

Sentinel at Scale

Microsoft Sentinel を迅速に展開するための複数顧客向けワークショップ

FastTrack for Azure

概要: このデリバリー モデルは、Sentinel SIEM/SOAR ソリューションを既存の FTA エンゲージメントの一部として、または新規の実装として導入したいお客様を対象にしています。このデリバリー モデルは、2 時間のセッションで連続 4 日間行われ、最終的なゴールは使用可能なベースラインの Sentinel 実装です。お客様は FTA エンジニアと一緒に Sentinel を実装することになります。

お客様の要件

1. 既に展開されている Sentinel は存在しない
2. 単一のテナントに単一の Log Analytics ワークスペースを展開する
3. [必須] サブスクリプションの共同管理者権限、Azure AD のグローバル管理者権限、
[オプション] およびオンプレミスサーバーにエージェントをインストールする権限を持つユーザー
4. 各セッションの前に、特定の Azure ドキュメントを読むことが前提
5. 毎日 2 時間、4 日間連続で参加することができる
6. 他のお客様の前で、ご自身の技術環境について話すことができる（複数のお客様が参加するため）

事前学習

1. [MITRE Attack Framework](#).
2. [Microsoft Sentinel とは?](#)
3. Log Analytics の [概要](#) と [チュートリアル](#).
4. [Microsoft Sentinel Architecture](#).
5. [Kusto Query Language \(KQL\)](#)

セッションの概要

Day 1 導入とコネクタのオンボーディング	Day 2 分析 ルール	Day 3 インシデント調査、ハンドリング、脅威の探索
<ol style="list-style-type: none"> 1. アーキテクチャ 2. Log Analytics ワークスペース, RBAC. 3. コストと課金の構造 4. コネクタのオンボード <ol style="list-style-type: none"> a. Security Events/Syslog b. Azure Active Directory c. Azure アクティビティ 	<ol style="list-style-type: none"> 1. イベント、アラート、インシデント. 2. 分析ルールの解説 3. エンティティ 4. ルールの種類 5. UEBA の有効化 	<ol style="list-style-type: none"> 1. UEBA の理解 2. 脅威インテリジェンスの理解 3. 脅威のハンティング 4. ライブストリームとブックマーク 5. GUI を使用した調査
Day 4 ダッシュボード、ベストプラクティス		
<ol style="list-style-type: none"> 1. ウォッチリストの作成 2. ワークブック. 3. データのリテンション 4. ベストプラクティス 		

「FastTrack for Azure」は、「オンライン サービス条件」および「オンライン サービス データ保護補遺」の「プロフェッショナル サービス条件」の対象となる「プロフェッショナル サービス」です。本ドキュメントは、「現状有姿」で提供され、いかなる種類の保証も行いません。マイクロソフトは、品質、権原、非侵害、商品性、特定目的への適合性を含め、明示、黙示、法定を問わず、一切の保証を行いません。