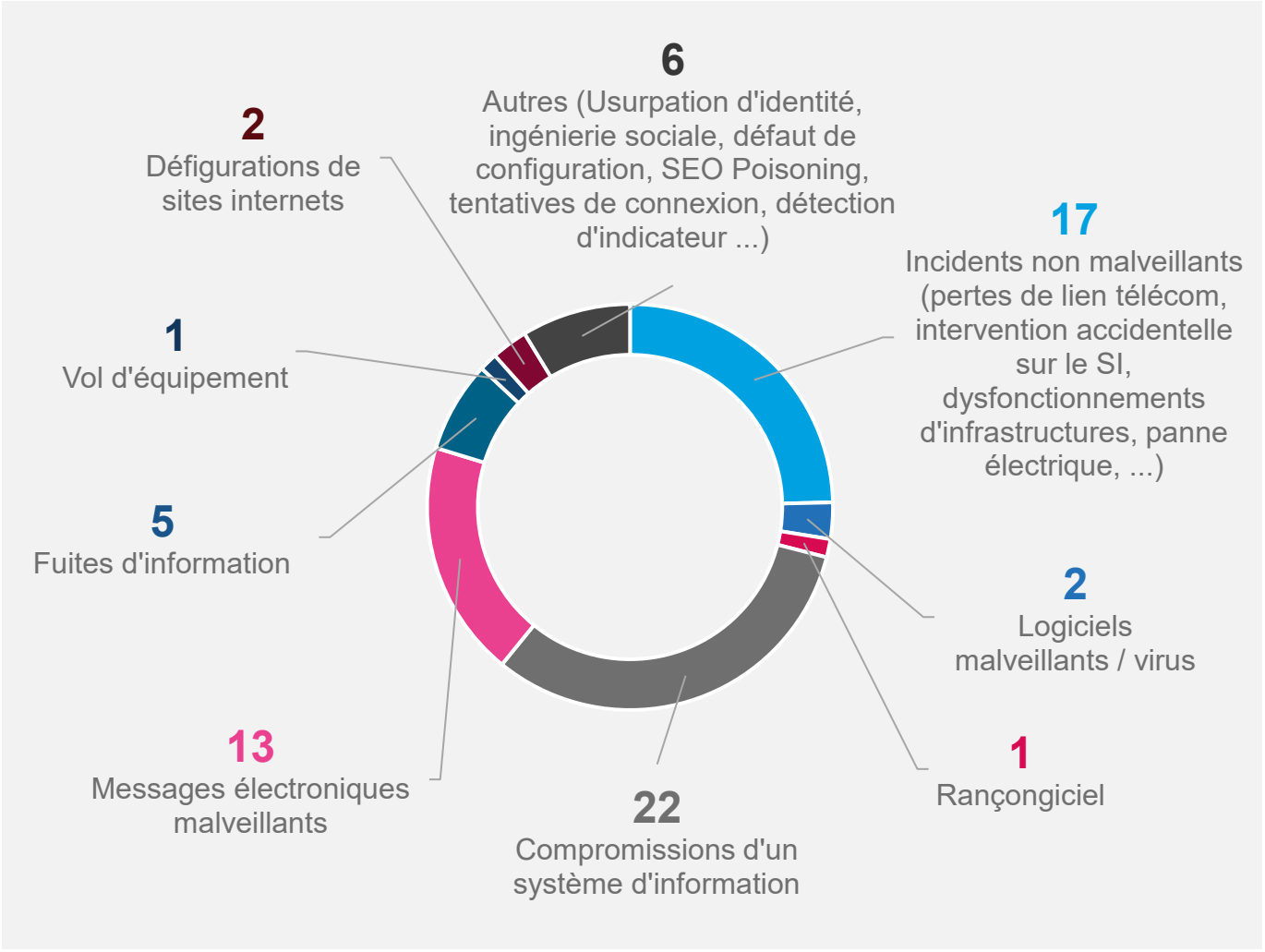
CERT Santé

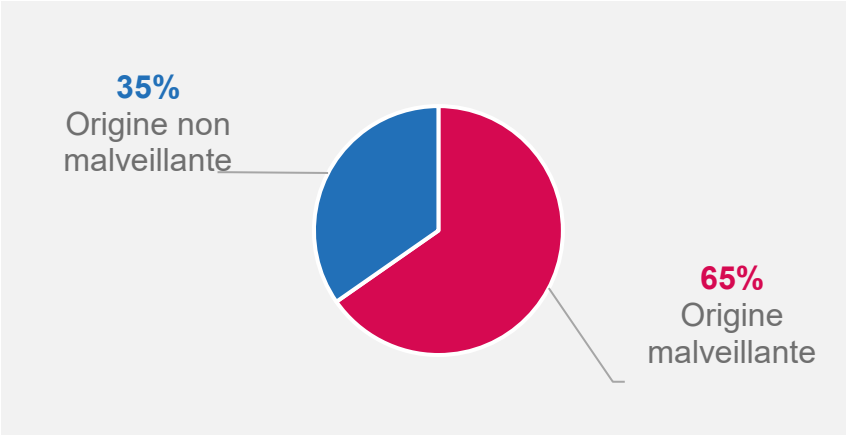
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

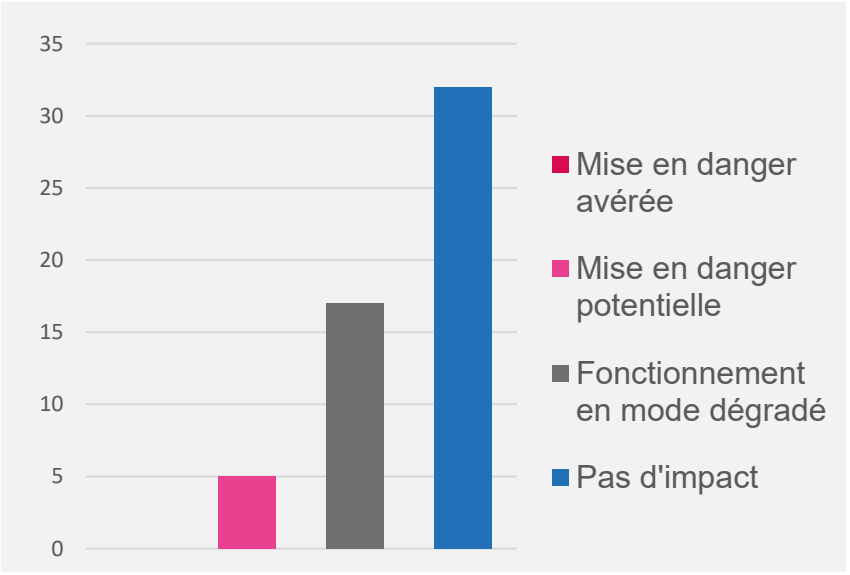
Indicateur sur l'origine des incidents déclarés pour le mois de août

Septembre 2026

Origine des incidents déclarés – Août 2026







Origine des incidents déclarés – Août 2026

Compromissions de sites web

Exploitation d'une vulnérabilité d'un plugin WordPress ayant permis une attaque de type SEO poisoning sur plusieurs sites web d'établissements de santé, via l'injection de code malveillant et la modification de métadonnées indexées par les moteurs de recherche, conduisant à l'affichage de liens frauduleux dans les résultats de recherche.

Exploitation de vulnérabilités sur des composants WordPress (comme Pods) ayant conduit à la création de comptes à privilèges, à l'implantation de mécanismes persistants et à l'altération des contenus de sites web (défiguration, référencement frauduleux).

Exploitation des vulnérabilités CVE-2025-59718 et CVE-2025-59719 sur un pare-feu non corrigé, ayant permis la création d'un compte administrateur local non autorisé et l'accès à la configuration de sécurité de l'établissement.

Origine des incidents déclarés – Août 2026

Compromissions de SI, logiciel malveillant, message électronique malveillant & fuites d'information

Infection d'un poste personnel par l'infostealer Acreed, ayant entraîné l'exfiltration de plusieurs identifiants et la compromission d'un compte Microsoft 365 professionnel utilisé pour l'envoi de plusieurs centaines de courriels non autorisés.

Compromission d'un prestataire de services via l'exploitation de la vulnérabilité CVE-2026-72898 affectant la solution Metabase, ayant conduit à l'accès non autorisé, à l'exfiltration et à la divulgation de données de reporting.

Compromission d'un poste de travail ayant permis le détournement de comptes utilisateurs et l'accès non autorisé à plusieurs services contenant des données de santé, dont le téléservice INSI, conduisant à la récupération d'un volume important d'informations.