

# SOC cybersécurité



- Solution managée complète de **sécurisation de votre périmètre informatique** par nos experts SOC de proximité en **24/7**.



Clients

# Ils nous font confiance

Clients de tous secteurs, PME et ETI sécurisés par Cyna

LANVIN  
PARIS

agnès b.

GRUPE  
ABCD  
INTERNATIONAL

Hôpital  
Saint  
Camille

SPORT  
2000

JOBTEASER

instant system

6WIND  
Virtualized Networking Software

Enerdata

NEOBRAIN

transatel  
NTT

GRUPE  
marie claire

BIG MAMMA

FF judo

DNCA  
INVESTMENTS

GM  
EV

LE  
M  
A  
R  
C  
H  
É  
RIVE GAUCHE

SILVR

HelloCSE

RIELLO

isara  
AGRO SCHOOL FOR LIFE

SLF  
Groupe Sombank-Lung Ferry

AVENIR  
SANTÉ  
FORMATION

andera  
PARTNERS

MINLAY

association  
hospitalière  
de Bretagne

Fondation  
tara océan  
explorer et partager

AUZOU

ifocop

emineo  
EDUCATION

# Pourquoi nos clients ont pris le SOC ?

Comment Cyna a répondu à leurs besoins ?

## ❖ Améliorer le niveau de sécurité

- ✓ Remplacer l'anti-virus peu efficace
- ✓ Passer sur un accompagnement spécialisé en cybersécurité

## ❖ Se protéger suite à une cyberattaque

- ✓ Se prémunir des futurs risques et attaques

## ❖ Bénéficier d'une expertise cyber

- ✓ Externaliser la gestion de la cybersécurité pour libérer les ressources en interne d'une tâche chronophage
- ✓ Se faire accompagner en 24/7

## ❖ Se mettre en conformité

- ✓ Régulation :
- ✓ Assurance
- ✓ Supply Chain



# Prévenez les attaques grâce à une surveillance continue de votre SI

Le tout géré par une équipe d'experts en 24/7

## EDR/Digital Workplace Protection



- ✓ Postes de travail
- ✓ Téléphones
- ✓ Serveurs
- ✓ Utilisateurs
- ✓ E-mails
- ✓ Données

## SOC 24/7 Service managé



- ✓ Détection, analyse et remédiation
- ✓ Expertise cyber reconnue de SOC analysts

## Pilotage Personnalisé



- ✓ Personnalisé avec le nom du MSP
- ✓ Rapports de vulnérabilité
- ✓ Rapports d'activité mensuel

## Cyna CERT Réponse à incident



- ✓ 1 journée allouée
- ✓ En 24/7

Le +

# Sécurisez votre entreprise grâce à une défense proactive de l'EDR

Détection

Analyse

Remédiation

## ❖ Les fonctionnalités clés

- ✓ 3 moteurs de détections (réputation, AI embarquée, comportementale)
- ✓ Multi OS (Windows, MacOs, Linux et Os Legacy)
- ✓ Protection en ligne et hors ligne
- ✓ Inventaire et vulnérabilité
- ✓ Fonctionnalité hygiène IT (USB, Bluetooth, Firewall)
- ✓ RI : Blocage / Isolation / Hash / Remote Ops / RollBack
- ✓ Faible consommation CPU

## ❖ Données hébergées en Europe

# Un accompagnement cyber de nos experts

Nos SOC Analystes à votre service



# Nos différents modules

Découvrez nos 3 modules

## PC & serveurs

- ✓ **Détection par réputation**
- ✓ **Détection comportementale**
- ✓ **Analyse statique**
- ✓ **Règles custom**
  - Blocage d'IOC connu (CTI) Détection d'outils de PENTEST
  - Mapping de la menace Mitre Attack
  - Outils non autorisés (VPN, Remote tools, etc.)

## Digital Workplace

- ✓ **Entra ID**
  - Connexion depuis un pays étranger au pays de travail
  - Création de compte utilisateur
  - Ajout de rôles/permissions admin
- ✓ **Sharepoint**
  - Téléchargement massif de fichiers depuis les données partagées
  - Suppression massive de fichiers depuis les données partagées
- ✓ **Règles custom**
  - Création de règles de redirection de mails
  - Modification des règles de transport
  - Ajout de permissions aux boîtes mail

## Capacité de réponse

- ✓ **EDR**
  - Quarantaine
  - Kill
  - Isolation du réseau
  - Restauration système
- ✓ **Digital Workplace**
  - Reset password
  - Suspension de compte

# Présentation des rapports

Découvrez nos deux types de rapport



## 1. Rapport d'activité

- Rappel du scope de protection
- Résumé & évolutions des menaces
- Obsolescences
- Indicateurs de vulnérabilités (CVE)

## 2. Rapport de vulnérabilités

- Priorisation des vulnérabilités
- Préconisation pour la remédiation

# Notre équipe

Nos experts à votre service

## Analystes SOC

- Traitement des alertes
- Investigation
- MCO EDR



**Yanniss**  
SOC Manager

## Analystes CERT

- Veille de vulnérabilité
- Gestion de crise



**Nathan**  
Head of Cyber &  
referent CERT

## Développement & Automation

- Intégration
- Workflow
- Automatisation
- Reporting



**Avétis**  
CTO

## Purple Team

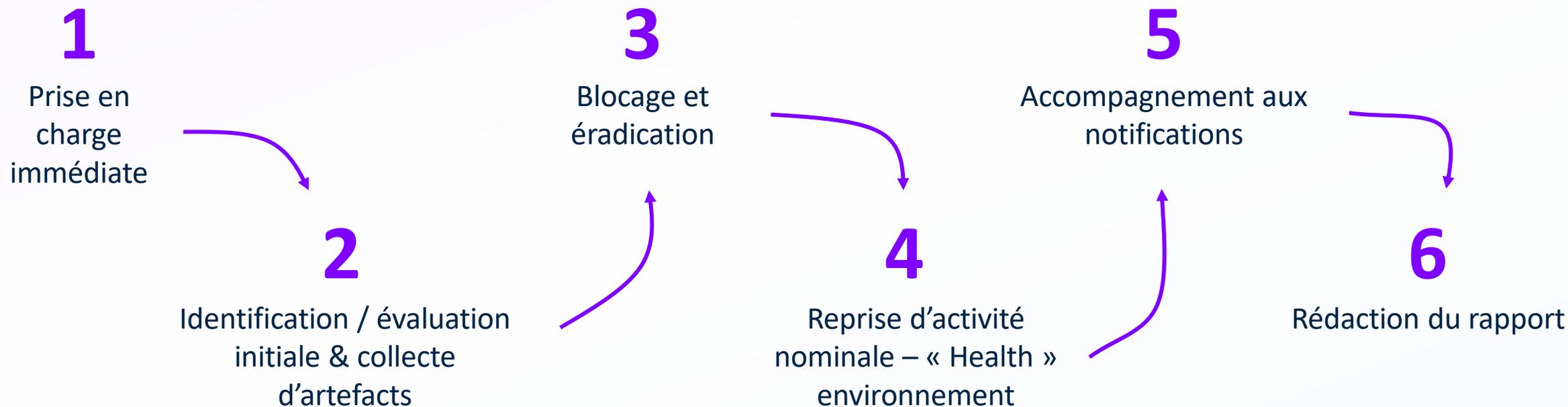
- Amélioration continue de la détection



**Benjamin**  
Referent Pentest

# Cyna CERT – Intervention en gestion de crise

Réponse à incident : les étapes 1 à 4 sont réalisées en moins de 24 heures



Dès qu'une **intrusion est détectée**, le temps devient l'**élément clé** dans la lutte contre les attaquants.

Nos experts vous prennent en charge et œuvrent dans l'urgence pour **bloquer l'attaque et vous accompagner** sur les plans technique et organisationnel.

# Notre intervention au sein de l'Hôpital Saint Camille

Retour client suite à notre accompagnement SOC



« On se sent vraiment **épaulé par une équipe d'expert** au quotidien, ce qui apporte une **vraie tranquillité d'esprit**.

C'est plus qu'un simple accompagnement, c'est une proximité quotidienne avec une **équipe dynamique qui se rend disponible** à tout moment pour réagir et renforcer notre sécurité »

Ahmed SALHI  
DSI

# Notre intervention au sein de l'Hôpital Saint Camille

## Retour client suite à notre accompagnement SOC

### Problématiques

#### Ressources limitées :

- Manque de ressources en internes dédiées à la gestion chronophage de la cybersécurité.

#### Contraintes budgétaires :

- Budget restreint malgré la taille de l'établissement

#### Antivirus insuffisant :

- L'antivirus n'est pas suffisant pour l'hôpital, confronté à des risques significatifs en matière de cybersécurité.

#### Conformité et gouvernance interne :

- Défis liés à la gestion de la conformité et à la gouvernance en interne, nécessitant une attention particulière.

### Objectif : mise en place du SOC

#### Valeur ajoutée :

- ✓ Des experts dédiés pour sécuriser en continue votre SI.

#### BUILD :

- ✓ Mise en place de l'EDR pour une sécurité proactive.
- ✓ Intégration des logs pour une vision complète.
- ✓ Analyse approfondie des besoins du client, pouvant conduire à l'implémentation de règles spécifiques.

#### RUN :

- ✓ Détection et analyse en temps réel des événements de sécurité.
- ✓ Remontée et priorisation des vulnérabilités.
- ✓ Mise en œuvre d'une gouvernance cyber.

Powered by

**cyna**

**Votre **sécurité** est notre métier.**

Construisez vos projets en toute **sérénité**.

