Microsoft

# 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契約の一部として、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 5 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. サブスクリプションの共同管理者権限、グローバル管理者権限、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、5 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お話しいただける方（複数のお客様が参加するため）

### 事前に一読してください

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<br>導入とコネクタのオンボーディング | Day 2 Analytic ルール | Day 3<br>インシデント調査、ハンドリング、脅威の探索 |
|---|---|---|
| 1. アーキテクチャ<br>2. Log Analytics ワークスペース, RBAC.<br>3. コストと課金の構造<br>4. コネクタのオンボード<br>a. Security Events/Syslog<br>b. Azure Active Directory<br>c. Azure アクティビティ | 1. コネクタのベストプラクティス – Syslog,<br>2. WEF/WEC.<br>3. イベント、アラート、インシデント.<br>4. 分析ルールの解説<br>5. エンティティ<br>6. ルールの種類<br>UEBA の有効化 | 1. UEBA の理解<br>2. 脅威インテリジェンスの理解<br>3. 脅威のハンティング<br>4. ライブストリームとブックマーク<br>5. GUI を使用した調査 |
| **Day 4<br>ベストプラクティス と自動化** | **Day 5<br>KQL と Q&A** | |
| 1. ウォッチリストの作成<br>2. ワークブック.<br>3. データのリテンション<br>4. ベストプラクティス<br>5. プレイブックの展開 | 1. 基本的な KQL (top10/find/search/join).<br>2. コミュニティの利用<br>3. Q&A | |