

社員とリスクの管理

デル・テクノロジーズでは、世界各地の全社員に対して信頼とセキュリティの文化を重視しています。私たちは、信頼できる「インサイダー」によって、故意かどうかを問わずリスクが引き起こされる可能性があることを理解しており、そのようなセキュリティ インシデントを検出、阻止、防止するために広範囲に及ぶプログラムを考案してきました。



トレーニングと意識の向上

Dellのチームメンバーは、セキュリティアプローチ全体において重要な役割を担っています。オンボーディングから月刊ニュースレター、年次トレーニング、特別な啓発キャンペーンまで、チームメンバーには、無意識のうちにインサイダーになるリスクとその危険を防ぐ方法、リスクの高いセキュリティ行動の結果について定期的に教育しています。Dellでは、チームメンバーがキャリアを通じてセキュリティリスクを認識し、報告することを奨励しています。

開発者やIT管理者など、特別な役割やアクセス権を持つチームメンバーには、役割固有のトレーニングが必要です。より高いセキュリティリスクにさらされるイベントに参加するチームメンバーには、ジャストインタイムのトレーニングが提供されます。財務的影響や解雇の可能性など、リスクの高い行動を示す社員には、段階的な懲戒処分が適用されます。

社員のライフサイクル全体にわたるセキュリティ

適切な人材を採用することは非常に重要です。社員はチームに加わる前に、詳細な経歴審査を受ける必要があります。信頼できるワークフォースを注意深く構築することで、Dellとお客様の双方のセキュリティ要件を満たすことができます。

さらに、当社は高度なテクノロジーと分析を活用し、システムや情報にアクセス権を持つユーザーによる異常なインサイダーアクティビティが観察された場合は、セキュリティチームにアラートが送信されます。こうした体制は24時間365日稼働している先進的なセキュリティオペレーションセンターによって支えられています。