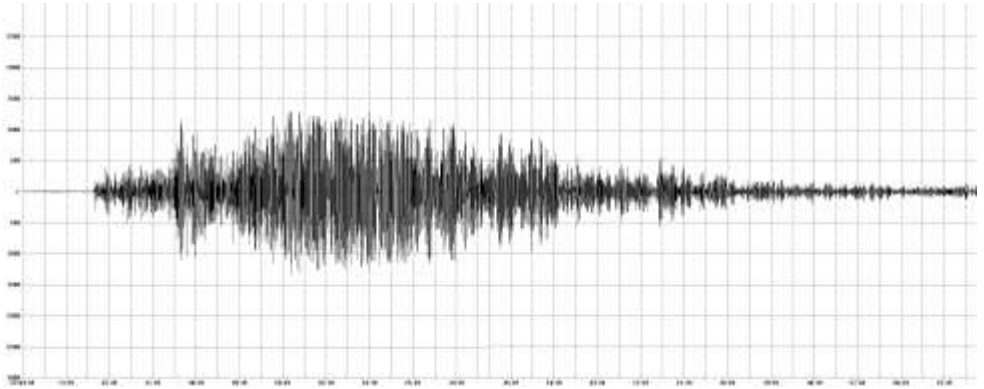
L'élément le plus précieux d'un système de Défense est l'Humain.
Il est rare, manque de temps et d'informations contextuelles pour pouvoir agir.
Le Renseignement repositionne l'humain au centre d'une défense rendue plus efficace.

THREATQUOTIENT

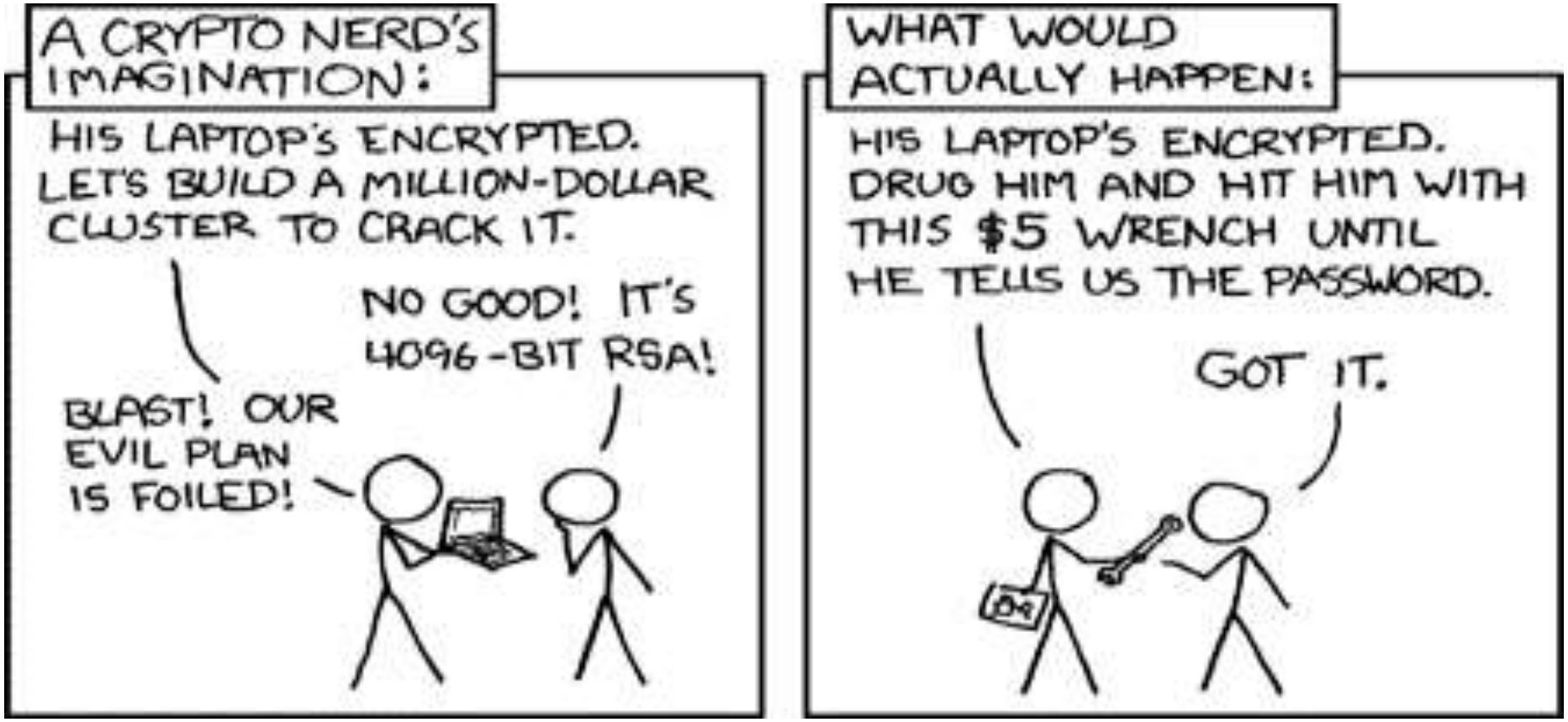
Cybersecurity

- *Hurricanes*

- *Earthquakes*



Threat Intelligence: Comprendre les menaces



Qu’est ce que le Renseignement

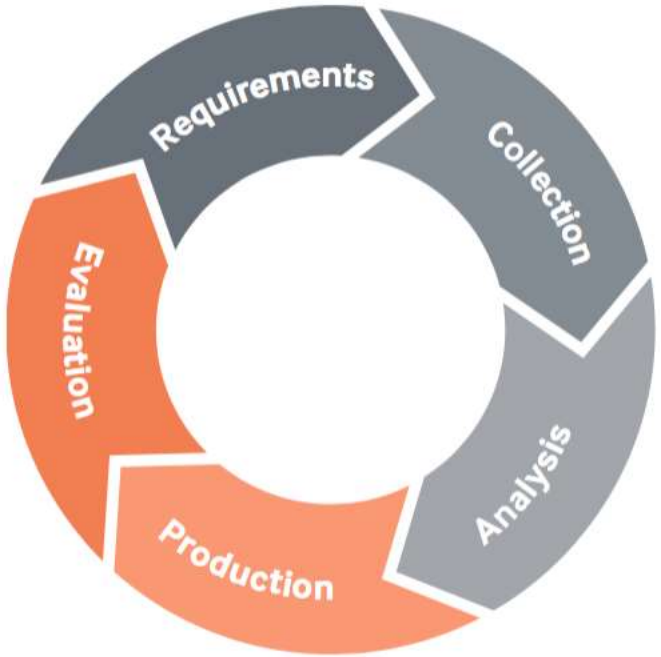
Définitions propres au Renseignement*

- Le Renseignement est un Processus qui vise à fournir des informations contextuelles et actionnables à sa défense en réponse à un besoin précis. On parle de cycle du Renseignement.
- On distingue trois éléments :
  - La Donnée : sa qualité essentielle est d'être "donnée" ou disponible ou encore accessible
  - L'Information : sa qualité essentielle est d'être précise ou signifiante ou encore porteuse de sens
  - Le Renseignement : sa qualité essentielle est de répondre à une demande précise et définie au début du cycle et d'être actionnable par son destinataire

** http://www.operationspaix.net/69-resources/details-lexique/information-renseignement.html*

Traduction dans le monde Cyber / IT

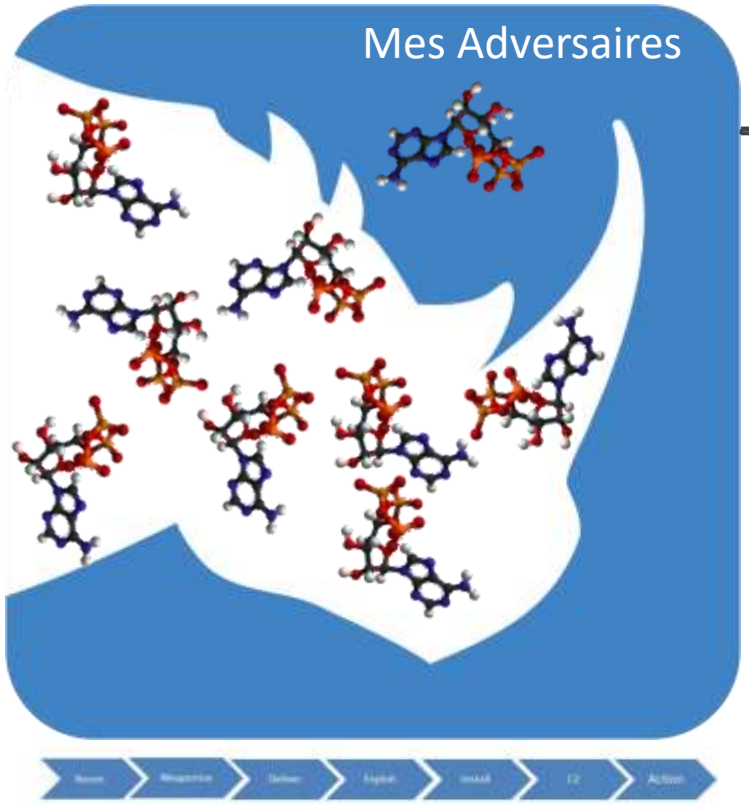
- Besoin initiant le cycle de renseignement :
  - Identifier mes adversaires pour adapter ma capacité/stratégie de défense en conséquence
- On distingue trois éléments :
  - La Donnée : Indicateur/Marqueur (technique ou non) provenant de Feeds OSInt, Feeds commerciaux, Rapports de Cert, Editeurs, Groupe d'échange …
  - L'Information : Ensemble des données disponibles organisées au sein d'une bibliothèque accessible à toute ma chaine de défense
  - Le Renseignement : Information contextuelle actionnable distribuées à l'issue d'un cycle de renseignement (pour répondre à un besoin précis)



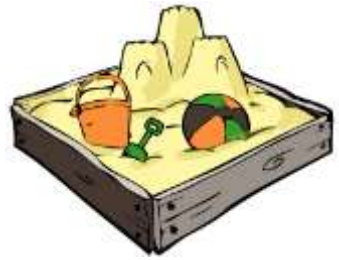
Données externes :
OSINT, Rapports, …

Données amies :
Groupe MISP, CERT, Emails…

Données Monde Réel:
Ticketing / SIEM / IR / SANDBOX



Détection, Priorisation & Prévention



THREATQUOTIENT

Un exemple

Cycle de vie d'un indicateur

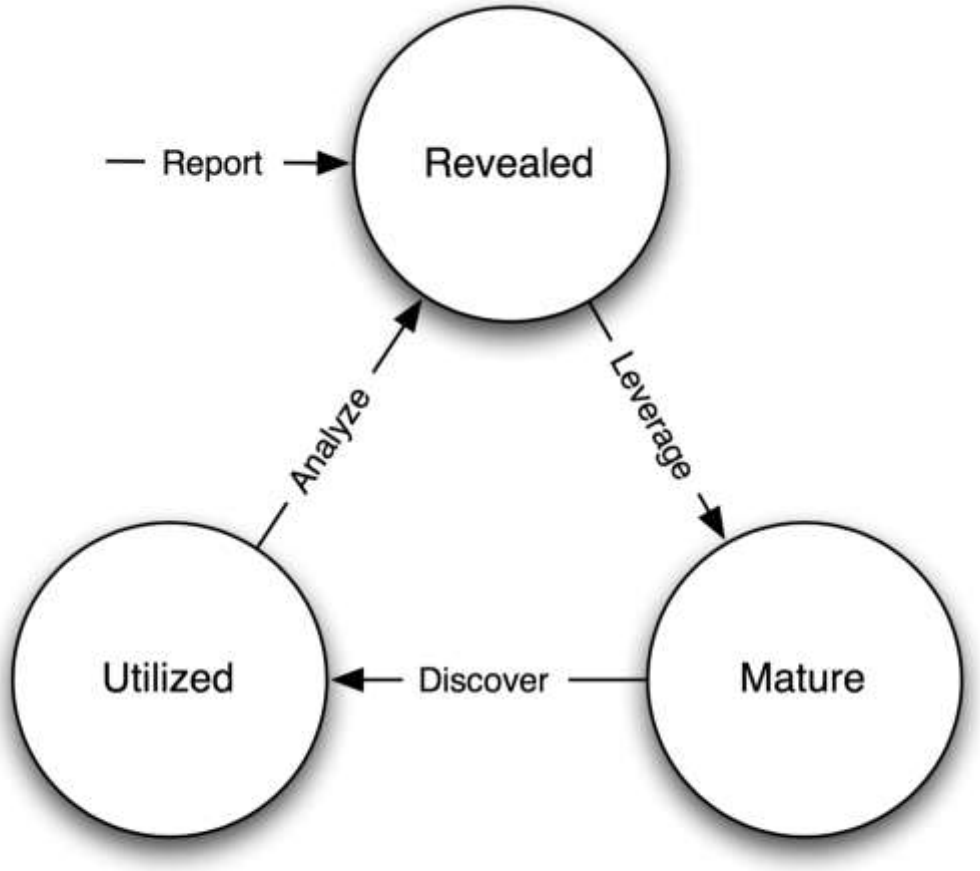


Figure 1: Indicator life cycle states and transitions

Source: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Hutchins, Cloppertf, Amin, LMC

Dans la vraie vie

Table 4: Intrusion Attempts 1, 2, and 3 Indicators

Phase	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	[Recipient List] Benign PDF	[Recipient List] Benign PDF	[Recipient List] Benign PPT
Weaponization	Trivial encryption algorithm		
	Key 1		Key 2
Delivery	[Email subject] [Email body]	[Email subject] [Email body]	[Email subject] [Email body]
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Exploitation	CVE-2009-0658 [shellcode]		[PPT 0-day] [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp		
C2	202.abc.xyz.7 [HTTP request]		
Actions on Objectives	N/A	N/A	N/A

Source: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Hutchins, Cloppertf, Amin, LMC

A quoi sert le Renseignement au sein d'une chaine de Cyberdéfense

Trois niveaux d'usage du Renseignement*

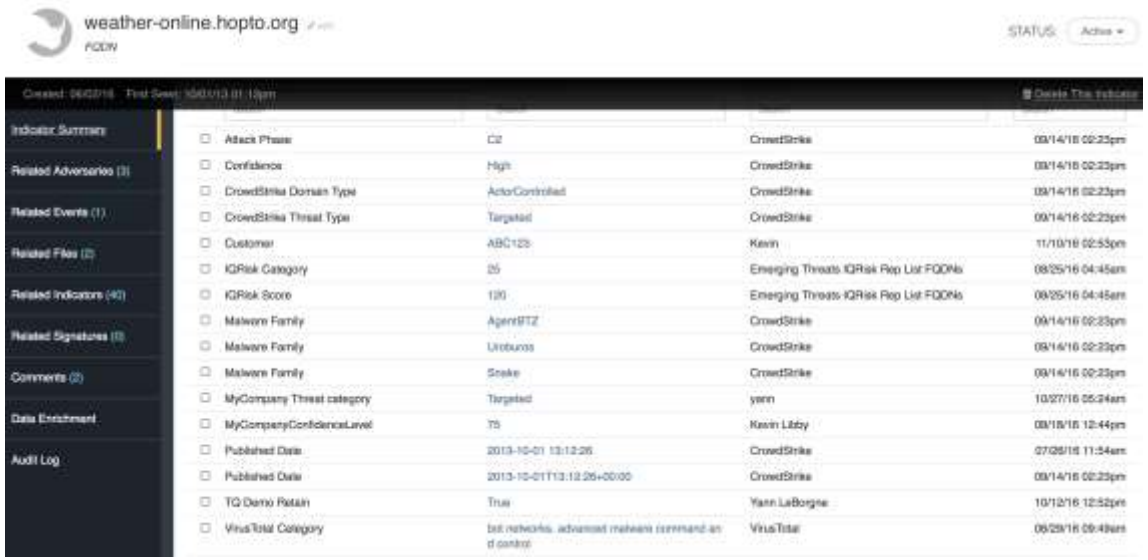
- **Tactique** : Ce renseignement permet au commandant tactique de préparer et de mener à bien des opérations tactiques à son niveau (zone d'opérations restreinte ; niveau chefs de composantes et les différentes unités civiles, militaires ou de police)
- **Opérationnel** : Ce renseignement est nécessaire pour la planification et la conduite de campagnes d'opérations importantes visant à atteindre des objectifs stratégiques dans des théâtres ou des zones opérationnels (niveau chef de mission et équipe de direction)
- **Stratégique** : Ce renseignement est constitué d'une part du renseignement nécessaire à la prise de décision au plan national ou international (ONU, OTAN, UE), et, d'autre part, du renseignement utile en matière de planification d'une opération (civile ou militaire) en appui à cette décision

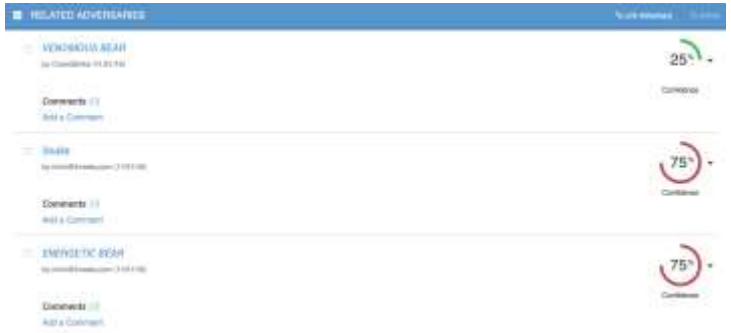
** http://www.operationspaix.net/69-resources/details-lexique/information-renseignement.html*

Traduction dans le monde Cyber / IT

- **Tactique:**
  - Améliore l'éfficacité des analystes
  - Capitalisation de l'analyse / Permet l'implémentation des process
- **Opérationnel:**
  - Priorisation des événements
  - Automatisation
- **Stratégique**
  - Analyse des adversaires
  - Permet l'anticipation
  - Rôle dans l'analyse de risque

Tactique


weather-online.hopto.org
FQDN
STATUS
Active
Indicator Summary
Related Adversaries (3)
Related Events (1)
Related Files (2)
Related Indicators (40)
Related Signatures (0)
Comments (2)
Data Enrichment
Audit Log
Attack Phase C2 CrowdStrike 09/14/16 02:23pm
Confidence High CrowdStrike 09/14/16 02:23pm
CrowdStrike Domain Type ActorControlled CrowdStrike 09/14/16 02:23pm
CrowdStrike Threat Type Targeted CrowdStrike 09/14/16 02:23pm
Customer ABC123 Kevin 11/10/16 02:55pm
IQRisk Category 25 Emerging Threats IQRisk Rep List FQDNs 08/25/16 04:45am
IQRisk Score 120 Emerging Threats IQRisk Rep List FQDNs 08/25/16 04:45am
Malware Family AgentBTZ CrowdStrike 09/14/16 02:23pm
Malware Family Urouburos CrowdStrike 09/14/16 02:23pm
Malware Family Snake CrowdStrike 09/14/16 02:23pm
MyCompany Threat category Targeted yann 10/27/16 05:24am
MyCompanyConfidenceLevel 75 Kevin Libby 08/18/16 12:44pm
Published Date 2013-10-01 13:12:26 CrowdStrike 07/26/16 11:54am
Published Date 2013-10-01T13:12:26+00:00 CrowdStrike 09/14/16 02:23pm
TQ Demo Retain True Yann LeBorgne 10/12/16 12:52pm
VirusTotal Category bot networks, advanced malware command and control VirusTotal 08/29/16 09:49am

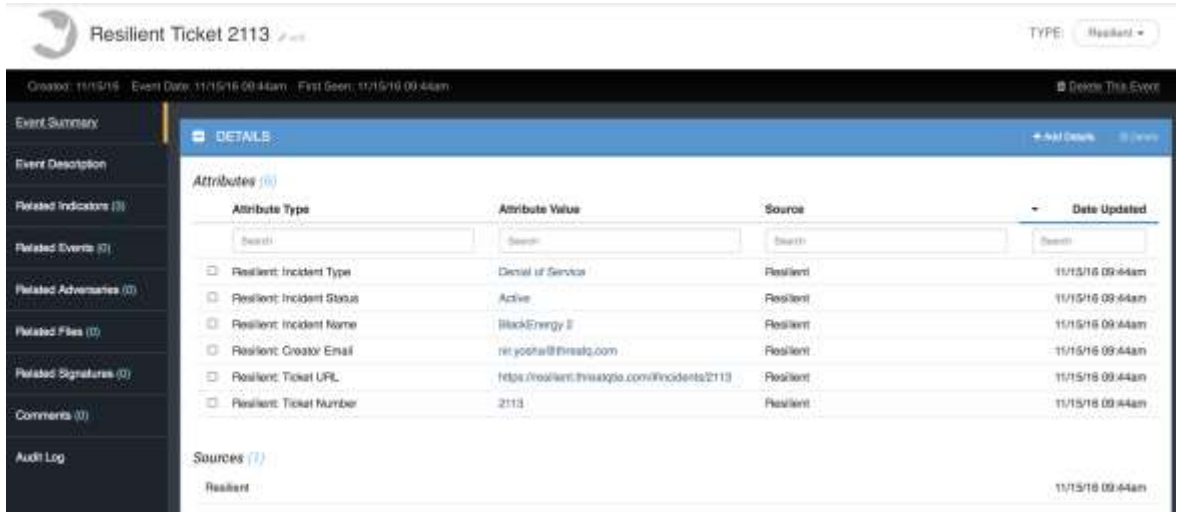

RELATED ADVERSARIES
25
75
75

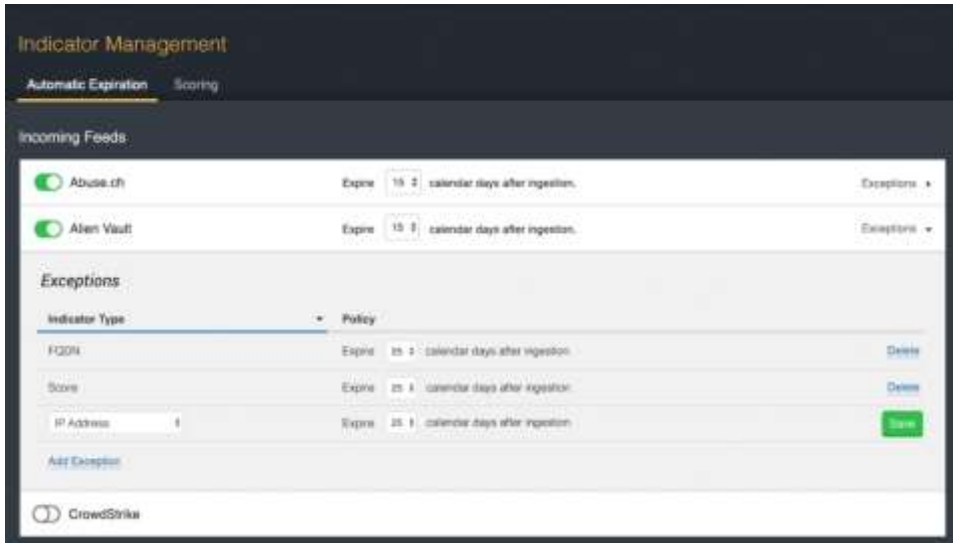

Indicator Summary
Related Adversaries (3)
Related Events (1)
Related Files (2)
Related Indicators (40)
Related Signatures (0)
Comments (2)
Data Enrichment
Audit Log

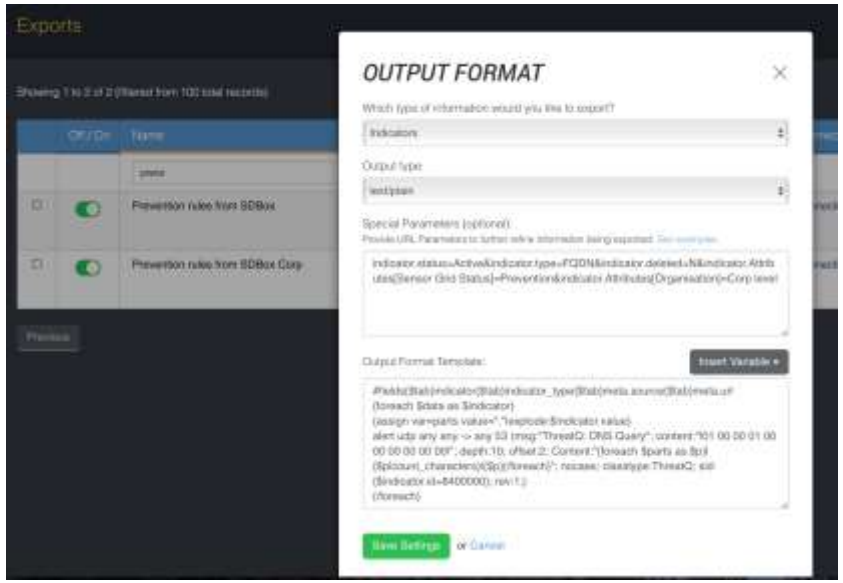

Sources (4)
Emerging Threats IQRisk Rep List FQDNs 08/25/16 04:45am
Neal Humphrey 06/13/16 01:22pm
CrowdStrike 10/01/13 01:12pm
Snake Campaign & Cyber Espionage Toolkit 06/13/16 11:31am


COMMENTS
Add a Comment

Opérationnel

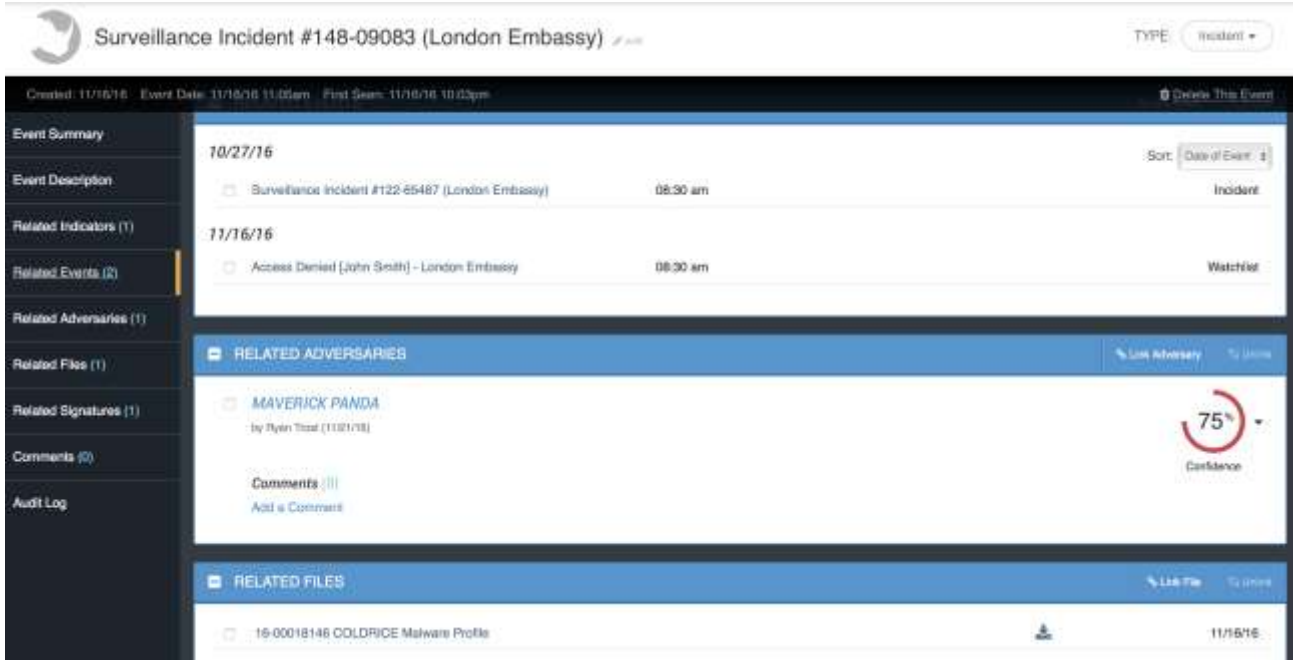






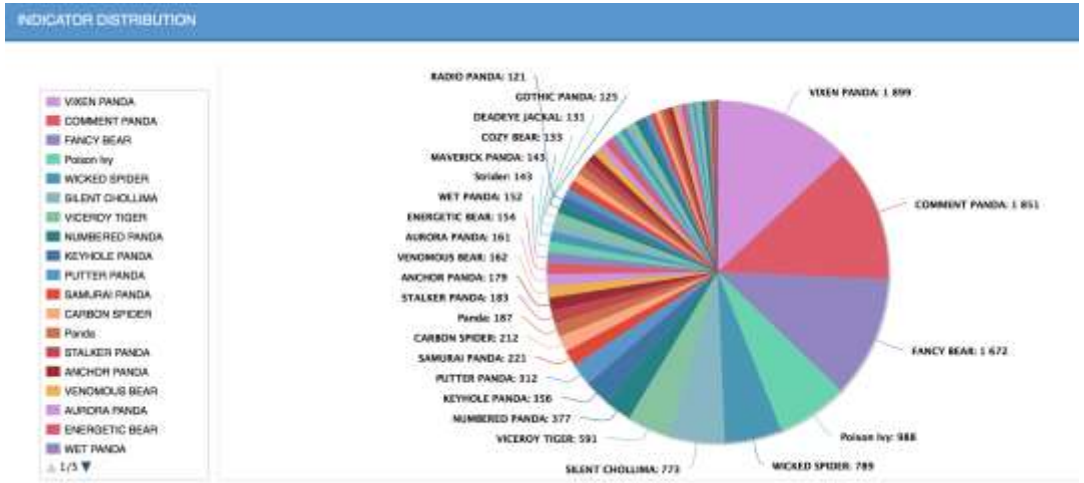
THREATQUOTIENT

Stratégique



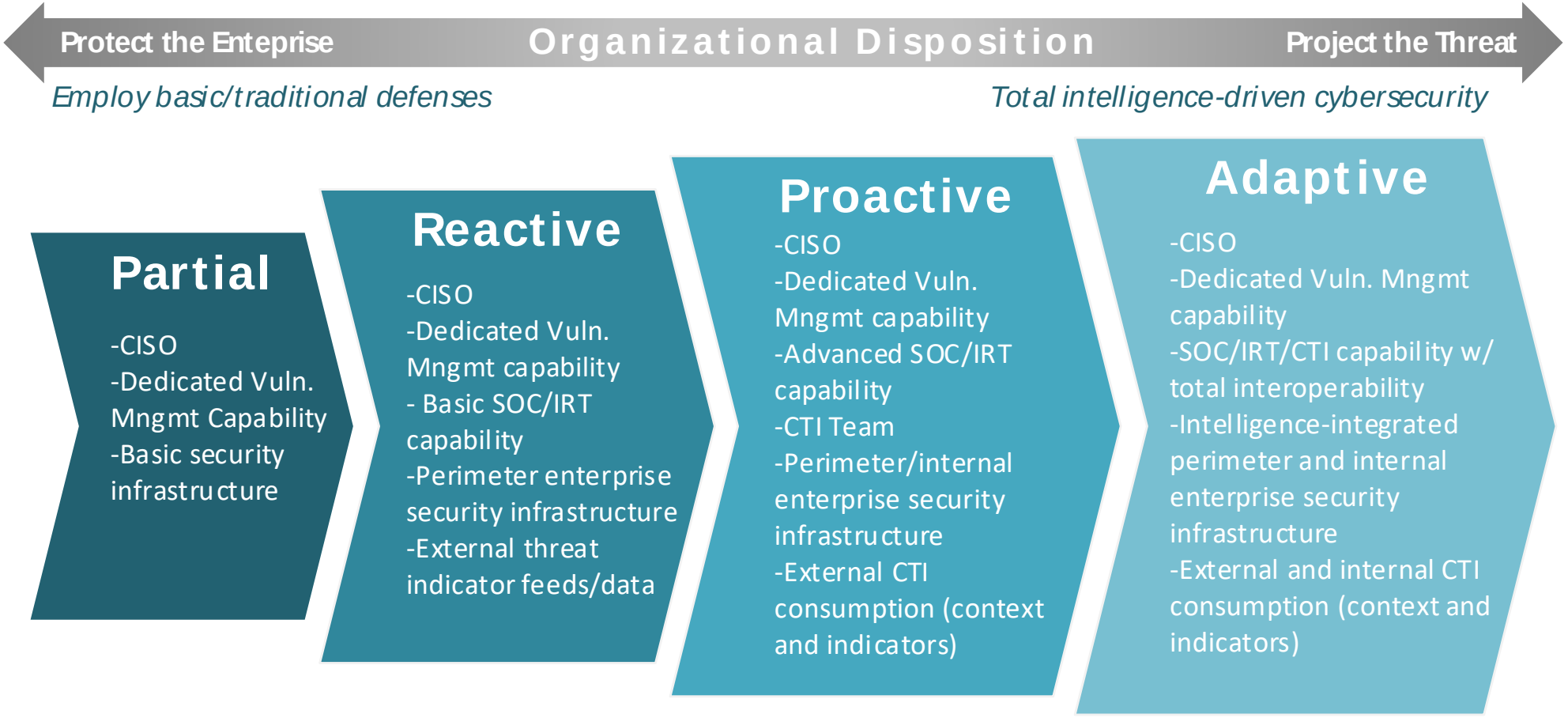
Top 10 Matched Feeds

count	Feed	count	percent
7	Emerging Threats IQRisk Rep List IPs	45	100
7	CrowdStrike	4	9
7			



Conclusion

Evolution naturelle d’un système de Défense



Merci