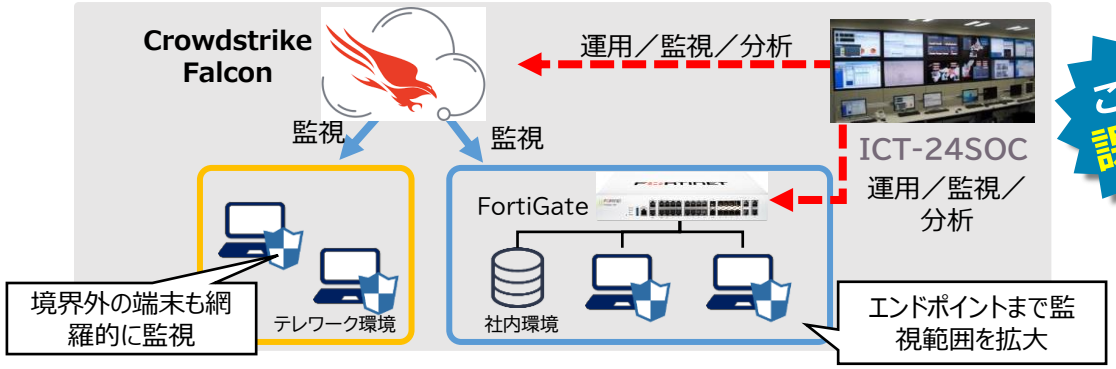
FortiGateSOCサービス プラスEDRオプション（CrowdStrike　Falcon）

FortiGateの外部接続ポイントの監視と端末（Endpoint）監視の併用により、働く環境に依存しない総合的なセキュリティ対策を支援します



こんな課題に

端末のセキュリティを強化したいが、運用業務の負担が大きい。

サービスメニュー	摘要
簡易分析および通知	発生したアラートをICT-24 SOCにて簡易分析、通知
エンドポイントの隔離	Falconセンサー導入済みの端末をNWから切り離し
詳細分析	インシデントの影響範囲や発生経緯等の特定に向けた詳細分析
回復支援	環境の復旧に向けた推奨案を提示CrowdstrikeFalcon上で実施可能な推奨案の実行を代行
問い合わせ対応	各問い合わせへの回答

価格（税込）

お問合せ下さい。

EDRのみのご契約も可能です。
UTMについては、FortiGate,PaloAltoの組み合わせが可能です。

アナリストがCrowdStrikeの分析機能を活用

CrowdStrikeのアラート通知による分析に加えて必要ならば、CrowdStrikeのコンソールから端末のプロセスやプログラムの履歴も含めて分析します。これにより、マルウェアの侵入経路の観点も含めて分析します。

macOS,Linux端末も対応

Windows以外のLinuxやmacOSなどの端末の監視も対応しています。

EDRが導入できない社内端末の監視

社内環境でEDR導入が出来ないFAX機器などのマルウェア感染時の異常な通信も社内環境との外部接続ポイントに設置したFortiGateで監視します。

詳細・お問合せ
https://www.ntt-at.co.jp/product/fortigate-soc/edr/crowdstrike/

対象業界：全ての業界

提供形態： 運用

セキュリティ

NTT AT