

Le paysage des menaces selon l'ENISA: formation à la gestion des risques

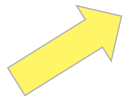
Louis Marinos| analyste des menaces et des risques

Conférence 2016 sur la recherche sur les cyberrisques en Suisse

European Union Agency for Network and Information Security (ENISA)

Le renseignement sur les menaces est la clé de tous les secteurs de la gestion des risques et du système de gestion de la sécurité de l'information (SGSI):

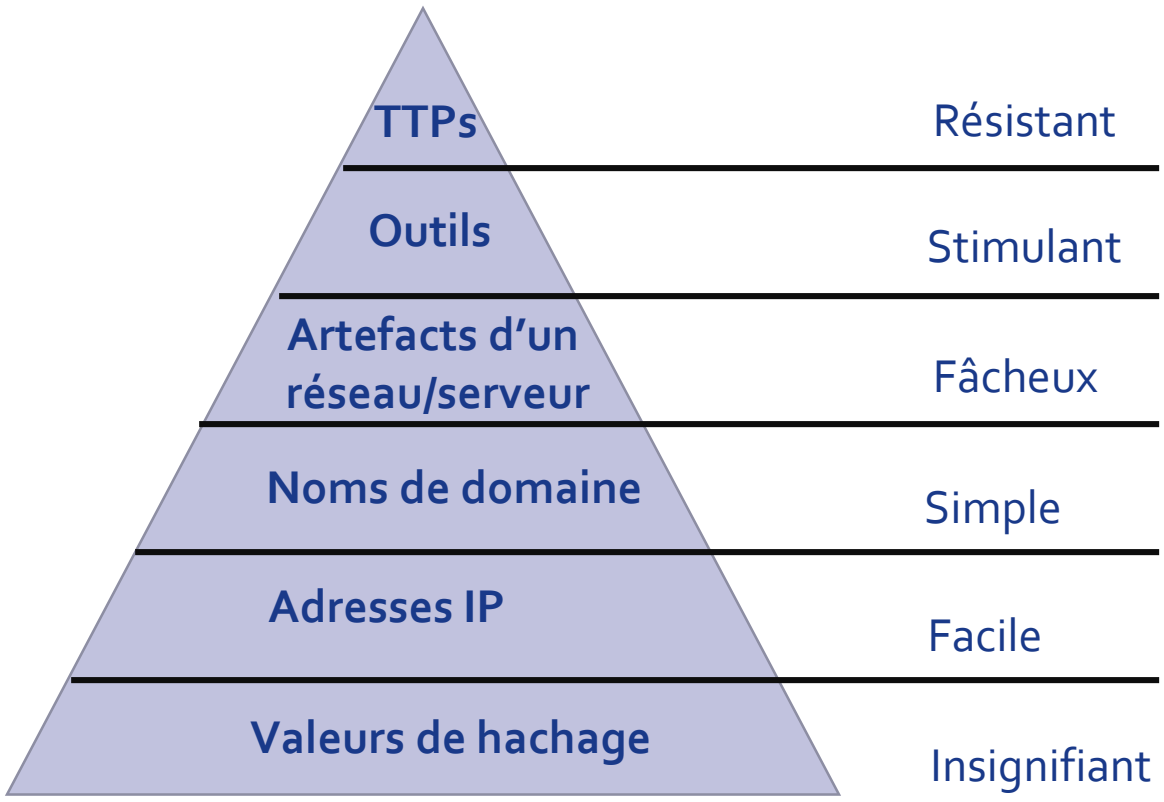
Dynamisation

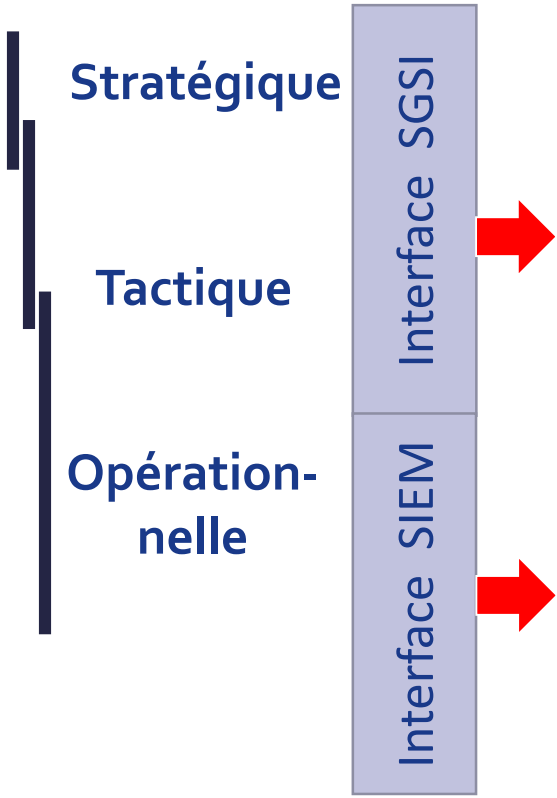
Risques: [Acquis, vulnérabilités, contrôles], 

[Menace, agent de menace], 

[Impact, valeur, influence] 

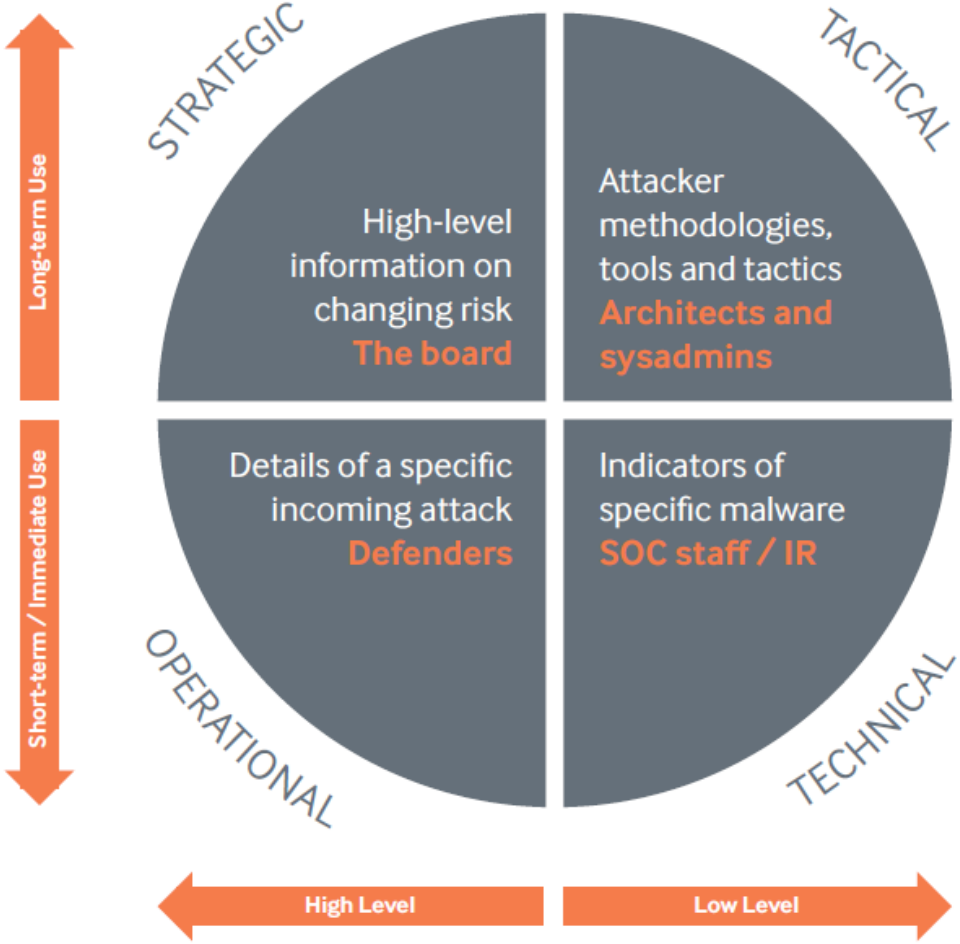
L’information sur les menaces est une pyramide





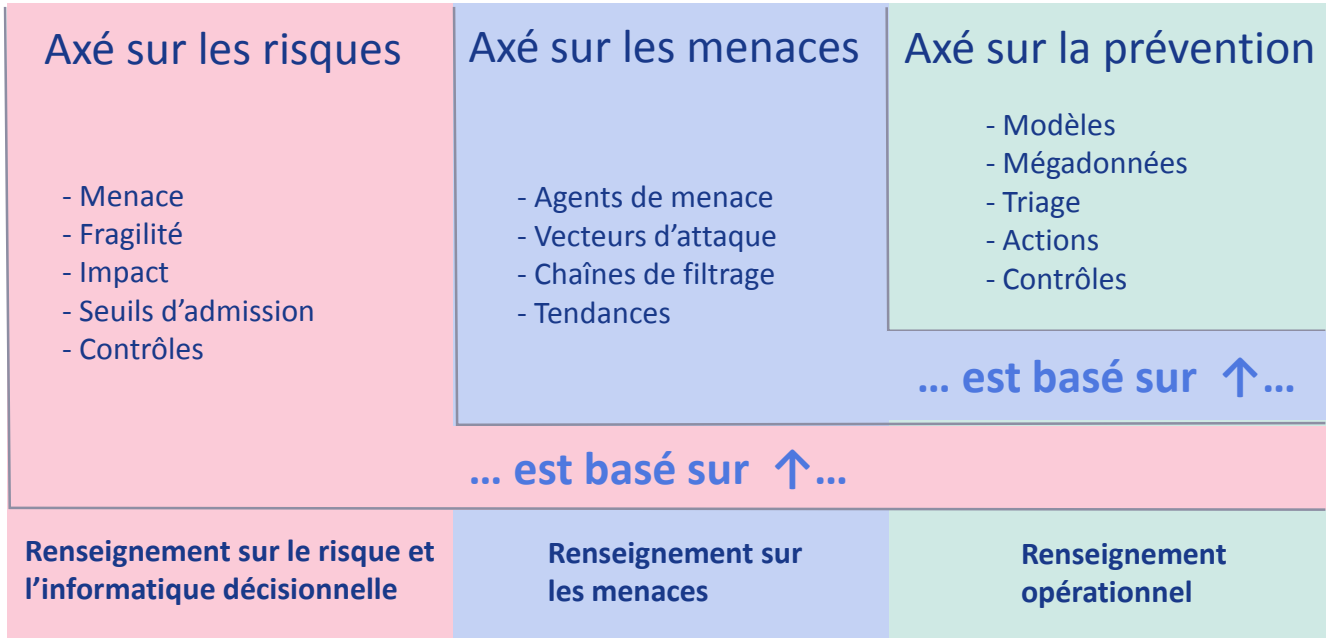
http://detect-respond.blogspot.gr/2013/03/the-pyramid-of-pain.html

Paysage des menaces et vue d'ensemble du renseignement



© MWR - CERT-UK/CPNI

Positionnement du renseignement sur les menaces



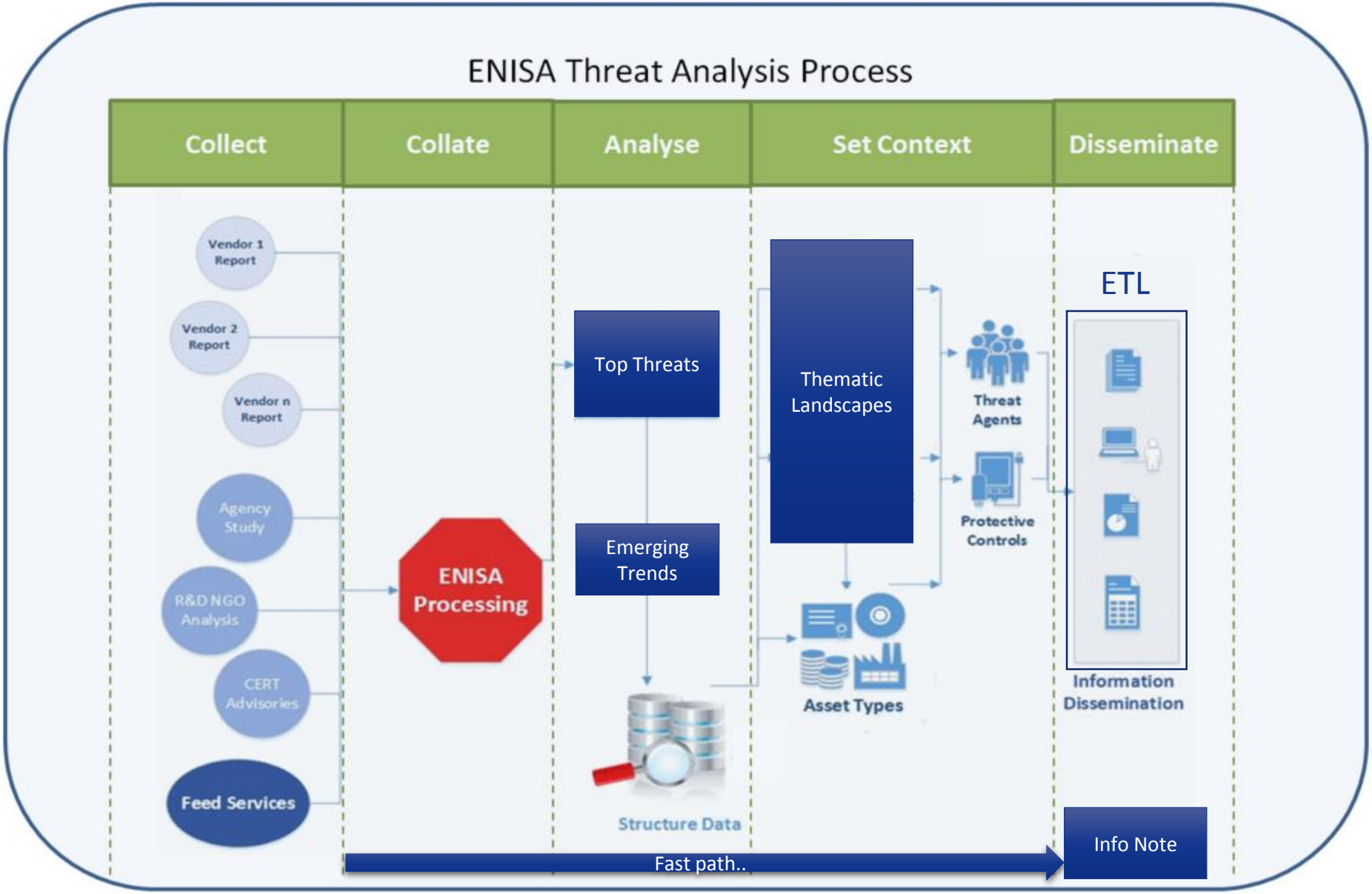
Il faut ***augmenter*** la vitesse de réaction à tous les niveaux!

Le paysage des menaces cybernétiques

Dans son paysage des menaces cybernétiques, l'ENISA établit une vue d'ensemble des menaces et des tendances actuelles et émergeantes.

Fondée sur des données accessibles au public, cette étude émet un avis indépendant sur les menaces observées, les agents de menace et les tendances de menace.

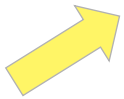
L'ENISA a analysé plus de 380 rapports récents provenant des sources les plus diverses.


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
Info Note
Fast path..

Sujets couverts:

Dynamisme

Risques: [Acquis, vulnérabilités, contrôles],



[Menace, agents de menace],

[Impact, valeur, influence]

Les classement des menaces

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	→	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	→	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓

Temps forts: les bonnes choses

- Les actions orchestrées pour démonter les infrastructures malveillantes et analyser les incidents afin d'identifier plus facilement les responsables.
- Le renforcement de la conscience gouvernementale, des dépenses consacrées à la cyberdéfense, des capacités et du niveau de coopération entre Etats.
- De nombreux développements dans le renseignement sur les menaces: prolifération de partages d'informations, d'outils et de produits pour améliorer la prise de conscience, l'état de préparation (capacité opérationnelle) et l'efficacité de la défense.
- La R&D pour adapter les mesures, les méthodes et les outils de protection existants aux évolutions du paysage des cybermenaces.

Temps forts: les moins bonnes choses

- Des attaques persistantes visant le matériel informatique, bien en deçà des «radars» équipant les outils et méthodes de défense disponibles.
- Une intensification de la fourniture du «cybercrime en tant que service», de développement d'outils pour les profanes et de programmes affiliés.
- Des armes malveillantes hautement efficaces et des outils d'infection qui s'appuient sur les vulnérabilités détectées.
- Des opérations très rentables, lancées par des infrastructures et des campagnes malveillantes, visant à provoquer une faille dans la sécurité des données pour exercer un chantage.

Conclusions quant à la politique à suivre

- Intégrer le renseignement sur les menaces dans les capacités nationales de cyberdéfense.
- Effectuer des analyses des incidents signalés et utiliser les résultats pour améliorer la planification des défenses.
- Disséminer les connaissances sur les cybermenaces dans tous les milieux du cyberespace.

Conclusions sur le plan commercial

- Simplifier le contenu du renseignement sur les menaces pour parvenir à une plus large dissémination dans la communauté des parties prenantes.
- Travailler sur des modèles d'agents de menace et en faire une partie intégrante du renseignement sur les menaces.
- Produire une information corrélée et contextualisée sur les menaces dans le but d'augmenter sa durée et sa pertinence.
- Investir dans une meilleure gestion de la vulnérabilité et une meilleure exploitation de la face obscure d'internet (*dark web*).

Conclusions sur le plan de la recherche

- Développer des modèles de statistique appliquée pour augmenter la comparabilité des informations relatives aux cybermenaces et aux incidents.
- Elaborer des modèles pour des contrôles de sécurité irréprochables pouvant être intégrés dans des environnements complexes d'utilisateurs finaux connectés.
- Développer des modèles de confiance pour l'interopérabilité ad hoc des périphériques dans les environnements connectés.

Communauté de la sécurité: innover

- Donner au renseignement sur les menaces la place qui lui revient
  (le rendre possible dans les sociétés de toute taille)
- Appliquer les principes de l'aménagement du paysage des menaces
  (risques, acquis, protection)
- Utiliser le paysage des menaces pour tester la protection (réalité simulée)

Merci de votre attention

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu