# CORTEX & MISP + THE HIVE : LA CYBERDÉFENSE À PORTÉE DE MAIN

*ITrust renforce son SOC par de nouveaux algorithmes et des modules de Threat Intelligence. Cette nouvelle version du SOC, plus performante, permet à nos clients de puiser dans la base de données enrichie d'ITrust en ouvrant un flux entre votre plateforme SOC/ Reveelium et nos serveurs.*

## QUEL EST L'INTÉRÊT DE LA THREAT INTELLIGENCE POUR REVEELIUM ?

Reveelium, l'outil de cybersécurité au cœur du SOC d'ITrust, renforce son module de Threat Intelligence.

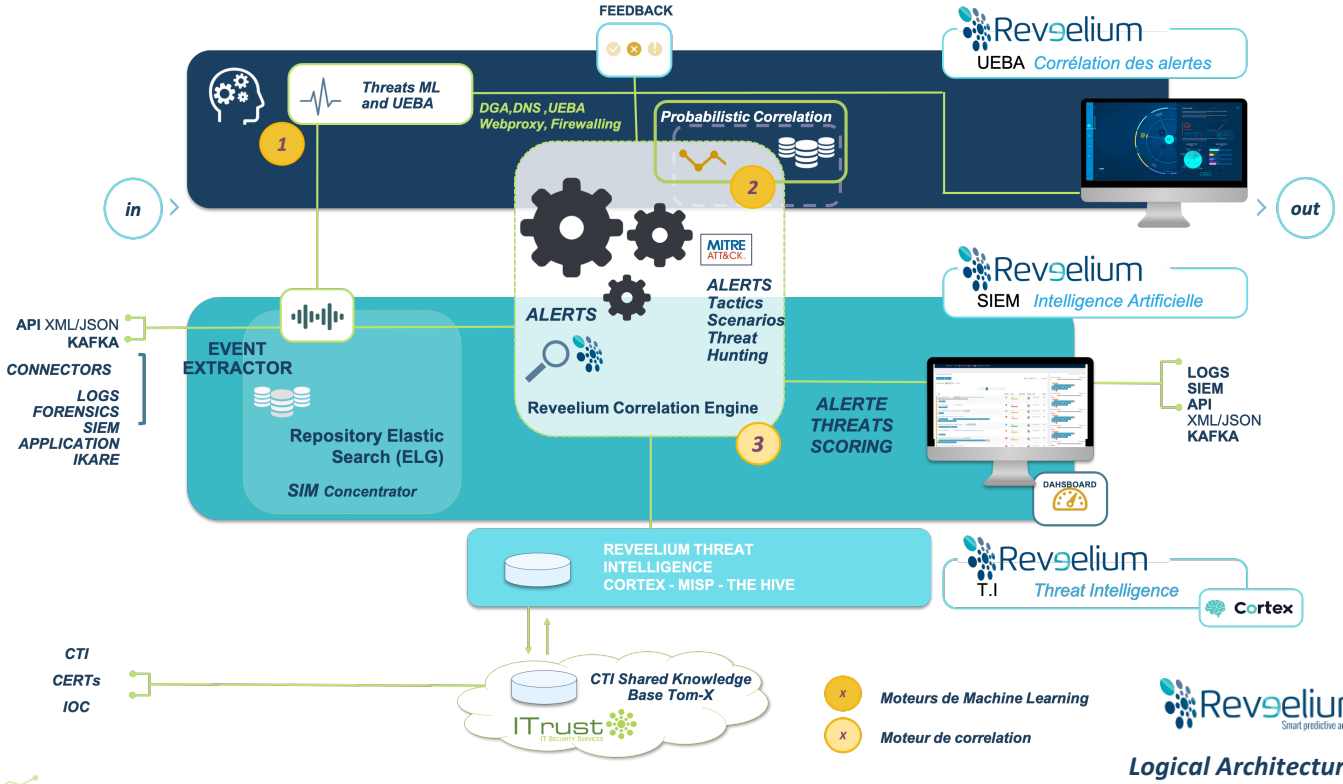
**Reveelium SIEM** *Corrélation des alertes* — **Reveelium UEBA** *Intelligence Artificielle* — **Reveelium T.I** *Base de Threat Intelligence*

En complément de THE HIVE, déjà présent dans votre SOC, les outils de CTI CORTEX et MISP couplés à REVEELIUM améliorent le traitement des alertes :

Cette synergie entre nos outils permet :

- ✓ **L'enrichissement automatique** des alertes, pour une meilleure qualification du danger potentiel.
- ✓ **Un gain de temps grâce à des informations plus claires**, qui amènent à une prise de décision plus rapide
- ✓ **L'accès à la base de Threat Intelligence d'ITrust**, synthèse de nos connaissances et de notre expérience en gestion des menaces

**Cette mise à jour, désormais proposée à tous nos nouveaux clients, n'entrainera aucun frais supplémentaire.**




*Logical Architecture*

## LA THREAT INTELLIGENCE

Le renseignement sur les menaces (« threat intelligence », « cyber threat intelligence » ou « CTI ») se compose d'informations organisées, analysées et affinées sur les attaques potentielles ou actuelles qui menacent les organisations.

Plusieurs grandes entreprises ou institutions mettent à disposition des bases contenant des informations sur les menaces (IOC). Les informations tirées de ces bases permettent une meilleure contextualisation et compréhension des menaces.

## THE HIVE

The Hive est capable de recevoir et de traiter des informations venant de plusieurs services.
En effet, The Hive s'appuie sur CORTEX, qui analyse en masse des éléments et des indicateurs de compromission (IOC) (comme des adresses IP ou mail, des noms de domaines, des fichiers, ou des "hash").

Ces indicateurs portent le nom d'observables dans The Hive et sont visibles au niveau des alertes et des cases.

Ces analyses sont les résultats de demandes d'informations (sous forme de requêtes API) à plusieurs bases de Threat Intelligence connues.

The Hive s'appuie également sur un serveur MISP, qui est une plateforme de partage des menaces. Ce serveur se base sur la communauté cyber et permet de publier et de récupérer des évènements (ransomware / malware…) ainsi que leurs IOC associés.

Grâce à MISP vos données seront corrélées aux dernières compromissions & attaques publiées par des organiques publics comme privés (CERT, CSIRT…)

## WORKFLOW

MISP et CORTEX communiquent entre eux et récupèrent des informations, pour les centraliser ensuite sur The Hive.

**> WORKFLOW - The Hive / Cortex / MISP**

Résumé technique des outils :

**Cortex :**

1. Récupération des informations concernant les IOC présents dans les cases / alertes The Hive (observables) via le les IHM
2. Interrogation des bases de Threat Intelligence
3. Génération de rapports en fonction des criticités
4. Ajout de tags (score, cvss, etc…)

**MISP :**

1. Récupération des informations concernant les IOC présents dans les cases / alertes The Hive (observables) via l'IHM
2. Interrogation de la base MISP
3. Remontée sous forme des évènements où l'IOC à été repéré.