



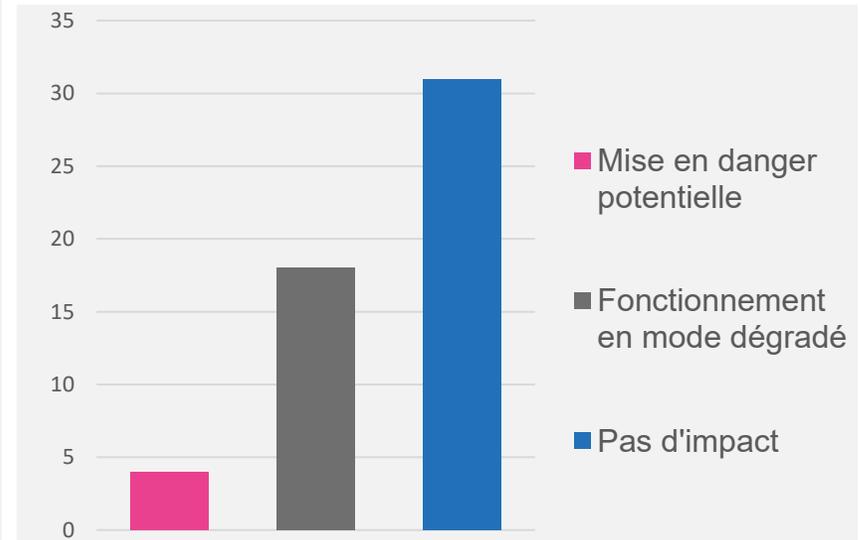
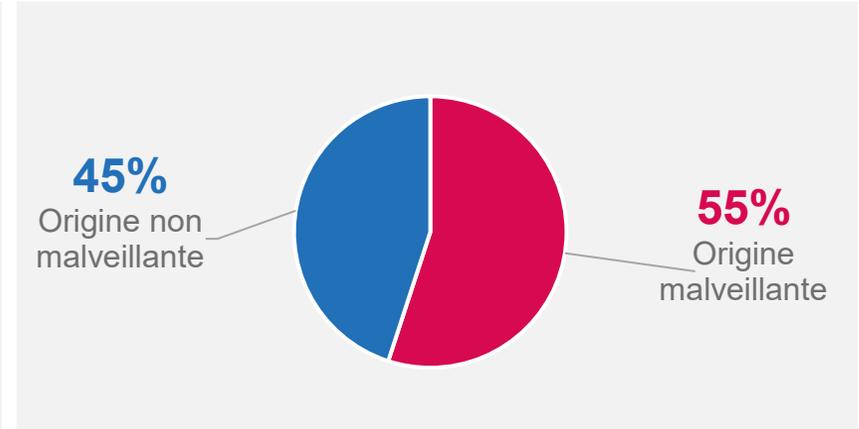
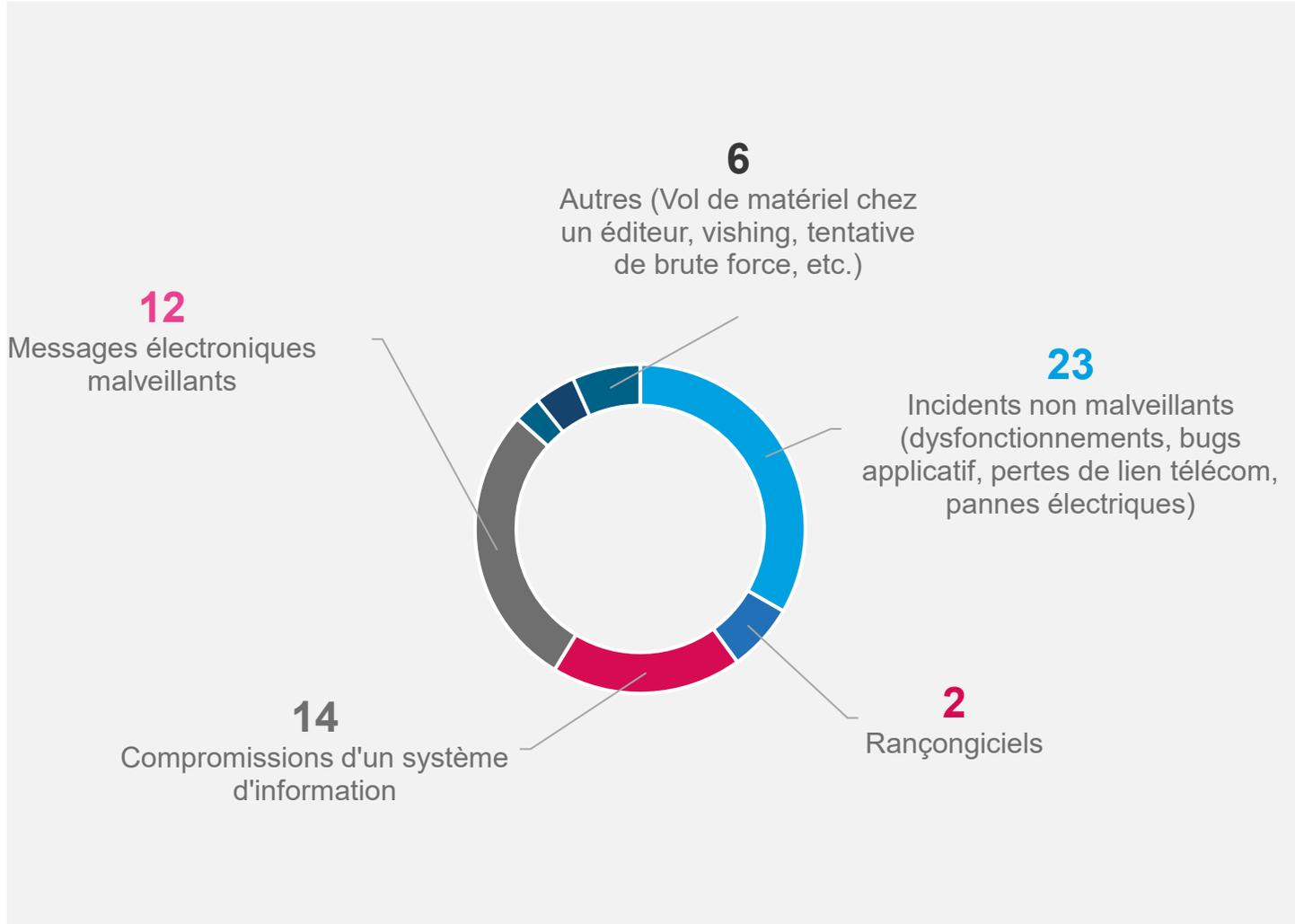
**AGENCE
DU NUMÉRIQUE
EN SANTÉ**

La transformation commence ici 



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

Septembre 2025



Origine des incidents déclarés – Aout 2025

Messages malveillants et rançongiciels



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



Fuite d'informations patients suite à la compromission d'un compte utilisateur sur l'outil régional due à une faiblesse dans la fonctionnalité d'auto-habilitation. Cette dernière a été désactivée suite à l'attaque



Attaque par un rançongiciel «.HEnisAhvA» suite à la compromission du compte VPN (compte de maintenance) entraînant le chiffrement intégral de l'ensemble des fichiers du SI. L'attaque a exploité les vulnérabilités de la machine virtuelle SRV-AD (Windows Server 2019 Standard) à l'aide de l'outil Mimikatz



Attaque par le rançongiciel «.Hush» suite à la compromission par bruteforce d'un compte d'accès RDP exposé sur Internet entraînant le chiffrement intégral du SI