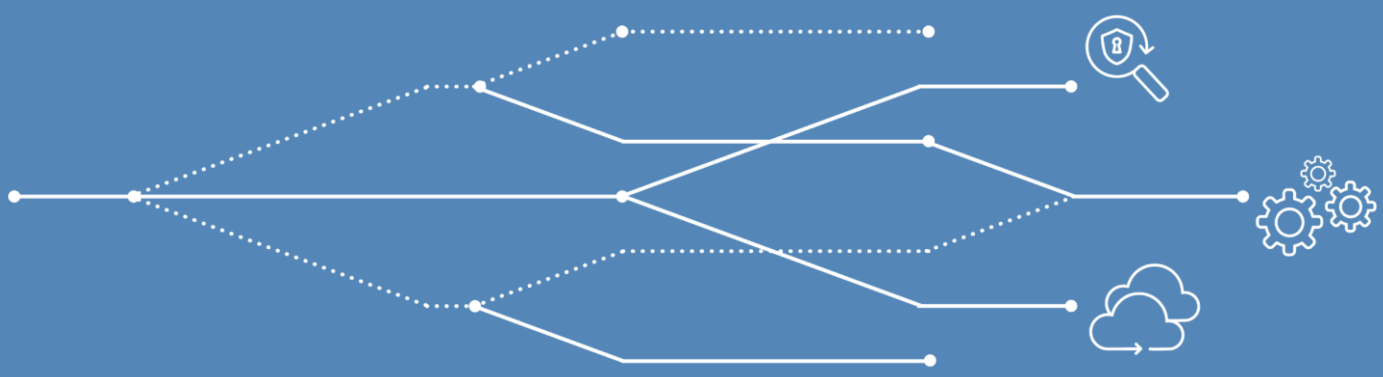

Awake Labs 展開&インテグレーション・サービス

セキュリティ = 人 + テクノロジー

このドキュメントでは、適切な販売サービス契約の条項に基づいて Awake Labs がお客様の代わりに行うサービスについて説明します。

アリスタの Awake Labs は、大規模なセキュリティ技術展開、ネットワーク・フォレンジック、脅威インテリジェンスについてエキスパートの専門知識を提供することにより、業界をリードするアリスタのネットワーク脅威検出・対応（NDR）技術の運用化を支援します。このアプローチは、ほかに例を見ないネットワーク可視化を実現し、アリスタのお客様のネットワーク・セキュリティ体制の強化、環境リスクの特定、セキュリティ・インシデントの低減、脅威アクターの活動の遮断を可能にします。

メリット

Awake Labs は次のサービスを提供します。

- お客様のニーズにタイムリーかつ効率的に対応できる実装を行うためのプロジェクト管理とコンサルティングのサービス
- お客様固有の環境とネットワーク構成に合わせた詳細な実装計画
- プロジェクトを完全に成功させ、影響を最小限に抑えるための実績ある展開手法
- お客様がプラットフォームを理解し、セキュリティのベスト・プラクティスを導入し、組織に関連する脅威を効果的に検出する方法を学ぶことを支援するエキスパート・チーム

段階的アプローチ

プロジェクト・キックオフ

プロジェクトのこのフェーズでは、次の項目をアリスタがレビューし、話し合います。

- エンゲージメント前チェックリスト
- プロジェクトの目標とマイルストーン
- お客様の環境の情報
- 計画と構成セッションのスケジュール
- プロジェクト計画活動の文書化

イネーブルメント

イネーブルメント・フェーズでは、次の項目を実施します。

設計

- システムの記述書と仕様書のレビュー
- 展開前の依存関係（ブラウザの要件やプラットフォームの制限など）のレビュー
- システムの機能（攻撃モデル、疑わしいドメイン、IOC、状況、Adversarial Modeling 言語に基づく脅威ハンティングなど）のレビュー
- 運用設計情報（ネットワーク通信ポートなど）のレビュー
- データ・フロー設計と認証メカニズムのレビュー
- バックアップと復旧のベスト・プラクティスのレビュー
- レポーティング・オーディエンスと標準（OOTB）レポートのレビューと定義
- アプライアンスのアップグレード、スキルおよびモデル構成のアップグレード、IOC のアップグレードのベスト・プラクティスのレビューと定義
- SIEM へのログ記録のレビューと定義
- サード・パーティ製品（エンドポイント脅威検出・対応、オーケストレーション、チケッティング・システムなどのソリューション）との連携の構成のレビューと支援

テスト

テストには次のものがあります。

- ユーザー・ロール・アクセスのセットアップと検証
- スキルおよび攻撃モデル作成のセットアップと検証
- IOC インポートのテストケース
- モデル電子メール通知のテストケースとレポート

展開

Awake Labs のエキスパートが適用性に応じて Arista NDR Nucleus および Sensor を構成します。

- ネットワーク設定の特定と収集
- セットアップ情報（IP アドレス、サブネット・マスク、ゲートウェイなど）を使用したアプライアンスの構成
- 適切なデバイス情報（シリアル番号など）の文書化
- クラウド・インフラストラクチャへのアプライアンス接続の検証
- アプライアンス上でのサービスの実行の確認

エキスパート・チームは次のユーザー構成も支援します。

- アプライアンスにアクセスするユーザー・ロールの特定
- アカウント、電子メール通知、ダッシュボード構成の作成

基礎知識の伝達

Arista NDR プラットフォームがインストールされ、ネットワークを解析できるようにセットアップされたら、Awake Labs のエキスパートが次のトピックに関する基礎知識伝達セッションを提供します。

- Arista NDR プラットフォームの基礎知識
- このプラットフォームを使用したネットワーク・フォレンジックとインシデント対応
- 脅威ハンティングの基礎知識
- 高度な脅威ハンティング

運用化

このフェーズでは、環境におけるモデル一致モニタリングと脅威ハンティングに使用する標準運用手順とプロセスを支援します。

- イネーブルメント後に、例外、調整、高度な脅威ハンティングについて行われる対話型セッション
- 状況の調査とレポート
- スキル開発と検出調整のベスト・プラクティス
- 脅威ハンティングと調査に関するその他の知識伝達
- アリスタの TAC に製品に関する支援を求める手順

サービス成果物

このサービスでは次の成果物が提供されます。

日次または週次（あるいはその両方）のステータス・レポート：

- 完了した活動の概要
- 注意を要する問題点と次の報告期間の計画

テクノロジー・イネーブルメント：

- Arista NDR プラットフォームの基本構成と調整
- お客様のスタッフがこのプラットフォームを管理および保守するために必要な主要ドキュメントと知識の伝達
- 基本的なハンティング、攻撃モデルのセットアップ、および調査のためのスキル構成の支援

提供可能なサービス・レベル

サービス・レベル	サイズ	タイムライン
クラス I	5GB のネットワーク・トラフィック、センサー数最大 2	最大 1 週間
クラス II	10GB のネットワーク・トラフィック、センサー数最大 10	最大 2 週間
クラス II インクリメンタル*	10GB のネットワーク増分	スケーラブル（最大 2.5 日間）
スタッフ派遣 1	すべてのアプライアンスが対象	3 か月間
スタッフ派遣 2	すべてのアプライアンスが対象	1 年間
ヘルス・チェック	すべての既存のアプライアンスが対象	なし（1 年に 1 回を推奨）

これらのサービスの料金と詳細については、アリスタの担当者または awake@arista.com までお問い合わせください。

* お客様のネットワーク・トラフィックが 10GB 増えるごとにインクリメンタル・アドオンが必要です。

** 事前に必要な場合を除き、プロセスの概要を記載したサービス記述書は、お客様との最初のキックオフ・コールの際に提供されます。

*** スタッフ派遣には、カスタムの SOW が必要になります。

**** 交通費・経費（T&E）SKU は別になります。

アリスタネットワークスジャパン合同会社

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル　27F
Tel:03-3242-6401

西日本営業本部
〒530-0001　大阪市北区梅田 2-2　ヒルトンプラザウエストオフィスタワー　19F
Tel: 06-6133-5681

お問い合わせ先

Japan-sales@arista.com

www.arista.com/jp

2021 年　11 月 29 日