

攻撃が実行不可能な状況を作りだす 『Morphisec』 概要資料



主な内容

企業が抱えるセキュリティ課題である「高度な攻撃に対する対策」と、「パフォーマンス・運用負荷」の視点からMorphisecの3つの特徴をご紹介している資料です。実際の導入事例についてもご覧いただけます。現在の課題やお困りごと、料金などについてはお気軽にお問合せください。

こんな方へおすすめしている資料です

1. セキュリティフレームワークからMorphisecがどのような役割かわからない方
2. なぜMorphisecがゼロデイ攻撃に対応可能か詳しく知りたい方
3. なぜ誤検知、運用負荷が少ないか詳しく知りたい方

目次

1. NIST サイバーセキュリティフレームワーク
 - 1-1. 脅威のフロー（フレームワーク上のMorphisecの役割）
 - 1-2. 企業が抱える課題
2. Morphisecとは
3. 攻撃手法に依存せず防御する(Moving Target Defense)
 - 3-1. Moving Target Defenseのコンセプト
 - 3-2. Windowsプロセスの仕組み
 - 3-3. Moving Target Defenseによる攻撃の防御
 - 3-4. Morphisec防御実績
 - 3-5. 攻撃イベント詳細画面
4. Microsoft Defenderを活用（Defender 連携機能）
 - 4-1. Morphisecとアンチウイルスの守備範囲の違い
 - 4-2. Microsoft Defenderとの組み合わせ
 - 4-3. Microsoft Defender との連携機能
 - 4-4. 管理コンソールダッシュボード
 - 4-5. Microsoft Defenderイベント詳細画面
 - 4-6. Windows OSセキュリティ機能ステータス表示
5. 導入後の運用負荷が低い
 - 5-1. Install & Forget
6. まとめ
7. 導入事例
8. 参考資料
9. お問い合わせについて

無料ダウンロード