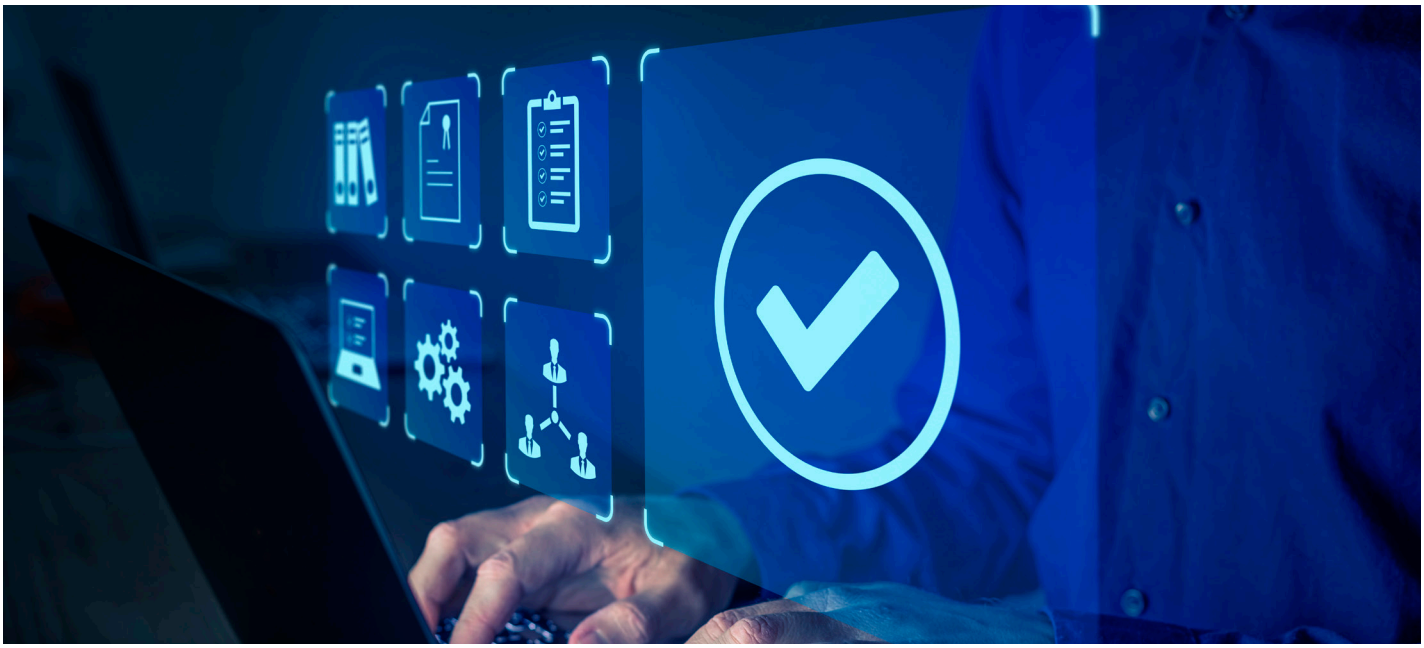
Übersicht

Mitarbeiter- und Risikomanagement

Dell Technologies konzentriert sich auf eine Kultur des Vertrauens und der Sicherheit in der weltweiten Belegschaft. Wir sind uns der Risiken bewusst, die von vertrauenswürdigen „Insidern“ – sowohl wissentlich als auch unwissentlich – ausgehen können. Wir haben umfangreiche Programme entwickelt, durch die diese Art von Sicherheitsincidents erkannt, verhindert und vermieden werden sollen.



Schulung und Sensibilisierung

Unsere Teammitglieder sind ein wichtiger Bestandteil unseres allgemeinen Sicherheitsansatzes. Vom Onboarding über monatliche Newsletter bis hin zu jährlichen Schulungen und speziellen Sensibilisierungskampagnen – wir informieren Teammitglieder regelmäßig über die Risiken, die einen wissentlichen Insider erwarten können, wie diese Gefahr verhindert werden kann, und die Folgen von riskantem Sicherheitsverhalten. Wir ermutigen Teammitglieder, Sicherheitsrisiken während ihrer gesamten Karriere zu erkennen und zu melden.

Rollenspezifische Schulungen sind für Teammitglieder mit spezialisierten Rollen oder besonderem Zugriff erforderlich, z. B. EntwicklerInnen und IT-AdministratorInnen. Just-in-Time-Schulungen werden Teammitgliedern angeboten, die an Veranstaltungen mit einem höheren Sicherheitsrisiko teilnehmen. Progressive Disziplinierung wird für diejenigen durchgesetzt, die riskantes Verhalten zeigen, einschließlich finanzieller Auswirkungen und potenzieller Kündigung des Beschäftigungsverhältnisses.

Sicherheit während des gesamten Mitarbeiterlebenszyklus

Die Einstellung der richtigen MitarbeiterInnen ist entscheidend. Alle MitarbeiterInnen durchlaufen eine eingehende Hintergrundprüfung, bevor sie in unser Team aufgenommen werden. Der sorgfältige Aufbau einer vertrauenswürdigen Belegschaft trägt dazu bei, die Sicherheitsanforderungen sowohl von Dell als auch unserer Kunden zu erfüllen.

Darüber hinaus setzen wir fortschrittliche Technologien und Analysen ein, um unser Sicherheitsteam zu alarmieren, wenn bei einer Person mit vertrauenswürdigem Zugriff auf unsere Systeme und Informationen ungewöhnliche Insideraktivitäten beobachtet werden, was durch unser fortschrittliches Security Operations Center unterstützt wird, das rund um die Uhr besetzt ist.