ASM セキュリティ勉強会プラン

基本情報

- **時間**: 80 分（質疑応答 10 確認テスト 10 分含む）
- **対象**: 10-15 名程度
- **形式**: 企業規模を考慮した対面またはweb、動画での受講

必要機材/環境

- プロジェクター・スクリーン
- プレゼンテーション PC
- アンケートシステム（Microsoft Forms 推奨）
- 配布資料（PDF）
- 受講者用 Wi-Fi 環境
- zoom または Teams などのビデオ会議ツール

タイムテーブル

1. ASM の基礎（15 分）

- Attack Surface Management の定義
- なぜ ASM が必要なのか
- 攻撃表面とは何か
    - インターネットに公開されている資産
    - 外部から見える脆弱性
    - 潜在的な侵入経路
- ASM の具体的な実施方法

2. 攻撃者視点からの組織（15 分）

- 攻撃者が見る組織の姿
- 公開されている情報の種類
    - ドメイン情報
    - クラウドサービス
    - 従業員情報
    - その他デジタル資産
- 実際の攻撃事例紹介

3. シャドー IT のリスク（15 分）

- シャドー IT と ASM の関係性
- 把握されていない資産がもたらす脅威
- インシデント事例の解説
- 適切な管理の重要性

4. ディスカッション（15 分）

テーマ：「私の考える公開資産」

- 3-4 人のグループに分かれて討議
- 自部門で把握している公開資産の確認
- 参加者自身が考えるシャドーIT、公開資産の確認
- グループのためのルームを用意（ブレイクアウトルーム）
- グループ発表

5. 質疑応答（10 分）

6. 確認テスト（10 分）

運営上の工夫

1. 心理的安全性の確保

- 攻撃者視点の説明を通じた当事者意識の確立
- サイバーセキュリティ意識の向上
- 報告による改善の重要性の強調

2. 実践的な内容

- 実際の攻撃表面を例示する
- 具体的な脆弱性の解説
- 業務に関連した事例の紹介