



## RESULTATS DE LA MICRO- ENQUETE 2017

MARTINE GIUSTI

RESPONSABLE DEVELOPPEMENT PARTAGE SANTE

mgr31@free.fr

[contact@partage-sante.fr](mailto:contact@partage-sante.fr)

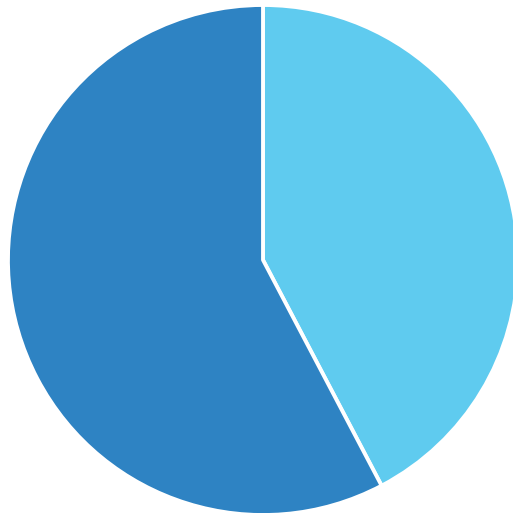
06 76 29 65 48

# PREAMBULE

- ▶ Système d'information: priorité à la sécurité!
- ▶ Hébergement de données de santé, identitovigilance , ransomware , sécurité des logiciels...la gestion par les risques et la maîtrise de la sécurité informatique est au cœur des responsabilités des établissements de santé.
- ▶ Comment assurer une sécurité maximale alors que les établissements de santé tant sanitaires que médico-sociaux s'ouvrent davantage vers la ville ?
- ▶ Quelles bonnes pratiques doit on développer ?

# Votre établissement a-t-il subi des attaques informatiques?

71 REPONSES

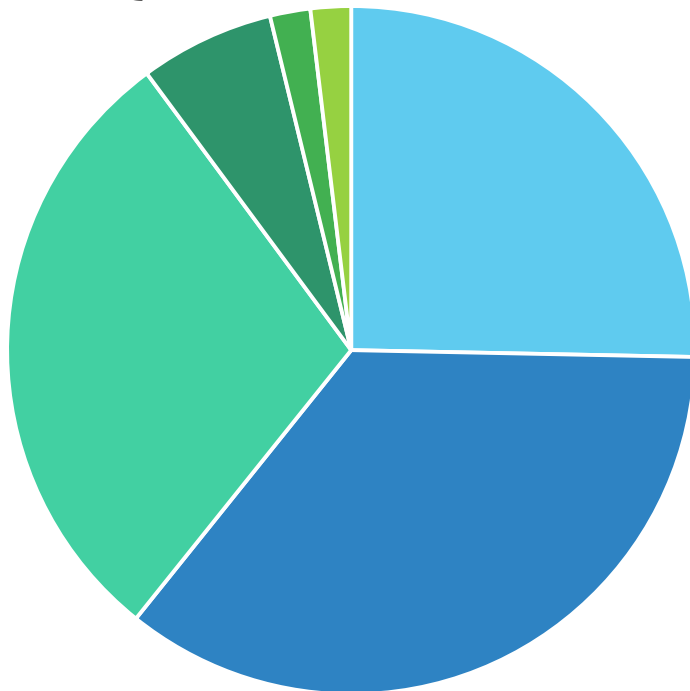


■ OUI ■ NON

- ▶ OUI A 42%
- ▶ NON A 57.7%

# NATURE DE CES ATTAQUES:

ATTAQUES



- PAR ORDRE DE FREQUENCE:

- ▶ 1/ LES LOGICIELS MALVEILLANTS 56,7%
- ▶ 2/ LA DEMANDE DE RANCON 46,7%
- ▶ 3/ LE HAMECONNAGE 40%
- ▶ 4/ DES ESCROQUERIES DIVERSES 10%
- ▶ 5 /PARASITES SUR MESSAGERIE 3,3%
- ▶ 5 BIS/ VIRUS 3,3%

■ HAMECONNAGE

■ DEMANDE DE RANCON

■ PARASITES SUR MESSAGERIE

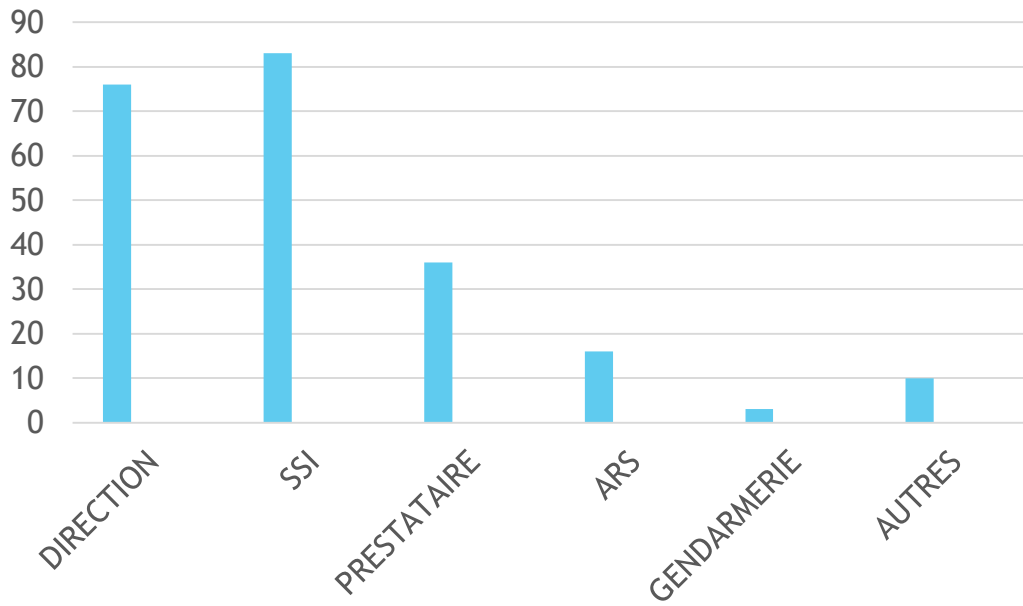
■ LOGICIELS MALVEILLANTS

■ ESCROQUERIES DIVERSES

■ VIRUS

# ACTIONS MISES EN OEUVRE

## DECLARATIONS AUPRES:

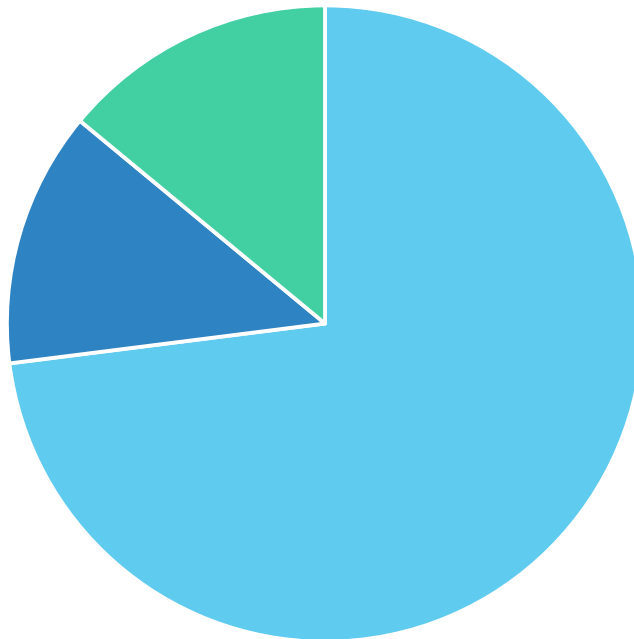


## ▶ PAR PRIORITE

- ▶ SSI 83%
- ▶ DIRECTION 76%
- ▶ PRESTATAIRE 36%
- ▶ ARS 16%
- ▶ AUTRES 10%
- ▶ GENDARMERIE 3%

# FORMATIONS/SENSIBILISATION

NATURE DES FORMATIONS

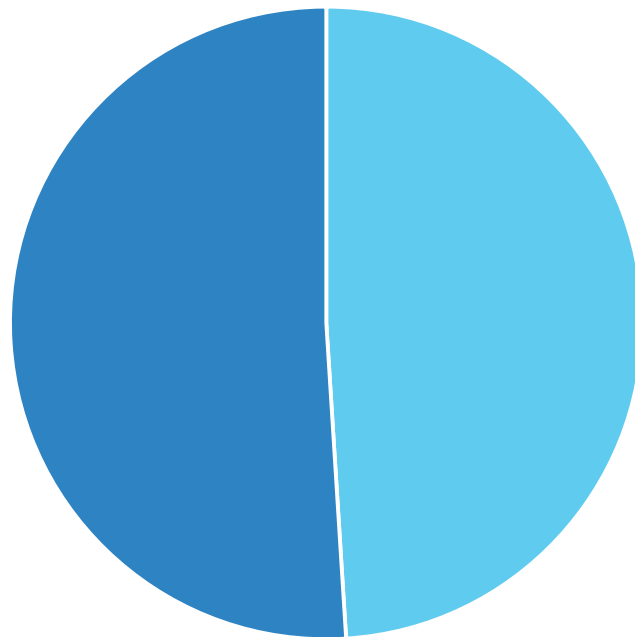


- ▶ FORMATION INTERNE 73%
- ▶ FORMATION EXTERNE 12%
- ▶ AUCUNE FORMATION 15%

■ FORMATION INTERNE ■ FORMATION EXTERNE ■ AUCUNE FORMATION

# PROGRAMMATION A VENIR D'UNE ACTION DE FORMATION OU DE SENSIBILISATION

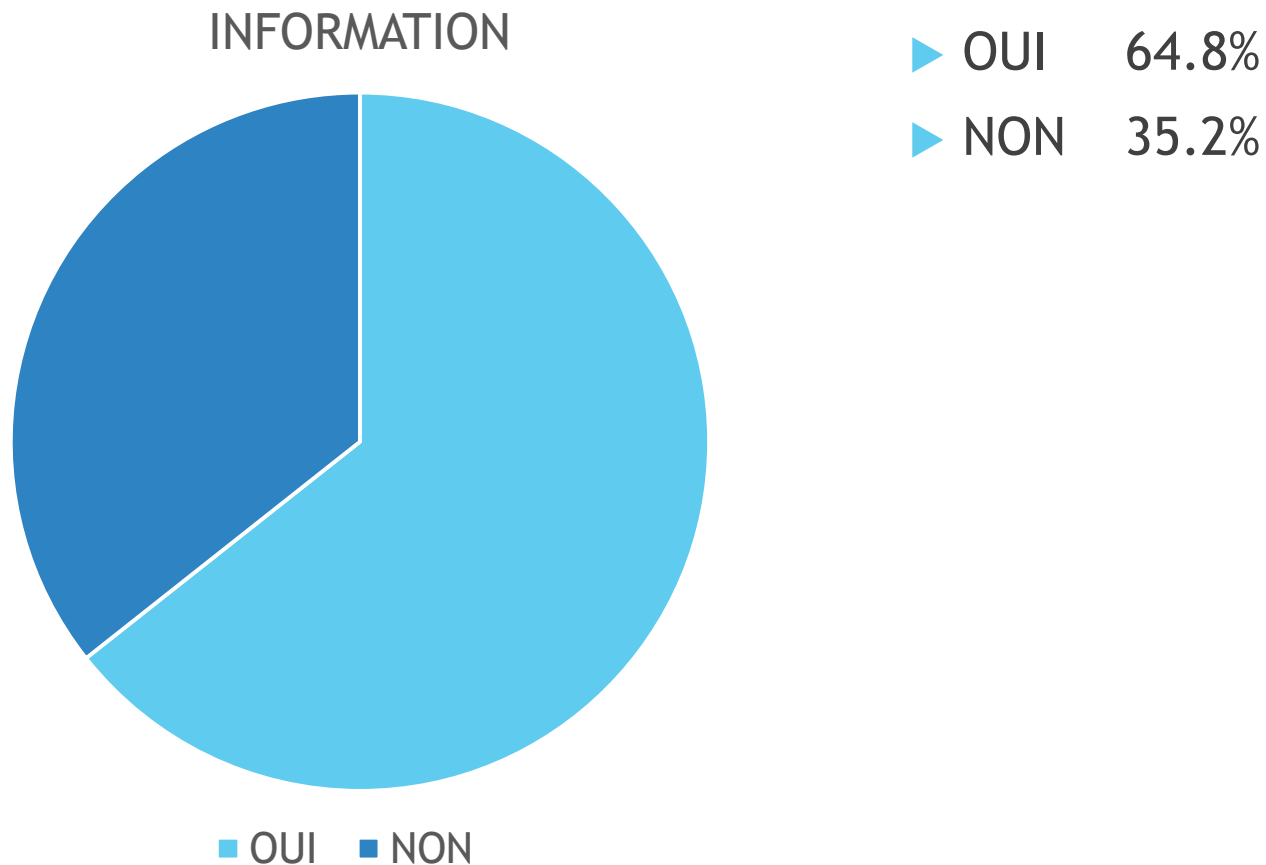
## PROJET DE FORMATION



■ OUI ■ NON

- ▶ OUI A 49.3%
- ▶ NON A 50.7%

# SERIEZ VOUS INTÉRESSÉS PAR UNE INFORMATION GÉNÉRALE SUR LES CYBER MENACES ?





# QUELQUES COMPLÉMENTS DE REFLEXION

## ■ APPUI DOCUMENTAIRE:

- ▶ CERTIFICATION :GESTION DES SYSTÈMES D'INFORMATION
- ▶ HÔPITAL NUMERIQUE: POLITIQUE NATIONALE RELATIVE AUX SYSTEMES D'INFORMATION HOSPITALIERS
- ▶ PLAN DE SÉCURISATION D'ÉTABLISSEMENT(PSE) : CYBER ATTAQUE (PERTURBATION, INTRUSION, VOL D'INFORMATIONS)
- ▶ INCIDENT DE SÉCURITÉ SUR UN POSTE DE TRAVAIL INFORMATIQUE
- ▶ INSTRUCTION N° SG/HFDS/DGCS/2017/219 DU 4 JUILLET 2017 RELATIVE AUX MESURES DE SÉCURISATION DANS LES ÉTABLISSEMENTS ET SERVICES SOCIAUX ET MÉDICO-SOCIAUX.

# QUELQUES COMPLÉMENTS DE REFLEXION

## ▶ AU NIVEAU DE L'ETABLISSEMENT :

- ▶ ACQUISITION DE LA CULTURE SECURITE DES SI: NOMINATION RSSI, SSI DANS LES INSTANCES.
- ▶ PROCEDURE DE FONCTIONNEMENT EN MODE DEGRADE
- ▶ MISE EN PLACE D'UN LIEN PRIVILEGIE AVEC LE SERVICE QUALITE
- ▶ FORMALISATION DES DOCUMENTS INSTITUTIONNELS (PSSI, CHARTE INFORMATIQUE, CHARTE DE LA SECURITE DU SYSTEME D'INFORMATION ...)

# AU SEIN DE LA CERTIFICATION: RAPPEL GESTION DU SYSTÈME D'INFORMATION

- ▶ **Éléments d'investigation :**
- ▶ Schéma directeur du système d'information (SDSI)\* défini en cohérence avec les orientations stratégiques et prenant en compte les besoins des utilisateurs.
- ▶ Politique de sécurité du système d'information.
- ▶ Organisation permettant le pilotage et le suivi du SDSI (cellule de coordination intégrant des utilisateurs).
- ▶ Identification des ressources dédiées au système d'information dont un responsable Sécurité du Système d'Information.
- ▶ Existence d'un plan de reprise de l'activité (PRA) et de procédures dégradées connues des professionnels
- ▶ Identification des niveaux d'habilitation par application
- ▶ Dispositif de traçabilité des actions au sein du système d'information.
- ▶ Dispositif d'évaluation et suivi d'indicateurs quantitatifs et qualitatifs (enquête de satisfaction, indicateurs de suivi...).
- ▶ Dispositif d'évaluation de la sécurité
- ▶ Actions d'amélioration mises en œuvre avec les professionnels, au regard des résultats obtenus.