heliaq
Solutions

# CYBERSÉCURITÉ : CE QUE VOS HACKERS SAVENT DÉJÀ... ET QUE VOUS IGNOREZ ENCORE

Audit cybersécurité : identifiez vos failles avant les attaquants.

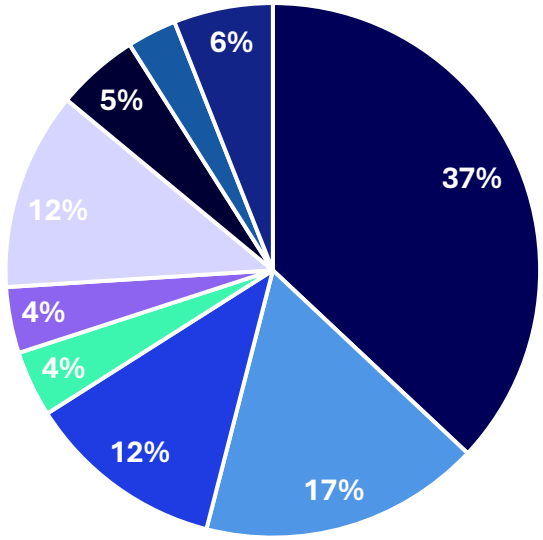
# 1

# Contexte de la menace

heliaq
Solutions

# Panorama de la cybermenace 2024

## Répartition des victimes d'attaques par le biais de rançongiciels




- PME/TPE/ETI
- Entreprise stratégique
- Association
- EPA, EPIC (1)
- Autre
- Collectivité territoriale/locale
- Etablissement de santé
- Etablissement d'enseignement supérieur
- Ministère

(1) Établissement public administratif / industriel et commercial

**3,8M€**

Le coût moyen d'une violation de données pour une entreprise en France (perte de productivité, réparation des systèmes, impacts réputationnels)

**93%**

Des actions malveillantes répertoriées en 2025 reposent sur seulement dix techniques principales. Parmi elles, l'exfiltration de données chiffrées et l'injection de processus furtifs

**86%**

Des incidents et signalements transmis à l'ANSSI entre janvier 2022/décembre 2023 dans le secteur de la santé concernaient des établissements de santé

**47%**

Des données professionnelles hébergées sur le cloud peuvent être considérées comme sensibles

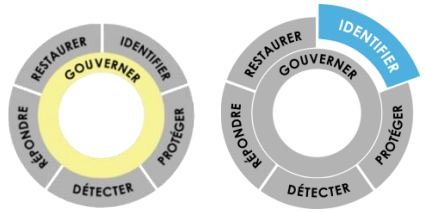
***Sources :***
*Panorama de la cybermenace 2024- ANSSI*
*CERTFR-2024-CTI-010 – Secteur de la Santé*
*CERTFR-2025-CTI-001 – Cloud Computing*

# 2

# Vocabulaire

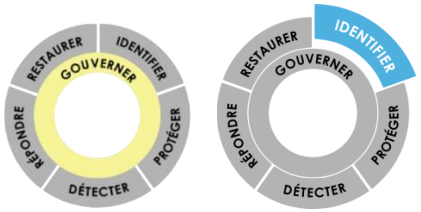
heliaq
Solutions

# Vocabulaire


- Vulnérabilité : point faible d'une ressource susceptible d'être exploité par une menace
- Mesure de sécurité ou remédiation : action(s) apportée(s) afin de résoudre ou limiter l'impact d'une vulnérabilité
- Gouvernance SSI : définition des objectifs, des moyens et de l'organisation de la sécurité des systèmes d'information
- Test d'intrusion : cartographier un périmètre cible, détecter les vulnérabilités présentes et tenter de les exploiter afin d'évaluer le risque et les remédiations associés
- Boite noire : scénario de test d'intrusion sans aucune information sur la cible
- Boite grise : scénario de test d'intrusion avec un identifiant sans privilège sur la cible

# Vocabulaire





- Surface d'attaque externe : les actifs d'une organisation visibles depuis Internet
- OSINT : Open Source Intelligence, recherche et analyse de données d'une organisation accessibles publiquement
- Référentiel : ensemble de recommandations, de bonnes pratiques ou d'exigences
- IEC/ISO 27001 : norme internationale de sécurité de l'information qui définit des exigences selon 15 capacités opérationnelles et 93 points de contrôle
- Heliaq CyberBox : Appliance virtuelle ou physique packagée et maintenue par Heliaq, nécessaire pour les collectes d'audit technique sur un périmètre interne

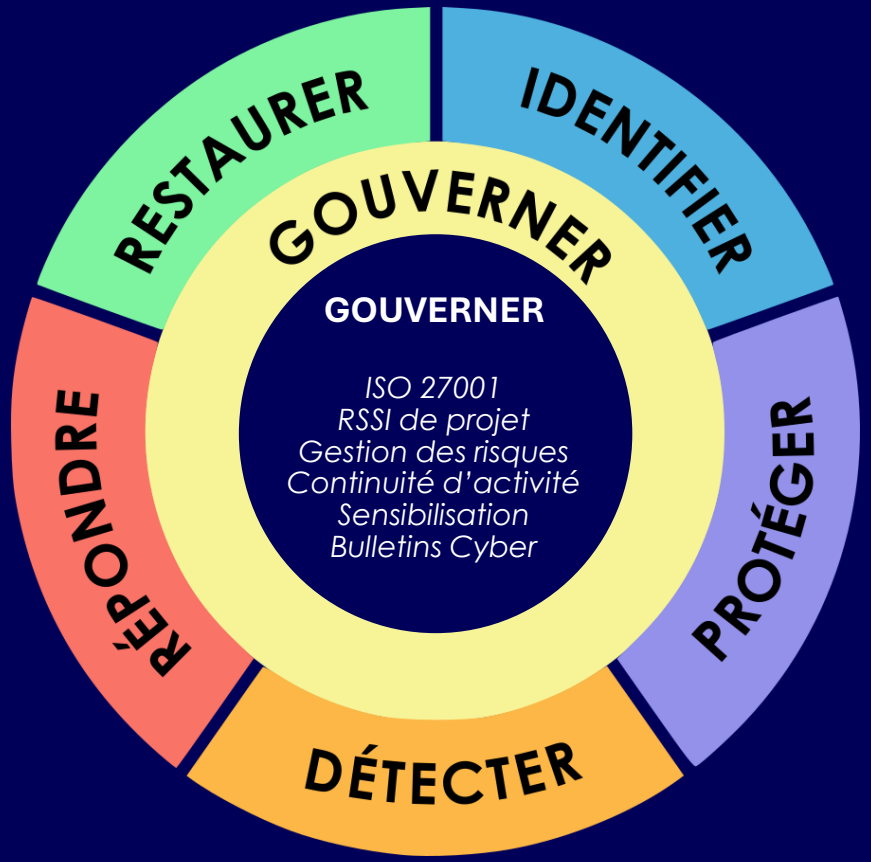
# 3

# Notre démarche

heliaq
Solutions

# Notre démarche maîtrisée pour une protection 360°

Basée sur le référentiel NIST (National Institute of Standards and Technology)  CSF v2.0




**RESTAURER**

*Backup aaS*
*Disaster Recovery aaS*

**IDENTIFIER**

*Audit d'exposition*
*Tests d'intrusion*
*Audit de configuration*
*Audit d'architecture*
*Audit de code*
*Audit Dark web*
*Audit organisationnel*

**RÉPONDRE**

*CyberRescue*

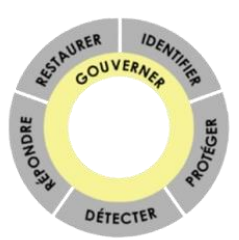
**PROTÉGER**

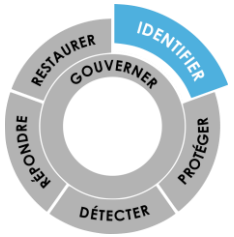
*Mode projet et as a service*
*Périmètres on premise/Cloud*

**DÉTECTER**

*SOC*

# Nos objectifs



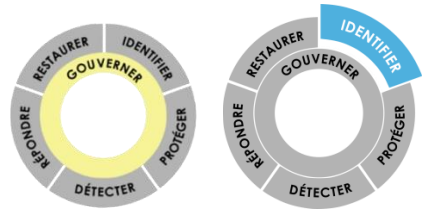

- Evaluer la **posture** de sécurité du système d'information de l'entité auditée au travers de deux piliers :
  - ✓ Les audits techniques
  - ✓ La gouvernance SSI
- Définir une vision globale de la maturité SSI d'une organisation permettant de cartographier ses risques Cyber.
- Accompagner nos clients au **renforcement de leur cyberfiabilité** via différentes missions comme :
  - ✓ des tests d'intrusions
  - ✓ des ateliers de cellule de crise
  - ✓ des audits d'écart à la norme ISO 27001
  - ✓ des analyses de risque
- Suivre sur la durée les risques Cyber de nos clients via des missions d'audit technique et de gouvernance.

# 4

# Notre offre AuditsCyber+

heliaq
Solutions

# Chiffres clés




**6** **Audits techniques**

LE + : Un suivi de la qualité des mécanismes techniques de défense

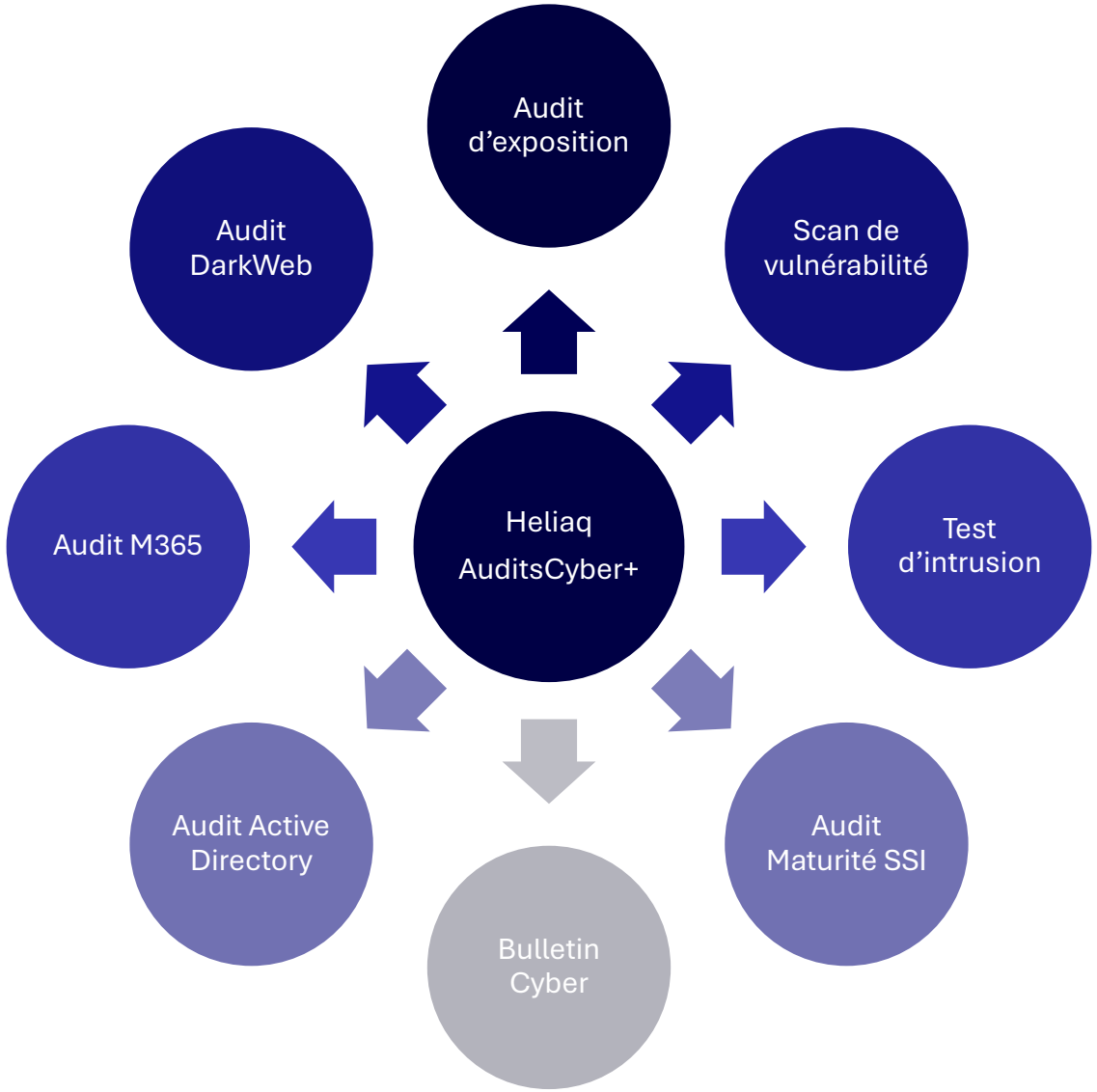
**2** **Accompagnements gouvernance**

LE + : Un suivi régulier augmentant la maturité Cyber

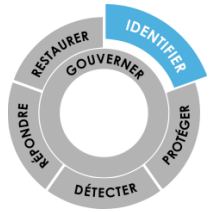
**3** **Packages**

LE + : Des missions complémentaires

# L’offre AuditsCyber+



# Audits techniques




## Audit d'exposition

Via une découverte OSINT, cet audit permet d'énumérer votre surface d'attaque visible depuis l'extérieur et fournit une cartographie des empreintes applicatives

Livrable : rapport d'exposition de la surface d'attaque externe
Restitution des résultats

Fréquence trimestrielle

## Scan de vulnérabilités

Cet audit permet de cartographier les vulnérabilités du périmètre choisi. Périmètre externe ou interne (1).

Livrable : cartographie des vulnérabilités et proposition de remédiations
Restitution des résultats

Fréquence trimestrielle

## Test d'intrusion

Tester les mécanismes de défense en exploitant les vulnérabilités découvertes sur le périmètre choisi. Scénario test externe en boite noire et test interne en boite grise (1).

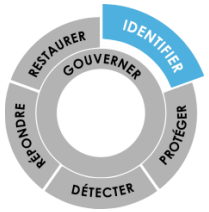
Livrable : rapport d'audit incluant preuves d'intrusion et proposition de remédiations
Restitution des résultats

Fréquence annuelle

Suivi des risques Cyber via des collectes et analyses récurrentes

(1) Une collecte sur un périmètre interne nécessite une instance Heliaq CyberBox

# Audits techniques




## Audit Active Directory

Audit de configuration pour vérification de conformité de la sécurité de l'annuaire. (1)

Référentiel : ANSSI

Livrable : rapport de conformité et mesures de sécurité
Restitution des résultats

Fréquence semestrielle

## Audit Microsoft 365

Audit de configuration pour vérification de conformité de la sécurité du Tenant.

Référentiel : CIS Benchmark

Livrable : rapport de conformité et mesures de sécurité
Restitution des résultats

Fréquence semestrielle

## Audit Dark Web

Analyse des informations potentiellement présentes sur le DarkWeb : détection d'éventuelles fuite de données, d'éventuelles compromissions de données.

Livrable : rapport d'audit DarkWeb
Restitution des résultats

Fréquence semestrielle

Suivi des risques Cyber via des collectes et analyses récurrentes
(1) Une collecte sur un périmètre interne nécessite une instance Heliaq CyberBox

# Accompagnement gouvernance


## Maturité SSI

Cet audit déclaratif d'écart à la norme ISO 27001 permet d'évaluer votre maturité SSI au travers de sessions d'interviews.
Nos auditeurs collectent les informations s'appuyant sur les 15 thématiques référant à environ 250 de points de contrôle.

Fréquence annuelle

## Bulletin Cyber

Consolidation de multiples sources d'alertes selon les produits sélectionnés, suivi des vulnérabilités avec score CVSS criticité élevée ou critique.

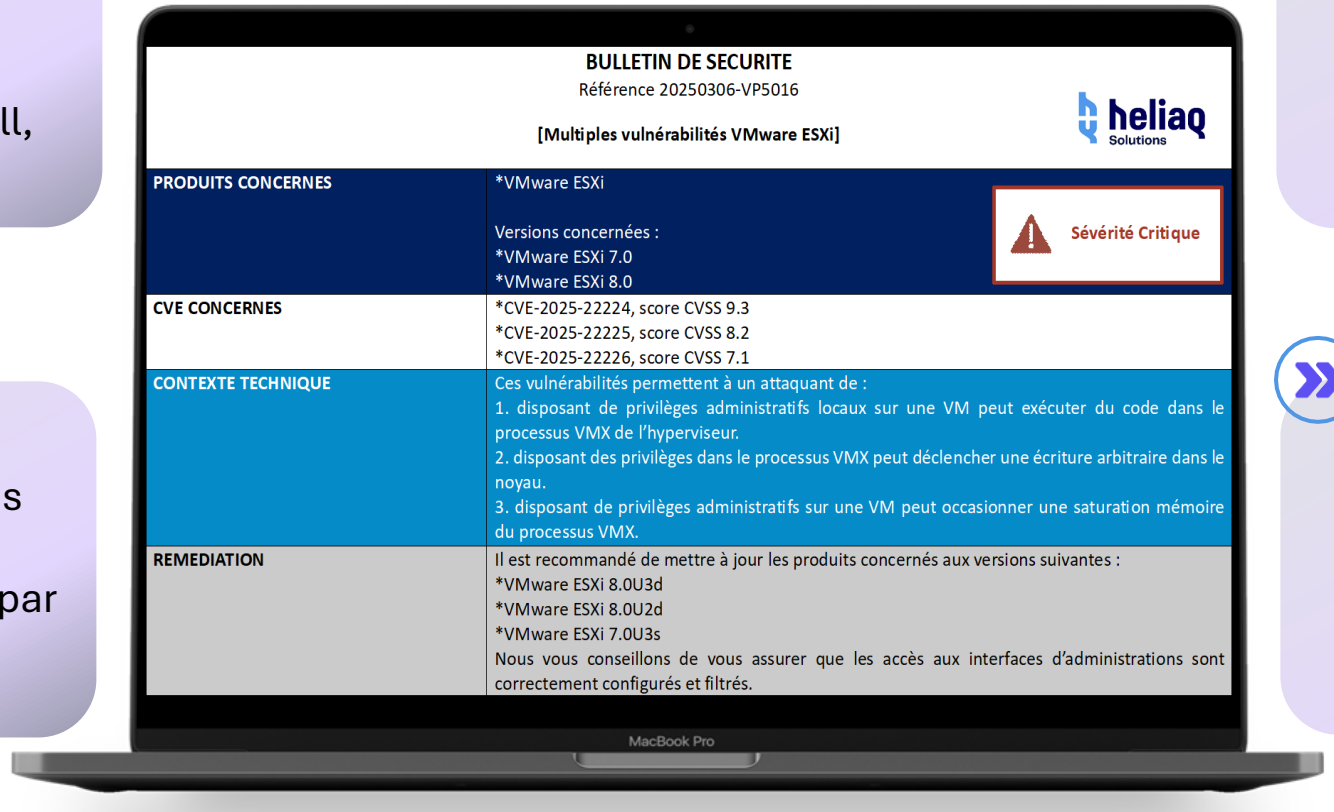
5 familles inclues par défaut : Windows Workstation, Windows Server, Linux RedHat, Linux Ubuntu, Linux Debian

Envoi lors publication CVE

# Bulletin Cyber

Sélection parmi des familles de produits
Windows, Linux, SGBD, serveur Web, CMS, Firewall, VPN/SSL, switch, Wifi, ...

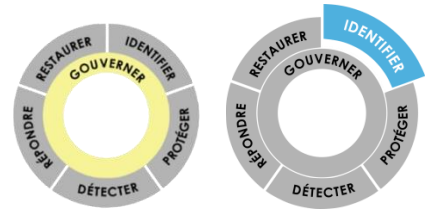
Consolidation de multiples sources
Notification automatique par email




Sévérité CVSS
Système affecté
Description de la vulnérabilité
Proposition de remédiation

Possibilité de suivi de nos équipes pour le maintien en condition de sécurité

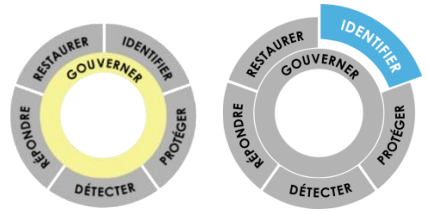
# Offres packagées et à la carte




| | A LA CARTE | ACCESS | STANDARD | PREMIUM |
|---|---|---|---|---|
| Audit d'exposition | ☐ | ☑ | ☑ | ☑ |
| Scan de vulnérabilités | ☐ (1) | ☑ (1) | ☑ (1) | ☑ (1) |
| Test d'intrusion | ☐ (1) | | ☑ (1) | ☑ (1) |
| Microsoft 365 | ☐ | | | |
| Active Directory | ☐ | | | |
| Dark web | ☐ | | | |
| Audit flash Maturité SSI | ☐ | | | ☑ |
| Bulletin cyber | ☐ (2) | | | ☑ (2) |

(1) Limité à 200 actifs maximum pour périmètre interne et 10 actifs maximum pour périmètre externe
(2) Limité à 15 produits maximum – add on possible par pack de 5 produits minimum

# Suivi des risques Cyber sur la durée




## 1 COLLECTE / CONSOLIDATION / ANALYSE

Collecte d'informations trimestrielle, semestrielle ou annuelle en fonction des périmètres

Enumération, cartographie et exploitation en fonction du bundle choisi

Consolidation, analyse, conclusions d'audit et remise du livrable

**LE + : Une équipe d'auditeurs spécialisés en sécurité offensive**

## 2 PILOTAGE ET SUIVI

Initialisation du contrat - Validation et signature des documents de référence

Comité de pilotage trimestriel, semestriel ou annuel en Visio en fonction du package choisi

Bulletin Cyber pour un suivi des vulnérabilités

**LE + : Un suivi régulier augmentant la maturité Cyber**

## 3 ET PLUS ENCORE

3 packages de journées de mise en place de remédiations au travers de nos équipes de maintien en condition de sécurité

**LE + : Une synergie entre nos équipes de sécurité offensive et défensive**

# MERCI !

heliaq
Solutions