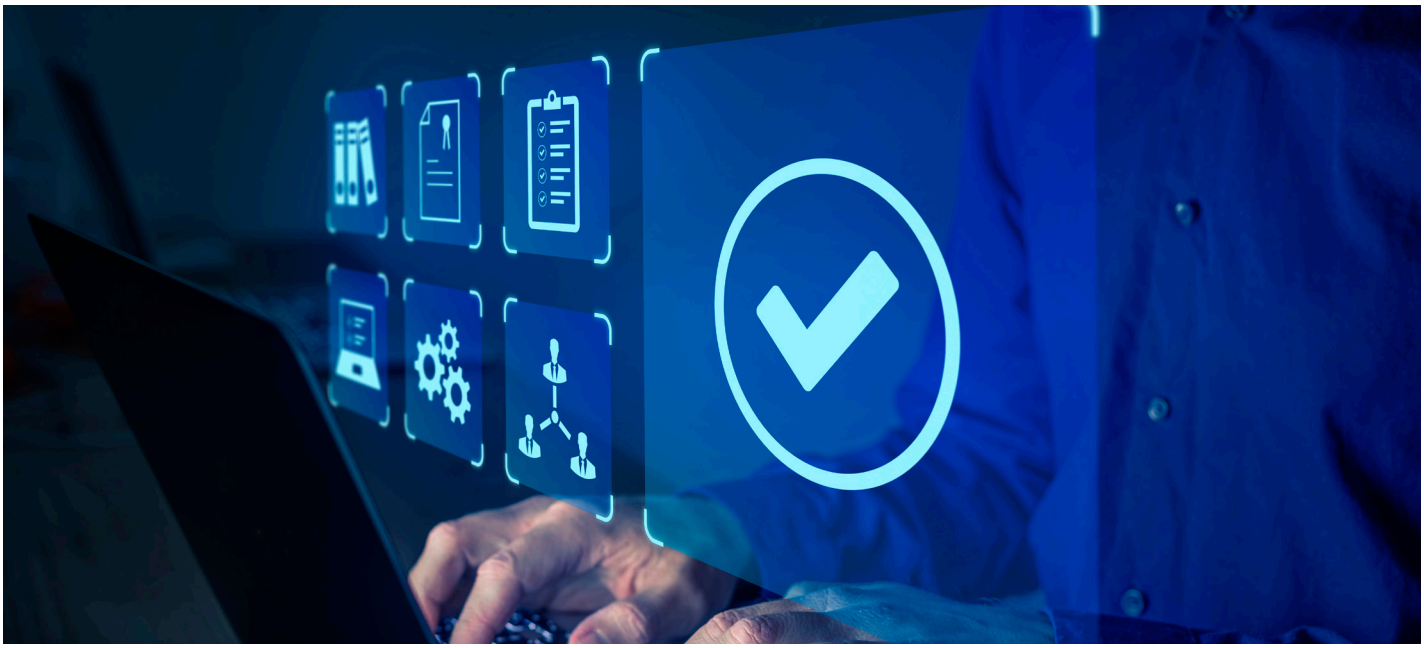
Présentation

Gestion des risques et du personnel

Dell Technologies s'efforce d'entretenir une culture de la confiance et de la sécurité au sein de ses collaborateurs à l'échelle mondiale. Nous avons conscience des risques que peuvent engendrer, volontairement ou non, les « initiés » de confiance et nous avons mis au point des programmes complets conçus pour détecter, dissuader et éviter ces types d'incidents de sécurité.



Formation et sensibilisation

Nos collaborateurs jouent un rôle clé dans notre approche globale de la sécurité. De l'intégration aux bulletins d'information mensuels, en passant par la formation annuelle et les campagnes de sensibilisation spéciales, nous informons régulièrement nos collaborateurs sur les risques de devenir involontairement des initiés, sur la façon de se prémunir contre ce danger et sur les conséquences d'un comportement à risque en matière de sécurité. Nous incitons les membres de l'équipe à reconnaître et à signaler les risques liés à la sécurité tout au long de leur carrière.

Une formation spécifique au rôle est requise pour les membres de l'équipe disposant de rôles ou d'un accès spécialisés, tels que les développeurs et les administrateurs IT. Une formation ponctuelle est fournie aux membres de l'équipe qui participent à des événements qui les exposent à un risque de sécurité accru. Une sanction progressive est appliquée à l'encontre des personnes qui manifestent un comportement à risque, qui peut inclure des conséquences financières et entraîner un licenciement.

Sécurité tout au long du cycle de vie des collaborateurs

Il est essentiel d'embaucher les bonnes personnes. Tous les collaborateurs sont sujets à une étude approfondie de leurs antécédents avant de rejoindre notre équipe. La création d'une main-d'œuvre de confiance permet de répondre à la fois aux exigences de sécurité de Dell et de nos clients.

En outre, nous utilisons une analytique et des technologies avancées afin d'alerter notre équipe de sécurité en cas d'activité d'initié inhabituelle provenant de toute personne disposant d'un accès fiable à nos systèmes et informations, en s'appuyant sur notre centre des opérations de sécurité avancé 24h/24, 7j/7.