Enterprise solutions provided by CITYASCOM



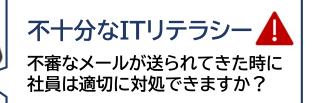
知らず知らずのうちに高まるセキュリティリスク

放置された脆弱性 古いバージョンのOSやソフト ウェアを放置していませんか?

設定ミス

不要なポートがネットワーク 機器に設定されたままになって いませんか? 把握していないIT資産

インターネット上に公開された IT資産を把握していますか?



攻撃者の視点で調査を実施 御社のセキュリティ対策を総合的に評価し、レポートを作成します

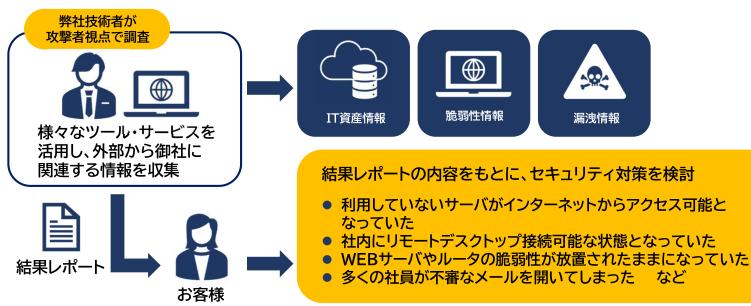
IT資産状況	ポート開放状況	脆弱性状況	SSL構成状況
メールアカウント 認証情報漏洩状況	IPA情報セキュリティ 自社診断	標的型攻撃メール訓練	
株式会社シティアスコム 営業本部 営業戦略部 ☎092-852-5130 ⊠sales@city.co.jp			

Enterprise solutions provided by CITYASCOM





インターネット上に公開されているIT資産について、「不要なポートの開放」「脆弱性の放置」「SSL 設定の不備」といったセキュリティリスクを調査します。合わせて、メールアドレスをもとに「ID・パ スワード」などのクレデンシャル情報が漏洩していないかを調査します。



他社と比較して、セキュリティ対策はどのレベルなのか? どこから対策を行うべきか?総合的に評価します!

評価項目	詳細	標準価格
IT資産状況	インターネットからアクセス可能な御社のIT資産(サーバ、ルータ等)を 調査します。	
ポート開放状況	インターネットからアクセス可能な御社資産に不要且つ危険性のある ポートが開放されていないかを調査します。	
脆弱性状況	インターネットからアクセス可能な御社資産に脆弱性がないかを調査 します。	
SSL構成状況	御社WebサーバのSSL構成状況に脆弱性がないかを調査します。	500,000円
メールアカウント 認証情報漏洩状況	御社社員が利用しているサービスの認証情報が漏洩していないかを 調査します。(※メールアドレスのリストをご提供いただきます)	
IPA情報セキュリティ 自社診断	IPAの診断項目にご回答いただき、御社の強化ポイントを抽出します。 (※25項目の診断にご回答いただきます)	
標的型攻撃メール訓練	疑似攻撃メールの訓練を通じて、社員のセキュリティ意識向上に繋げます。	

※評価対象の公開資産のアセットは10までとします。 ※価格は税抜きです。

※メール訓練の送信先<u>メールアドレスは100まで</u>とします。

類似サービスとの違い

①ASM

攻撃者の視点から、攻撃対象 となり得るデジタル資産を継続 的に監視、変化を通知 ②脆弱性診断

既知の脆弱性を検出する ツール/サービス ①②を含む幅広い 項目で現状を把握!

本サービス

Enterprise solutions provided by CITYASCOM