Crowdstrike
導入支援/運用支援サービス

CrowdStrike × DigitalArtsConsulting

ここ数年で働き方が大きく変わっていく中で、セキュリティの考え方も大きく変わってきています。
例えば、リモートワークの対応をどうしよう？社内と社外のセキュリティは？そんな近々の課題に直面しているという担当者の方も少なくないかと思います。
そこで、ゼロトラストの仕組みを導入しよう！となっても、では実際どうするべきなのか？と考えると意外と考えなくてはならないことがあることに気づくでしょう。
そこで、i-FilterやM-Filterなどのセキュリティ製品の開発や運用に長年携わってきた弊社のセキュリティ領域のノウハウを持っている弊社と一緒に、EDR製品の導入を検討してみてはいかがでしょうか？

製品の特長

1. 様々な種類の端末、サーバ、ネットワーク機器に対応

- OSを問わず、オンプレとクラウドによる取り扱いの違いも基本的にありません。
- 導入端末にAgentをインストールするだけで、各端末への仕様変更も基本的にありません。

2. オールインワンのエンドポイントセキュリティ

- 従来型のAntiVirus対策だけでなく、振る舞い検知やファイルレス攻撃など、未知の脆弱性への対応もCrowdSttikeだけで対応できます。
- AIを実装しており、ビッグデータと人工知能を有効に活用し、お客様に素早く可視性を提供することができます。
- CrowdStrikeでは24時間365日体制で日夜未知との脅威を人の目を通して積極的に探索しています。CrowdStrikeの選りすぐりの脅威ハンター集団が24時間365日体制で目を光らせ、ほかのソリューションでは検知できないような脅威をとらえます。

3. ISMAP基準のセキュリティ支援

「Information system Security Management and Assessment Program（ISMAP）（イスマップ）」とは、国が主導している「政府情報システムのためのセキュリティ評価制度」のことです。
今後、セキュリティ基準の標準となりうる指標です。マルウェア対策では下記3点が重要視されていますが、CrowdStrikeならば包含可能です。

①「マルウェアに対する検出・修復ソフトウェア」について
②「情報セキュリティに対する認識」
③「システムへの適切なアクセス・変更管理についての管理策」

デジタルアーツコンサルティングに依頼するメリット

CrowdStrike技術者による導入のサポート

- CrowdStrikeの導入に必要な環境の確認や実際のインストール作業を一括で対応
- お客様のご希望に沿った動作設定を実施することが可能

SOC運用面での長期的なサポート

- CrowdStrikeを導入後のチューニングやアップデートなど定変更や運用をご支援。
- ノウハウがないと厳しいアラート対応や脅威対応などをサポート

サービス内容

CrowdStrike導入のご支援として大きく2つの工程に分けて提供いたします。

導入支援	構成のご提案から利用開始までの4フェーズに対してのご支援に加えて、スムーズな利用開始のためのお問い合わせ期間まで設けております。
運用支援	Crowdstrikeの導入完了後の運用面でのご支援を行います。日々のアラートや脆弱性対応などのSOC業務をまとめて対応いたします。ご要望によりカスタマイズしての対応も可能です。

導入支援

①テスト導入フェーズ

	工程	サービス内容
1	Poc、PoVの実施	• 動作に必要となる初期設定を実施します。 • PoC、PoVなどご要望に併せた検証を支援いたします。
2	Agent展開支援	Agentインストールを行う際のQ&A対応を行います。

②要件定義・設計・設定

	工程	サービス内容
1	要件定義・設計	• お客様のシステム環境を細かくヒアリング • システム構成にあった導入方法をご提案 • 要件確認と設計を実施します。成果物として弊社フォーマットでの要件定義書と設計書を御提出します。
2	設定作業	要件定義と設計の内容を踏まえ、必要な設定変更作業を実施します。
3	運用設計	CrowdStrikeの運用設計を行います。

③テスト運用

	工程	サービス内容
1	チューニング対応	• 発生したアラートに対し必要に応じてチューニングを実施します。 • アラートに対して対応方針の検討と対応を定期的に実施します。
2	Q&A対応	お問合せに対し回答をいたします。

運用支援

	業務範囲	サービス内容
1	SOC/マネージドサービス	• 発生したアラートに基づくチューニングや、CrowdStrikeで必要となる設定変更作業を代行して実施します。 • 危険度の高いアラートに対し弊社エンジニアにて解析を行い管理者へ通知します。
2	お問い合わせ対応	お問合せに対し回答をいたします。

本サービスに対するお問い合わせ先

デジタルアーツコンサルティング CISOサービス事業部
ismap-pro@con.daj.co.jp

デジタルアーツコンサルティング株式会社
東京都千代田区大手町1-5-1 大手町ファーストスクエア ウエストタワー14F
Tel: 03-6206-3421