サイバー攻撃からの復旧

インシデントの発生後、効果的かつ効率的に運用を回復しましょう。

包括的なセキュリティ リカバリー戦略

攻撃による影響の軽減 → セキュリティ侵害を受けたサービスとデバイスの再構築 → 運用の回復 → インシデントの分析と学習

サイバーセキュリティの成熟度を高めるためのステップ

1. **インシデントの封じ込め**
   影響を受けたシステムをネットワークから切断し、セキュリティ侵害を受けたアカウントを無効化することで、さらなる被害を阻止します。
2. **システムやデバイスの回復**
   セキュリティ侵害を受けたシステムを再構築、ソフトウェアを再インストールし、セキュリティ パッチとアップデートを適用します。
3. **データの復旧**
   バックアップからデータを回復する、あるいはデータを復旧するための特別な手法を利用することで、紛失したファイルや暗号化されたファイルを取得します。
4. **フォレンジック分析**
   今後のインシデントを阻止するため、攻撃のメカニズムと悪用された脆弱性を調査します。
5. **インシデント対応の評価**
   復旧後、プロセスを評価し、強化する必要がある領域を特定します。
6. **AI/MLの活用**
   影響を受けたシステムとデータを迅速に特定し、バックアップからの回復プロセスを自動化することで、復旧を加速化します。

サイバー リカバリーにはチームとしての協力が必要です。

プロフェッショナルなサービスとパートナーシップ
サイバーセキュリティ パートナーは、以下の有益な専門技術とリソースを提供してくれます。

- フォレンジック分析
- 侵害の原因の特定
- 今後のインシデントを回避するための対策

包括的なサイバーセキュリティ戦略の実施について、詳細をご覧ください。

e-bookを見る →

DELL Technologies