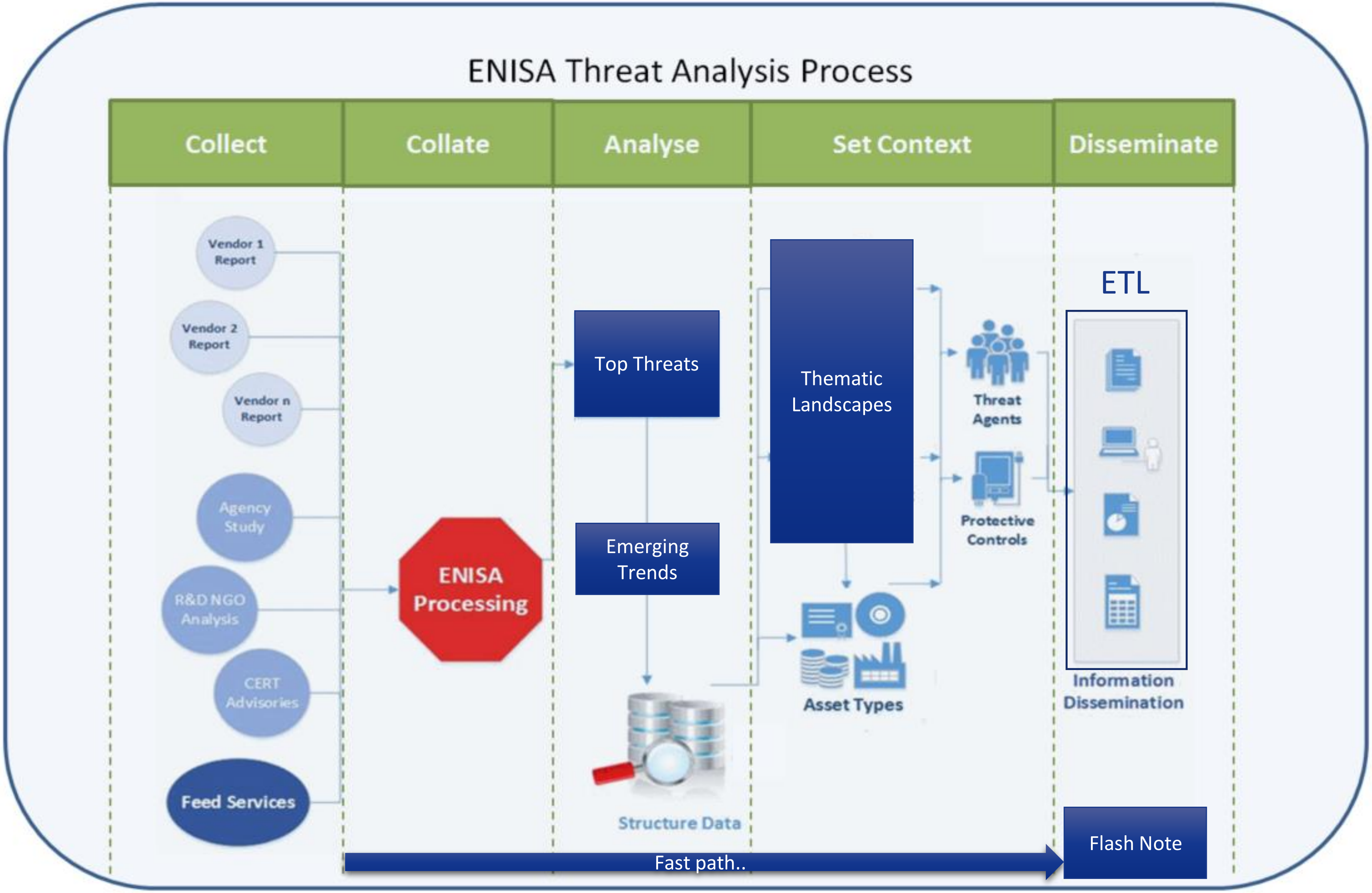
Louis Marinos

18 June 2015

European Union Agency For Network And Information Security

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

Collate

Analyse

Set Context

Disseminate

Vendor 1 Report

Vendor 2 Report

Vendor n Report

Agency Study

R&D NGO Analysis

CERT Advisories

Feed Services

ENISA Processing

Top Threats

Emerging Trends

Structure Data

Thematic Landscapes

Threat Agents

Protective Controls

Asset Types

ETL

Information Dissemination

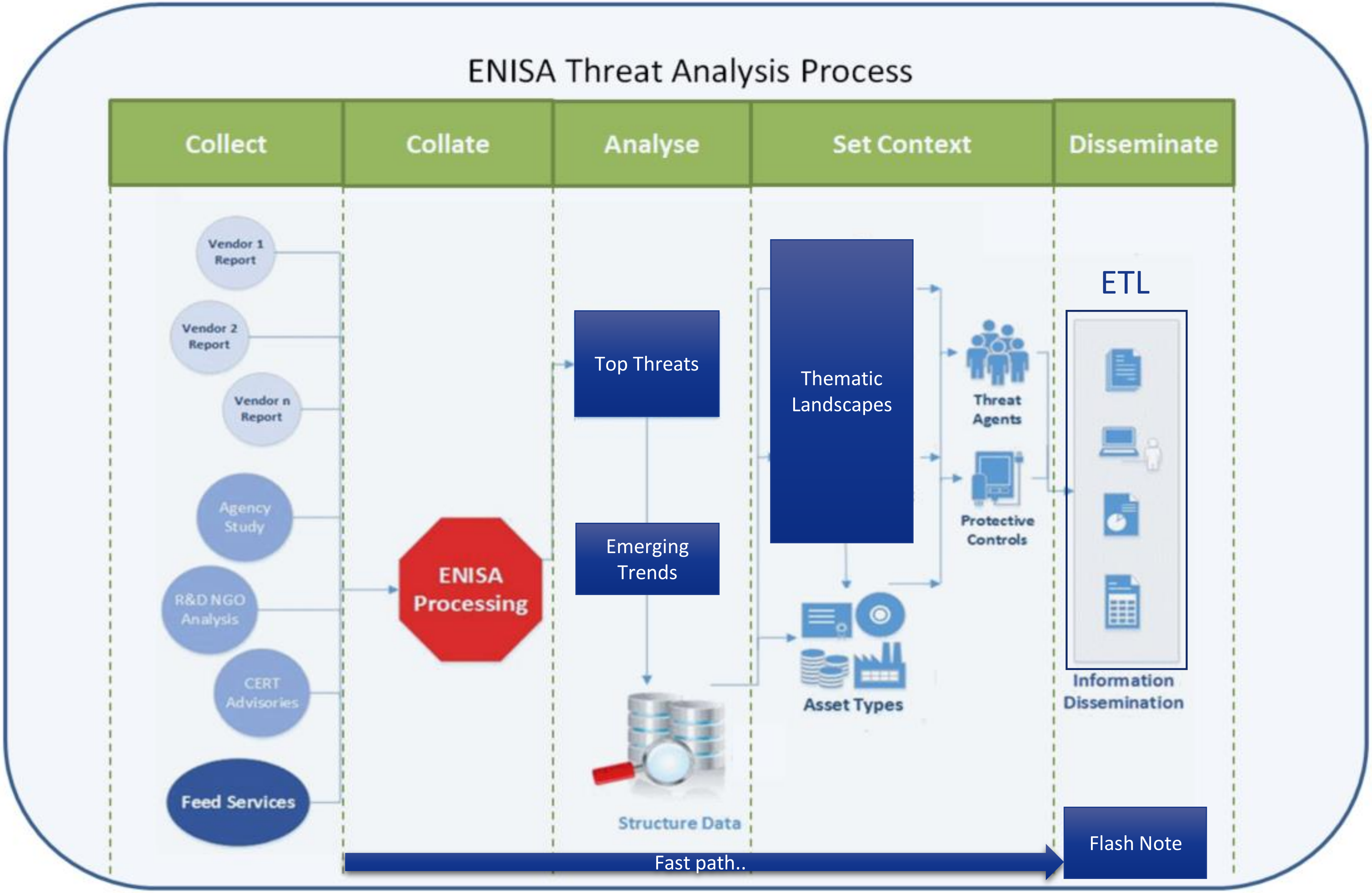
Flash Note

Fast path..

ETL State of play

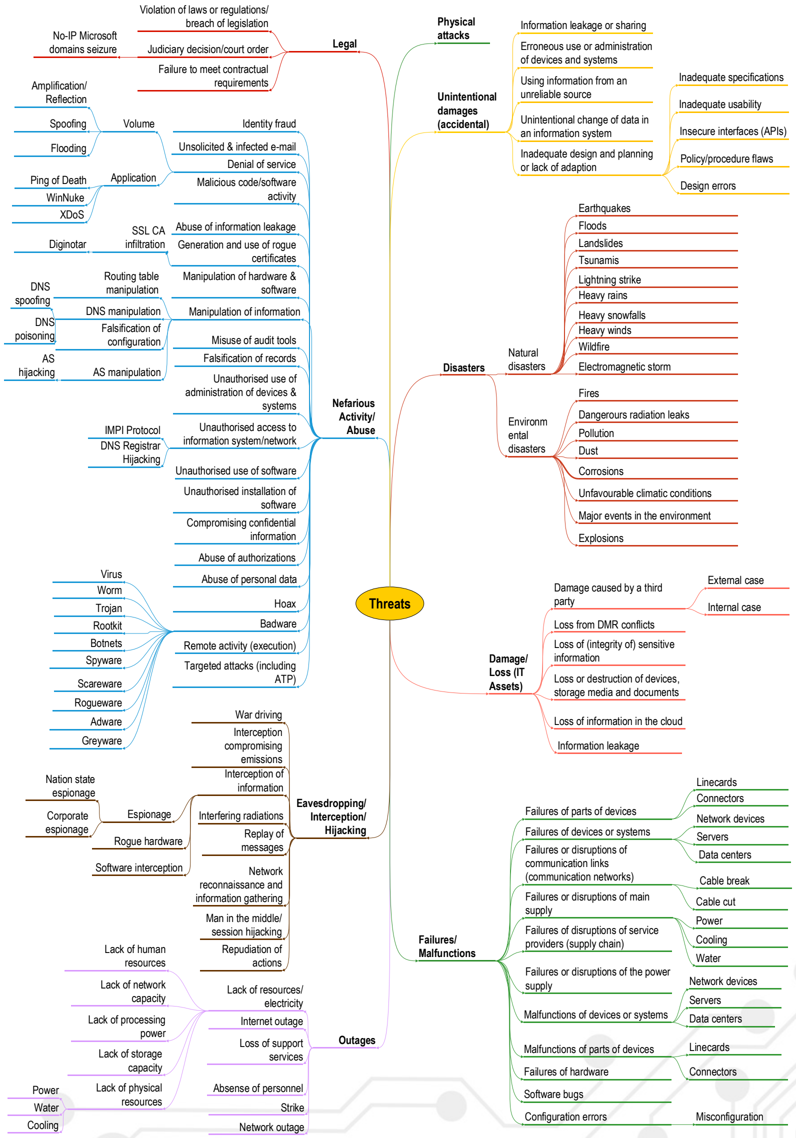
Content and quality

- **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

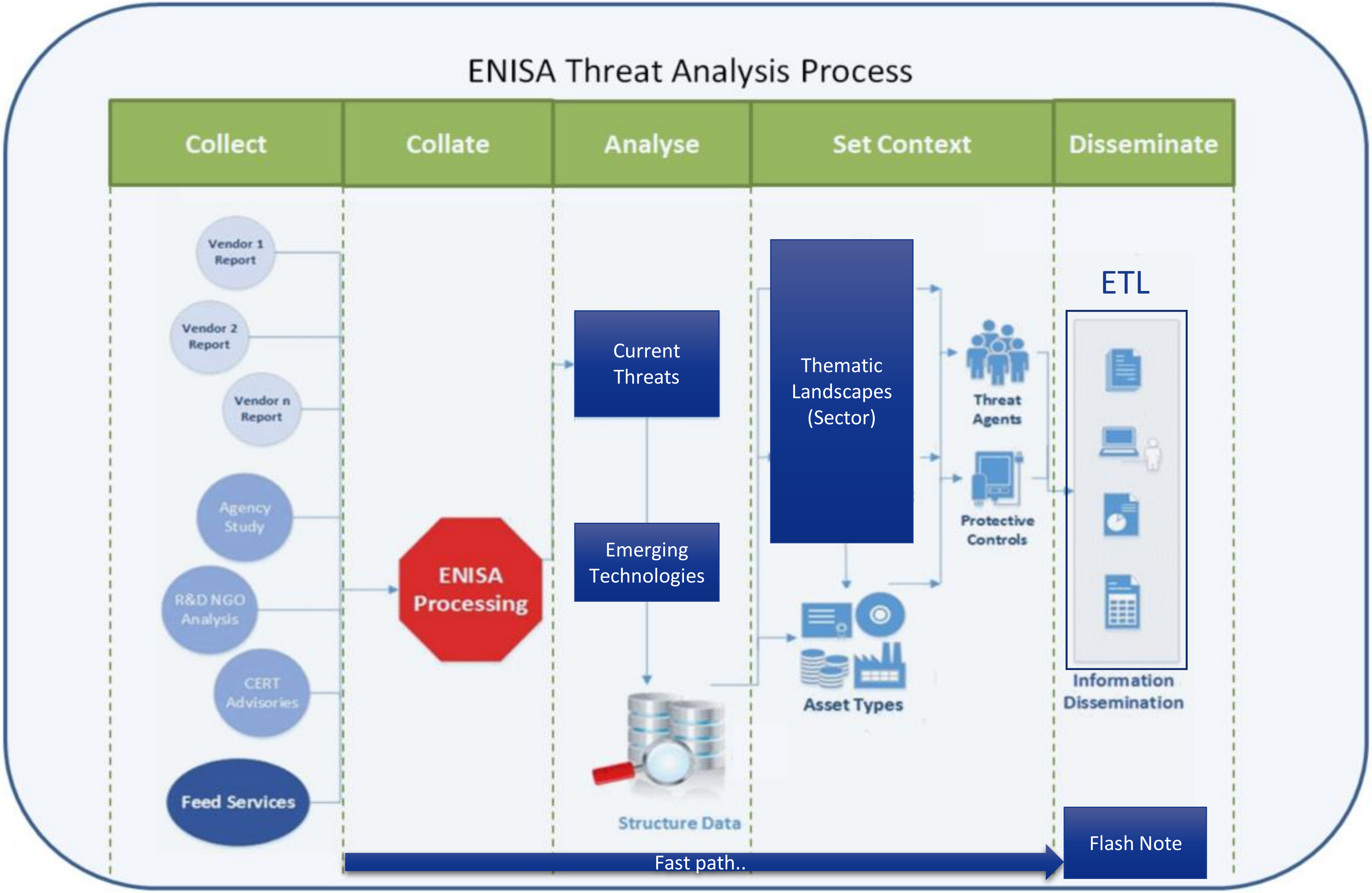


Facilitate input processing

Better management of input/output..

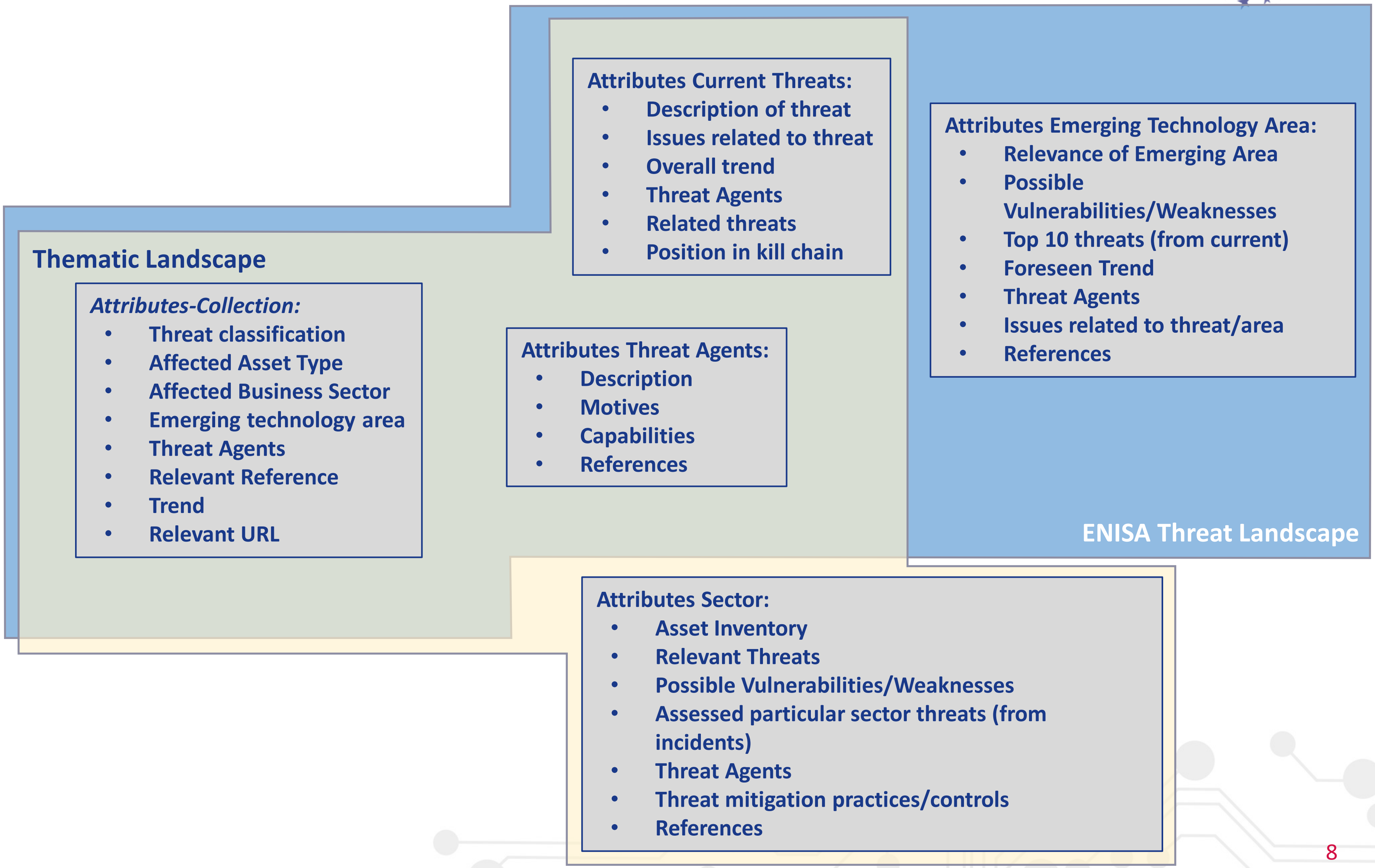


- Threats
  - Legal
    - Violation of laws or regulations/ breach of legislation
    - Judiciary decision/court order
      - No-IP Microsoft domains seizure
    - Failure to meet contractual requirements
  - Nefarious Activity/ Abuse
    - Identity fraud
    - Unsolicited & infected e-mail
    - Denial of service
      - Volume
        - Amplification/ Reflection
        - Spoofing
        - Flooding
      - Application
        - Ping of Death
        - WinNuke
        - XDoS
    - Malicious code/software activity
    - Abuse of information leakage
    - Generation and use of rogue certificates
      - SSL CA infiltration
        - Diginotar
    - Manipulation of hardware & software
    - Manipulation of information
      - Routing table manipulation
      - DNS manipulation
        - DNS spoofing
      - Falsification of configuration
        - DNS poisoning
      - AS manipulation
        - AS hijacking
    - Misuse of audit tools
    - Falsification of records
    - Unauthorised use of administration of devices & systems
    - Unauthorised access to information system/network
      - IMPI Protocol
      - DNS Registrar Hijacking
    - Unauthorised use of software
    - Unauthorised installation of software
    - Compromising confidential information
    - Abuse of authorizations
    - Abuse of personal data
    - Hoax
    - Badware
      - Virus
      - Worm
      - Trojan
      - Rootkit
      - Botnets
      - Spyware
      - Scareware
      - Rogueware
      - Adware
      - Greyware
    - Remote activity (execution)
    - Targeted attacks (including ATP)
  - Eavesdropping/ Interception/ Hijacking
    - War driving
    - Interception compromising emissions
    - Interception of information
      - Espionage
        - Nation state espionage
        - Corporate espionage
      - Rogue hardware
      - Software interception
    - Interfering radiations
    - Replay of messages
    - Network reconnaissance and information gathering
    - Man in the middle/ session hijacking
    - Repudiation of actions
  - Outages
    - Lack of resources/ electricity
      - Lack of human resources
      - Lack of network capacity
      - Lack of processing power
      - Lack of storage capacity
      - Lack of physical resources
        - Power
        - Water
        - Cooling
    - Internet outage
    - Loss of support services
    - Absense of personnel
    - Strike
    - Network outage
  - Physical attacks
  - Unintentional damages (accidental)
    - Information leakage or sharing
    - Erroneous use or administration of devices and systems
    - Using information from an unreliable source
    - Unintentional change of data in an information system
    - Inadequate design and planning or lack of adaption
      - Inadequate specifications
      - Inadequate usability
      - Insecure interfaces (APIs)
      - Policy/procedure flaws
      - Design errors
  - Disasters
    - Natural disasters
      - Earthquakes
      - Floods
      - Landslides
      - Tsunamis
      - Lightning strike
      - Heavy rains
      - Heavy snowfalls
      - Heavy winds
      - Wildfire
      - Electromagnetic storm
    - Environmental disasters
      - Fires
      - Dangerours radiation leaks
      - Pollution
      - Dust
      - Corrosions
      - Unfavourable climatic conditions
      - Major events in the environment
      - Explosions
  - Damage/ Loss (IT Assets)
    - Damage caused by a third party
      - External case
      - Internal case
    - Loss from DMR conflicts
    - Loss of (integrity of) sensitive information
    - Loss or destruction of devices, storage media and documents
    - Loss of information in the cloud
    - Information leakage
  - Failures/ Malfunctions
    - Failures of parts of devices
      - Linecards
      - Connectors
    - Failures of devices or systems
      - Network devices
      - Servers
      - Data centers
    - Failures or disruptions of communication links (communication networks)
      - Cable break
      - Cable cut
    - Failures or disruptions of main supply
      - Power
      - Cooling
      - Water
    - Failures of disruptions of service providers (supply chain)
    - Failures or disruptions of the power supply
    - Malfunctions of devices or systems
      - Network devices
      - Servers
      - Data centers
    - Malfunctions of parts of devices
      - Linecards
      - Connectors
    - Failures of hardware
    - Software bugs
    - Configuration errors
      - Misconfiguration



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 Threat Agents:

- Description
- Motives
- Capabilities
- References

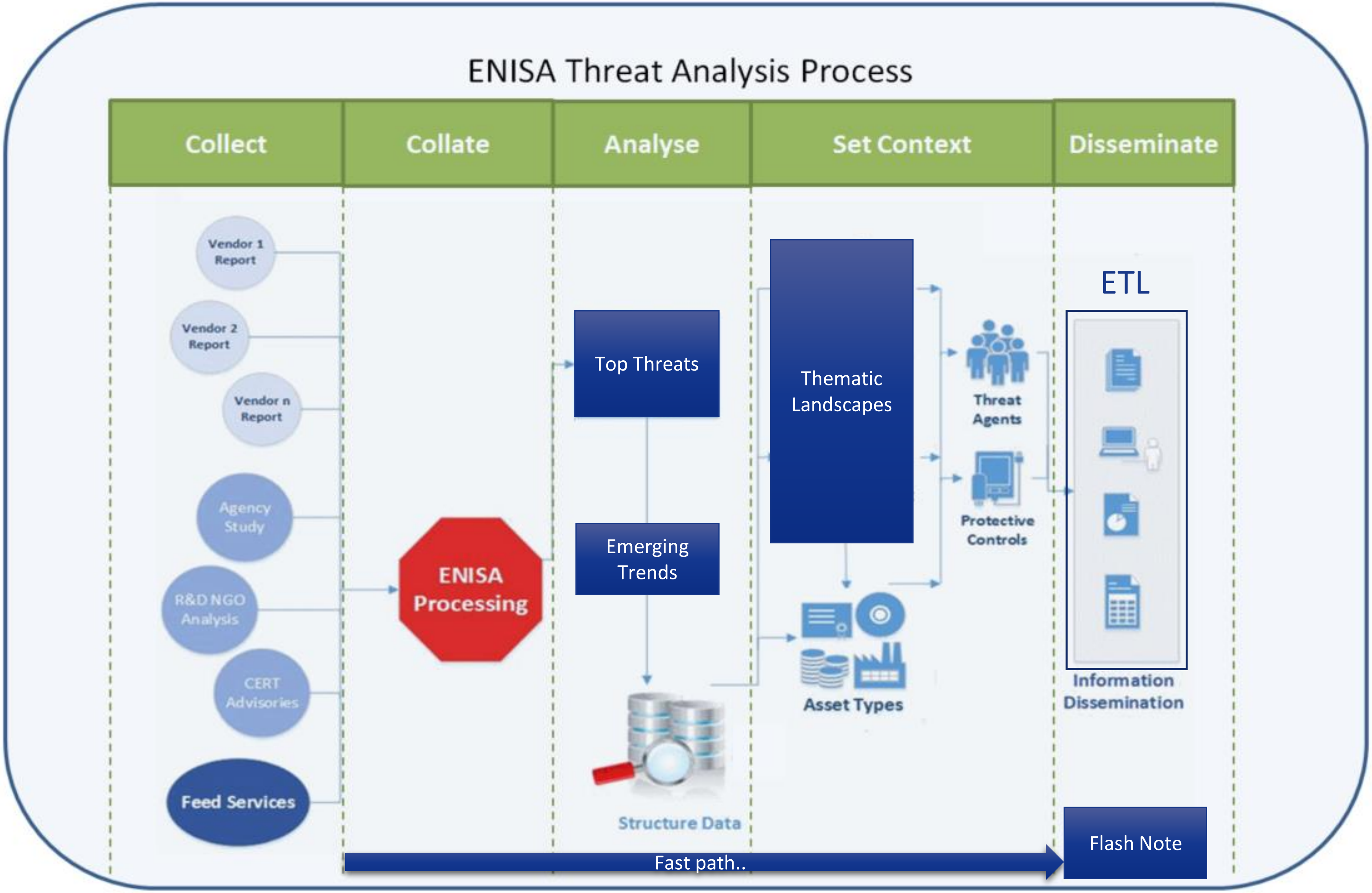
Attributes Emerging Technology Area:

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

ENISA Threat Landscape

Attributes Sector:

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



ENISA Threat Analysis Process

Collect

Collate

Analyse

Set Context

Disseminate

Vendor 1 Report

Vendor 2 Report

Vendor n Report

Agency Study

R&D NGO Analysis

CERT Advisories

Feed Services

ENISA Processing

Top Threats

Emerging Trends

Structure Data

Thematic Landscapes

Threat Agents

Protective Controls

Asset Types

ETL

Information Dissemination

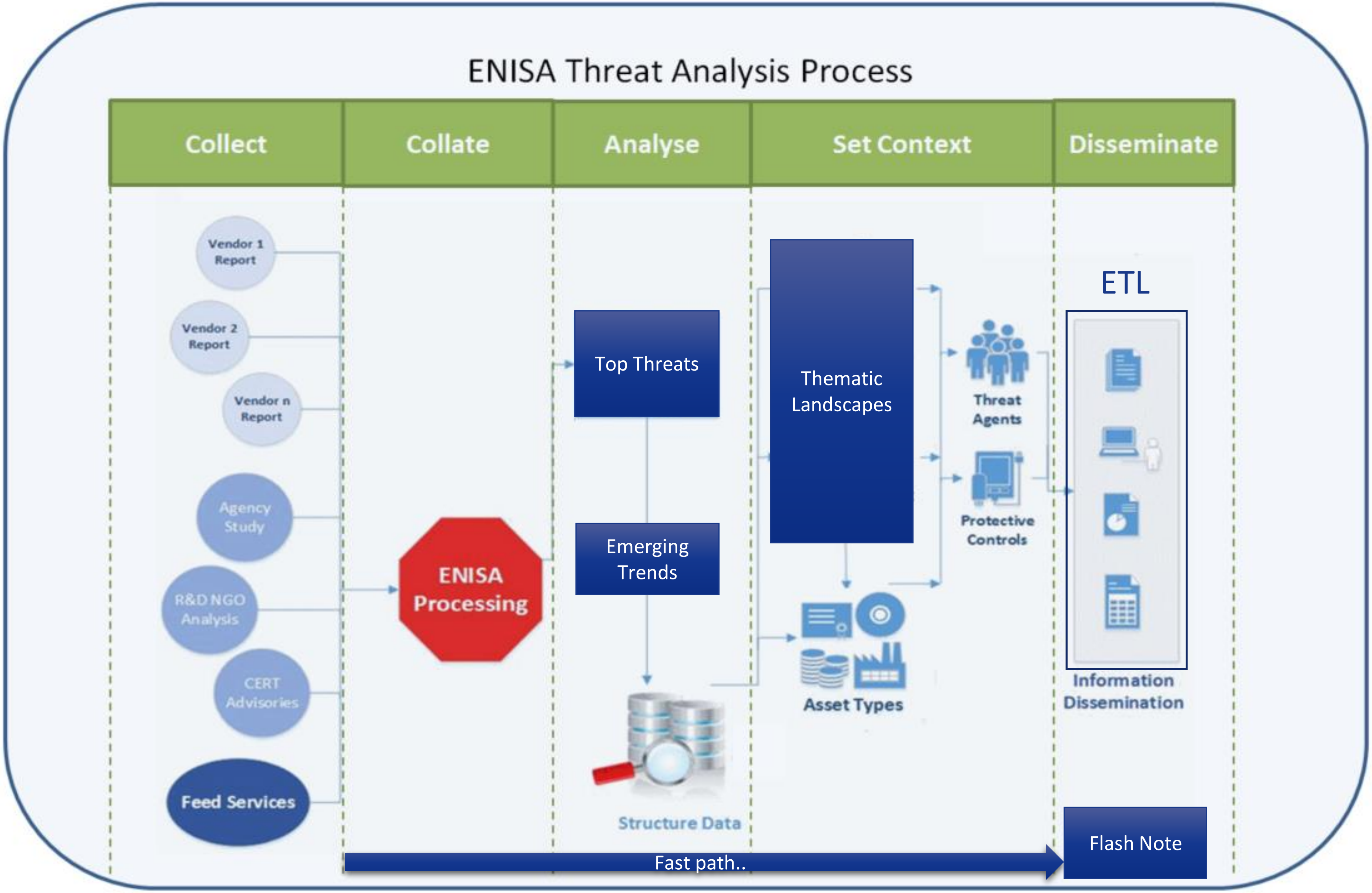
Flash Note

Fast path..

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..**

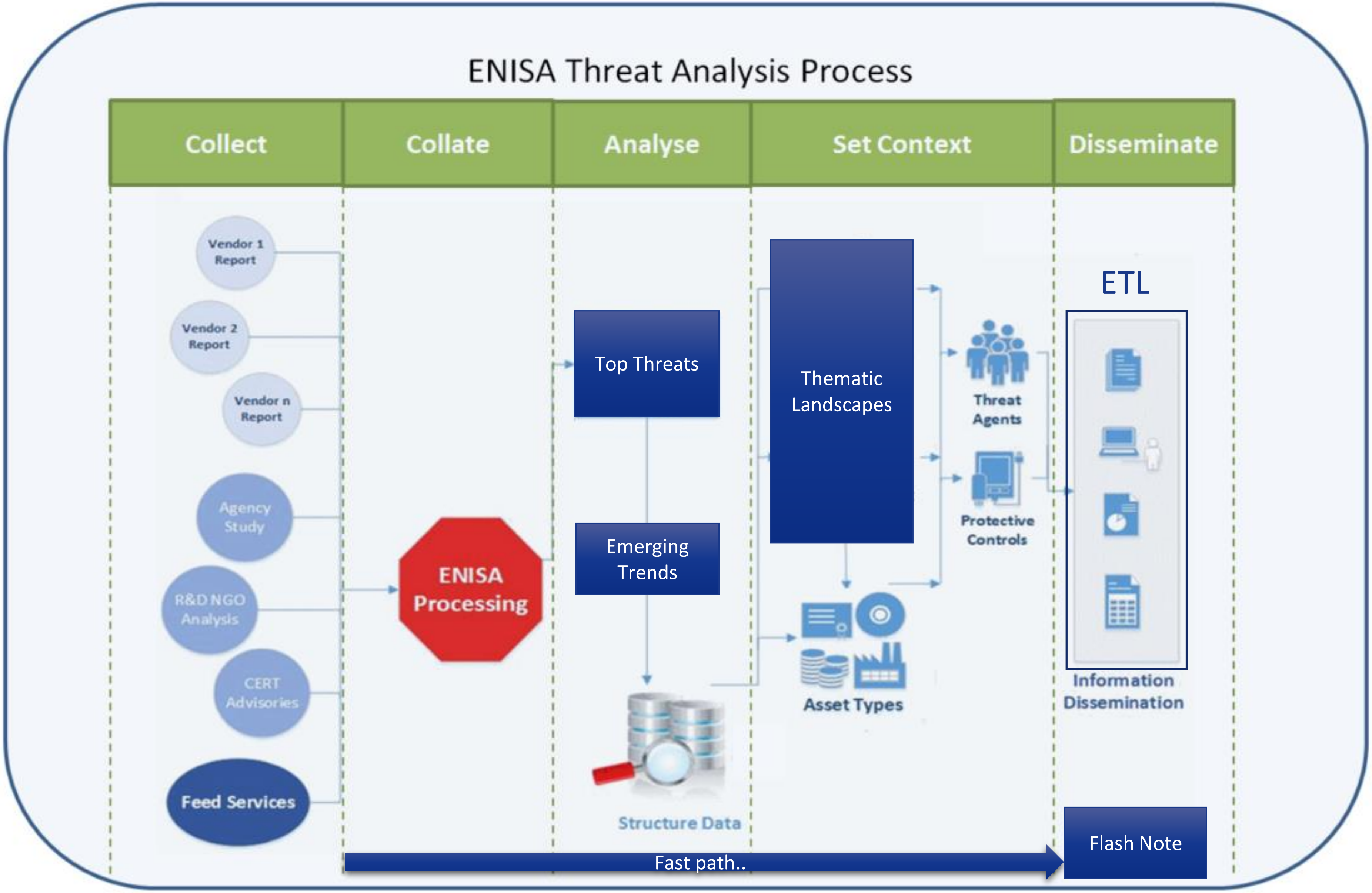

ENISA Threat Analysis Process
Collect
Collate
Analyse
Set Context
Disseminate
Vendor 1 Report
Vendor 2 Report
Vendor n Report
Agency Study
R&D NGO Analysis
CERT Advisories
Feed Services
ENISA Processing
Top Threats
Emerging Trends
Structure Data
Thematic Landscapes
Threat Agents
Protective Controls
Asset Types
ETL
Information Dissemination
Flash Note
Fast path..

Graphics / Presentation

- Presentation/Visualization of results increases use/re-use and efficacy

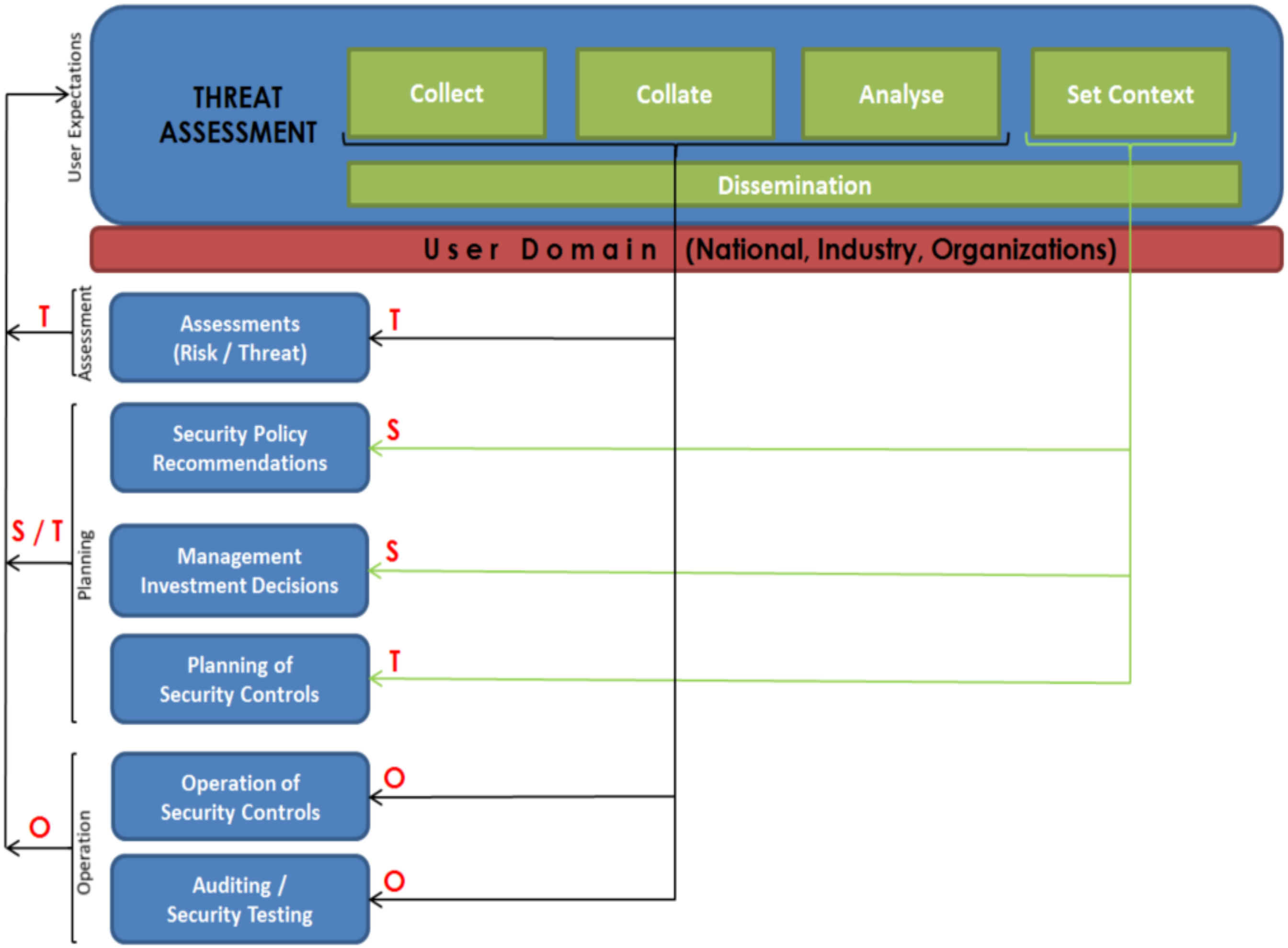
- It is expected that quite some approaches for presentation of TI will emerge soon.

- Current:
  - Good practices are: Verizon-DBIR, Hackmageddon, Kill-Chain…
  - STIX data format as presentation tool?
  - An interesting/novel approach is project Sinfonier

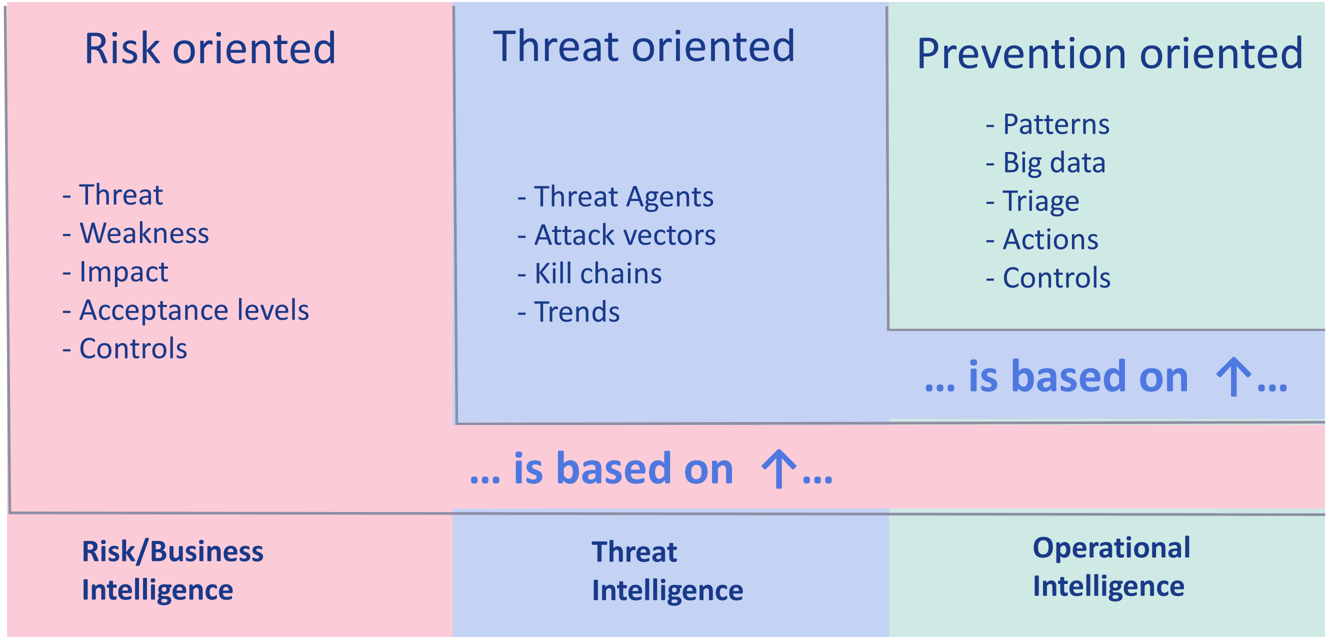


Develop realistic use cases

What to do with Threat Information?


User Expectations
THREAT ASSESSMENT
Collect
Collate
Analyse
Set Context
Dissemination
User Domain (National, Industry, Organizations)
Assessment
T
Assessments (Risk / Threat)
T
Planning
S / T
Security Policy Recommendations
S
Management Investment Decisions
S
Planning of Security Controls
T
Operation
O
Operation of Security Controls
O
Auditing / Security Testing
O

Why this landscape the painting?...



Risk oriented

- Threat
- Weakness
- Impact
- Acceptance levels
- Controls

Threat oriented

- Threat Agents
- Attack vectors
- Kill chains
- Trends

Prevention oriented

- Patterns
- Big data
- Triage
- Actions
- Controls

... is based on ↑...

... is based on ↑...

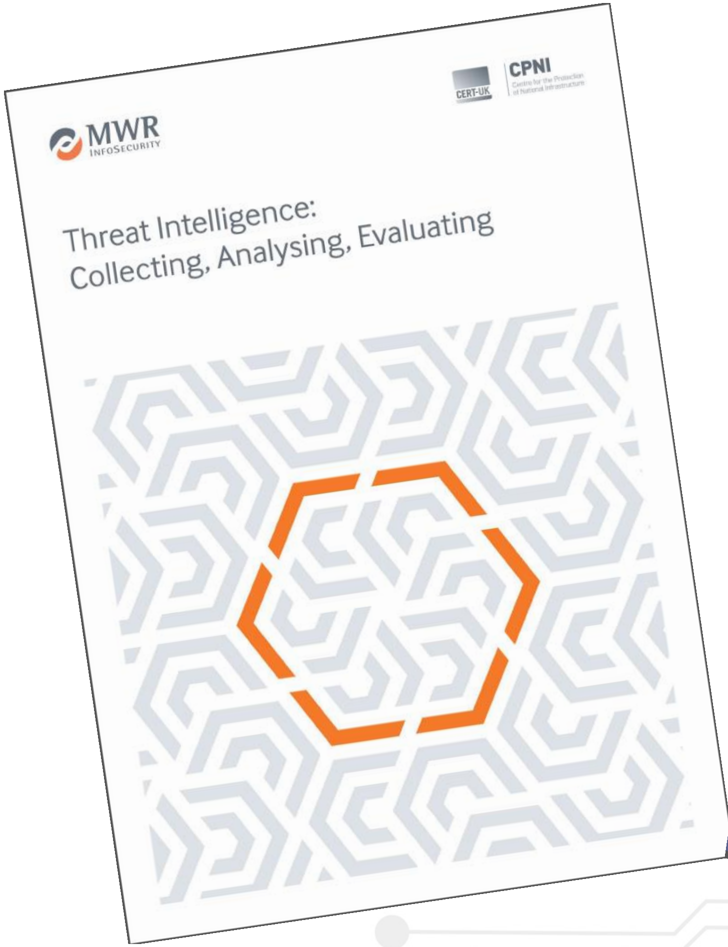
Risk/Business Intelligence

Threat Intelligence

Operational Intelligence

We need to ***increase*** reaction speed at all levels!

Takeaways: Great work just released


MWR InfoSecurity

CERT-UK

CPNI Centre for the Protection of National Infrastructure

Threat Intelligence: Collecting, Analysing, Evaluating

Threat intelligence

A buyer's guide

digital shadows_

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

Coverage

Source

- Internally-generated
- Shared feed inclusion
- Third party supplied
- Forensic intelligence

Data types

- Raw technical (IP Address)
- Domain Intelligence (DNS)
- Passive information
- File hashes
- Indicators of compromise
- Enhanced technical
- Geopolitical analysis
- Report-based intelligence (many to one)
- Tailored intelligence (one to one)

Social media

- Number of sites (domains) covered.
- Depth of sources.
- Whole firehoses? (Twitter)
- Non-English sites (e.g. Sine Weibo, VKontkate)

Closed web sources

- Active access
- TOR Hidden Services
- I2P/ Freenet
- Internet Relay chat (public)
- Internet Relay Chat (closed)
- Walled Garden Sites
- Forums (Deep Web)

Language support

- Western only?
- Non Roman Character sets?
- Full Unicode support?
- Trained analysts?
- Machine only translation?

Accuracy

Filtering and prioritization

- Does the source filter the results?
- Are incidents assigned a priority?

Cognitive bias removal

Has intelligence 'tradecraft' been applied to the outputs to ensure a consistent representation of the quality in the intelligence?

Intepretation required

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

Timeliness

Ingestion and discovery

- Seconds
- Minutes
- Hours
- Days

Reporting speed

- Seconds
- Minutes
- Hours
- Days

Access to historical data

- None
- Weeks
- Months
- Years

Ease of integration

Integrations

- STIX/TAXII/IODEF
- Maltego
- SIEM integration
- Incident Management

API available

- Is it RESTful?
- Does it support open standards?
- What level of bespoke engineering is required?
- Does it conform with a Service Level Agreement?

Relevance

Specificity

- General
- Geography
- Industry
- Company

Prioritization

- Alerted by severity
- Use of meta tags
- Accuracy of analysis reflected?
- Management report for multiple stakeholders?

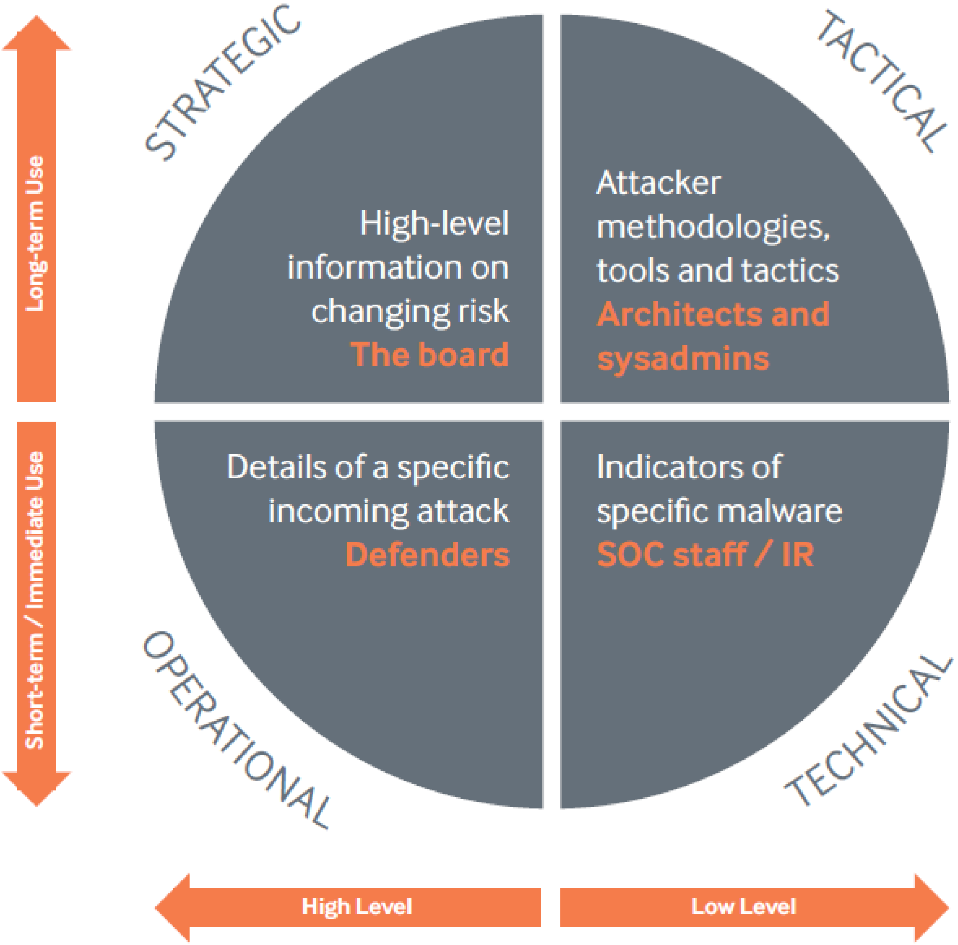
What do others do?

- 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



High-level information on changing risk
The board

Attacker methodologies, tools and tactics
Architects and sysadmins

Details of a specific incoming attack
Defenders

Indicators of specific malware
SOC staff / IR

© MWR - CERT-UK/CPNI