

Microsoft Sentinel導入支援

Microsoft Sentinelは、セキュリティ情報とイベントの集中管理、検出、対応を強化するためのクラウドベースのセキュリティ情報とイベント管理(SIEM)サービスです。お客様の要求事項に合わせ、以下のサービスを提供いたします。

実装できる内容

- セキュリティインシデントのリアルタイム検出と対応
- セキュリティデータの分析とダッシュボードの作成
- セキュリティレポートのカスタマイズ
- セキュリティイベントの自動化と応答
- クラウドベースのセキュリティ対策

実施内容・流れ

1. お客様の要求事項確認
2. セキュリティデータとログの収集と統合
3. カスタムセキュリティルールの作成
4. Microsoft Sentinelの導入とカスタマイズ
5. セキュリティテストとチューニング
6. ドキュメント納品



サービスのメリット

- セキュリティイベントの集中管理と迅速な対応
- Microsoftの高度なセキュリティツールとサービスの活用
- グローバルなセキュリティインテリジェンスと脅威インテリジェンスの統合
- セキュリティオペレーションと他のAzureサービスとのシームレスな連携