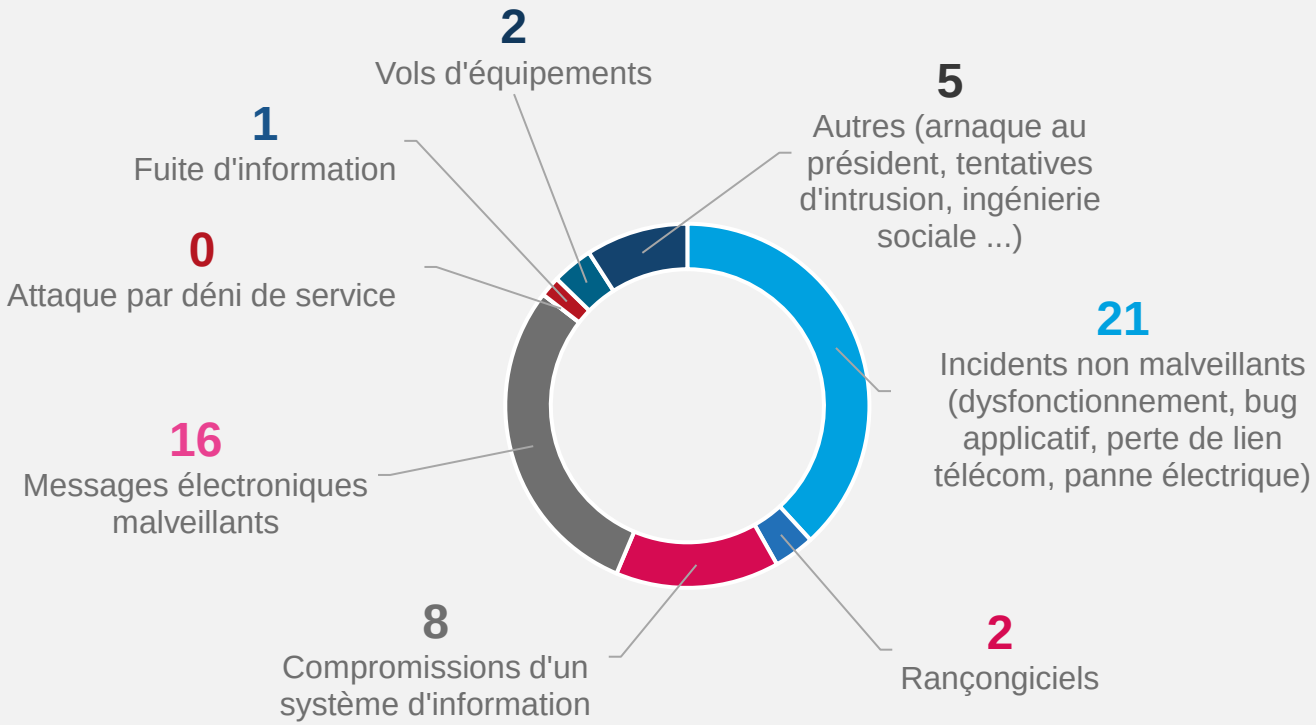
AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

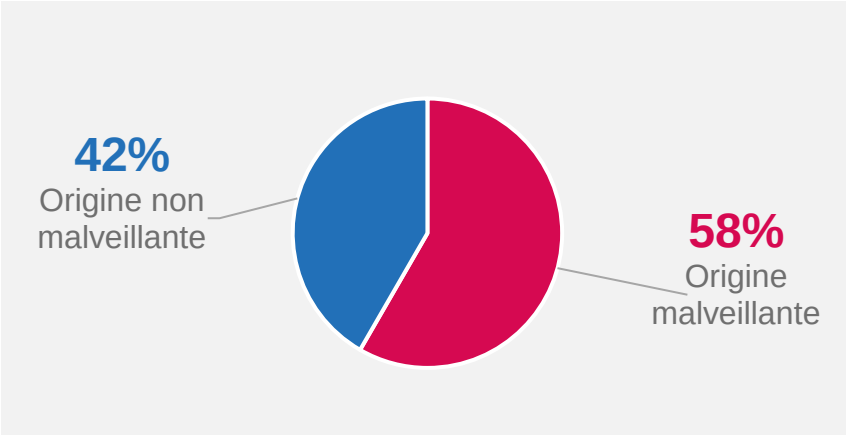
Indicateur mensuel sur l'origine des incidents déclarés

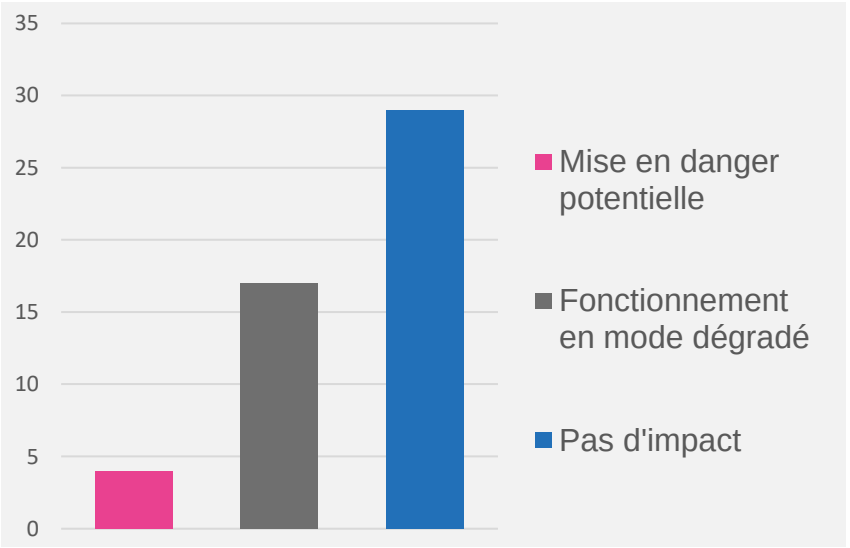
CERT Santé

Juin 2024

Origine des incidents déclarés – Mai 2024







Origine des incidents déclarés – Mai 2024

Message malveillants, compromission d'un système d'information et rançongiciel.

Comptes de messagerie et postes utilisateurs compromis via des messages d'hameçonnage ou contenant une charge malveillante

Compromission d'un compte utilisateur CITRIX puis tentatives de mouvement latéraux via des modifications de DLL signalées par l'EDR

Attaque par le rançongiciel **Trj/CI.A** suite à une mauvaise configuration du pare-feu - fort impact sur le système d'information de l'établissement avec arrêt du système pendant 2 jours ainsi que le chiffrement de serveurs virtuels et de sauvegardes

Attaque par le rançongiciel **Press Ransomware** suite à une compromission de compte RDP entrainant le chiffrement de serveurs de fichiers