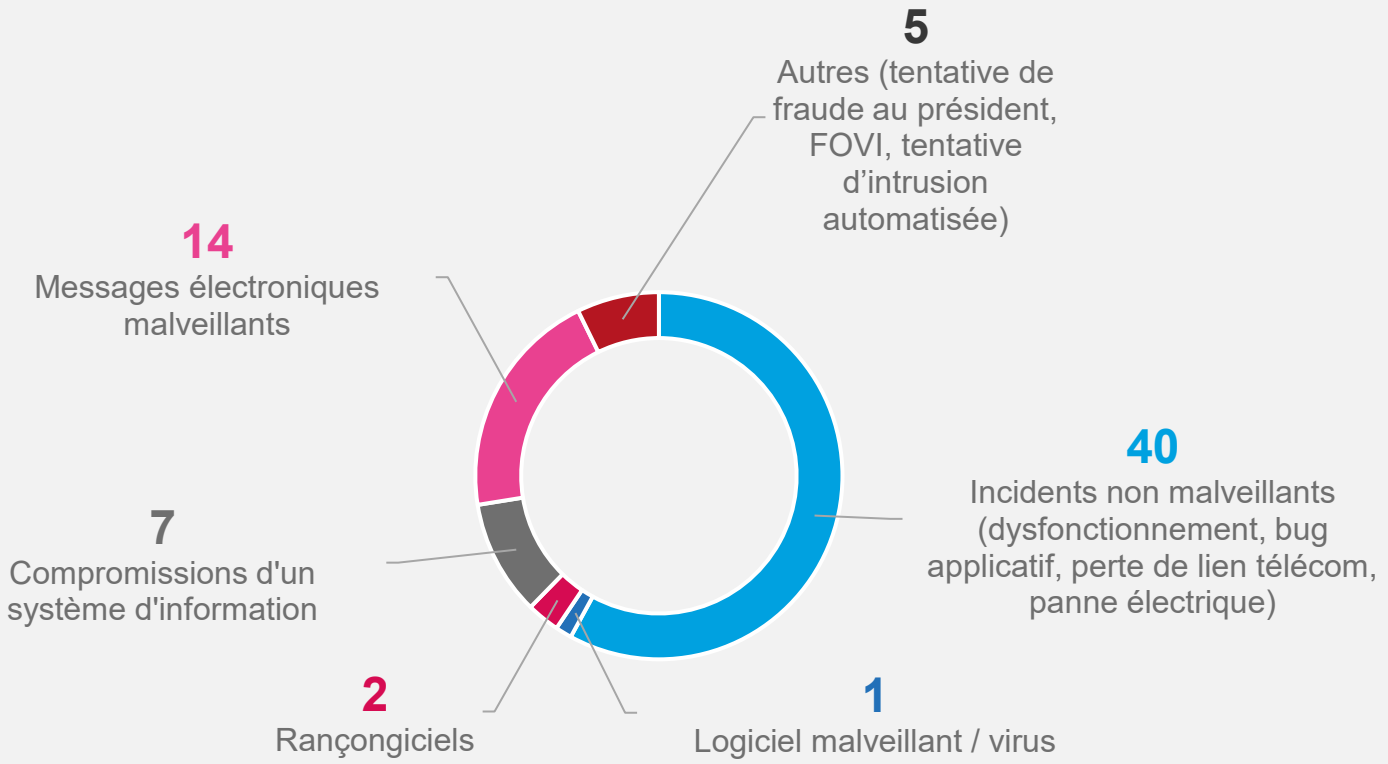
CERT Santé

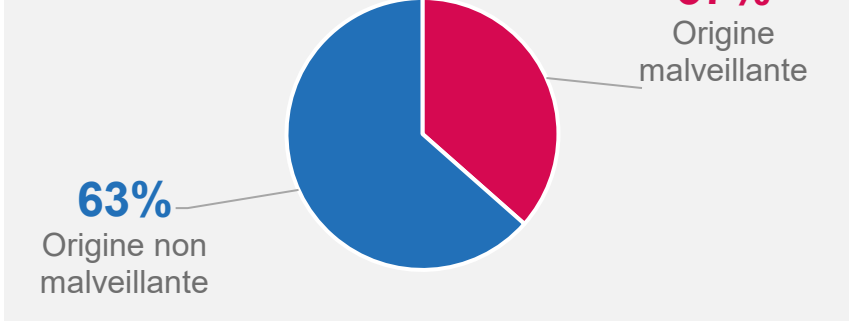
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

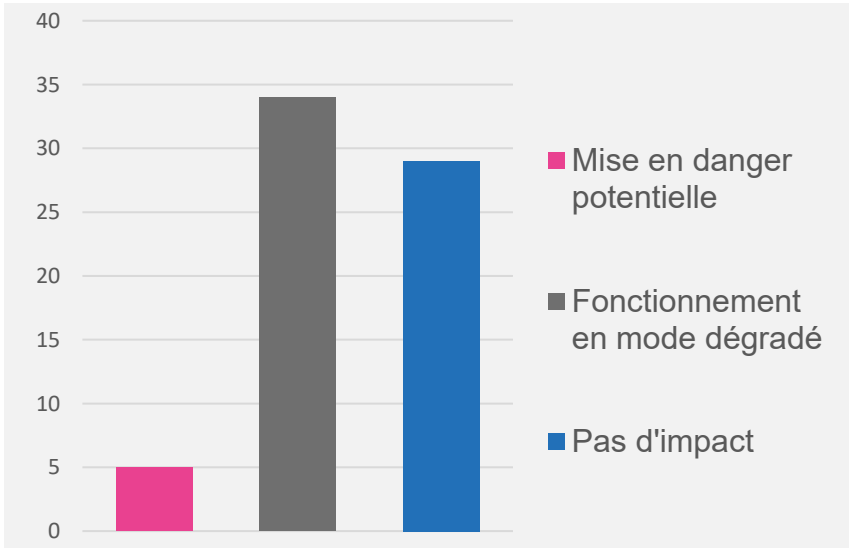
Indicateur sur l'origine des incidents déclarés pour le mois de juin

Juillet 2025

Origine des incidents déclarés – Juin 2025







Origine des incidents déclarés – Juin 2025

Messages malveillants, Compromission du SI et rançongiciel

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

Attaque par un rançongiciel INC Ransom suite à la compromission d'un compte VPN entraînant le chiffrement complet des données du serveur de fichiers, la suppression des sauvegardes et la mise hors service de l'infrastructure de virtualisation (ESXi / VMs détachées)

Attaque par rançongiciel bloquée par un EDR suite à la détection par analyse comportementale de la présence d'une note de rançon associée à CryptoWall.SP sur un serveur de fichiers central

Exécution d'un programme malveillant sur un poste utilisateur après redirection vers une page web avec un "faux" CAPTCHA suite à la réception d'une newsletter malveillante