

Mairie de Sainte-Maxime  
DSI

# PROJET SIEM

Lancelot MELLANO

Alternant R&T

Projet tuteuré par Clément Jacob

# BESOINS DE LA MAIRIE

Surveillance et Contrôle Continu sur un périmètre définit	Détection des Incidents de Sécurité	Gestion des Intrusions et des Menaces
Analyse Comportementale	Compatibilité Système	Maintenance Minimaliste et Intuitive
Intégration d' I.A	Prestataire aidant	Prix raisonnable

# PERIMETRE DE LA MAIRIE

## Protection des Pare-feu :

Les pare-feu servent de première ligne de défense en filtrant le trafic entrant et sortant pour sécuriser l'infrastructure réseau de la mairie.

## Infrastructure Virtuelle hyperviseur :

Ils orchestrent les machines virtuelles, cruciales pour le fonctionnement des services essentiels du réseau de la mairie.

## Serveurs Opérationnels :

Les serveurs hébergent des fonctions critiques, gérant à la fois les applications essentielles et la sécurité du réseau.

## Cloud environnement office 365 :

Cet environnement permet la surveillance complète des comptes de la mairie

# SOLUTION SIEM

Un SIEM (Security Information and Event Management) est un outil de sécurité informatique qui permet de :

- Collecter
- Centraliser
- Corréler
- Analyser
- Gérer



Evénements de sécurité provenant de diverses sources (serveurs, équipements réseau, applications, périphérique finaux etc...)

# COMPARATIF DES SOLUTIONS

Solution/Critères	Fonctionnalités	Facilité d'utilisation	Difficulté de mise en œuvre	Maintenance & Support	Coût (Moyen de facturation)
Securonix	10/10	9/10	10/10	10/10	8/10
Microsoft Sentinel	8/10	-	10/10	6/10	-
Rapid7	10/10	7/10	10/10	8/10	0/10
Elastic Security	10/10	5/10	10/10	7/10	0/10
Exabeam	10/10	-	10/10	5/10	-
Splunk	10/10	-	10/10	-	0/10
IBM	10/10	-	10/10	-	0/10
Log 360 Engine	10/10	8/10	5/10	6/10	0/10



# SOLUTION SECURONIX

## ■ Présentation de Securonix :

Fondée en 2007, Securonix est un leader de la sécurité des informations grâce à sa plateforme cloud native qui multiplie les technologies de pointe :

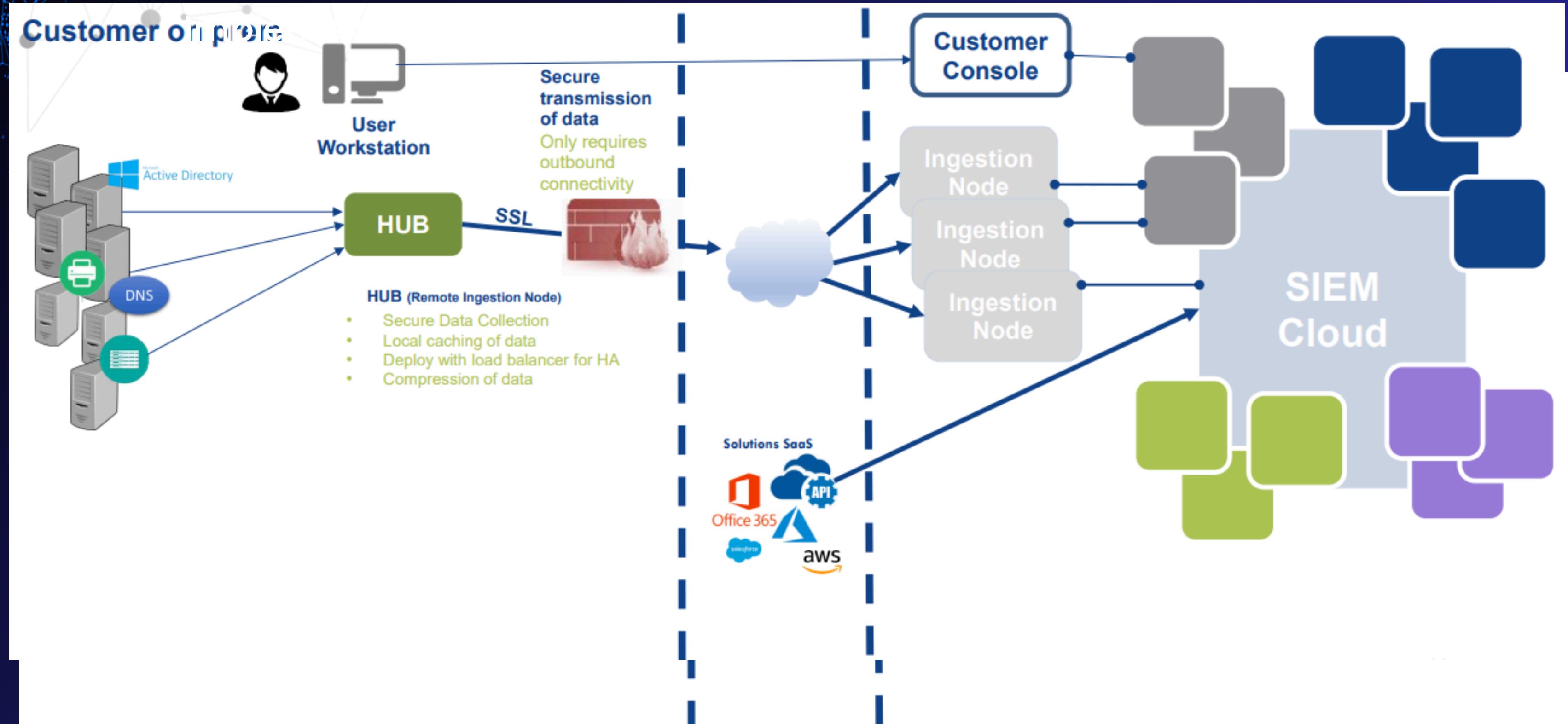
- Intelligence artificielle (IA)
- Apprentissage automatique (Machine Learning)
- Analyse comportementale
- Détection des menaces avancées
- Gestion des identités et des accès
- Réponses automatisé (SOAR)

Depuis 2018, la solution SIEM de Securonix est classée dans la catégorie « Leader » du Magic Quadrant pour les SIEM. Ce qui en fait une solution extrêmement fiable.

Securonix fournit une plateforme unique et unifiée pour tous ces cas d'usages :

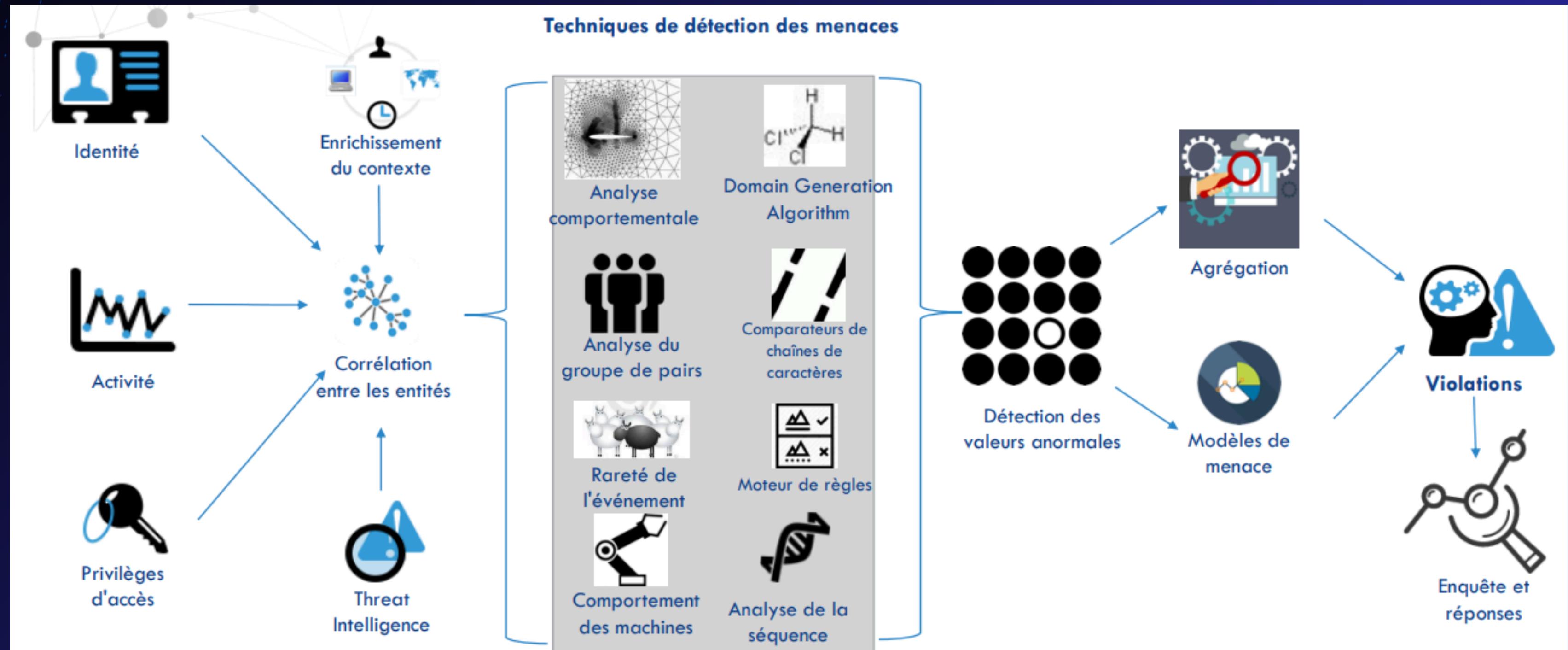
- SOAR (Sécurité Orchestration, Automatisation et Réponse)
- UEBA (Analyse comportementale)
- SIEM
- Security Data Lake(système de stockage)

# SOLUTION SECURONIX



# SOLUTION SECURONIX

## Fonctionnement du SIEM:



# SOLUTION SECURONIX

## Exemple d'un cas concret :

The diagram illustrates the Securonix threat model and analysis components across four main sections:

- Enrichissement:** A circular diagram showing the relationship between Identity, Entity, Access, Activity, Violations, and Cyber Threats.
- Rareté de l'événement:** A grid of circles where one circle is highlighted in red, indicating an unusual event.
- Analyse par les pairs:** A hexagonal diagram showing user Jane Doe's profile and her interactions with others, including Cohesiveness (100%), JobKey ('30003509'), Division ('SECURITIES OPERATIONS'), Dept ('INVESTMENT MGT'), Manager ('J.Smith'), Title ('SECOND VP'), and percentages (60%, 75%, 80%, 97%, 92%).
- Analyse comportementale:** A line graph titled "Suspicious Activities" showing Frequency over time from Jan 1, 2019 to Jan 7, 2019. It highlights an "Outlier" point at Jan 6, 2019, above a "Baseline".

**Threat Model des évènements internes**

**RISQUE INHÉRENT À L'UTILISATEUR** → **MAUVAIS USAGE DU COMPTE** → **COMPROMISSION DES DONNÉES** → **EXFILTRATION**

**Enrichissement**  
David est un consultant

**Rareté de l'événement**  
L'utilisateur se connecte à une heure inhabituelle - 5 heures du matin.

**Analyse par les pairs**  
Accès à des fichiers auxquels les utilisateurs de mêmes priviléges n'ont jamais eu accès

**Analyse comportementale**  
Transfert des données vers une clé USB - pic dans les fichiers copiés

# PRESTATAIRE DE SECURONIX

## Présentation :

Elit-Technologies est une entreprise française spécialisée en cybersécurité, cloud et réseaux, offrant des transformations numériques personnalisées depuis 2007 pour les secteurs public et privé.



### Depuis 2007

Accompagne les entreprises dans leur transformation durable



### + 15 Ans d'expertise

Réseau et sécurité des systèmes d'information



### 1 SOC

SOC externalisé qui analyse, réagit et améliore constamment le fonctionnement de notre SIEM



### 1 CSIRT

Surveillant et réagissant aux événements 24/7/365



# PRESTATAIRE DE SECURONIX

## ■ Ce qu'il nous apporte :

### Implémentation du SIEM de Securonix :

- Installation et Configuration
- Formation et Support

### Partenariat avec un SOC Externalisé :

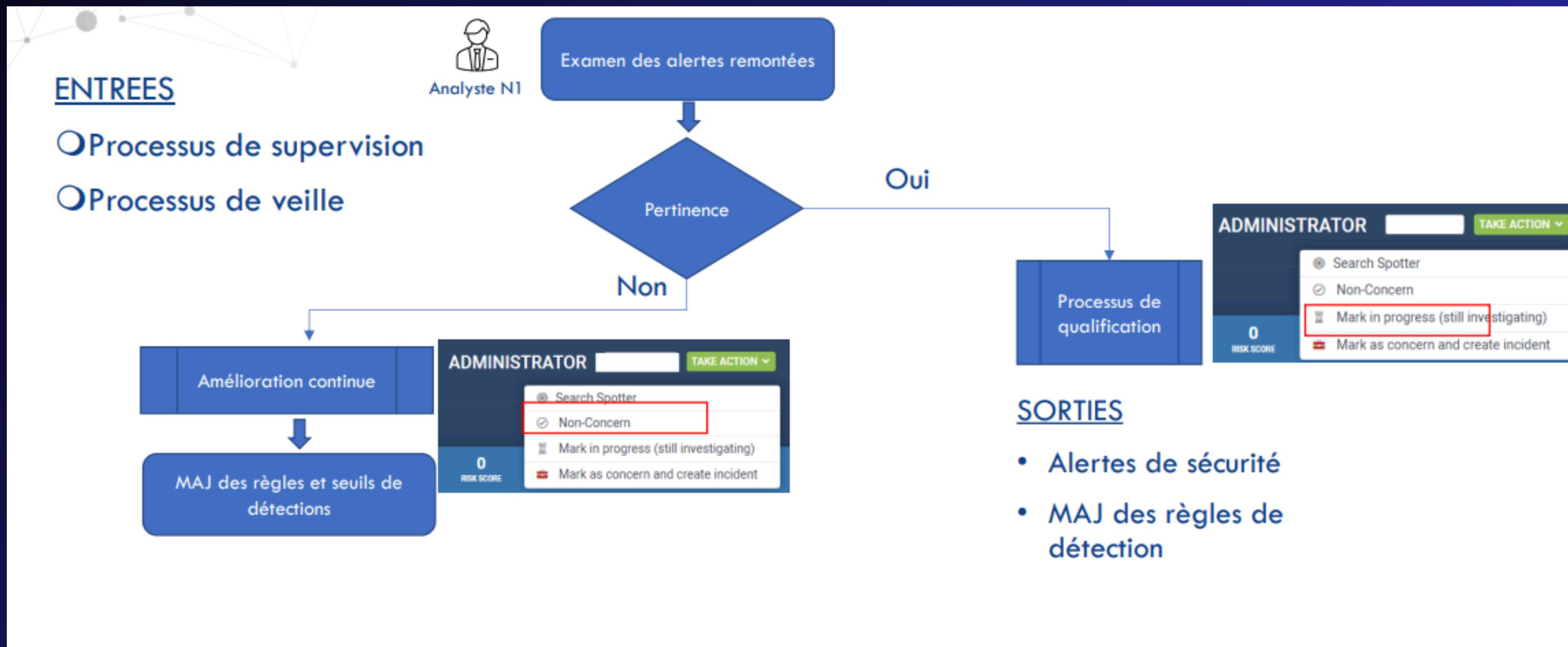
- Surveillance Continue
- Améliorations et Mises à Jour
- Réponse aux Incidents

### Rapports et Analyses :

- Rapports Mensuels
- Conseils Proactifs

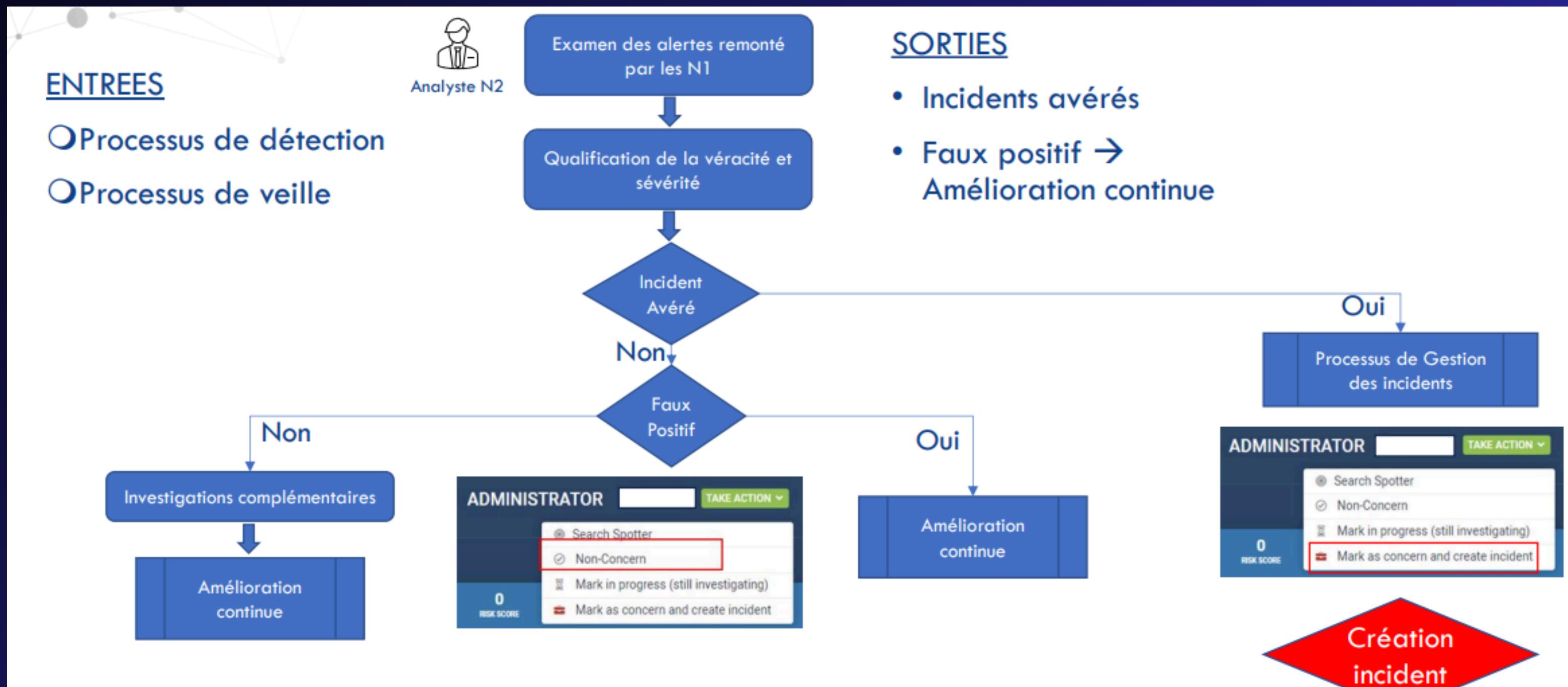
# PRESTATAIRE DE SECURONIX

## 1-Leur façon de traiter les menaces, processus de détection :



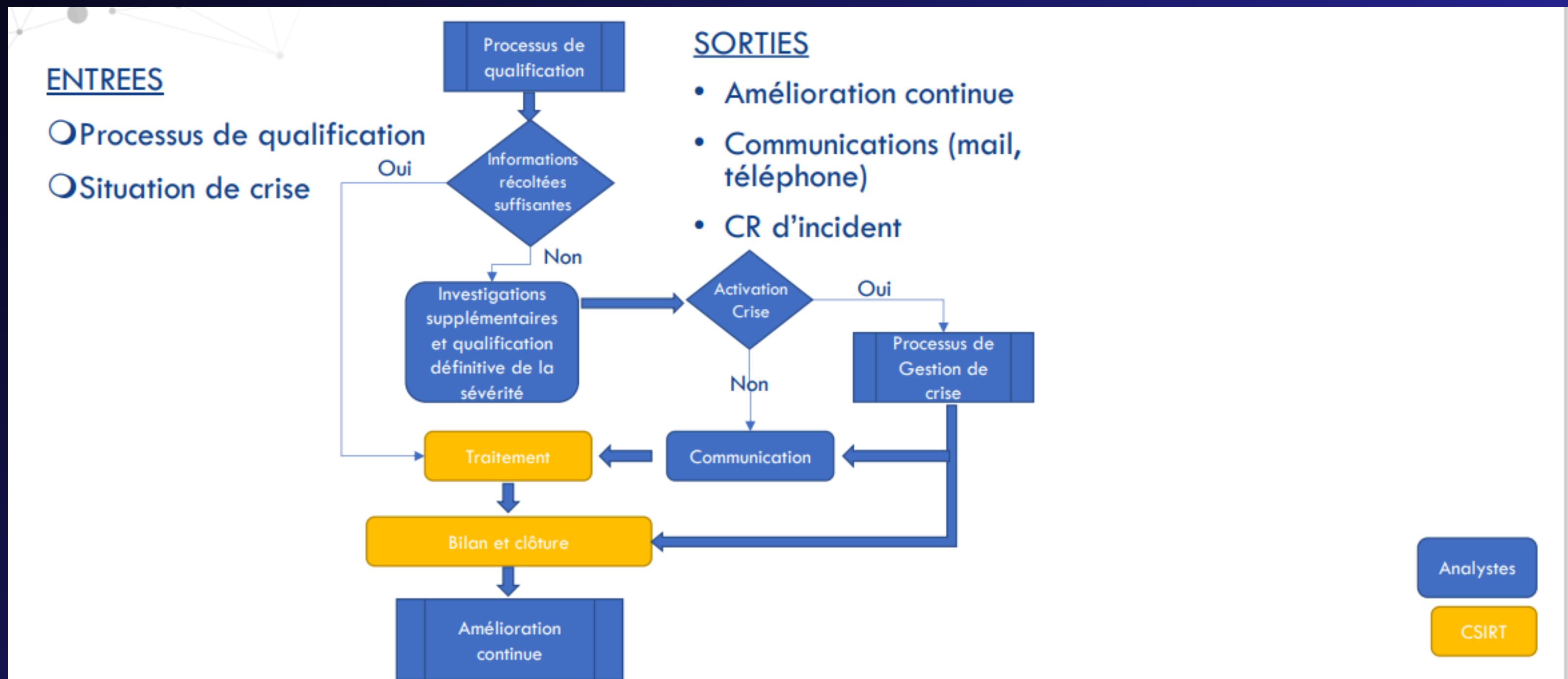
# PRESTATAIRE DE SECURONIX

## 2-Leur façon de traiter les menaces, processus de qualification :



# PRESTATAIRE DE SECURONIX

## 3-Leur façon de traiter les menaces, processus de gestion des incidents :



# PRESTATAIRE DE SECURONIX



Juin 2025



1 440 € frais mensuels (17 280 €)  
5 340 € frais d'installation

# RÉSUMÉ DE LA SOLUTION :

Avec l'implémentation de la solution SIEM de Securonix, renforcée par le support et la surveillance d'un SOC externalisé d'Elit-Technologies, nous pourrons établir une infrastructure robuste pour détecter, répondre et prévenir les menaces de sécurité de manière proactive.

## Avantages clés:

- Surveillance Améliorée
- Mises à jour constantes de la solution SIEM
- Support Expert
- Rapports et analyses mensuel
- Installation de la solution prise en charge
- Solution fiable reconnu par l'état

## Impact sur la Mairie:

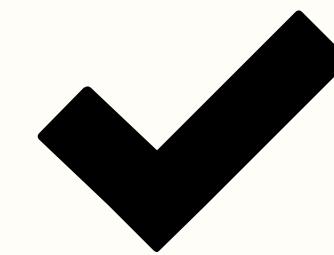
- Sécurité informatique renforcée
- Conformité Assurée
- Vision globale de tous les événements sur l'ensemble du périmètre

# POUR ALLER PLUS LOIN...



## PHASE **SOURCING**

Solution proposé Securonix  
Cout total  $17\ 280 + 5340 = 22\ 620$  €



## PHASE **VALIDATION**

Le budget alloué à ce projet  
est de ???? €

Deadlines ?



## **PROPOSITION DE CONTINUATION**

Nous pouvons envisager de  
continuer avec la solution de  
Securonix en passant à la  
phase de Réalisation