Octobre 2108

Journées Cyber Sécurité

Tunis JCS'2018

Spingy SIEM

Dr. Wassim Youssef

ALPHA ENGINEERING & TECHNOLOGIES

A Propos de nous

ALPHA ENGINEERING – **IT Division**

- Société de développement logiciel et services IT
- Créée en 2005 et présentée en Tunisie et France,
- IT Outsourcing, Cloud Computing, IoT, Big data, Solutions de surveillance et de sécurité,
- Des solutions IT avec une vraie valeur ajoutée pour le client.

A Propos de nous

ALPHA ENGINEERING – **IT Division**

- Monitoring, Gestion des performances et Fault Management
- Editeur d'une solution de supervision unifiée « Alphatron Unified Monitoring Platform »
- Intégration des solutions Open Source à très forte valeur ajoutée
- System Integration
- Cloud Computing

A Propos de nous

NOTRE ENGAGEMENT QUALITÉ

- SMQ mis en place selon ISO 9001 v2008
- Audits réguliers des processus par le RMQ et DQS
- Processus de la Qualité inclus dans le SMQ:
  - **Integration on Open Source & 3rd Party Software Solutions**
  - **TMA, Managed Services, Outsourcing & Support**
  - **Cloud Computing Service Broker**
  - **Cloud Computing Managed Services**
  - **Telecommunication & IT Equipments Integration**
  - **Telecommunication & IT infrastructure Engineering**
  - **Telecommunication & IT Equipments Manufacturing**


IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
CERTIFICATE
IQNet and
DQS GmbH Deutsche Gesellschaft zur Zertifizierung von Managementsystemen
hereby certify that the company
Groupe Alpha Engineering
B33 & 34 Bloc C, Imm El Habib
2 Rue Lac Annecy, Les Berges du Lac
1053 Tunis - Tunisie
has implemented and maintains a Quality Management System.
Scope:
Integration of Open Source & Third-Party Software Solutions
Third Party Maintenance, Managed Services, Outsourcing and Support
Telecommunications and IT Infrastructure Engineering
Telecommunications & IT Equipments Manufacturing
Cloud Computing Managed Services
Cloud Computing Service Broker
Telecommunications & IT Equipments Integration
Through an audit, documented in a report, it was verified that the management system fulfills the requirements of the following standard:
ISO 9001 : 2008
Date of certification 2013-07-11
Valid until 2016-07-10
Registration Number: DE-509578
Michael Drechsel
President of IQNet
Götz Blechschmidt
Managing Director of DQS GmbH
IQNet Partners*:
AENOR Spain AFNOR Certification France AIB-Vincotte International Belgium ANCE-SIGE Mexico APCER Portugal CCC Cyprus CISQ Italy CQC China CQM China CQS Czech Republic Cro Cert Croatia DQS Holding GmbH Germany DS Denmark FCAV Brazil FONDONORMA Venezuela ICONTEC Colombia IMNC Mexico INNORPI Tunisia Inspecta Certification Finland IRAM Argentina JQA Japan KFQ Korea MIRTEC Greece MSZT Hungary Nemko AS Norway NSAI Ireland PCBC Poland Quality Austria RR Russia SII Israel SIQ Slovenia SIRIM QAS International Malaysia SQS Switzerland SRAC Romania TEST St Petersburg Russia TSE Turkey YUQS Serbia
IQNet is represented in the USA by: AFNOR Certification, CISQ, DQS Holding GmbH and NSAI Inc.
* The list of IQNet partners is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

A Propos de nous

NOS CLIENTS

Services, Media & Telecom

Gouvernement et institutions

Industrie, Distribution, Energie

World Wide Projects

Algerie
Allemagne
Burkina Faso
Cote d’ivoire
CANADA
Dubai
France
Gabon
Guinea
Libye
Maroc
Mauritania
Niger
Royaumes unis
Senegal
Togo
Tunisia
U.S.A

1 À propos de nous

2 Métier et sécurité

3 Solution SIEM

4 Visite guidée

5 Démo

6 Next Step

ENGINEERING

FACTS

- Entreprise : métier composante la plus importante

  Le Métier est spécifique

- Données, **maitrise** des données : clés de voute de sucées entreprise, encore plus dans l'ère de la **digitalisation**

- Système d'Information : pierre angulaire pour assurer le métier de l'entreprise

FACTS

- Sécurité des données et du SI est un besoin fonctionnel

- Risques génériques de sécurité
- Risques spécifiques (liées au métiers)

- Besoins d'identifier les risques, prévenir et identifier rapidement les incidents, apporter rapidement une réponse
  - Outils informatiques
  - Processus, notamment RH
    - Diffusion de la culture de sécurité

Vision : des missions d'analyse des stratégies de sécurité qui passe par un cercle vertueux du changement

A **Métier**

Analyse de votre métier, votre structure, vos produits **pour définir** vos enjeux stratégiques de sécurité

D **RH**

Mise en place d'une culture du **changement permanent** intégrant les enjeux de sécurité et de bonnes pratiques dans tous les processus RH

B **Processus**

Alignement de vos processus sur les enjeux de sécurité portés par votre métier

C **SI**

Transformation du SI sur 3 axes :

- Le SI lui-même doit répondre aux enjeux de sécurité
- Le SI doit intégrer les bon outils de sécurité
- Le SI doit intégrer les outils d'analyses, reporting et monitoring de la sécurité

1 À propos de nous

2 Métier et sécurité

3 Solution SIEM

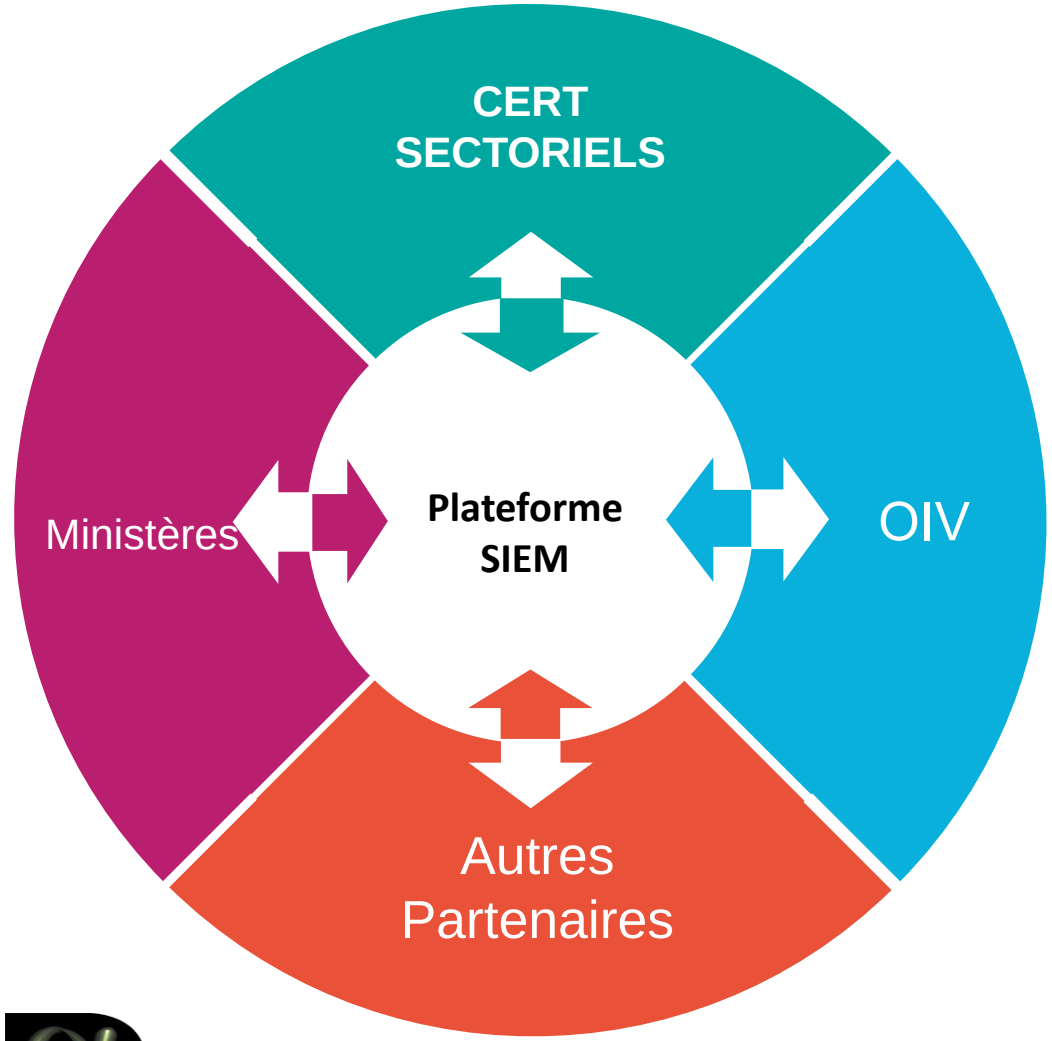
4 Visite guidée

5 Démo

6 Next Step

ENGINEERING

Notre plateforme de services à destination des CERT / CSIRT



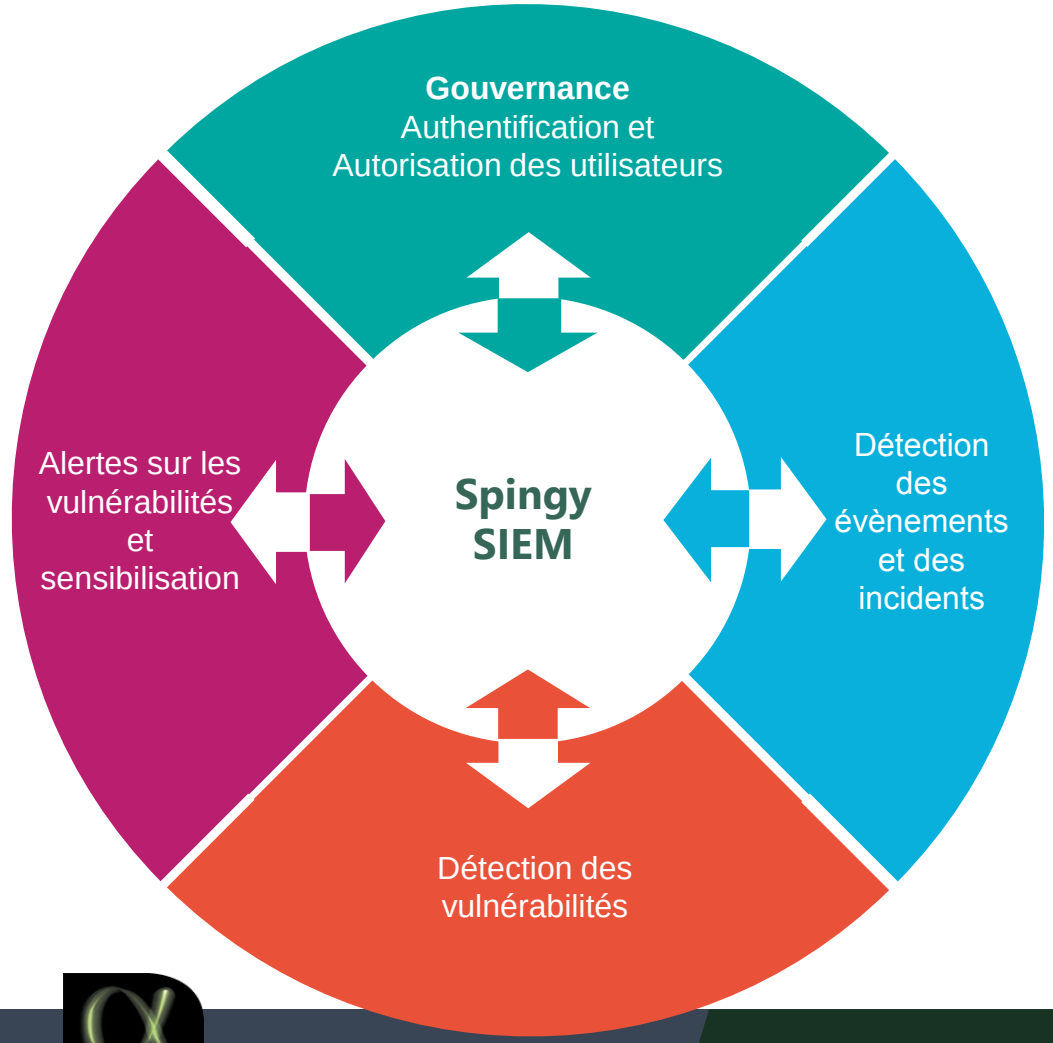
1. Une plateforme permettant d'orchestrer et d'animer la relation entre le CERT National de l'ANSI et les différents partenaires de la stratégie nationale de Cyber Défense

2. Un outil qui permet la mise en œuvre d'une stratégie sur 3 axes :
   1. **La résilience** : permettant de manager la qualité de service et l'amélioration continue
   2. **La réaction rapide** : partagée et collaborative
   3. **L'anticipation** : pour une gestion intelligente et proactive des risques

3. Une technologie ouverte qui laisse une totale indépendance aux différents partenaires

4. Une philosophie de co-construction itérative de la stratégie en mode agile

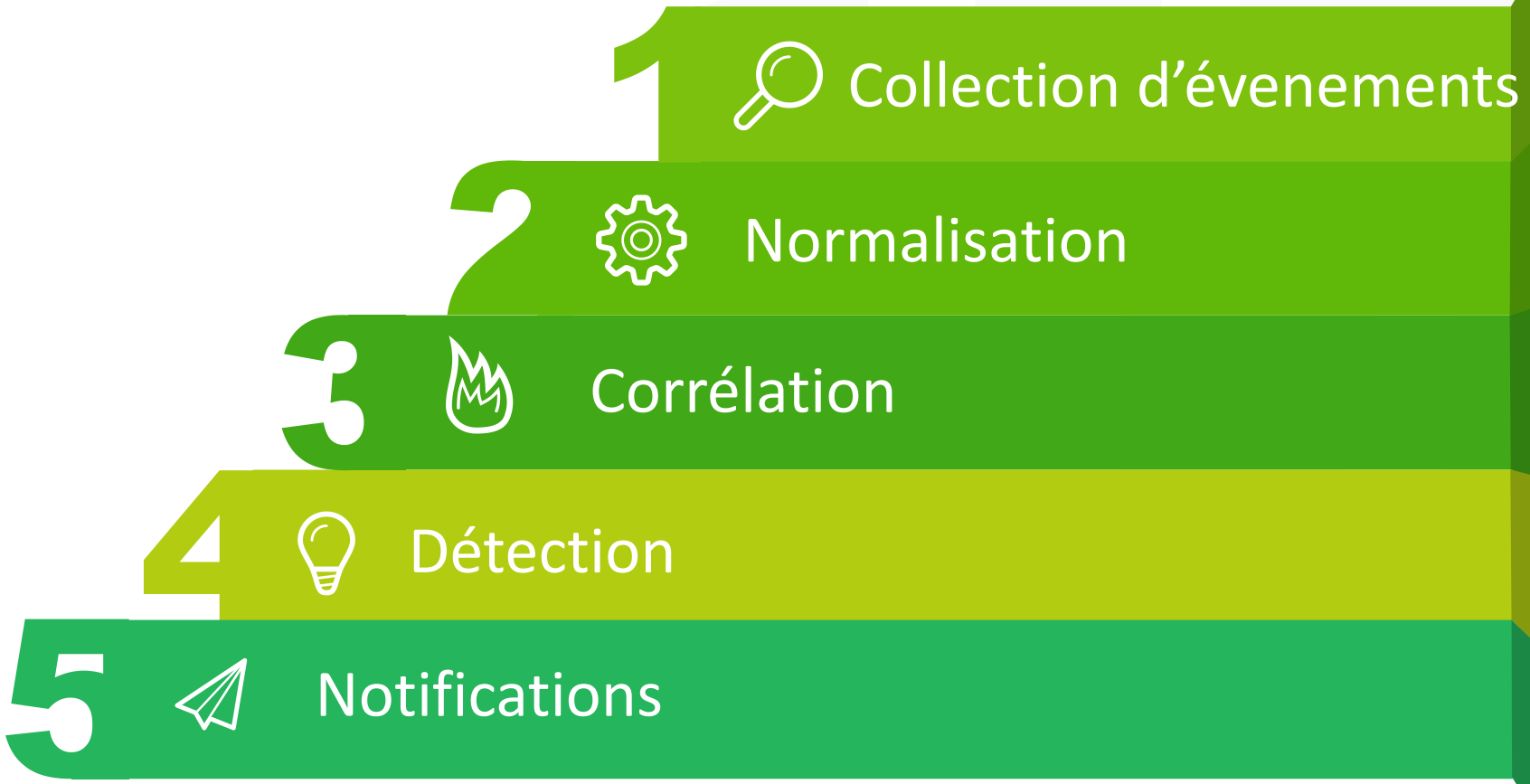
Notre plateforme de services à destination des CERT / CSIRT



7 Modules Clés

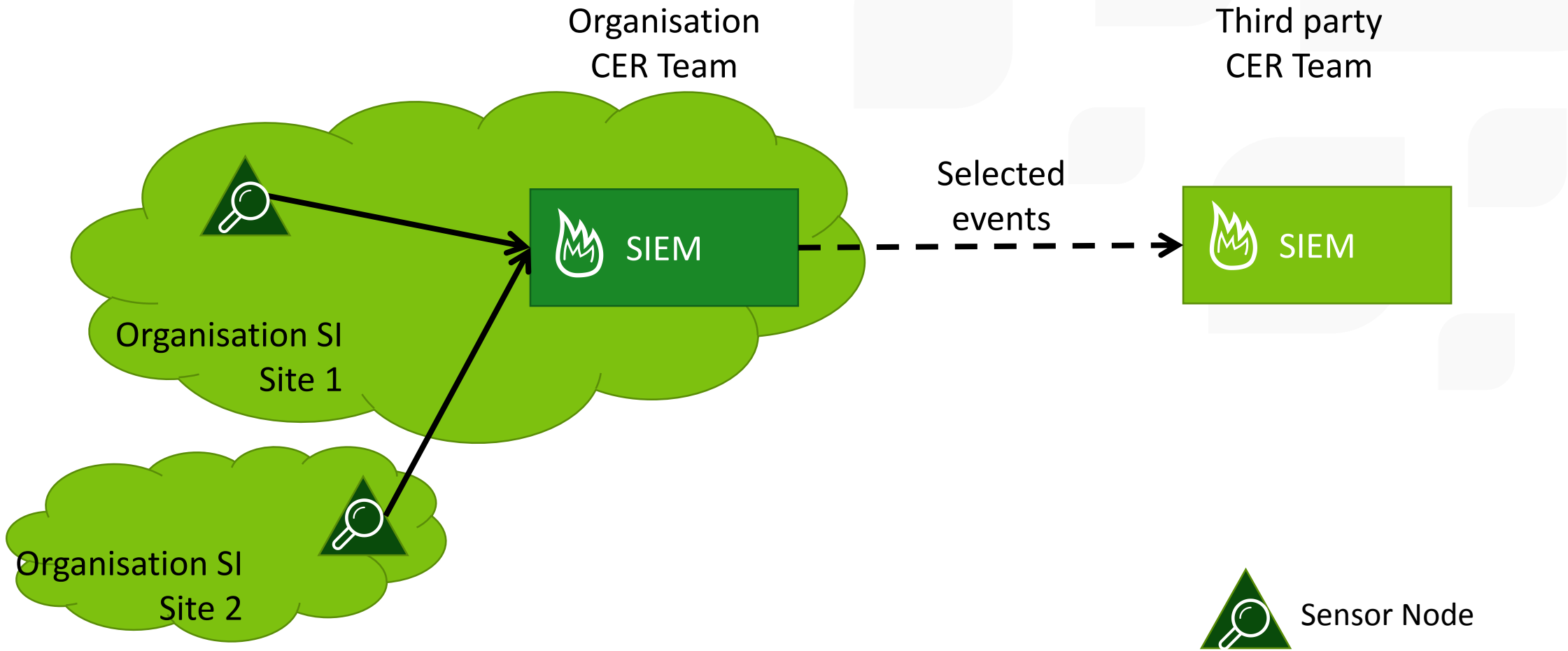
1. **Module Configuration**
2. **Module Dashboard**
3. **Module Evènements et Incidents**
4. **Module Détection de vulnérabilités**
5. **Module Alertes sur les vulnérabilités**
6. **Module Newsletters**
7. **Module Support**

Etapes clefs d'une solution SIEM



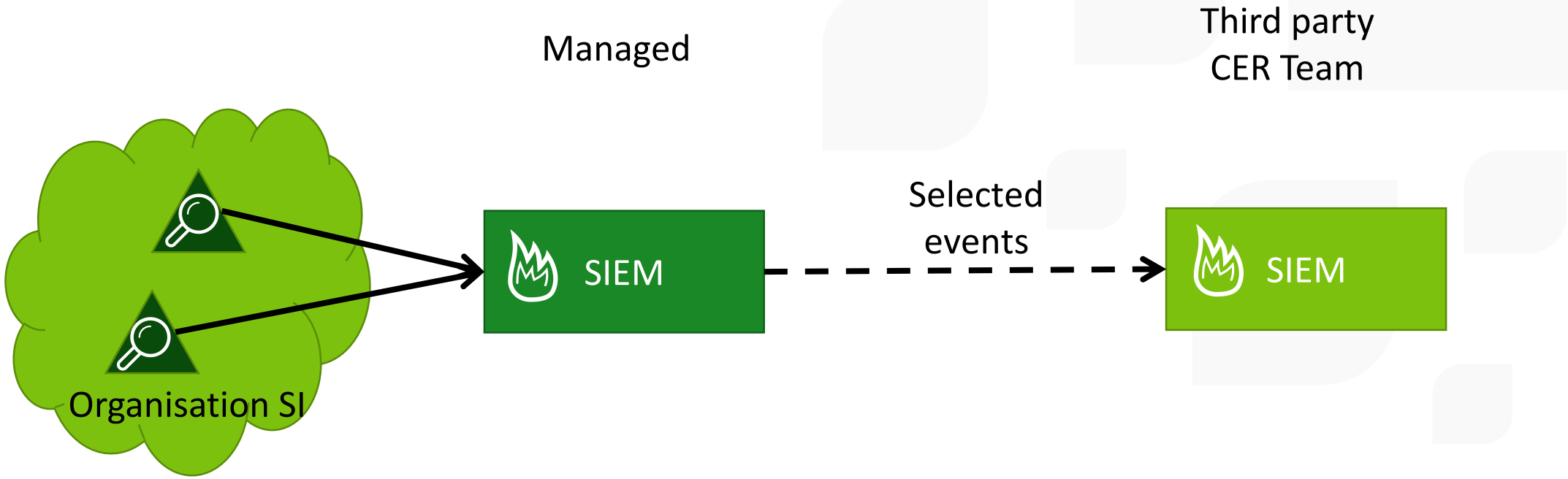
Modèles de déploiement

ON SITE / ON PREM – Multi site enabled



Modèles de déploiement

Managed SIEM



Sensor Node

Architecture de la solution SIEM

APP WEB

Coll / Corr.

Sensors

logstash

Extra Sensor

4 Visite guidée

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

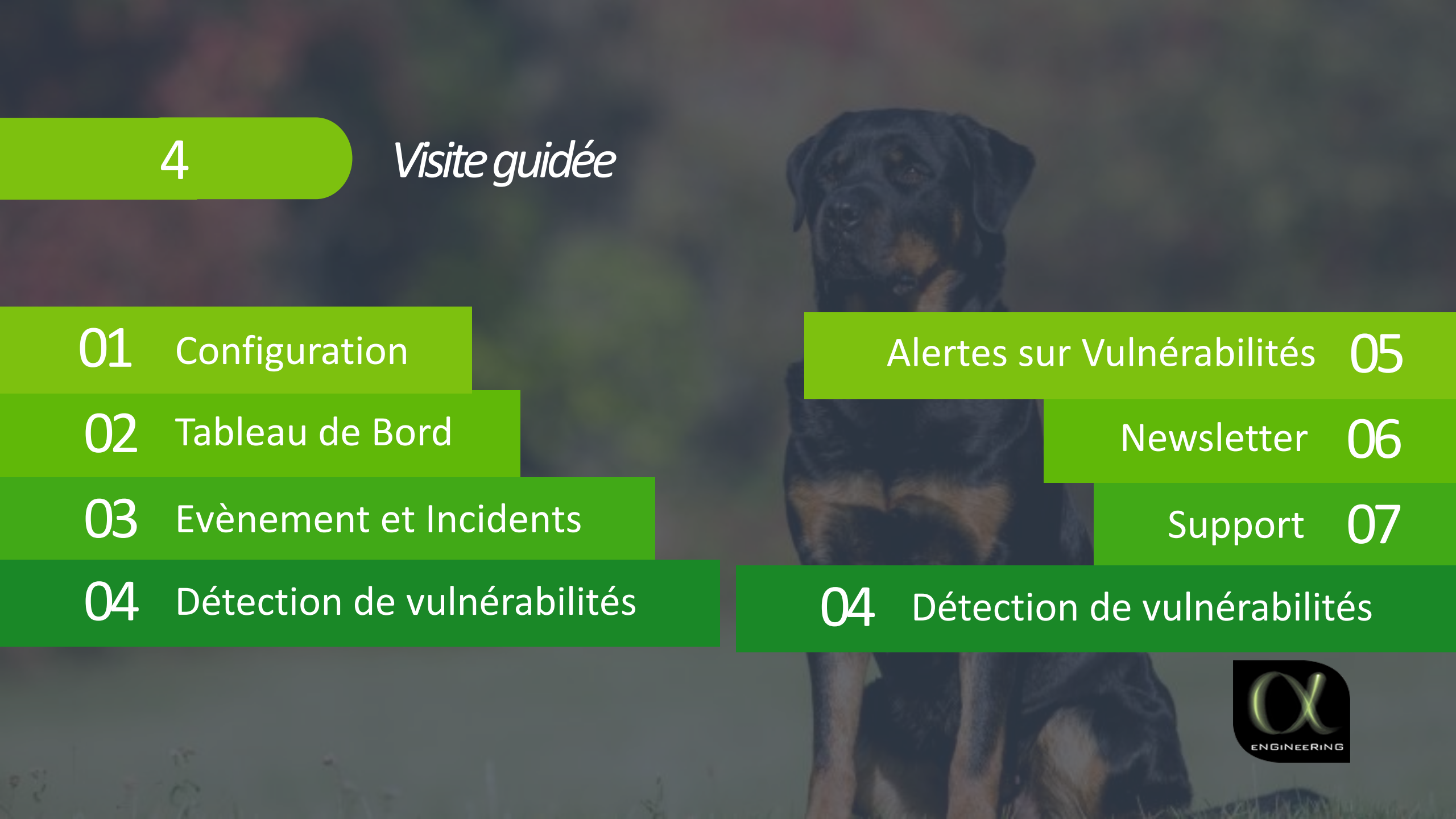
04 Détection de vulnérabilités

Alertes sur Vulnérabilités 05

Newsletter 06

Support 07

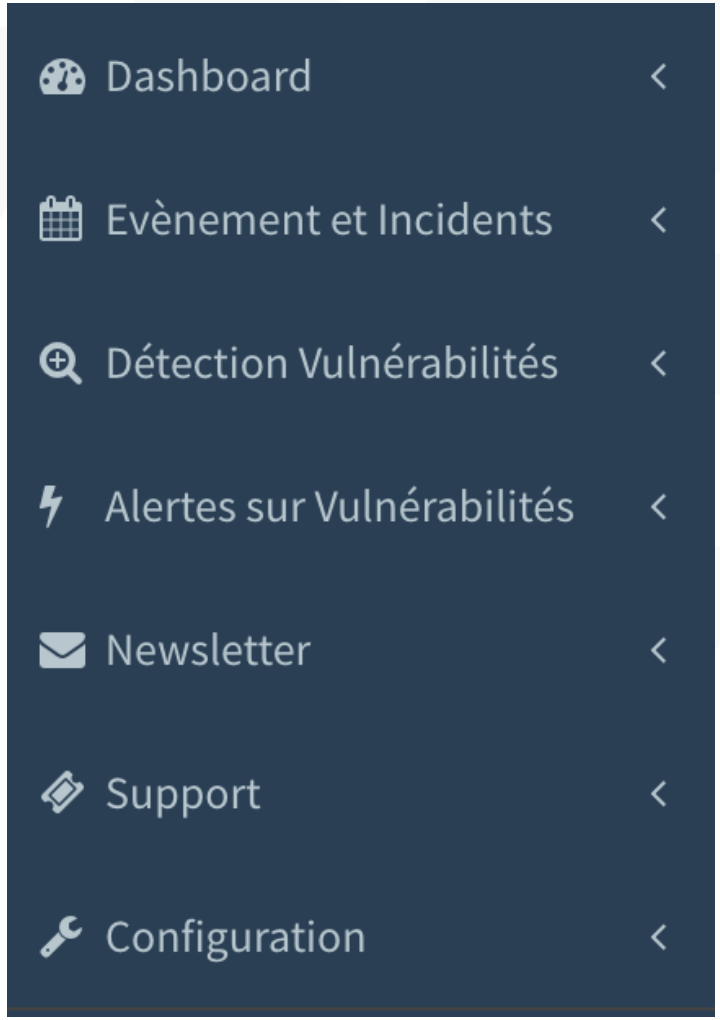
04 Détection de vulnérabilités



Organisation

- Solution organisée en forme de modules.

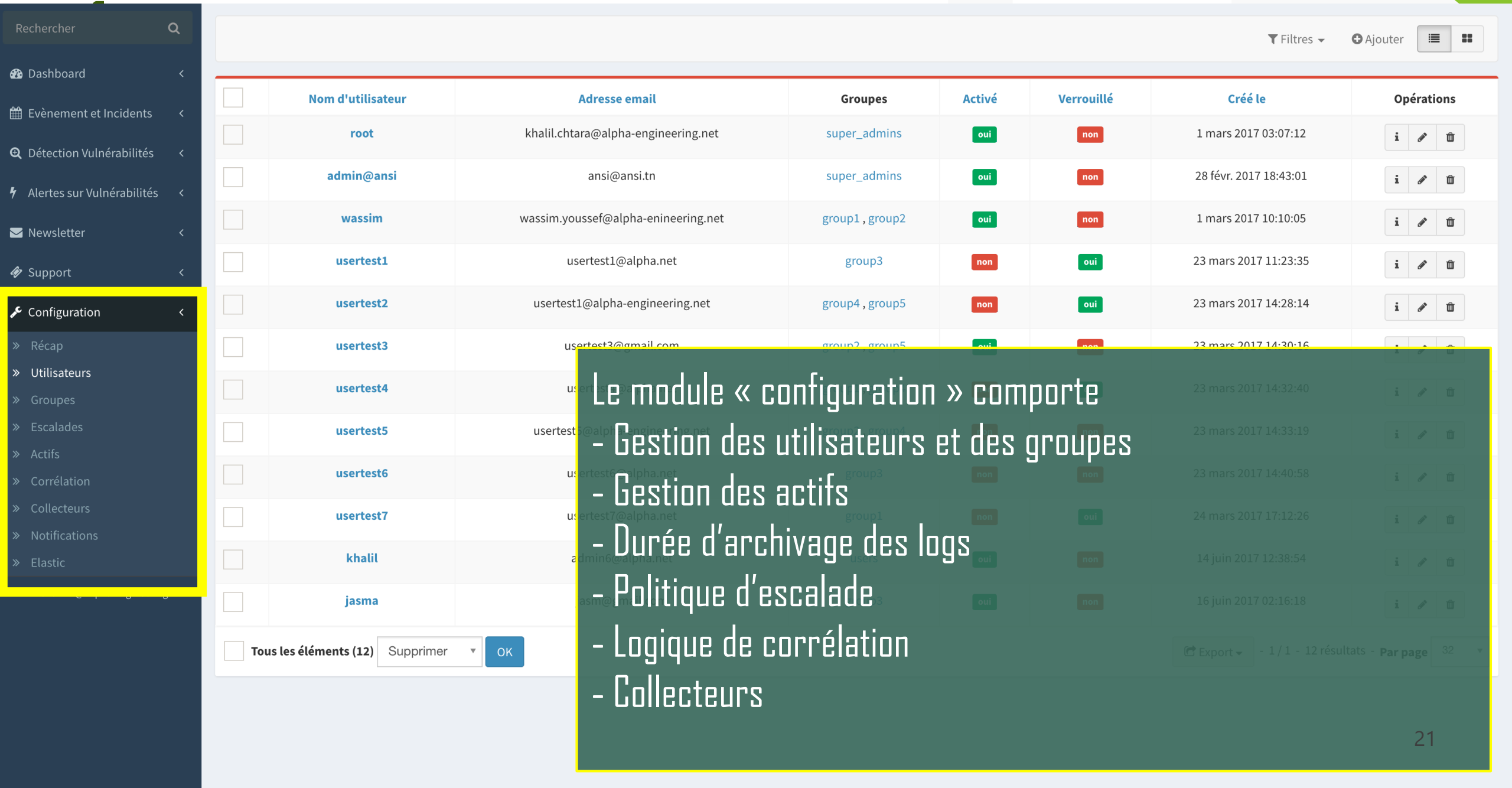
- Chaque module correspond à une entrée du menu principal.



Module Configuration

- Définition du périmètre
  - Identifier les Actifs et services associés
  - Leur affecter des TAG
- Gestion des Roles
  - Ensemble de privilèges fins (créer newsletter / valider newsletter)
- Gestion des Utilisateurs

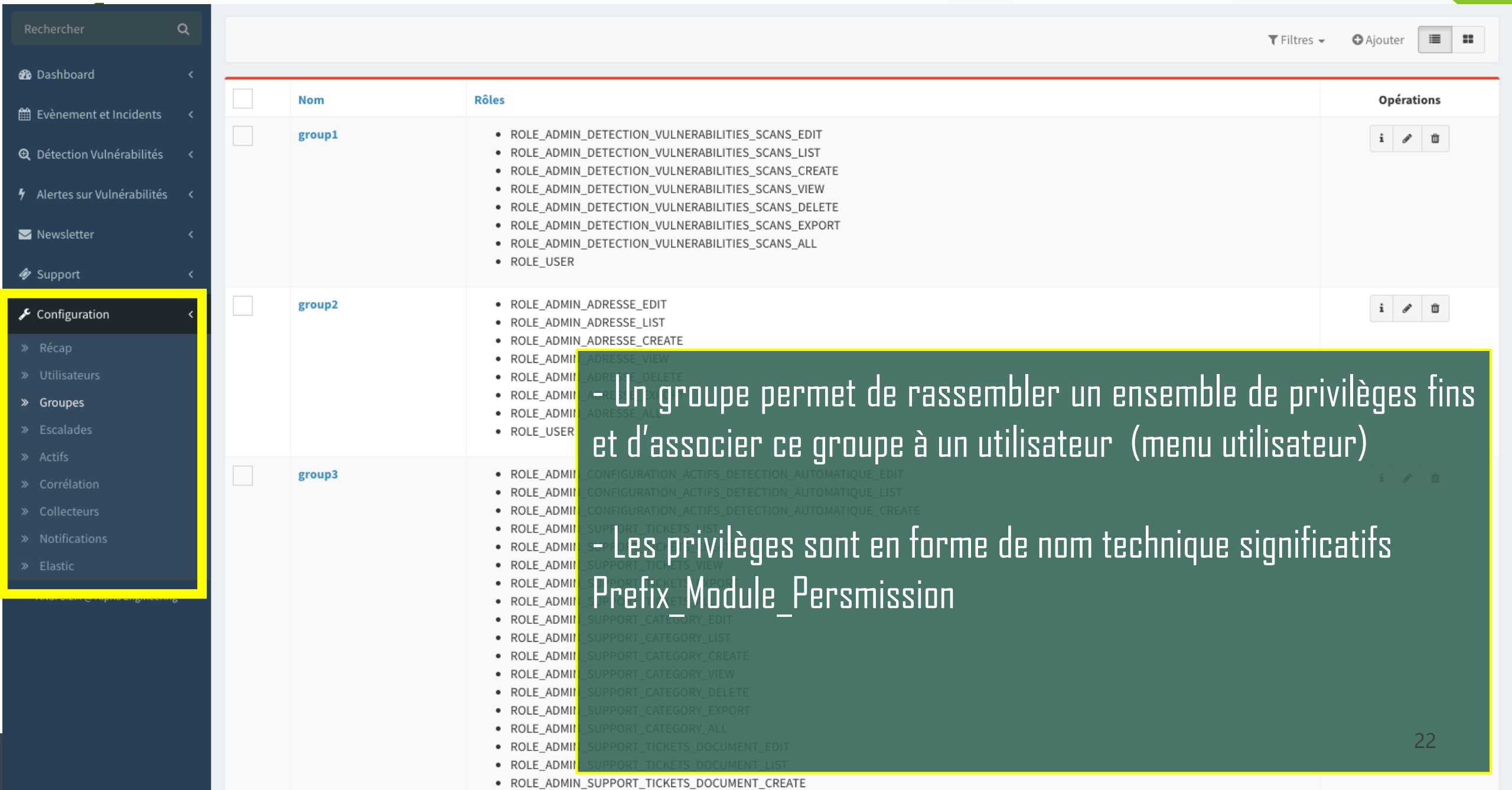
1. Module Configuration : Description



Le module « configuration » comporte

- Gestion des utilisateurs et des groupes
- Gestion des actifs
- Durée d'archivage des logs
- Politique d'escalade
- Logique de corrélation
- Collecteurs

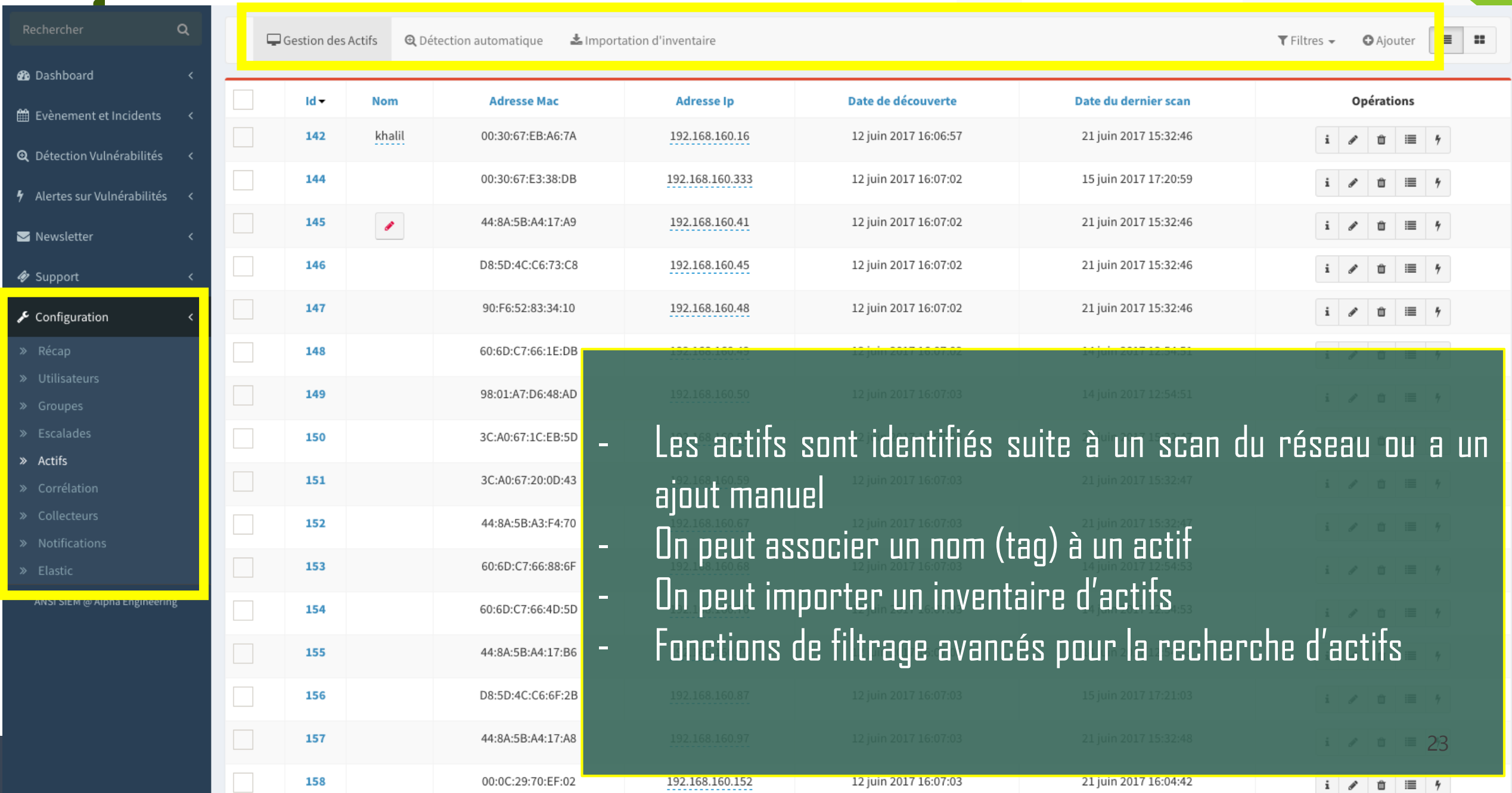
1. Module Configuration : Groupes



- Un groupe permet de rassembler un ensemble de privilèges fins et d'associer ce groupe à un utilisateur (menu utilisateur)

- Les privilèges sont en forme de nom technique significatifs Prefix_Module_Persmission

1. Module Configuration : Actifs



- Les actifs sont identifiés suite à un scan du réseau ou a un ajout manuel
- On peut associer un nom (tag) à un actif
- On peut importer un inventaire d'actifs
- Fonctions de filtrage avancés pour la recherche d'actifs

1. Module Configuration : Notifications

- Permet de lister les différentes notifications affichées à l'utilisateur

4 *Visite guidée*

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

04 Détection de vulnérabilités

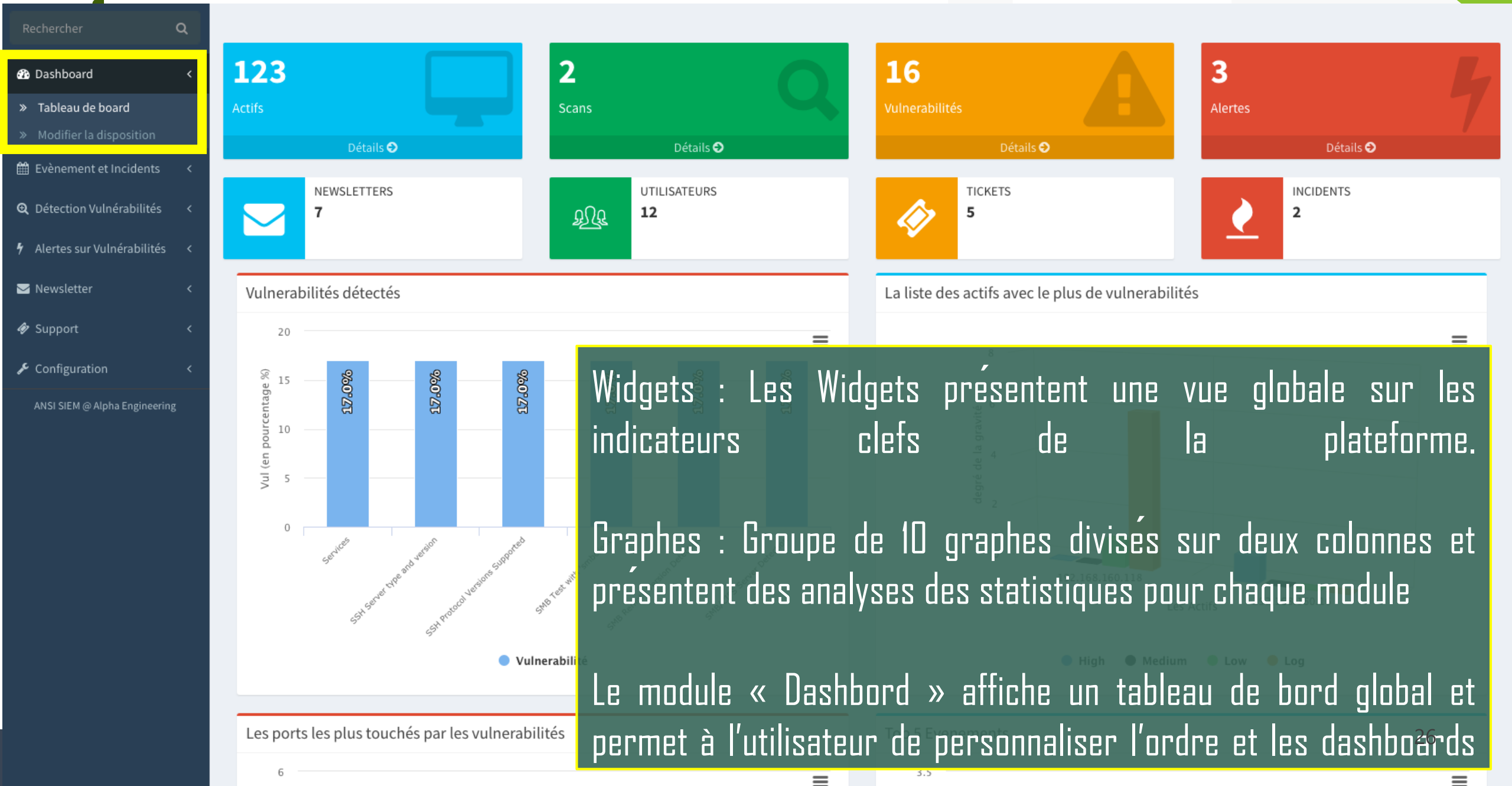
Alertes sur Vulnérabilités 05

Newsletter 06

Support 07

ENGINEERING

2. Module Dashboard : Description

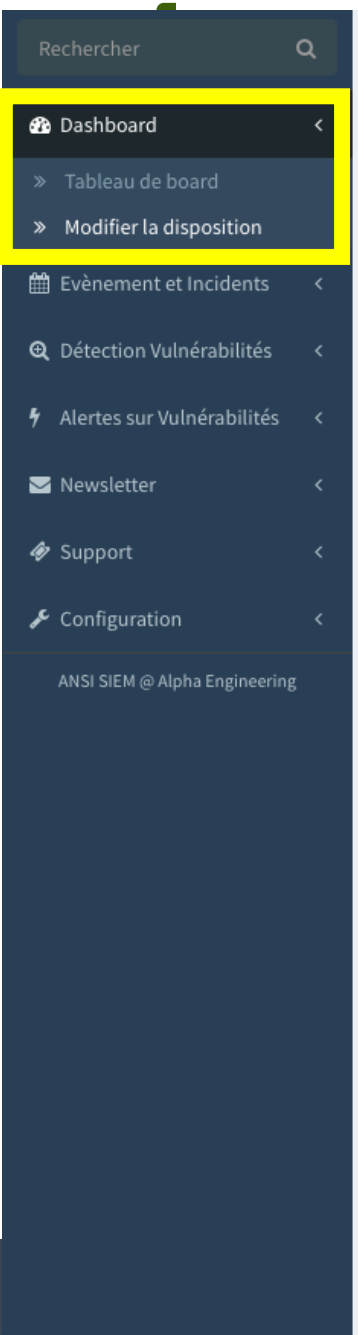


Widgets : Les Widgets présentent une vue globale sur les indicateurs clefs de la plateforme.

Graphes : Groupe de 10 graphes divisés sur deux colonnes et présentent des analyses des statistiques pour chaque module

Le module « Dashbord » affiche un tableau de bord global et permet à l'utilisateur de personnaliser l'ordre et les dashboards

2. Module Dashboard : Modifcation de la disposition



Le module « Dashbord » affiche un tableau de bord global et permet à l'utilisateur de personnaliser l'ordre et les dashboards affichés

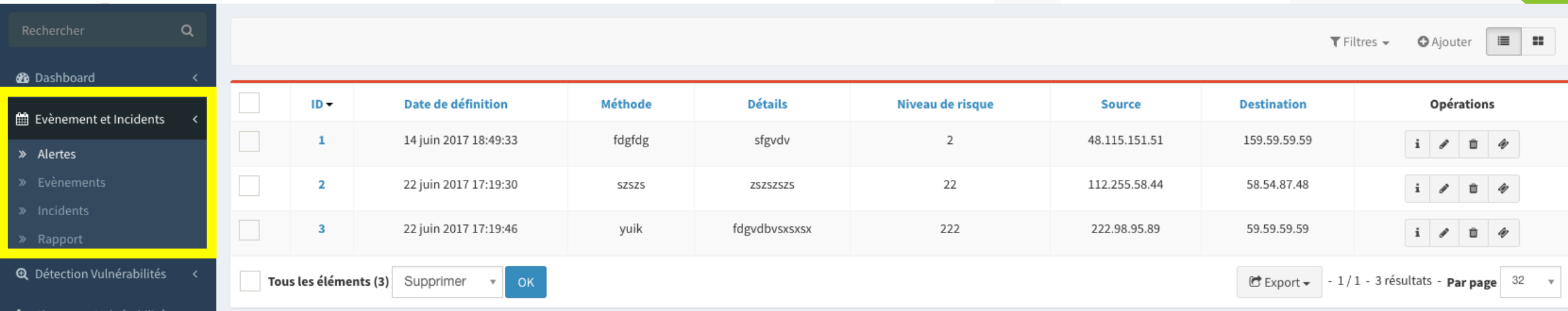
4 *Visite guidée*

3. Module Evènement et Incidents : Présentation

Le module « Evènements et Incidents » contient les sous modules :

- Alertes : Gérer et visualiser l'ensemble des alertes déclenchées relativement au périmètre supervisé par la plateforme.
- Evènements : Gérer et visualiser l'ensemble des évènements déclenchées.
- Incidents : Gérer et visualiser l'ensemble des incidents déclenchées.
- Rapport : Créer des rapports sur les alertes, évènements et incidents.

3. Module Evènement et Incidents : Présentation

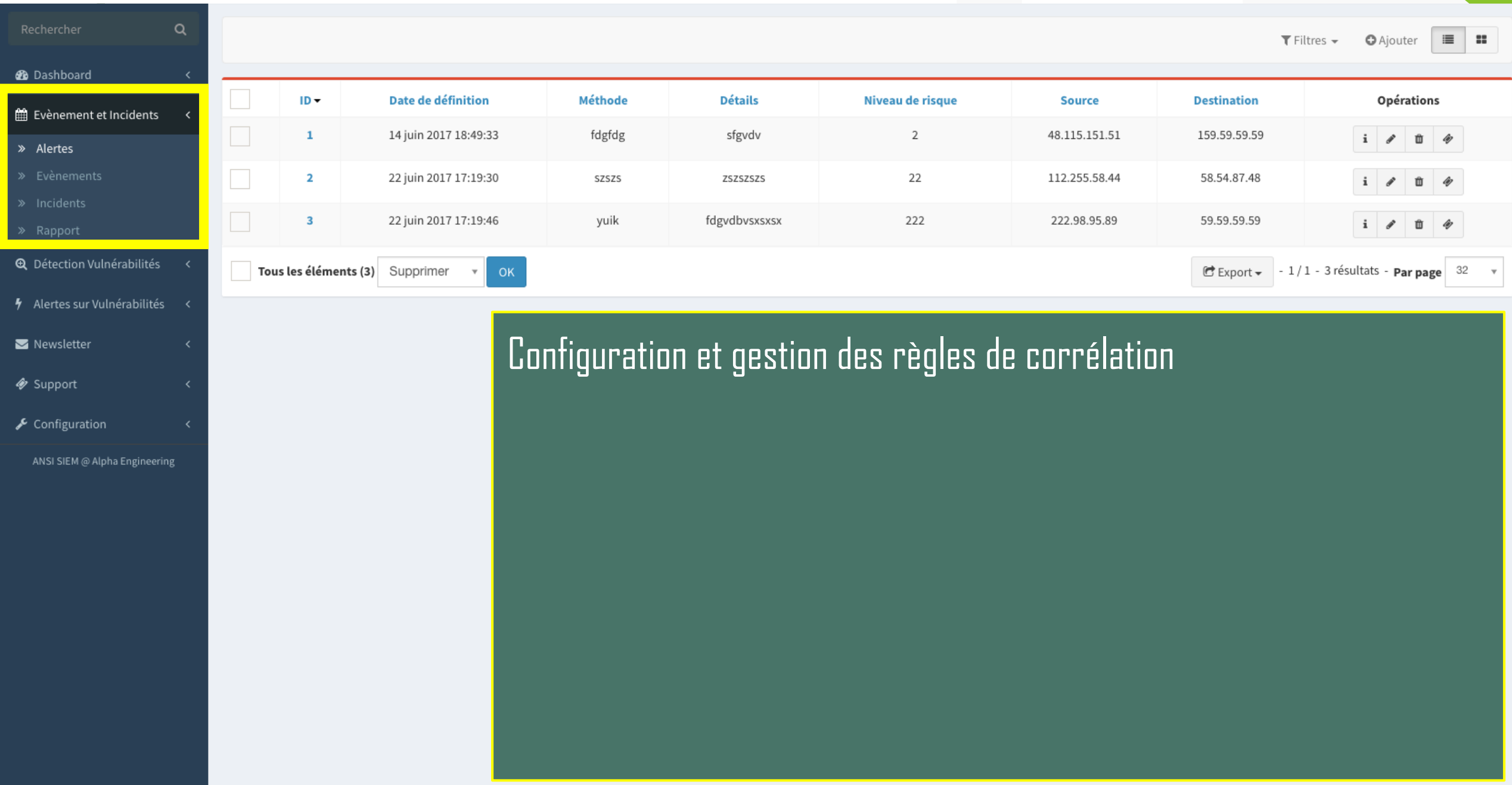


Ouverture possible de tickets par rapport à des Evt / Alertes

Le ticket peut être a destination du CERT local / CERT tier (paramètre de configuration)

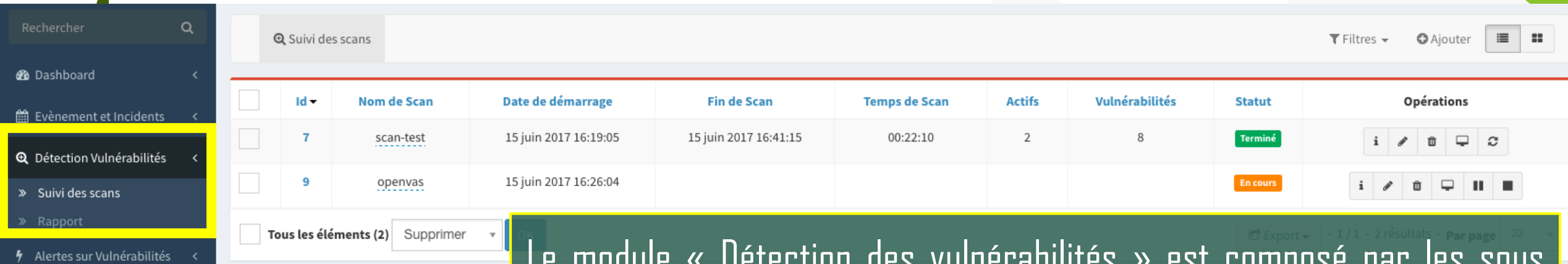
Permet d'envoyer donc des informations précises à un autre tier

3. Module Evènement et Incidents : Présentation



4 *Visite guidée*

4. Module Détection de vulnérabilités : Présentation



Le module « Détection des vulnérabilités » est composé par les sous modules :

- Planificateur de scan des vulnérabilités : Eviter impact sur le système en cours d'audit
- Rapports : La génération de rapports se base sur :

* Les informations déjà collectées au niveau du module

* Des bloc, à inclure au choix, contenant des sous ensemble de ces informations (tableaux / graphiques)

* Il est possible de personnaliser le rapport en fonction du choix des blocs d'informations à inclure.

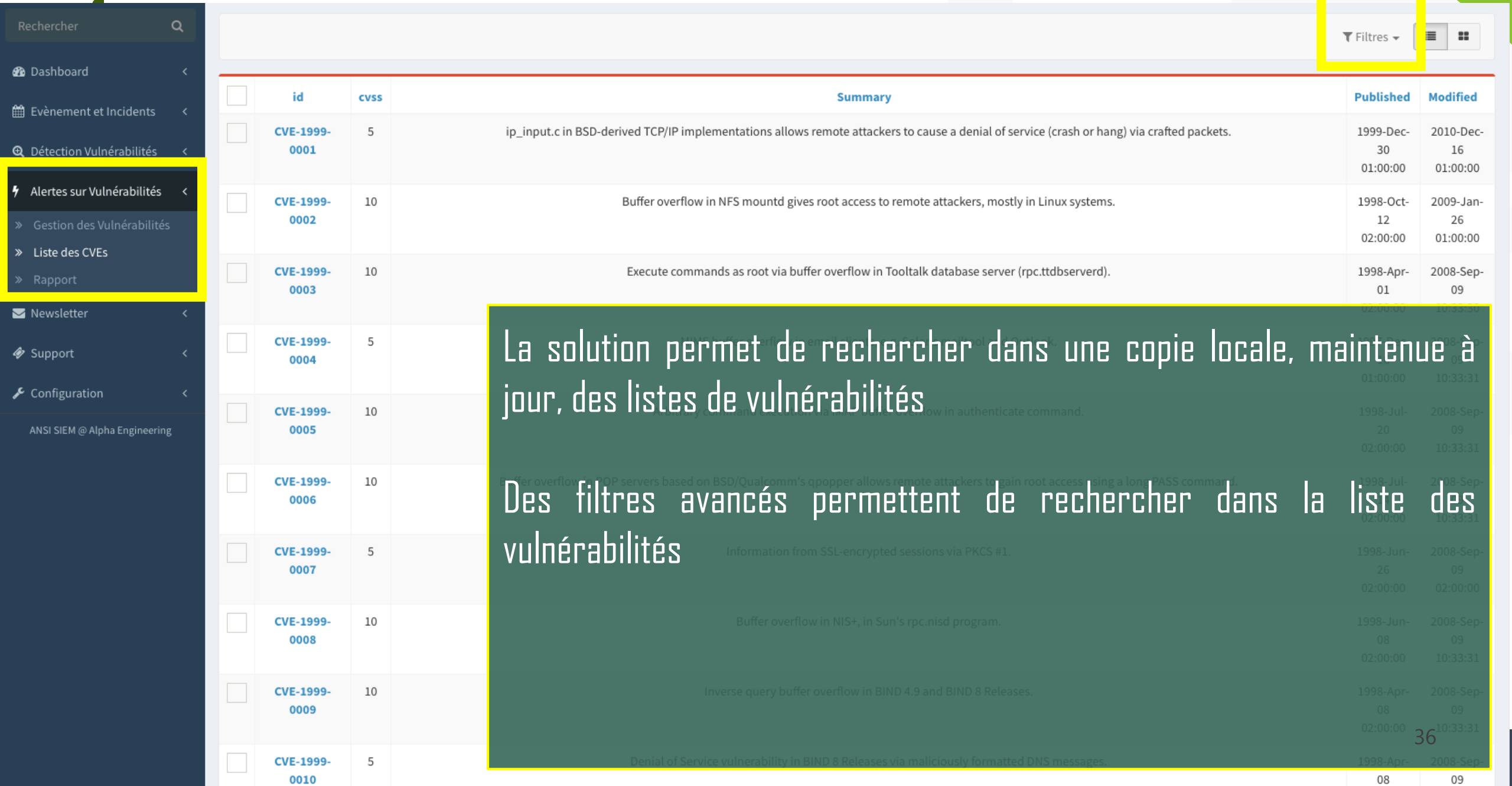
4 Visite guidée

5. Module Alertes sur les vulnérabilités : Présentation

Le module « Alerte sur les vulnérabilités » est composé par les sous modules :

- Gestion des Vulnérabilités : Gérer les vulnérabilités détectées depuis les scans
- Liste des CVEs : Lister les vulnérabilités (mise à jour automatique de la liste CVE et identification des actifs concernés)
- Rapports

5. Module Alertes sur les vulnérabilités : Liste CVE



La solution permet de rechercher dans une copie locale, maintenue à jour, des listes de vulnérabilités

Des filtres avancés permettent de rechercher dans la liste des vulnérabilités

4 *Visite guidée*

6. Module Newsletter : Présentation

Permettre l'envoi de newsletter de sensibilisation à des destinataires organisés en groupes

L'envoi se base sur des templates pré-préparées

Ajout de newsletter contenant le résultat de scan suite a la recommandation du comité de pilotage

Etapes de exploitation du module

1. Création d'un modèle (Template)

Peut contenir jusqu'à 10 clefs (Key) permettant de personnaliser le contenu de la newsletter

2. Création newsletter basée sur une Template

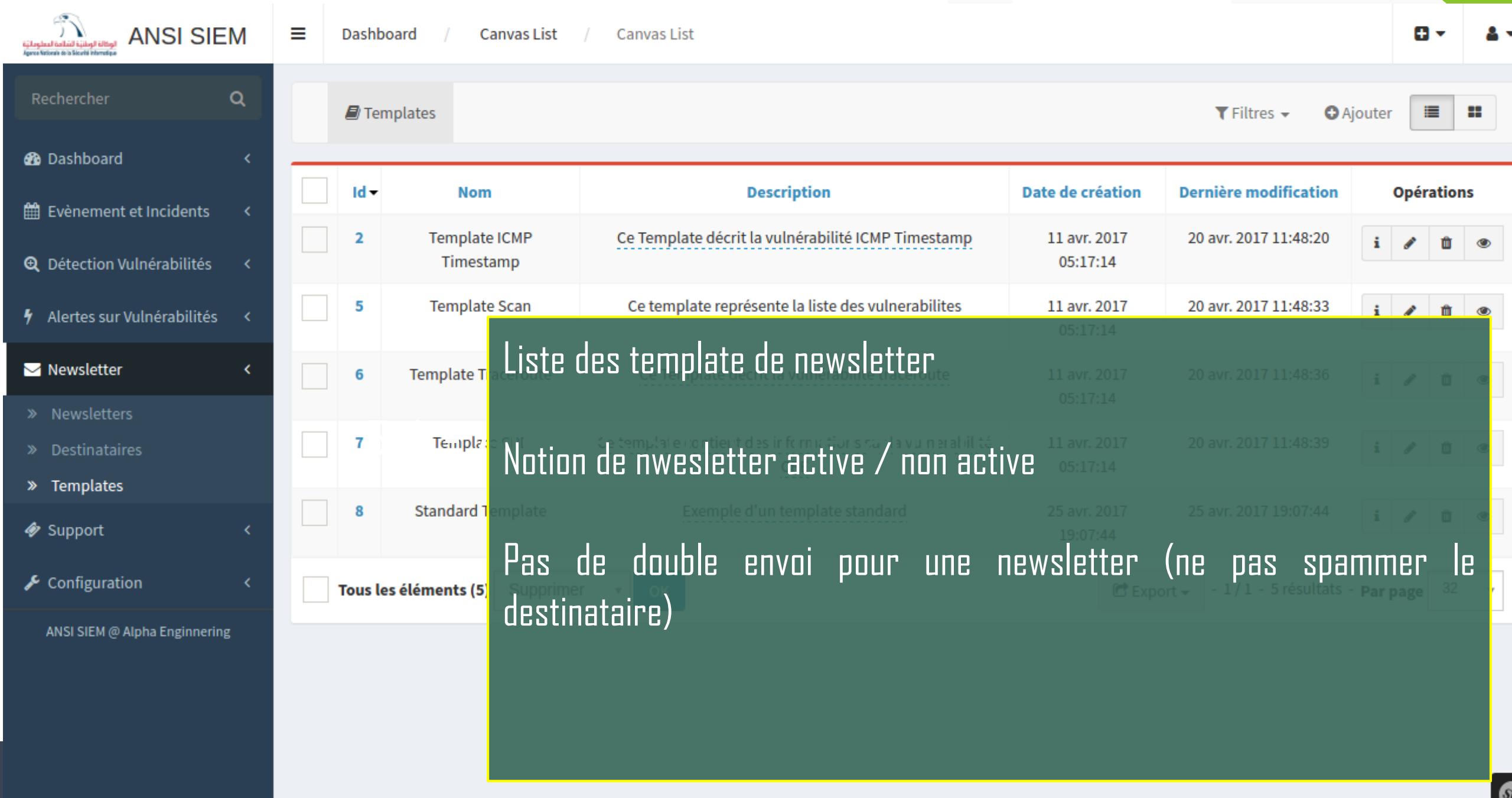
Donner une valeur aux clefs préparées dans le template

3. Sélection des destinataires / groupes de destinataires

Rubrique spécifique pour la gestion des destinataires

4. Envoi / Envoi planifié

Si la newsletter est active (validée)



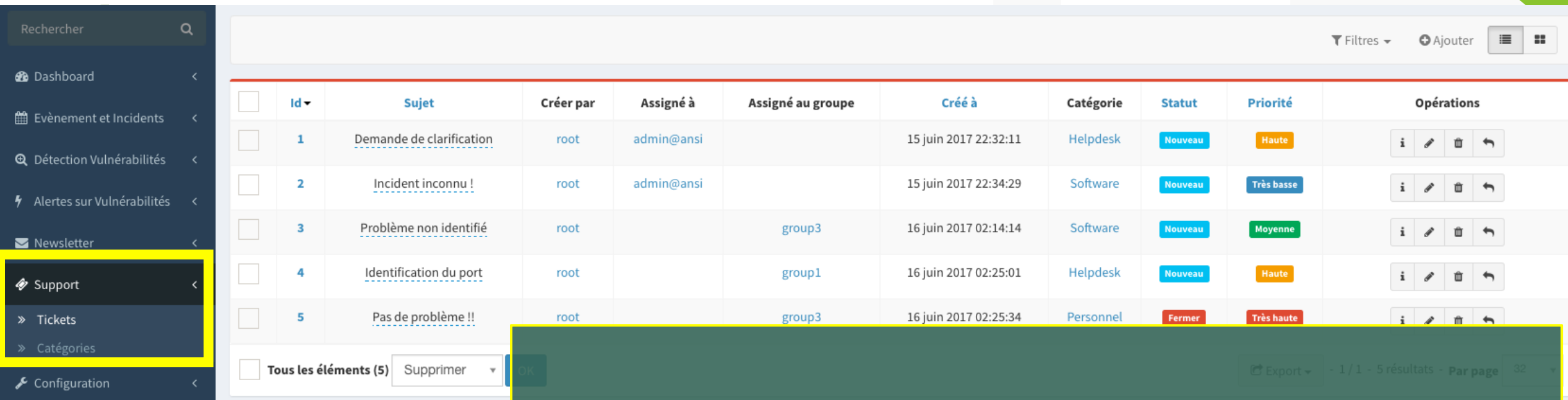
Liste des template de newsletter

Notion de nwesletter active / non active

Pas de double envoi pour une newsletter (ne pas spammer le destinataire)

4 Visite guidée

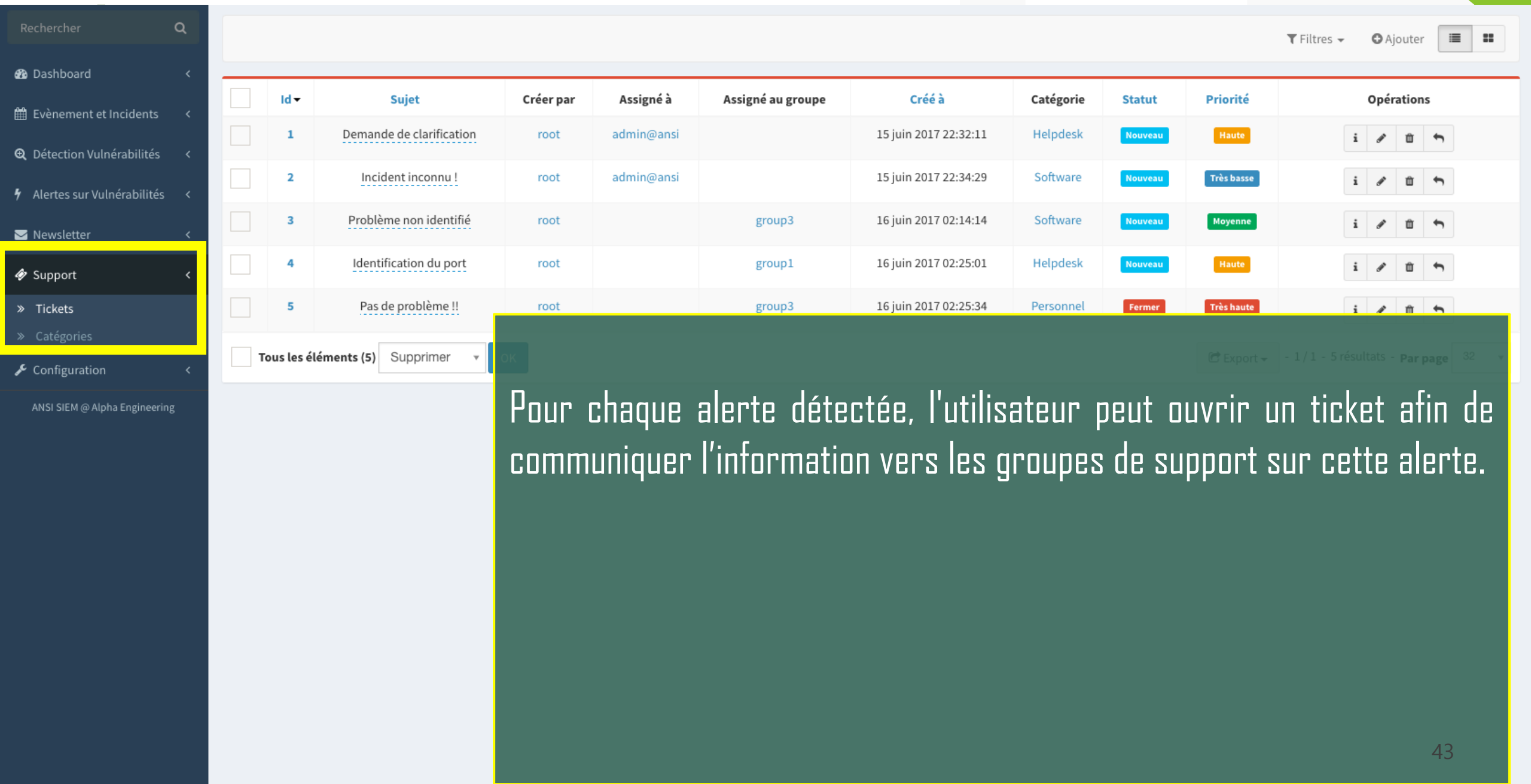
7. Module Support : Présentation



Le module « Support » est composé par les sous modules :

- Gestion des Tickets
  - Créer des tickets en sélectionnant des vulnérabilités / alertes
  - Gestion des commentaires sur les tickets
- Gestion des catégories
  - En accords avec les actifs / métier

7. Module Support : Présentation



Pour chaque alerte détectée, l'utilisateur peut ouvrir un ticket afin de communiquer l'information vers les groupes de support sur cette alerte.

TEAM WORK | WORK HARD

La clé de toute réussite

1 À propos de nous

2 Métier et sécurité

3 Solution SIEM

4 Visite guidée

5 Démo

6 Next Step

ENGINEERING

Vision : des missions d'analyse des stratégies de sécurité qui passe par un cercle vertueux du changement

A **Métier**

Analyse de votre métier, votre structure, vos produits **pour définir** vos enjeux stratégiques de sécurité

D **RH**

Mise en place d'une culture du **changement permanent** intégrant les enjeux de sécurité et de bonnes pratiques dans tous les processus RH

B **Processus**

Alignement de vos processus sur les enjeux de sécurité portés par votre métier

C **SI**

Transformation du SI sur 3 axes :

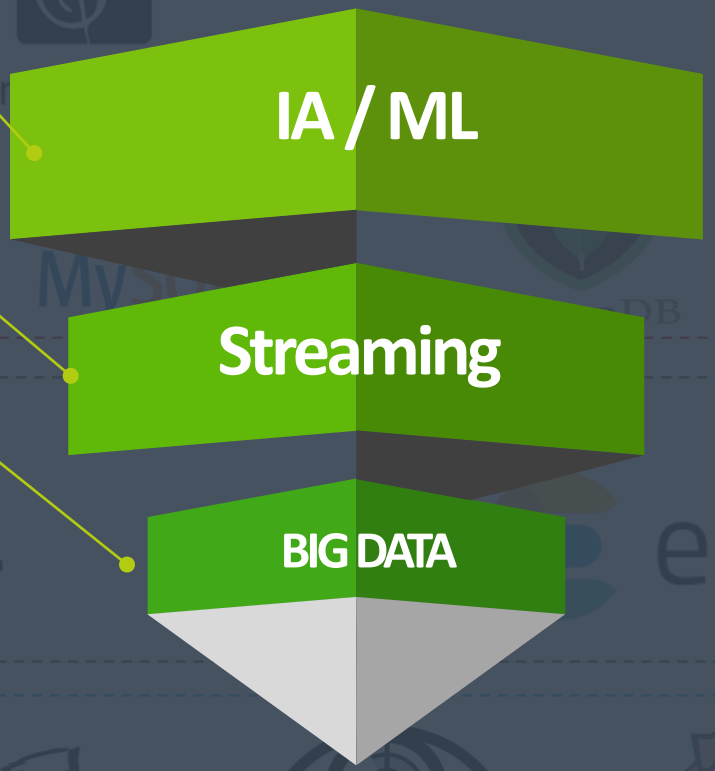
- Le SI lui-même doit répondre aux enjeux de sécurité
- Le SI doit intégrer les bon outils de sécurité
- Le SI doit intégrer les outils d'analyses, reporting et monitoring de la sécurité

Architecture de la solution SIEM

Int. Artificelle
Approches IA et ML pour faire face aux nouvelle menace

Streaming
Traitement des info à la volé

Big Data
Supporter un grand volume de'evenements



Accompagnement Métier
Adaptation des outils aux besoins sépcifiques du métier

ROSI
Indicateurs sur le retour d'investissement de sécurité

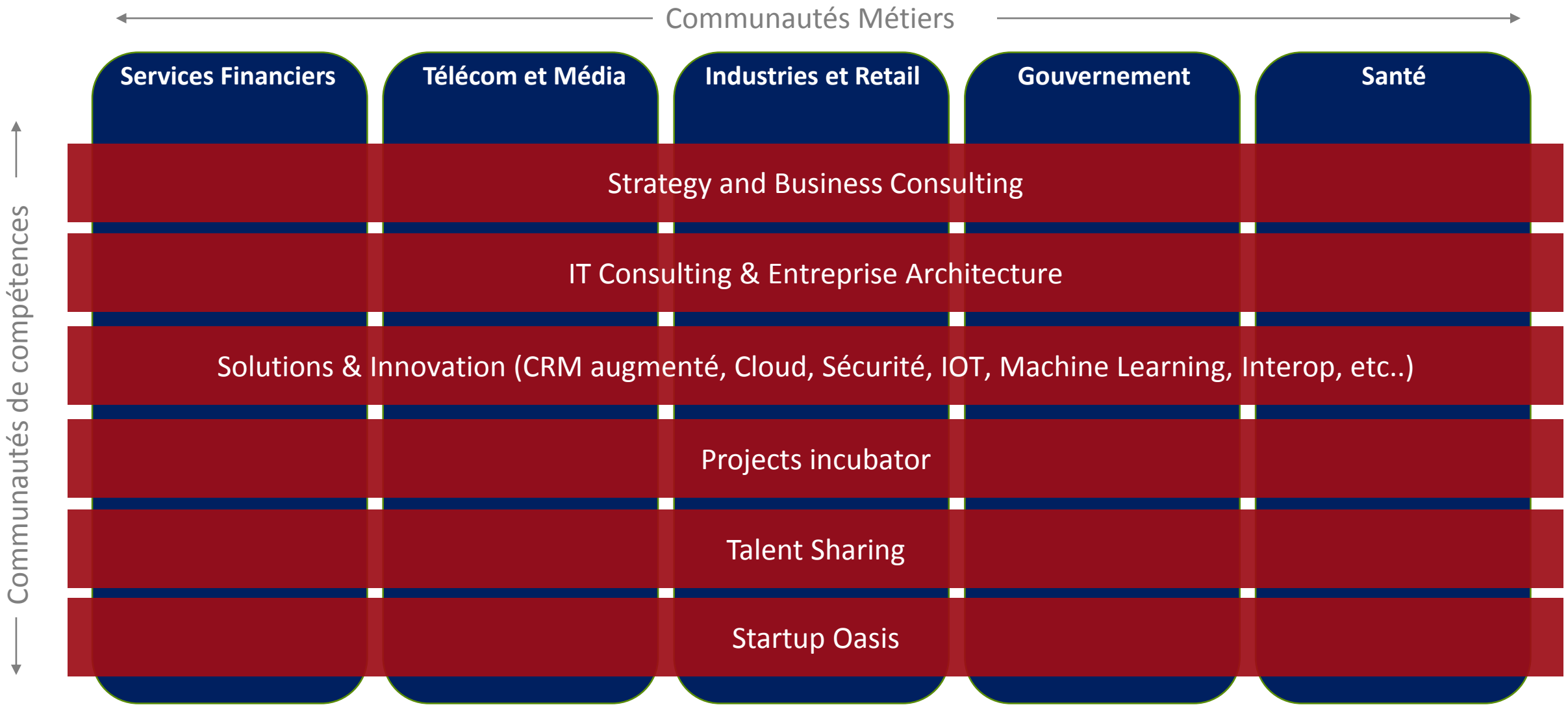
Processus métiers spécifques aux CERT
Collaboration entre CERT

Say hello to

enginov

enginov

- **enginov** une organisation innovante basée sur des communautés interconnectées:



ALPHA ENGINEERING

Capital Social: 1’000’000 TND

www.alpha-engineering.net

contact@alpha-engineering.net