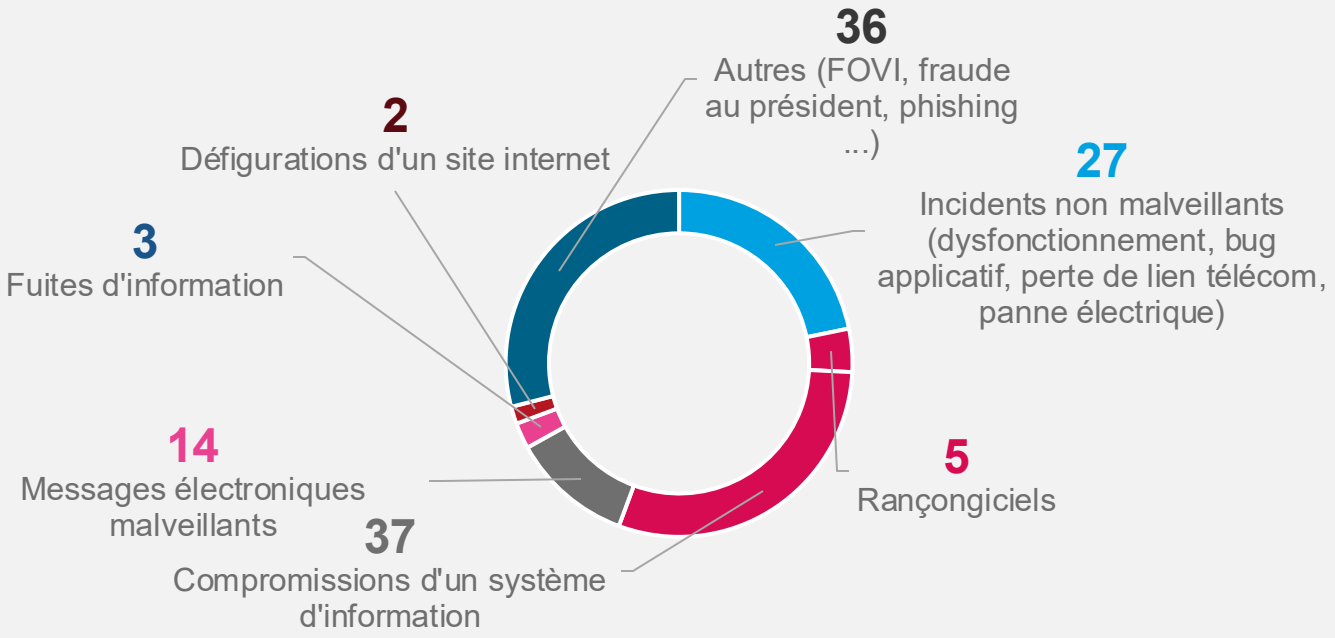
CERT Santé

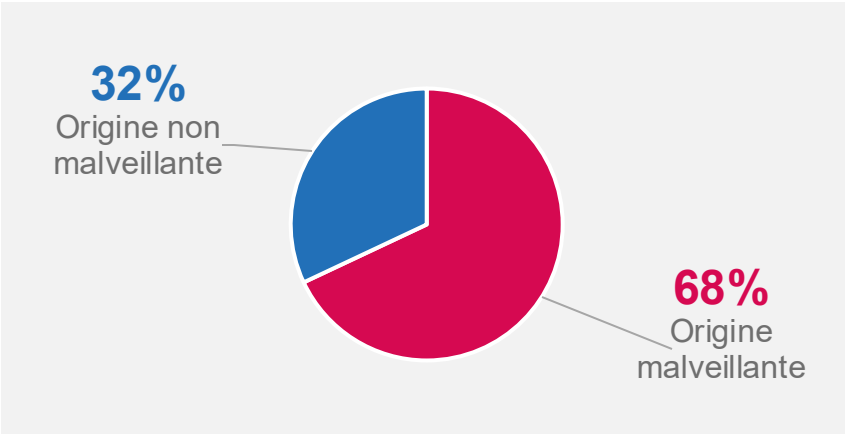
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

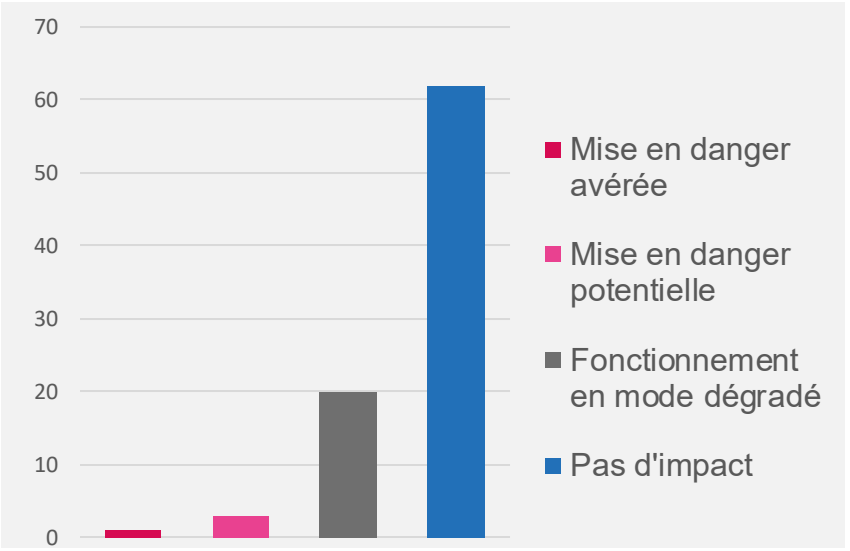
Indicateur sur l'origine des incidents déclarés pour le mois d'avril

Mai 2025

Origine des incidents déclarés – Avril 2025







Origine des incidents déclarés – Avril 2025

Défiguration site web, Compromission du SI et rançongiciel

Comptes de messagerie compromis via des messages d'hameçonnage (fraude au président), des messages contenant une charge malveillante.

Défiguration d'un site web et création d'une copie d'un site internet pour des utilisations frauduleuses de vente de médicaments

Exploitation d'une vulnérabilité du logiciel CrushFTP entraînant la création d'un compte utilisateur et l'accès à des fichiers sur le serveur

Attaque par rançongiciel par le groupe RançonHub suite à la compromission d'un compte administrateur de domaine au mot de passe faible

Attaque par rançongiciel par le groupe Qilin entraînant le chiffrement de données sur plusieurs serveurs internes et le chiffrement de l'ESX contenant l'AD

Origine des incidents déclarés – Avril 2025

Rançongiciels

Attaque par rançongiciel par le groupe 3AM entrainant le chiffrement du serveur AD et d'un serveur de fichiers

Attaque par un rançongiciel de la famille Medusa suite à l'ouverture d'un lien frauduleux entraînant le chiffrement de l'ensemble des documents présents sur les serveurs des fonctions support

Attaque par un rançongiciel de la famille Makop suite à l'exploitation d'une vulnérabilité sur un serveur Exchange non mis à jour et qui a entrainé le chiffrement d'une partie des sauvegardes de l'établissement