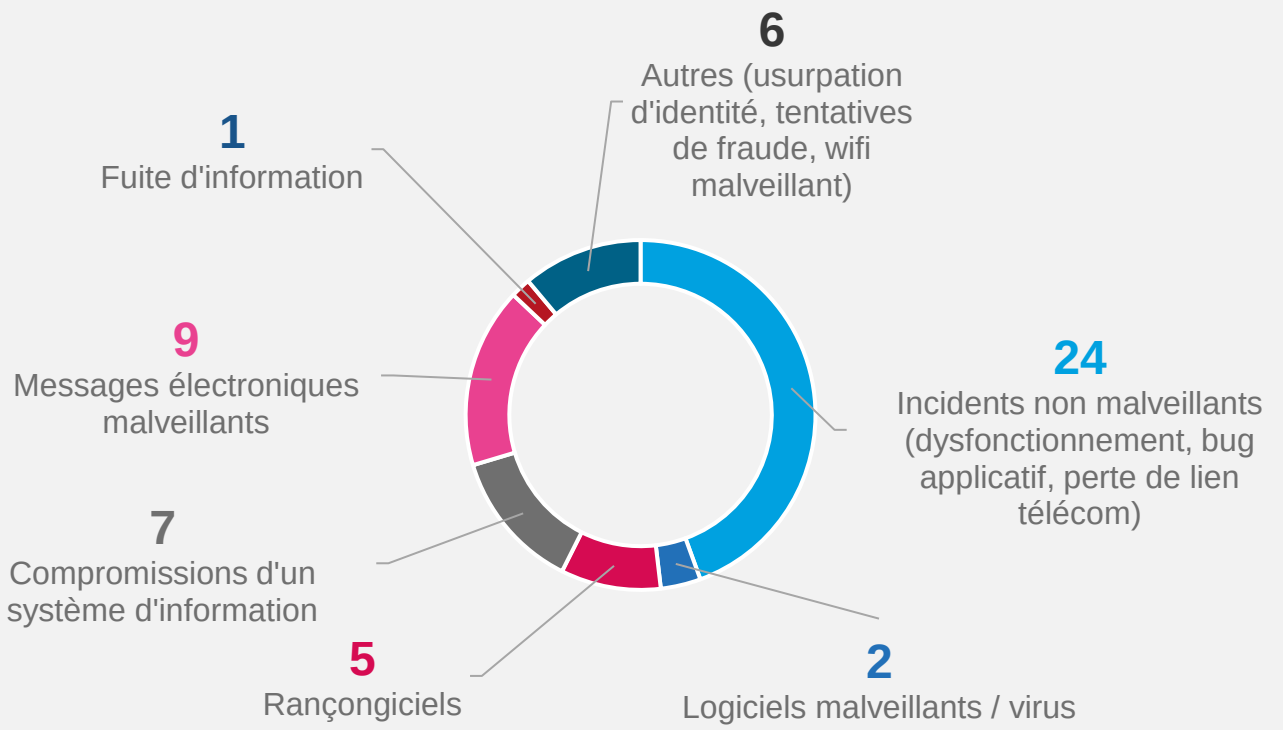
AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

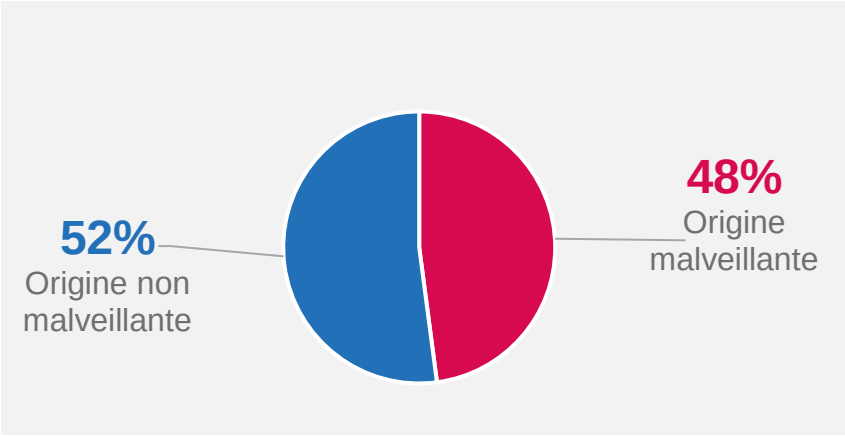
Indicateur mensuel sur l'origine des incidents déclarés

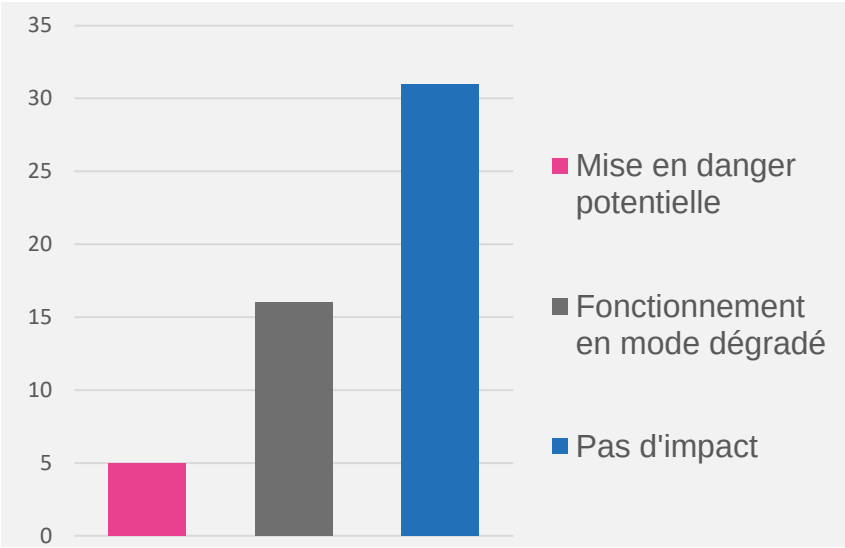
CERT Santé

Juillet 2024

Origine des incidents déclarés – Juin 2024







Origine des incidents déclarés – Juin 2024

Message malveillants, compromission de compte et rançongiciel

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

Exploitation de la CVE- 2023-27532 avec l'utilisation du port 9401 sur des versions de Veeam vulnérable entrainant la compromission d'un hyperviseur

Attaque par le rançongiciel **Lockbit** depuis un PC de radiothérapie d'un prestataire - impact très localisé car traitement très rapide du NDR en isolant le poste - données restaurées depuis les sauvegardes

Attaque par un acteur malveillant nommé « **Princeindia12@mailtor.com** » sur un NAS suite à l'exploitation d'une vulnérabilité sur la mire d'authentification, due à un défaut de patch management, entrainant l'exfiltration et la suppression des données et l'émission d'un message de rançon

Attaque par le rançongiciel **Blacksuit** d'un ESMS après compromission d'un compte AD ayant un mot de passe faible, élévation de privilèges et exfiltration de données et chiffrement de plusieurs serveurs