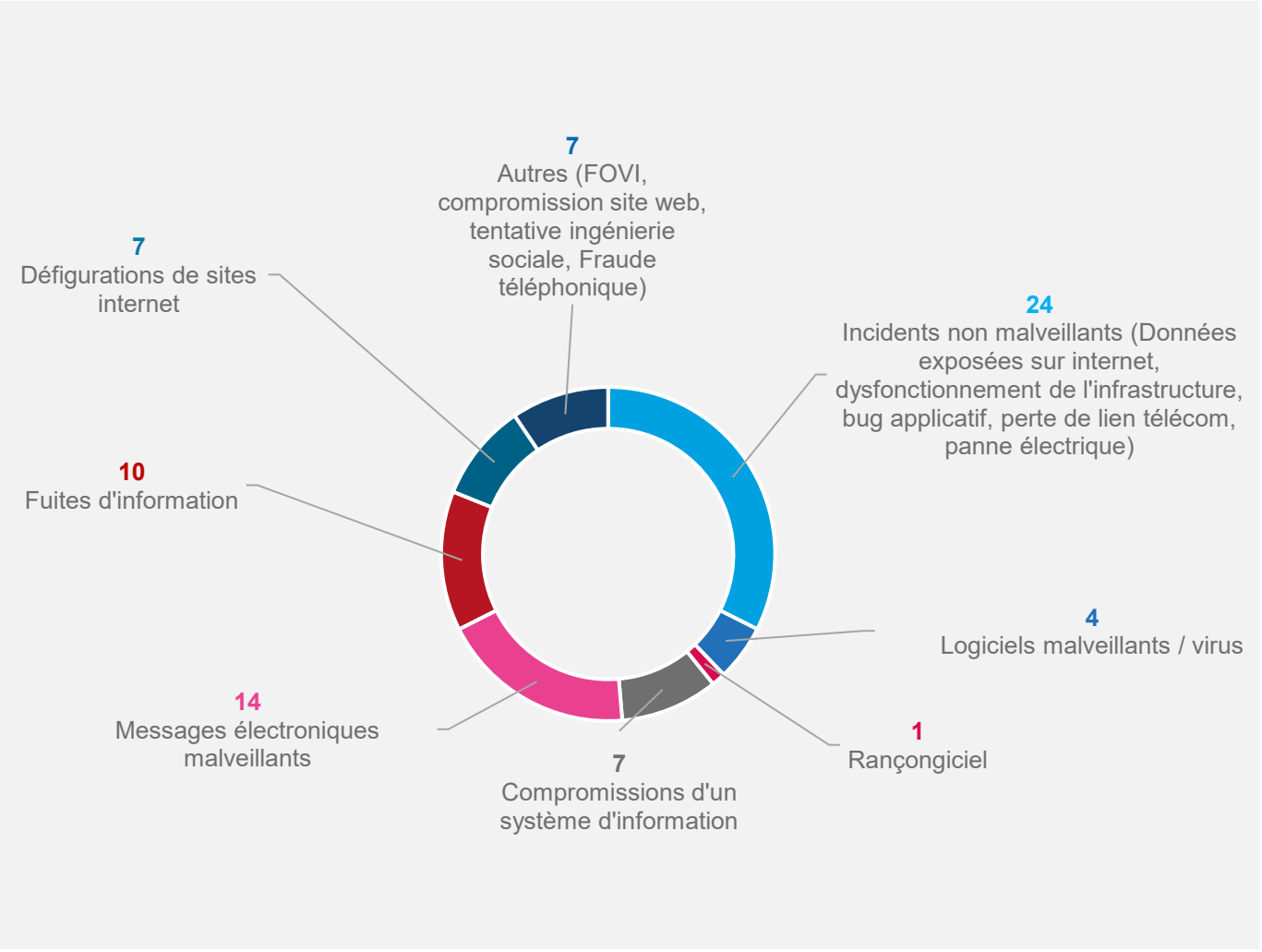
CERT Santé

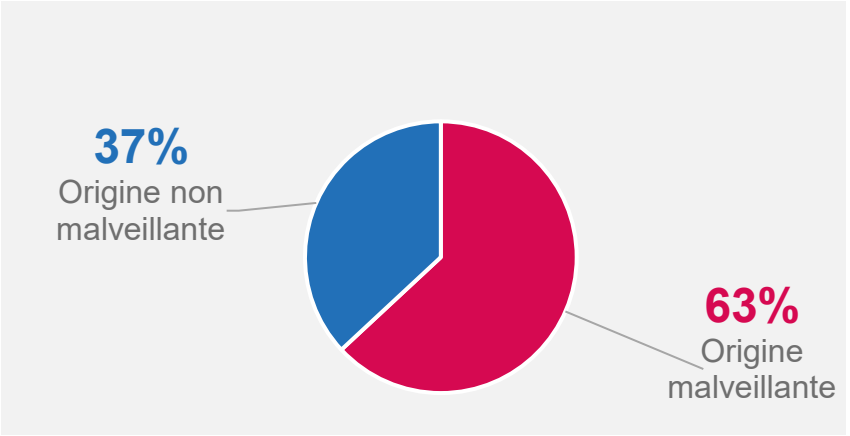
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

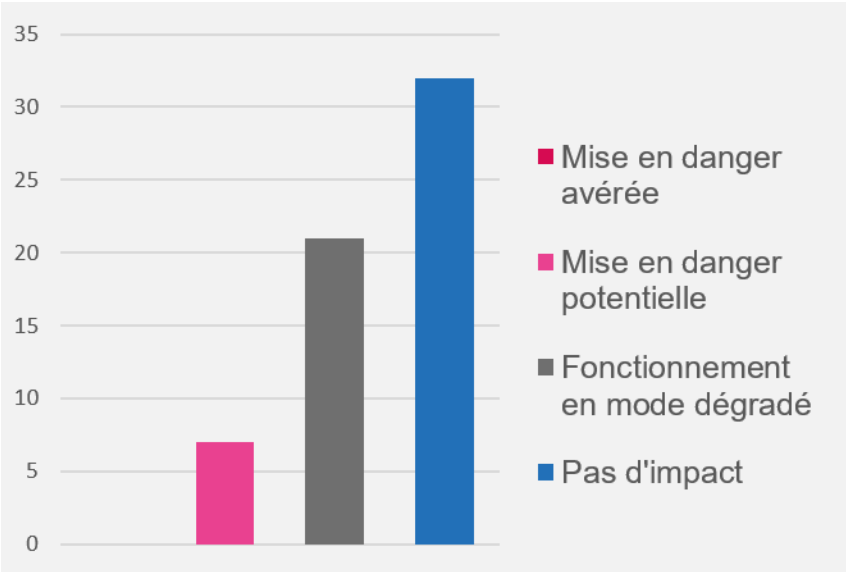
Indicateur sur l’origine des incidents déclarés pour le mois de Juillet

Aout 2026

Origine des incidents déclarés – Juillet 2026







Origine des incidents déclarés – Juillet 2026

Compromission SI et compromission de sites internet

Compromission d'un compte à privilège ayant permis des actions malveillantes sur le contrôleur de domaine de l'établissement, dans un contexte de récupération d'informations techniques.

Exploitation de la chaîne « WP2SHELL » sur un site Wordpress (CVE-2026-60137 et CVE-2026-63030), ayant permis une prise de contrôle de l'application puis une compromission du système.

Compromission d'un compte Microsoft 365 d'un agent hospitalier ayant permis l'accès à la messagerie Exchange Online et à OneDrive, l'envoi de courriels frauduleux par usurpation d'identité ainsi que l'exfiltration de données dont des identifiant appartenant à des organismes tiers