Risques cyber industriel

De l'audit à la gestion des menaces, anticiper les menaces de type rançongiciels?

28/11/2023

Hicham BEN HASSINE

algosecure

KEEP IT SAFE AND SECURE

Société de conseil **Indépendante** et **spécialisée** en sécurité informatique depuis 2008

Un **accompagnement SSI** complet

- **Audit**
- **Conseil**
- **Formation**
- **Réponse à incidents (CERT)**

Des **certifications et qualifications** reconnues

VISA DE SÉCURITÉ

ISO 27001 BUREAU VERITAS Certification

Une implication dans la **communauté Cyber**

CAMPUS CYBER

HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY

MLSSI

Entreprise à missions

Sommaire

Introduction

Introduction

Corpus documentaires/normes

NIST SP 800-82

IEC 62443

Enjeux OT:

- Sûreté
- Disponibilité
- Performance et fiabilité

Enjeux IT:

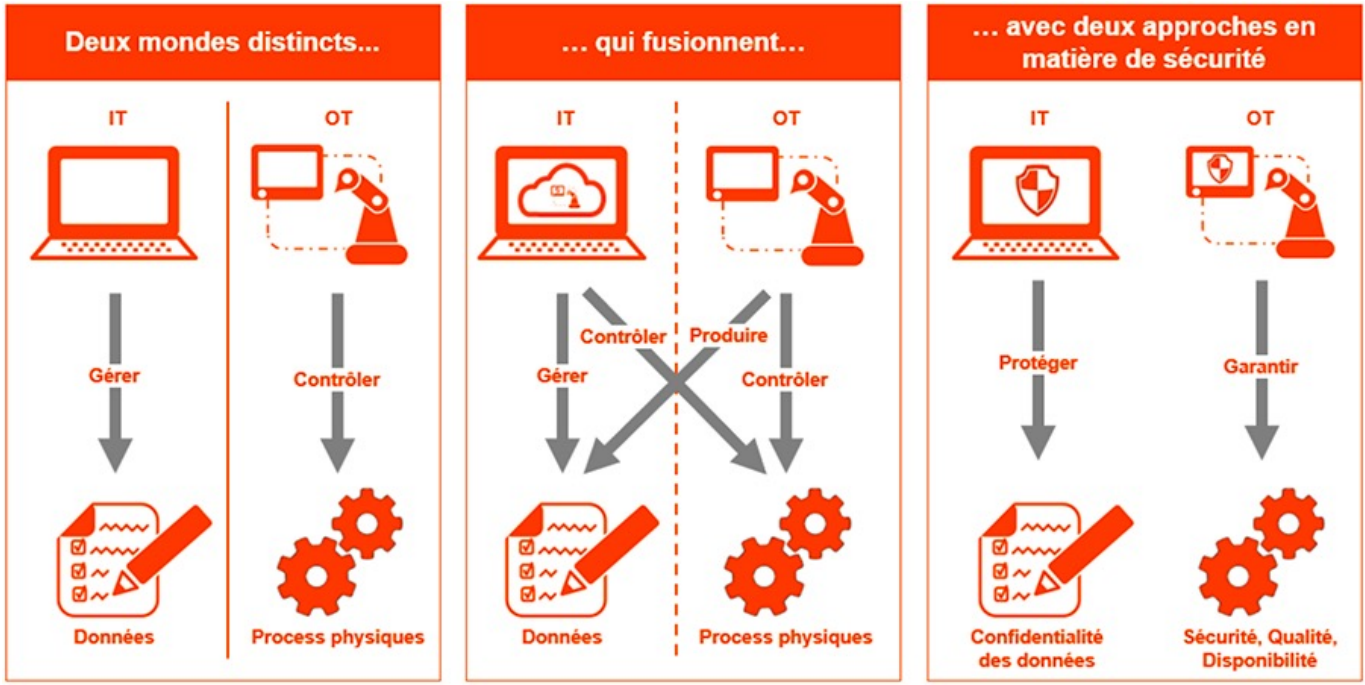
- Confidentialité
- Intégrité
- Disponibilité
- Preuve

Croyances sur la sécurité OT

- Les réseaux OT sont isolés
- Les réseaux OT ne sont pas accessibles depuis internet
- Utilisation de protocoles propriétaires donc sécurisés
- Les commandes depuis les IHM sont restreintes, impossible de les outrepasser
- Bonne implication de l'IT dans les réseaux et la sécurisation des réseaux OT

La réalité des systèmes industriels

- Vétusté des OS
- Sécurité By Design des équipements OT
- Gestion des comptes et mots de passe
- Structure des protocoles
- Manque de maitrise des réseaux
- Gestion et intervention des prestataires OT



Retex

Constats

- Le « legacy technique » est difficile à gérer !
- La problématique SSI dans le contexte industriel est multiple !
- Les équipes Cybersécurité sont surchargées (quand elles existent)
- La production ne doit jamais s'arrêter !
- Si un attaquant est à l'intérieur du SI, vous êtes dans **une situation critique!**

- Il s'agit d'un **challenge** technique et humain
- Il faut **limiter les surfaces d'attaques** (notamment externes)
- Paradigme: « **assume Breach** »

Retex Audit

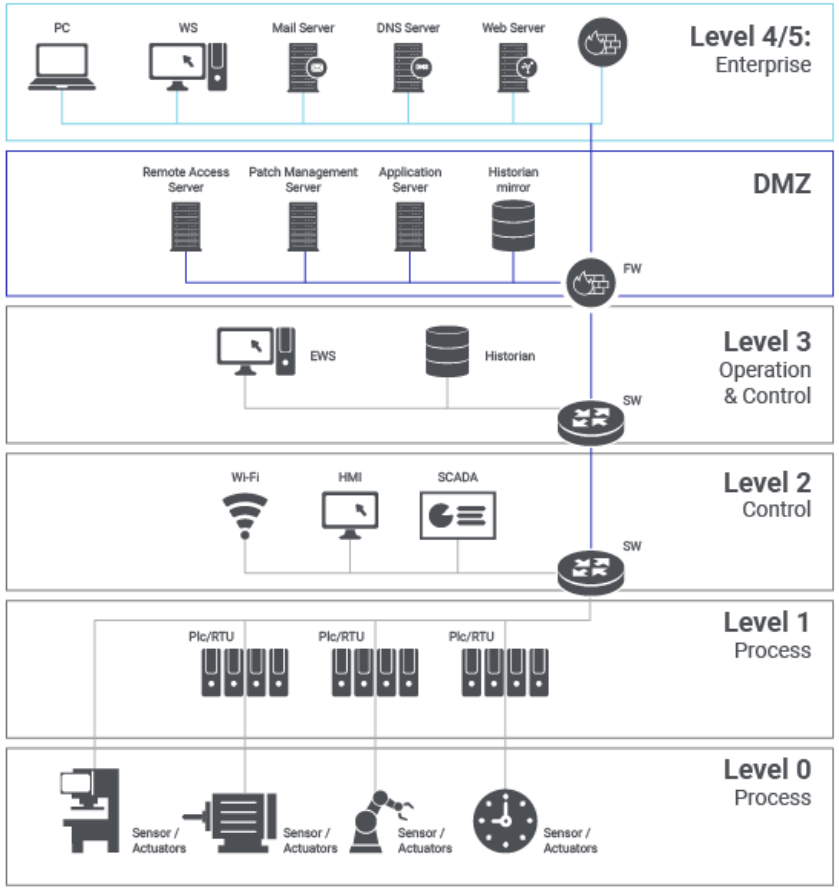
Retours d’expérience

- **100%** des audits ont révélé des failles majeures ou critiques
- Compromission de l’entreprise pour rebondir sur le SI industriel
- Compromission via l’externe sur des périphériques non maitrisés (caméras de surveillance…)
- Compromission via des solutions de télémaintenance maison

Recommandations

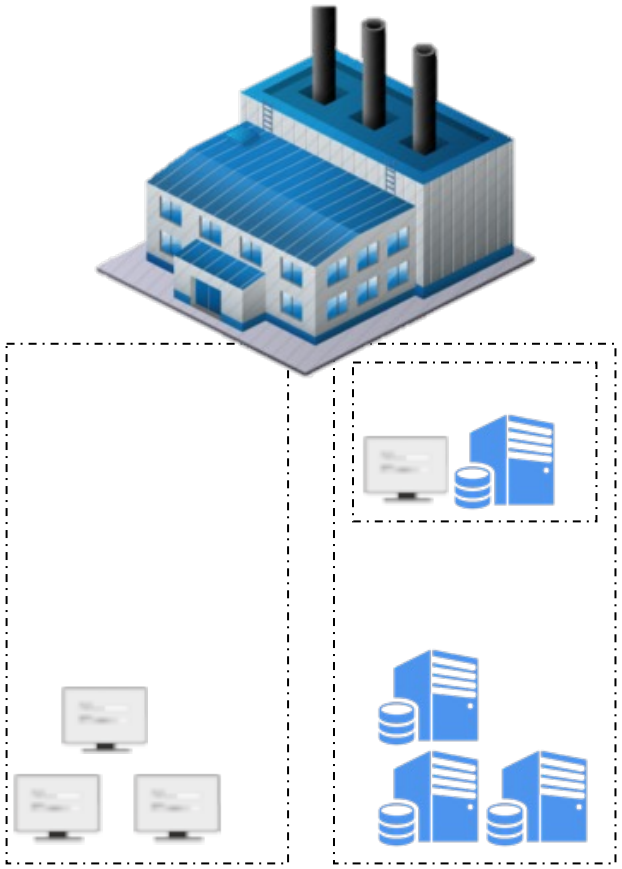
Maitrise de son SI

Audit et maitrise (Model PURDUE)



- Identification des risques
- Retrouver une maitrise (OS, réseau)
- Inventaire précis
- Cloisonnement par zone
- Processus de gestion d'incident

Recommandations pour l'intérieur du SI



Segmentation

Restriction des services

Filtrage IP / Port

Principe de moindre privilège

Architecture 3 tiers

Audit des **permissions**

Contrôle du parc

Maintien à jour

Élimination des solutions obsolètes ou **durcissement des OS**

Exigences pour les prestataires et contrôles (PAS)

Auditer son S.I. : pentests, configuration…

Réaliser les **sauvegardes**

Mot de passe

Politique de mot de passe

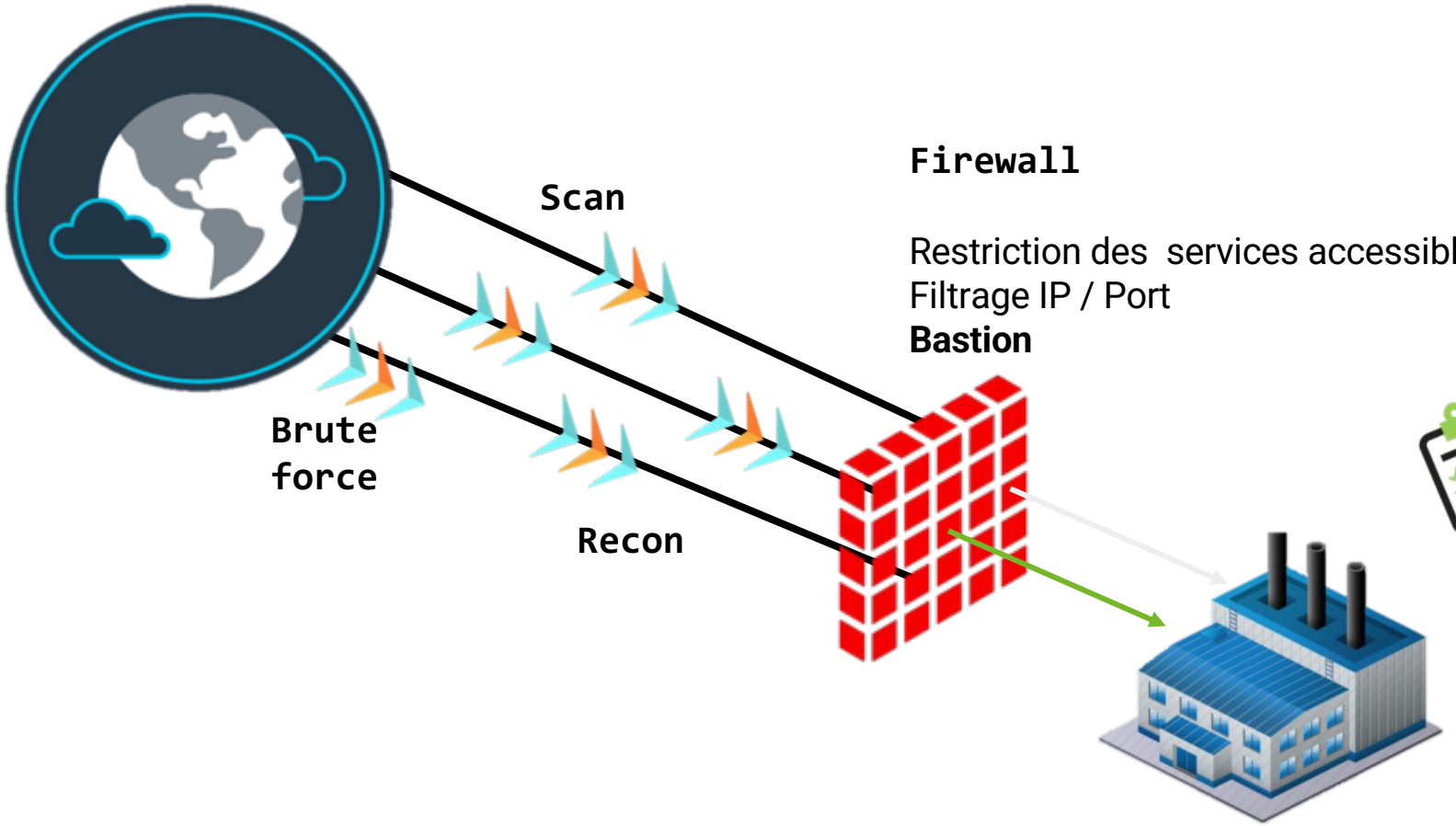
Auditer les endroits pouvant contenir des mots de passe mal sécurisés

Sensibilisation du personnel

Recommandations pour la surface externe de son SI

2FA

VPN
Mails
Services sensibles



Firewall

Restriction des services accessibles
Filtrage IP / Port
Bastion

Contrôle du parc exposé

Nom
Version
Vulnérabilité

Solutions pour la surface externe

Contexte de la cybercriminalité

- RaaS
- Info Stealer
- Network Access Brokers

- Ex: le groupe DarkSide

- Phishing
- Exploitation d’une vulnérabilité externe
- Compromission d’un compte utilisateur

Le mécanisme

Votre périmètre externe à surveiller

Outils de scans, de veille, d'OSINT, de Threat Intel, typosquatting

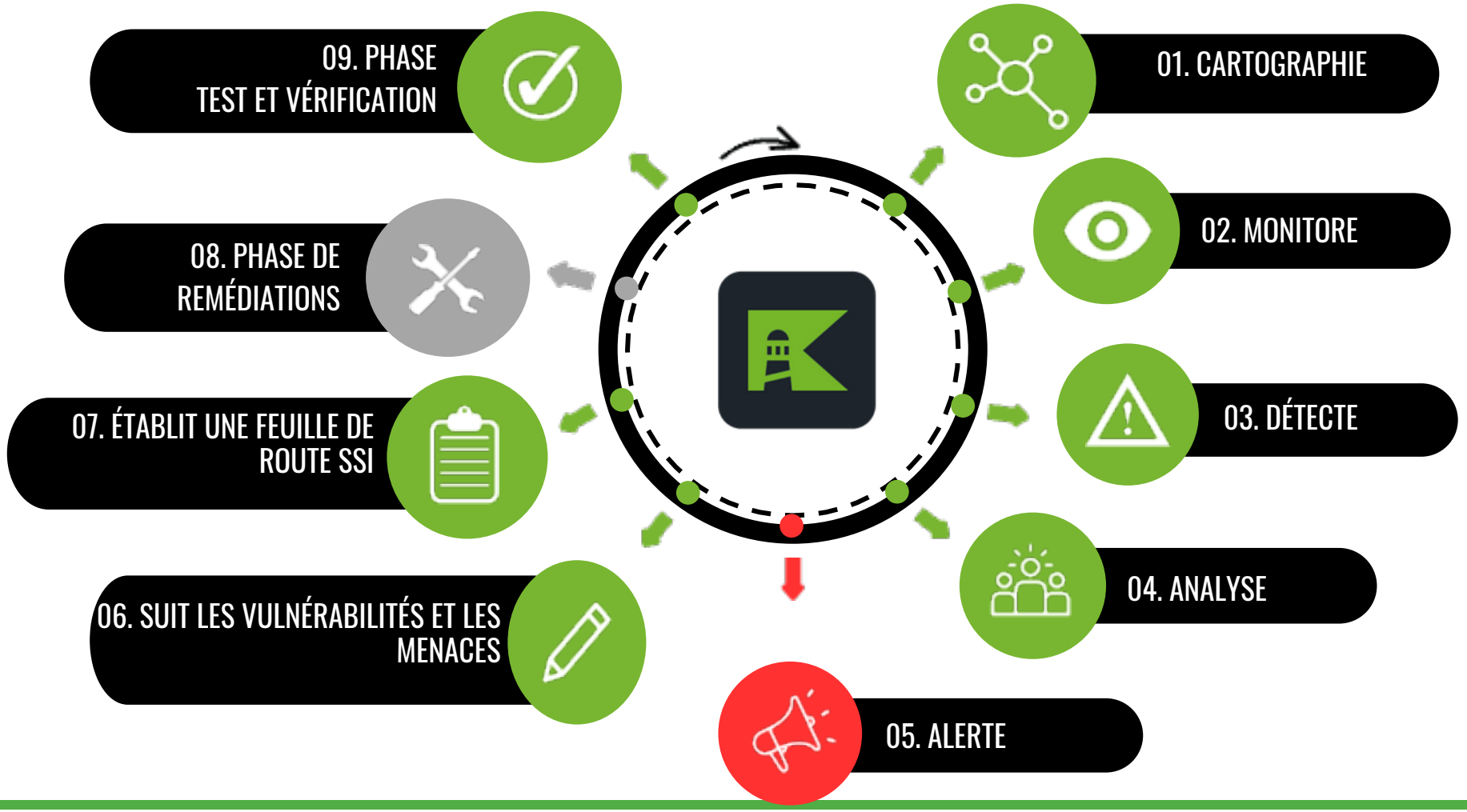
Une plateforme Saas avec tableau de bord

Des compétences offensives et forensiques

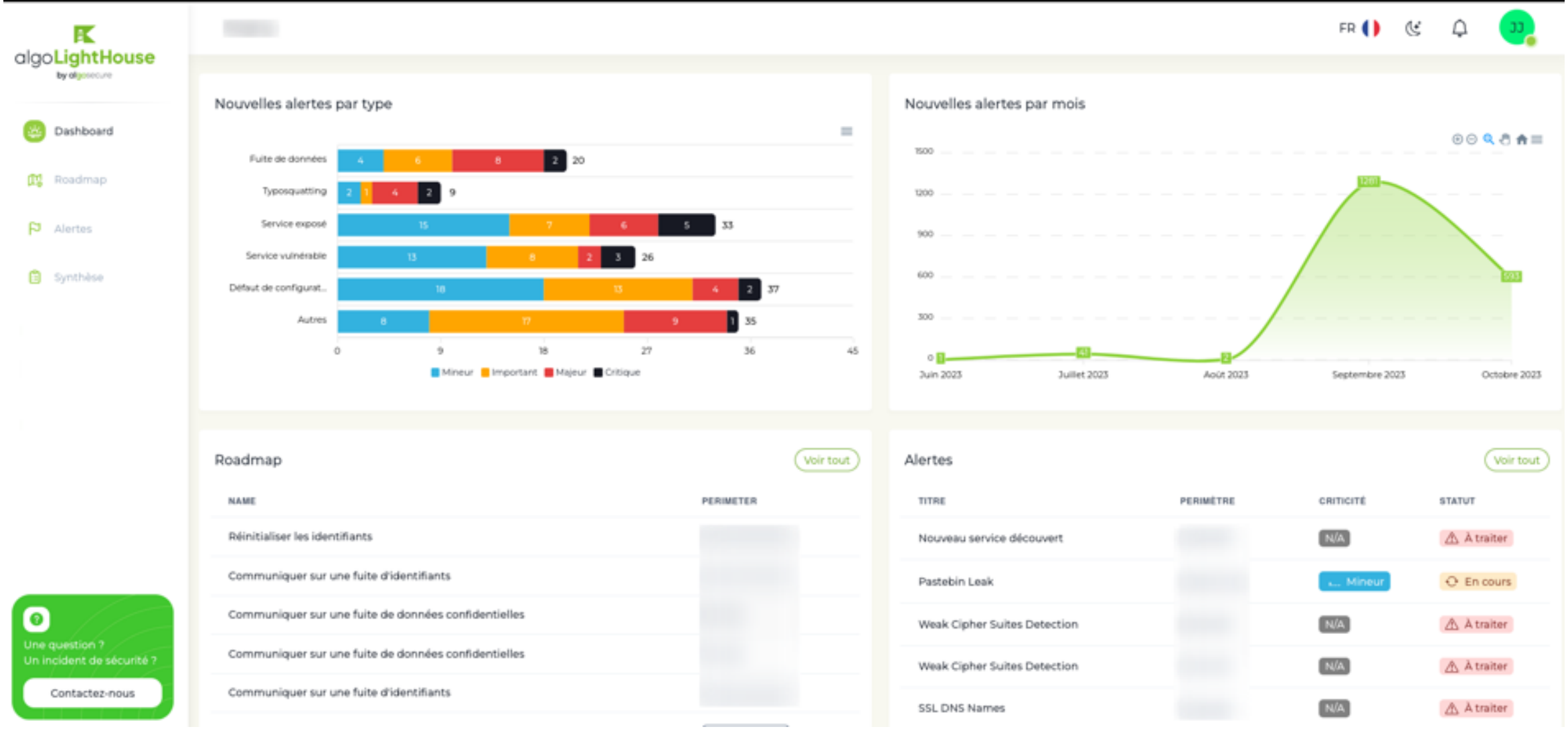
algoLightHouse

Notre approche

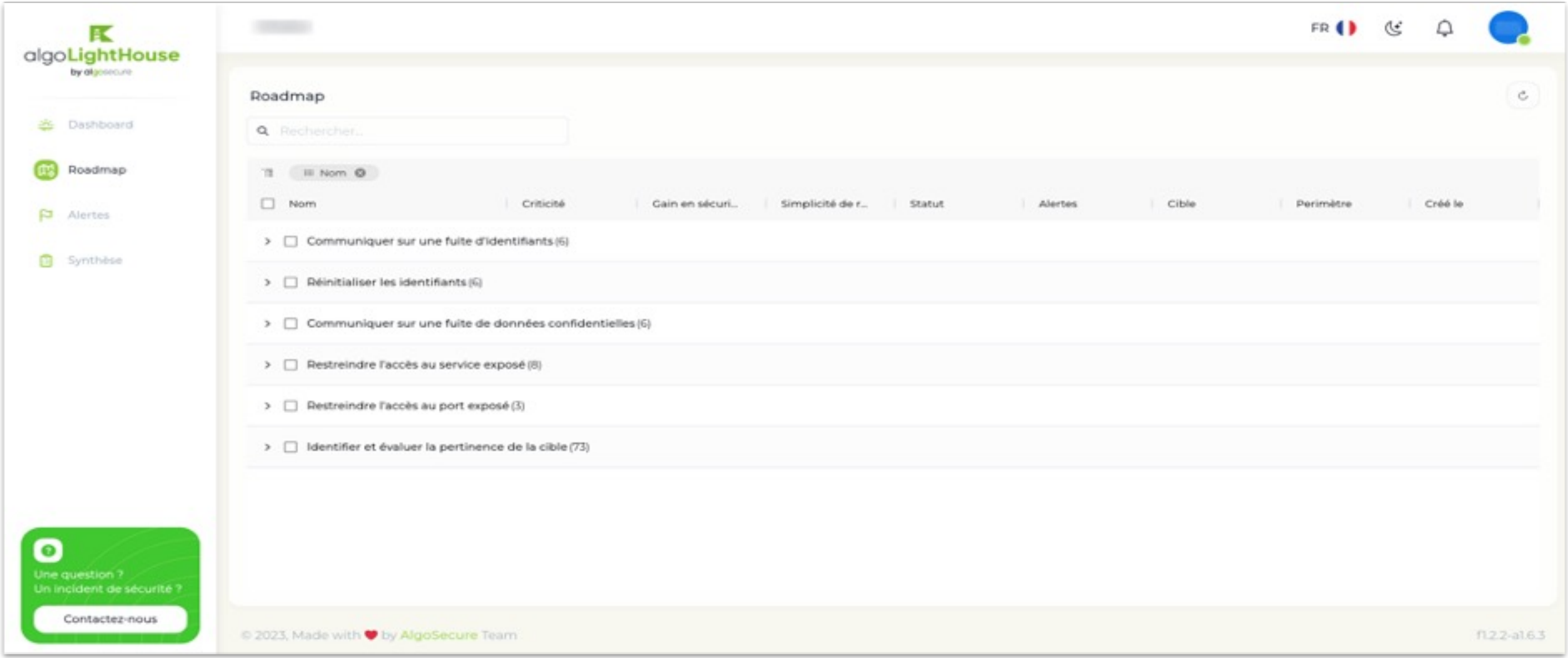
algoLightHouse



Dashboard


algoLightHouse
by algosecure
Dashboard
Roadmap
Alertes
Synthèse
FR
JJ
Nouvelles alertes par type
Fuite de données
Typosquatting
Service exposé
Service vulnérable
Défaut de configurat...
Autres
20
9
33
26
37
35
0
9
18
27
36
45
Mineur
Important
Majeur
Critique
Nouvelles alertes par mois
1500
1200
900
600
300
0
Juin 2023
Juillet 2023
Août 2023
Septembre 2023
Octobre 2023
Roadmap
Voir tout
NAME
PERIMETER
Réinitialiser les identifiants
Communiquer sur une fuite d'identifiants
Communiquer sur une fuite de données confidentielles
Communiquer sur une fuite de données confidentielles
Communiquer sur une fuite d'identifiants
Alertes
Voir tout
TITRE
PERIMÈTRE
CRITICITÉ
STATUT
Nouveau service découvert
N/A
À traiter
Pastebin Leak
Mineur
En cours
Weak Cipher Suites Detection
N/A
À traiter
Weak Cipher Suites Detection
N/A
À traiter
SSL DNS Names
N/A
À traiter
Une question ?
Un incident de sécurité ?
Contactez-nous

Vue Roadmap SSI



Synthèse

- Audit Externe et OSINT Continu : Surveillance en continu des actifs et des menaces, en utilisant de l'audit externe, de l'OSINT (Open Source Intelligence) et de la Threat Intelligence.

- Remontée Qualifiée et Actions de Remédiation : Vérification de chaque élément suspect par un analyste, avec priorisation et suivi des actions de remédiation

Il vaut mieux prévenir que guérir !

algosecure
KEEP IT SAFE AND SECURE

Hicham BEN HASSINE

Directeur technique
hicham@algosecure.fr
+33(0) 6 20 23 39 74

ALGOSECURE.FR

KEEP IT SAFE AND SECURE KEEP IT SAFE AND SECURE KEEP IT SAFE AND SECURE KEEP IT SAFE AND SECURE KEEP IT SAFE AND SECURE KEEP IT SAFE AND SECURE