

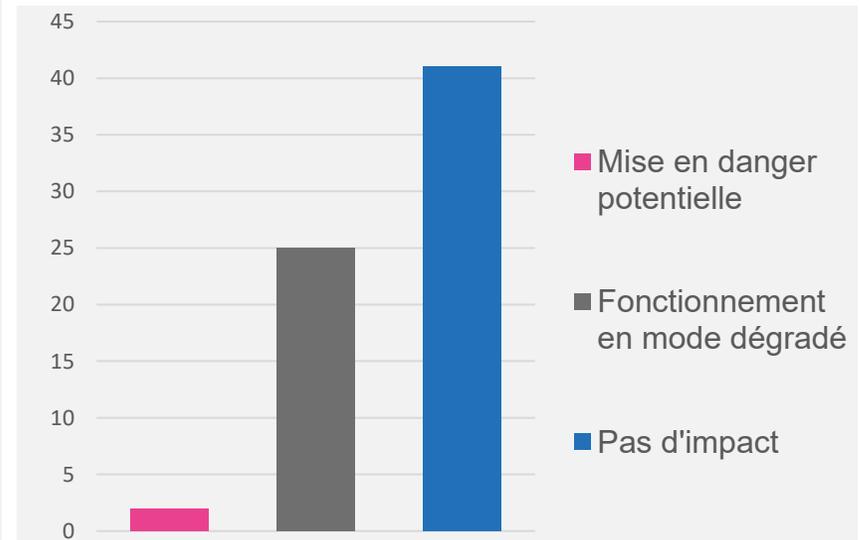
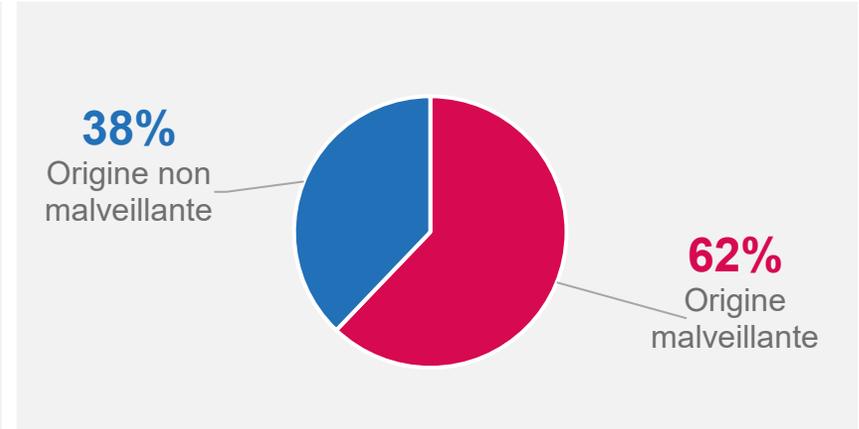
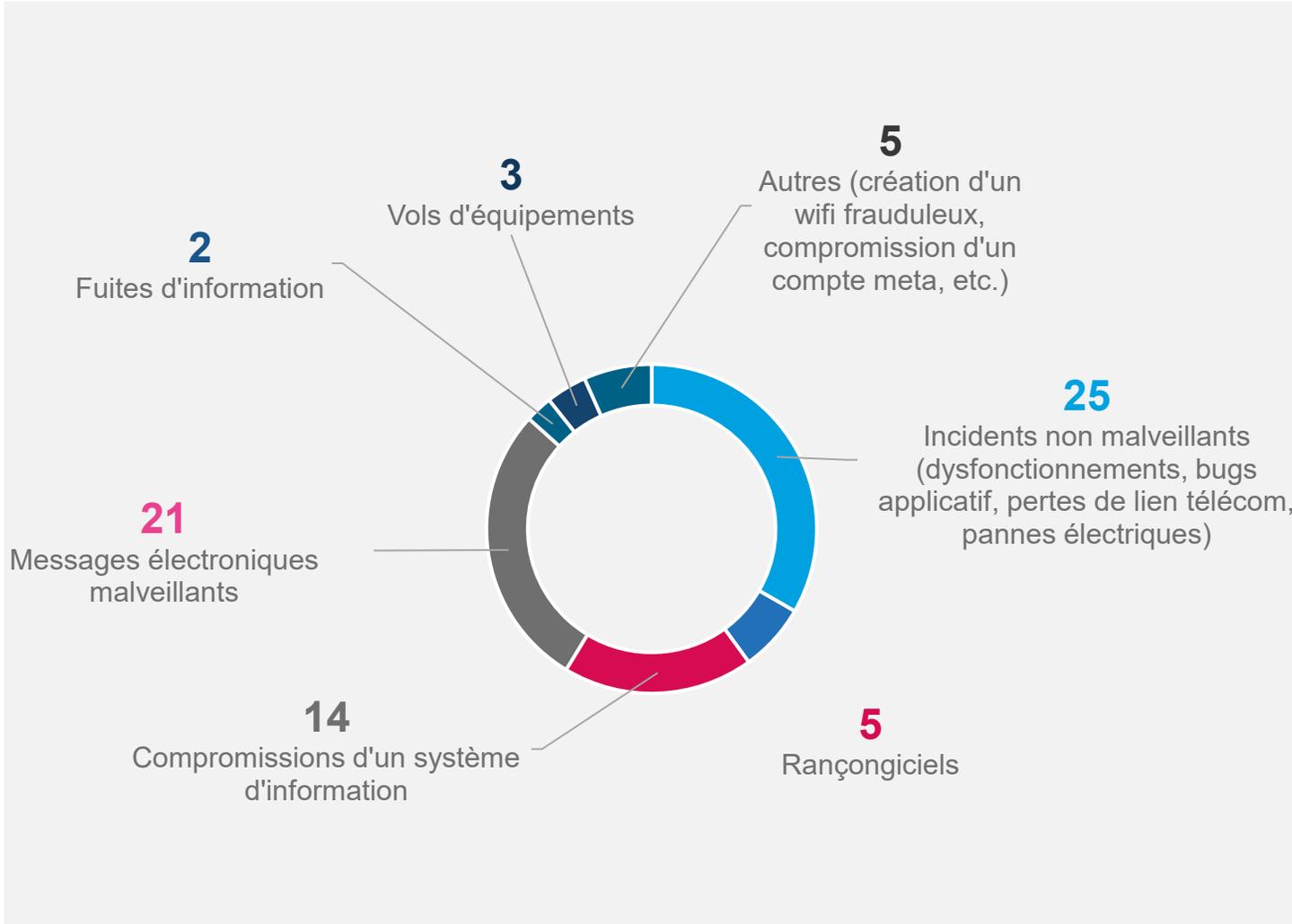


AGENCE  
**DU NUMÉRIQUE  
EN SANTÉ**  
La transformation commence ici 



# Indicateur sur l'origine des incidents déclarés pour le mois de juillet

Août 2025



# Origine des incidents déclarés – Juillet 2025

## Messages malveillants et rançongiciels



Comptes de messagerie compromis via des messages d'hameçonnage et tentatives de fraude au président



Attaque par un rançongiciel grâce à une prise en main RDP entraînant le chiffrement du contenu d'un ordinateur utilisé pour la facturation



Attaque par un rançongiciel "Wareisolation" suite à la compromission du VPN entraînant le chiffrement du serveur de l'établissement impactant les fonctions support de la structure



Attaque par un rançongiciel Deadlock suite à l'exploitation d'une vulnérabilité sur l'accès VPN entraînant la compromission de multiples serveurs et postes utilisateurs

## Rançongiciels



Attaque par un rançongiciel ayant entraîné le chiffrement du serveur de l'établissement suite à la compromission par bruteforce d'un accès Teamviewer sur le serveur exposé sur internet



Attaque par un rançongiciel AKIRA suite à la compromission d'un accès VPN entraînant le chiffrement d'un serveur utilisé par les RH de l'établissement



Fuite d'informations patients suite à la compromission d'un compte utilisateur sur le DPI de l'établissement