Business content

Consulting Business

コンサルティング事業

セキュリティコンサルティング —— P1

サイバーセキュリティ診断 —— P3

人 材 提 供 —— P5

セキュリティリスク分析サービス

お客様のご要望に応じて、現状を可視化するセキュリティリスク分析サービス
“V-Sec” の結果に基づいたセキュリティ強化実装に関しても総合支援が可能です。

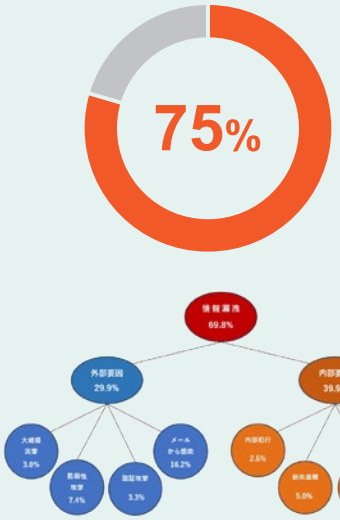
V-Sec | Visualizing Security は「IPA 情報セキュリティサービス基準適合サービスリスト」に掲載されています

STEP - 0

V-Sec IC Initial Check

無償提供

現状の情報漏洩
発生確率を算出



STEP - 1

V-Sec ST Standard
NIST SP800-171・ISO27001ISO27002・高度サイバー攻撃対処のためのリスク評価等のガイドライン、個人情報保護法など

V-Sec FA Factory
工場におけるサイバー・フィジカル・セキュリティ対策ガイドライン、自工会ガイドライン

V-Sec HO Hospital
医療情報システムの安全管理に関するガイドライン

本調査		分析・報告
Standard	**Premium**	**Standard**
・ネットワーク図の把握 ・ヒヤリング実施	・ネットワーク図の把握 ・ヒヤリング実施 ・現場視察 ・現場担当者ヒヤリング ・ギャップ分析	・脆弱性可視化 ・現状課題 ・強化の方向性 ・推奨セキュリティ対策のご提案

ひと目で分かりやすい報告書と、リスクとコストを考慮したセキュリティ対策ロードマップ。

STEP - 2

V-Sec SS Security Support

セキュリティ対策実装支援

- セキュリティ対策実装支援
- セキュリティ設計
- セキュリティポリシー策定
- ソリューション導入支援
- CSIRT サービス
- 段階的人材育成支援

＋

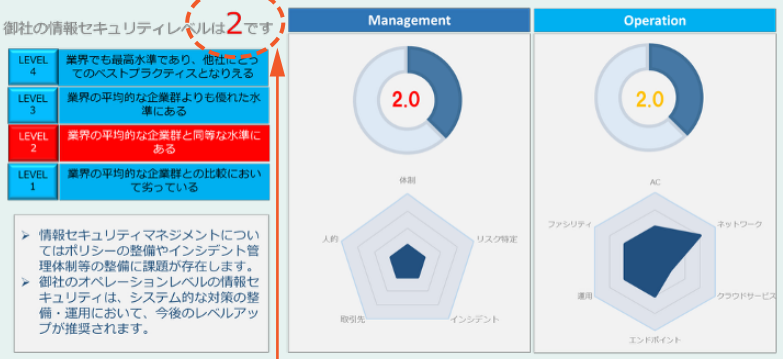
継続運用支援

- セキュリティ検知支援
  SOC サービス

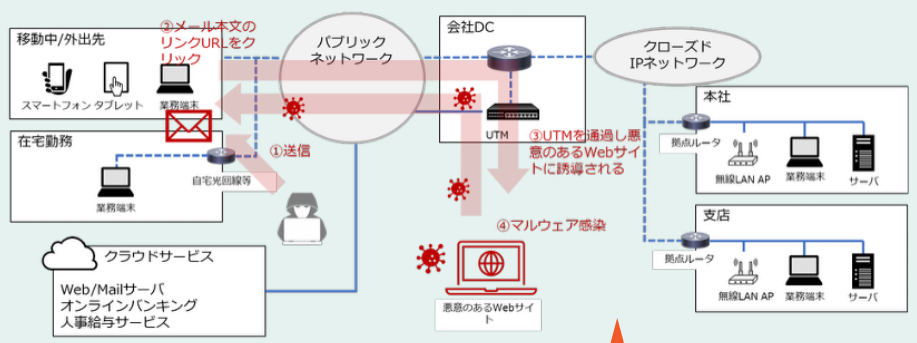
V-Sec により脆弱性を可視化

自社セキュリティレベルを可視化することで、
最新のサイバー攻撃に対応した対策立案や費用対効果の高いセキュリティ対策が可能です。
また、経営層にも理解いただきやすい視覚的な報告書を納品します。

総合評価



想定リスクシナリオ

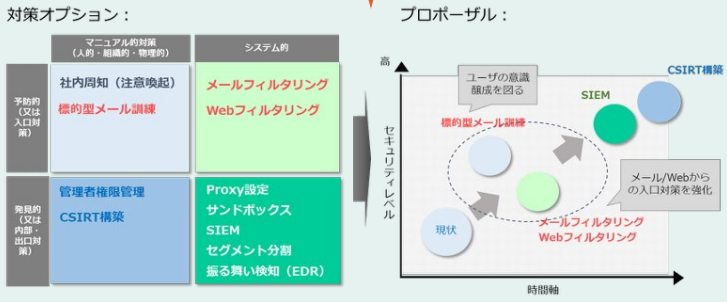


現状対策評価

No.	タイトル	関連システム	検出事項	懸念領域	対策優先度
2-1	認証認可の脆弱性	各種クラウドシステム	認証サーバは分散されており、また各種のクラウドサービスのユーザはシステム担当者が個別に登録している状況であった。	権限や公開範囲の設定ミス等が生じると権限外の者への情報漏えいにつながる。また、退職者等のアカウント削除等の漏れが生じる危険性が高まる。例えば退職者のSaaSアカウントが残ったままで、退職後にアクセスされてしまうケースなどが考えられる。	Mid
2-2	ネットワークセキュリティ対策	全システム	Webサイトの閲覧に関する制御がされていなかった。	不正なサイトにアクセスしたり、ファイルをダウンロードしてマルウェアに感染する。	High
2-3	エンドポイントセキュリティの脆弱性	USBメモリ	USBメモリに対する端末側の制御はされていないため、従業員が私物のUSBメモリを使うことができる状況であった。	マルウェアが仕込まれたUSBメモリを知らないうちにPCに挿入してしまい、端末がマルウェアに感染する恐れがある。内部不正によりファイルサーバから顧客情報や図面情報が持ちだされる危険がある。	High
2-4	クラウドサービス利用に関する脆弱性	各種クラウドシステム	組織として許可していないクラウドサービスの利用を監視、制御するための機能が存在しなかった。	個人アカウントのクラウドサービスに顧客から預かった情報をアップロードし、個人の端末にダウンロードする等のケースや個人アカウントの更改範囲の設定ミスにより情報が想定せずに外部公開されてしまうケース等が考えられる。	Mid

誰にでも分かりやすい表記

対策選択肢の提示

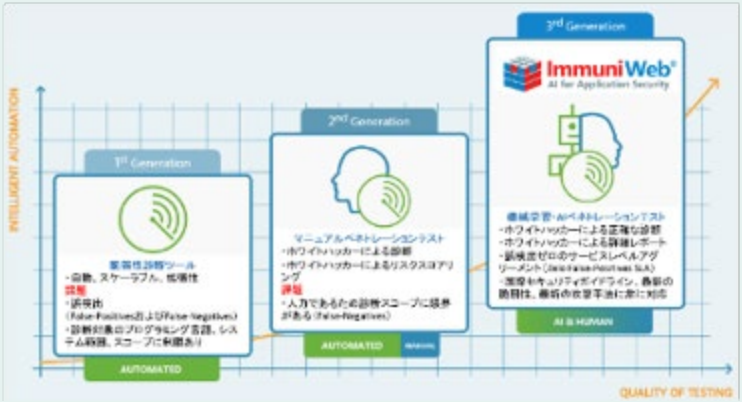


具体的で想起しやすい例示

脆弱性診断（多彩な脆弱性診断プログラム）

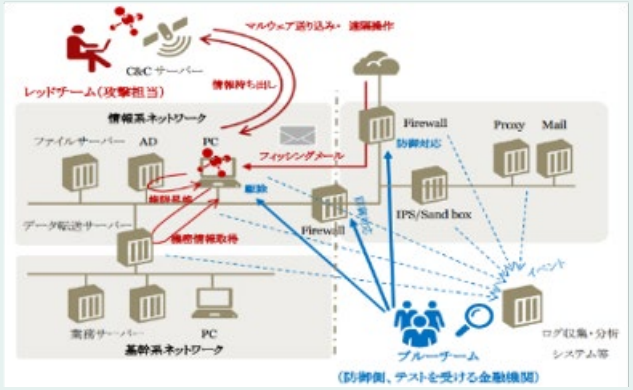
AI × ホワイトハッカー脆弱性診断 ImmuniWeb®

国内診断実績数 1,200 サイト以上。圧倒的なスピードで Web/ モバイルアプリの危険度の高い箇所を優先的に AI が診断し、高いコストパフォーマンスを実現。複数サイトの診断にも強みを発揮、新世代の脆弱性診断。



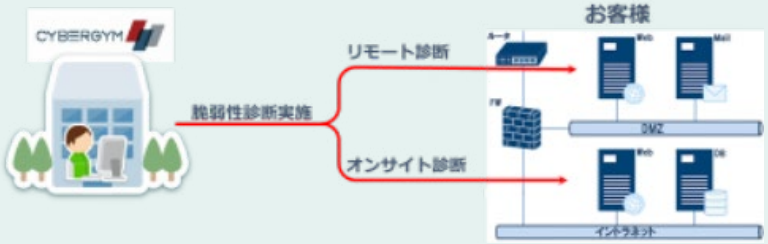
脅威ベースのペネトレーションテスト『TLPT』

侵入シナリオの網羅的なテスト。経験豊富なホワイトハッカーによる侵入テストにより、侵入拡大の調査、セキュリティ製品の検知状況、インシデントレスポンス能力など、多層防御能力を評価します。



ホワイトハッカーマニュアルハイブリッド診断

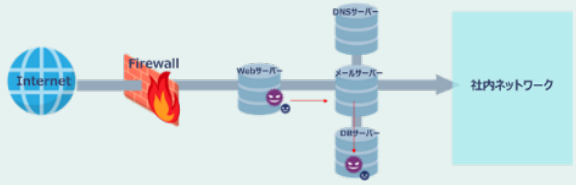
経験豊富なホワイトハッカーによる侵入シナリオの網羅的なテスト。
攻撃者視点による細部への診断ツールと手動（マニュアル）テストを組み合わせることにより、あらゆる脆弱性に対応しています。



ホワイトハッカーによる侵入侵害調査

【侵入調査】・・・ホワイトハッカーがネットワーク内への侵入調査を実施します。実際に攻撃者が Web アプリケーション等の脆弱性を利用して、貴社ネットワークへの侵入が可能かを調査します。

【侵害調査】・・・PC がマルウェア感染した 場合に、どこまで侵害範囲 が拡大するのかを調査します。



AIプラットフォーム脆弱性診断 ImmuniWeb

CYBERGYM の脆弱性診断“ImmuniWeb”は世界で高評価の次世代診断です
世界トップクラスの脆弱性データを蓄積
WEB サーバテスト 4,000 万件以上 / モバイルアプリテスト 50 万件以上

AI とホワイトハッカーの最適分担

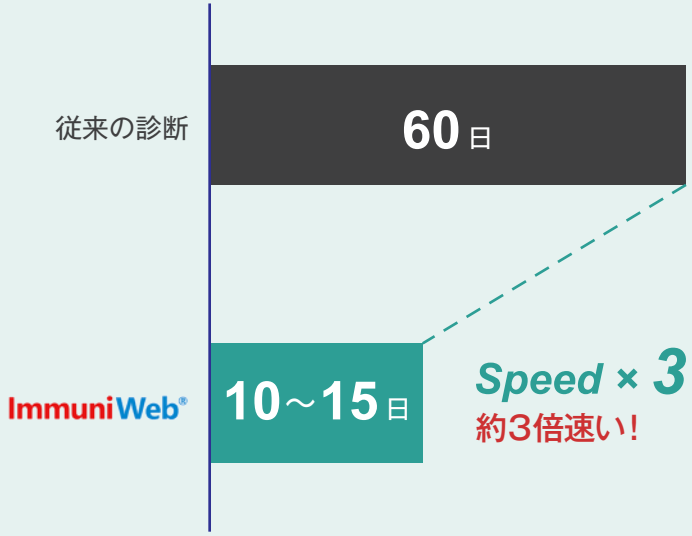
従来の診断

- 人力では診断範囲に限界あり
- エンジニアのスキルに依存

ImmuniWeb®

- 最新かつ豊富なデータを蓄積した AI が危険度の高い箇所を優先的に診断
- セキュリティスペシャリストのホワイトハッカーが適切に誤動作や誤検知を防止

診断時間を大幅短縮



高品質を低価格で

AI とホワイトハッカーの
最適な役割分担

セキュリティ検査費用
平均 **50%**削減

※従来の中・大規模アプリケーション診断手法との比較(当社比)

経験豊富なコンサルタント（人材）の提供

GBS
グローカルビジネスソリューションズ株式会社

サイバーセキュリティでのお客様の抱えているお悩み・課題を解決するため、経験豊富なコンサルタントをご提供いたします。

※期間等別途お打合せ

パートナー様

お客様

サイバーセキュリティでのお悩み・課題

・基本方針、ポリシー、手順作成等の策定
・教育、ツール、対策、シュミレーション
・イシンデント対応　等