IR & Forensic

アラート抽出・対応・報告時の課題

1. 制御/決裁システムへの攻撃対応遅延⇒サービス不履行、経営責任
2. インシデント対応遅延による被害拡大⇒株価低落、経営責任
3. インシデント報告不備によるブランド力低下⇒株価低落、経営責任

ソリューション

エキスパートの育成、インシデントの優先順位付け、迅速な対応及び、そのエビデンス、各ステークホルダーへの報告が行える仕組みを提供する

Why DAC

1. ワークフローの作成支援、C-SIRT業務の改善支援等、SOC運用に関わる業務支援が行える
2. 既存のSIEMや各セキュリティデバイス連携、アナリスト同士のコミュニケーション、各ステークフォルダ向けレポート作成等、一つのUIでSOC機能が完結できるプラットフォームが構築できる
3. 導入後も継続的な品質を担保するための“自動化作業の振り返り”、機能追加等のカスタマイズサポートが行える

SOC運用に関わる業務支援

導入後も継続的な品質を維持

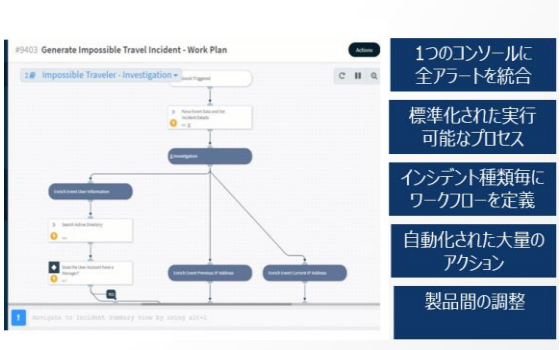
一つのUIでSOC機能を完結

サービス概要

ディスカッション&調査(Why DAC)

・C-SIRT各役割・外注業務調査
・自社資産の棚卸
・情報保管・検索・共有・伝達
・インテグレーション可否調査
・脆弱性対策が必要な部分の調査

インテグレーション(Palo DEMISTO)



・既存環境を１つのUIにインテグレーションし、UIの使い勝手を確認
・IRのワークフロー化、対応、対応記録の使い勝手を確認
・求めるレポーティングのカスタマイズ性を確認

カスタマイズ(Why DAC)

・コンサルタントとエンジニア常駐により、システムでカバーできないワークフロー作成、導入/マイグレーションプランを策定
・顧客のROI、リスク診断を考慮したPoC実施、各ステークフォルダ向けのレポート作成を支援

継続的品質担保(Why DAC)

・ワークフローの自動化後、変動制の高い業務への定期的な振り返り・改善を支援
・インテグレーション対象外のシステムや既存の設定変更等、Playbookのカスタマイズを実施
・システム全体の調査と関しを継続して実施

本資料に関するお問合せ
デジタルアーツコンサルティング株式会社
デジタルソリューション事業部
〒100-0005 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WEST 14階
TEL: 03-6206-3421（代表）
mail : info@con.daj.co.jp