



AGENCE
**DU NUMÉRIQUE
EN SANTÉ**

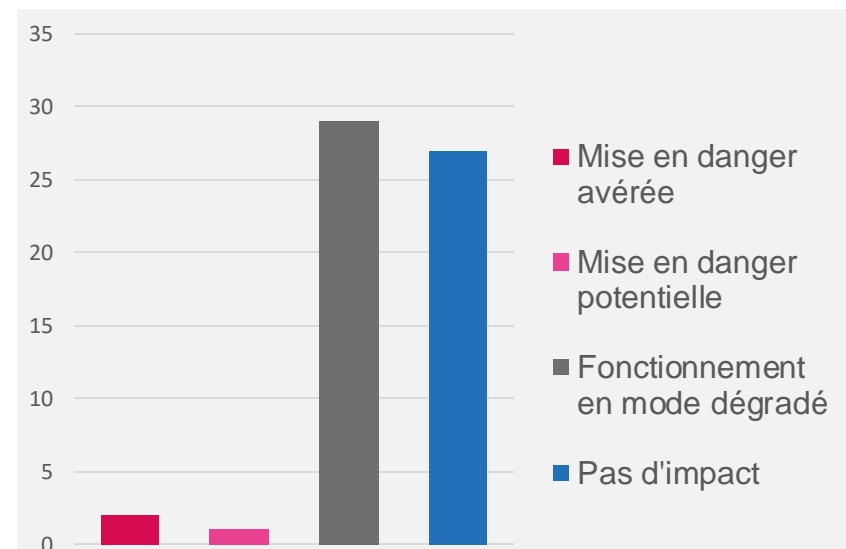
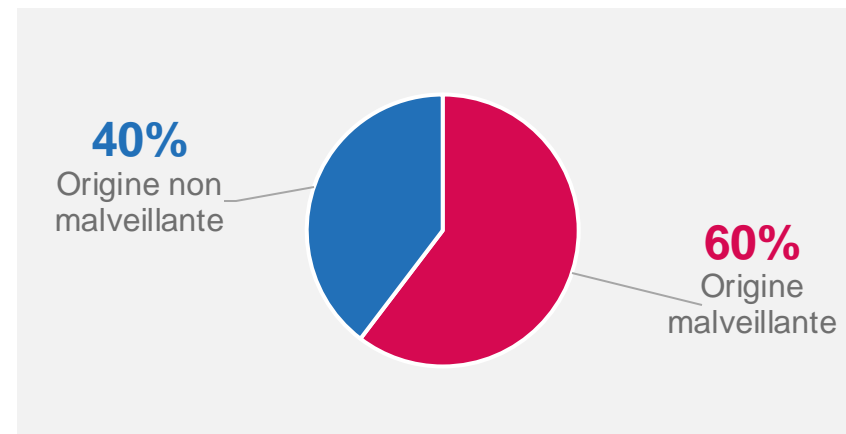
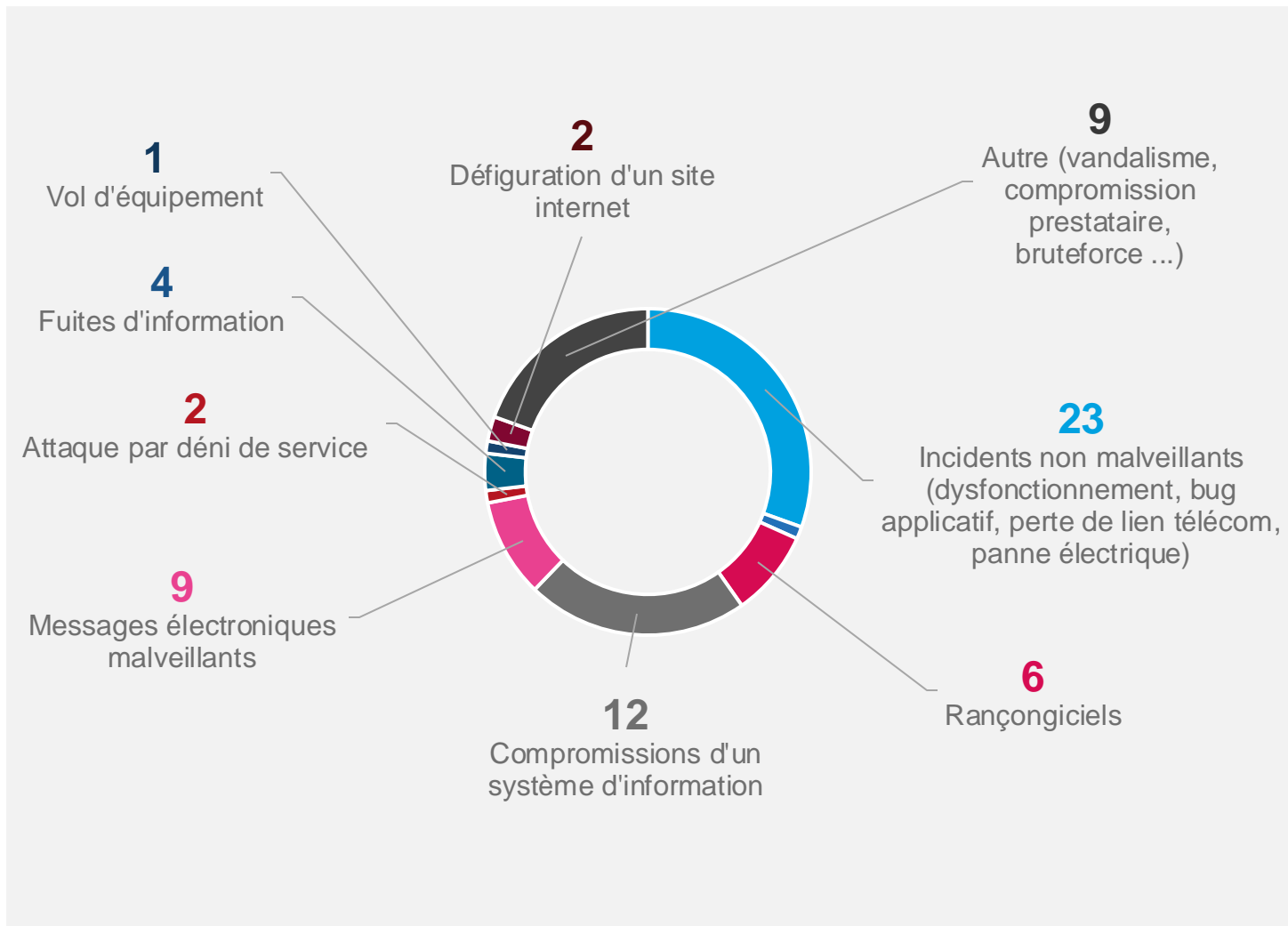
La transformation commence ici 



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

Décembre 2024

Origine des incidents déclarés – Novembre 2024



Origine des incidents déclarés – Novembre 2024

Message malveillants, logiciels malveillants, défiguration de sites web et rançongiciel



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



Défiguration d'un site web suite à la compromission d'un compte entraînant l'exposition sur Internet de données RH (CV et informations personnelles candidats)



Attaque par cryptovirus suite à l'exploitation d'une vulnérabilité Zimbra (CVE-2024-45518) chez un prestataire affectant le service de radiologie de plusieurs établissements



Attaque par rançongiciel suite à l'exploit d'une vulnérabilité Zyxel (CVE-2024-7261) entraînant le chiffrement d'un serveur métier ainsi que ses données.

Rançongiciels



Attaque par rançongiciel Waiting à la suite de la compromission d'un poste de travail entraînant le chiffrement de serveurs de fichiers



Attaque par rançongiciel suite à la compromission d'un compte VPN lié à la faiblesse des identifiants et à une version obsolète de Fortinet, entraînant l'impossibilité d'accès aux applicatifs



Attaque par rançongiciel suite à l'exploitation d'une faille de sécurité des Pare-feux entraînant le chiffrement de données ainsi qu'une fuite d'informations



Attaque par le rançongiciel Makop suite à la compromission d'un compte VPN sur un serveur en cours de décommissionnement n'ayant pas d'impact sur l'établissement car le serveur était isolé du réseau