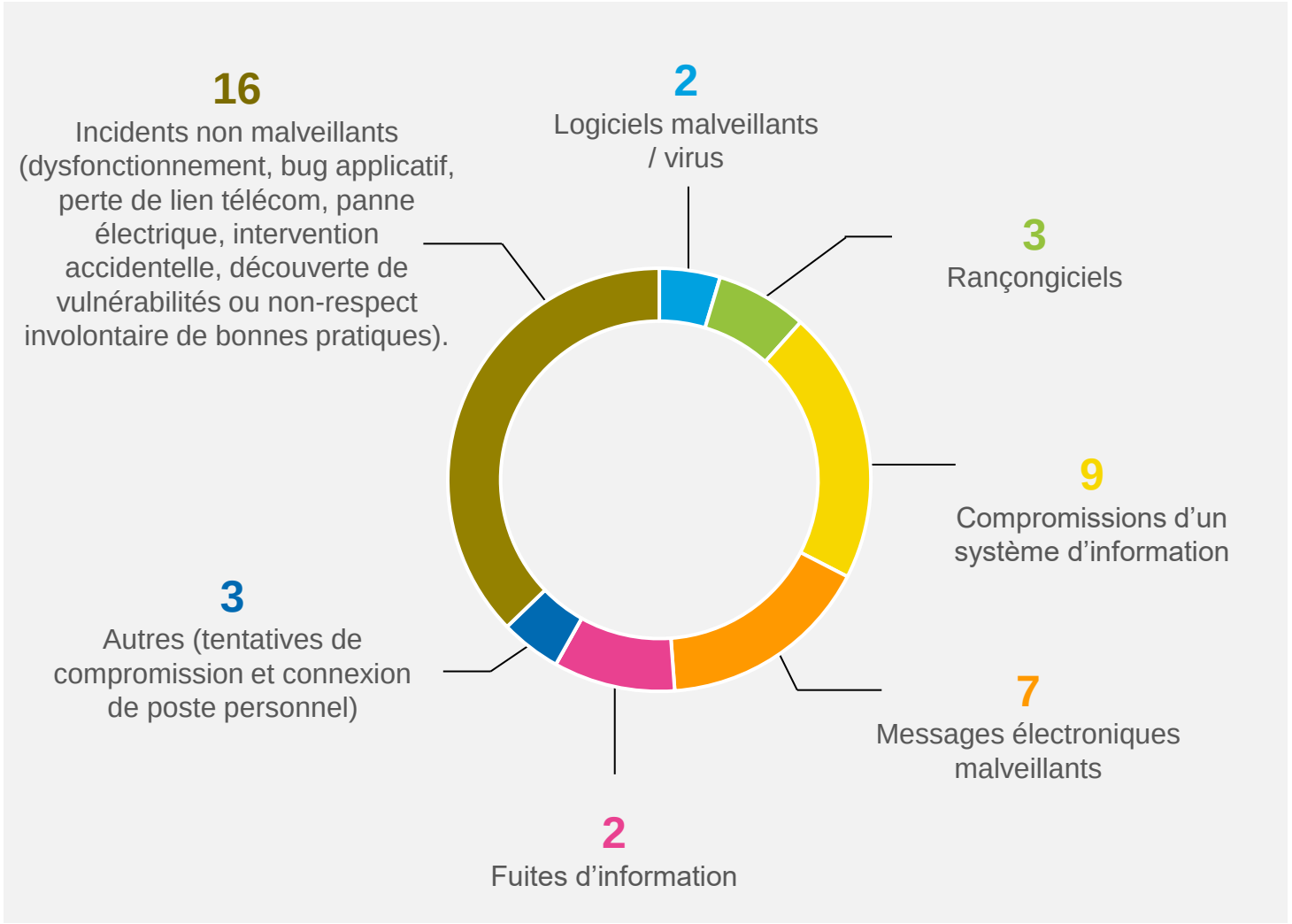
AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Indicateur mensuel sur l'origine des incidents déclarés

CERT Santé

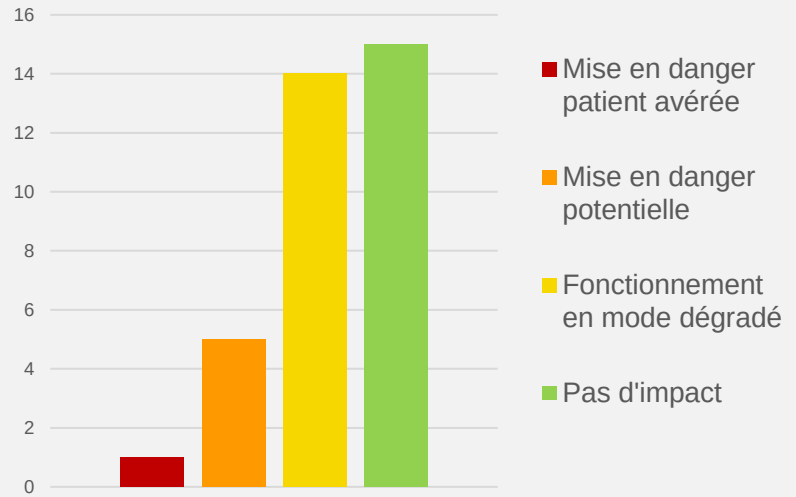
Mars 2023

Origine des incidents déclarés – Février 2023



51 %
Ont une origine malveillante

49 %
Ont une origine non malveillante



Origine des incidents déclarés – Février 2023

Compromission d'un système d'information, logiciels malveillants et rançongiciels :

Comptes de messagerie compromis via des messages malveillants de type phishing.

Compromission de comptes d'administration de domaines AD et d'un serveur RDP sans latéralisation ni exfiltration de données

Attaques par les rançongiciels *Elbie* et *Babyk* ayant abouti au chiffrement des services socles du SI (hyperviseur, sauvegarde, etc..)

Exploitation d'une faille VMware ESXi (CVE-2020-3992 et CVE-2021-21974) ayant conduit à l'indisponibilité et la défiguration d'un site web