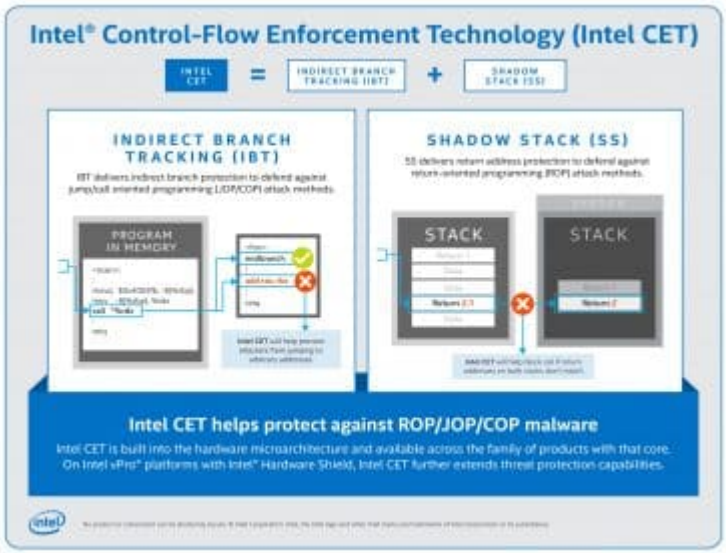
# Intel CET : débuts confirmés sur Tiger Lake

On l'attendait, c'est désormais officiel : Intel CET deviendra réalité avec les puces Tiger Lake*.

Cette technologie de sécurité est censée parer au détournement des flux de contrôle des programmes.

Les attaques ainsi fondées sont d'autant plus difficiles à déjouer qu'elles exploitent du code déjà présent en mémoire exécutable.

Pour les éviter, CET utilise deux éléments.
D'un côté, l'IBT (suivi de branche indirecte), pour empêcher la manipulation des sauts ou des appels.
De l'autre, une « shadow stack », pour bloquer la manipulation des adresses de retour.




La « shadow stack » consiste en une pile supplémentaire, distincte de la pile de données, et qui stocke une copie des adresses de retour des éléments en mémoire.
Si, pour un appel, l'adresse n'est pas la même que dans la pile de données (ce qui signifiera qu'elle a été manipulée), ledit appel est bloqué.

Intel avait publié les premières spécifications de CET en 2016.

L'implémentation sur Windows se nomme « hardware-enforced stack protection ».
Les développeurs peuvent en expérimenter la mise en place au sein de leurs applications à condition d'être sur l'anneau rapide du programme Insider.

** On attend les puces Tiger Lake, gravées en 10 nm, pour cette année.*

*Illustrations © Intel*