protiviti®
Global Business Consulting

サイバー脅威インテリジェンスを活用したセキュリティ強化支援

サイバー攻撃者と潜在的なサイバーリスク情報を収集・分析し、短期的／長期的な改善策の策定や実行を支援します。

進展するサイバー脅威情勢の中で、企業は多くの課題に直面しています。

リソースが豊富なサイバー攻撃者

サイバー攻撃者は、膨大なリソースと時間を使い、グローバル規模で特定組織の偵察活動を行い侵害を試みます。

リソースが不足しがちなサイバー防衛者（企業）

自社がなぜ狙われるのか、侵入や攻撃に利用される自社のIT資産は何なのかを把握するのは難しく、対策を検討・実行する要員も不足しています。

求められる対応と解決すべき課題

防衛者側は、自社のサイバーリスクや脅威情勢を把握するため、さまざまなソースやツールから情報を収集・分析・評価することが求められています。

要員のトレーニングや複数のツールの維持運用にかかるコストは高額で、専門のリソースを雇用することも困難です。

プロティビティが提供する価値

01 攻撃者視点から見える自組織のリスクの把握

- 外部からの視点で、企業やサプライチェーンへの攻撃に悪用可能なリスクの高い外部公開資産やデジタルフットプリントを特定
- 攻撃者に悪用される前に、企業がリスク低減策を実施することをグローバルレベルで支援

02 自組織にとっての攻撃者の特定と理解

- 企業や企業が属する業界、所在国を対象に活動している脅威主体やその活動、動機、TTP（戦術・技術・手順）、攻撃インフラの情報を分析
- 経営層や管理者層に対する脅威情勢の認識向上や、実務レベルでの能動的な技術的対策の検討を支援

03 インテリジェンスを活用した高度なセキュリティ対策

- 脅威やリスクを踏まえた次世代のサイバーセキュリティ戦略の立案
- SIEM/SOAR環境との連携による脅威の検知能力向上や、セキュリティ運用の高度化と効率化
- GRC基盤との連携によるインテリジェンスを活用したリスク管理

未認識のサイバー攻撃を受けるリスクを低減
プロアクティブなサイバー攻撃対策

プロティビティが提供するサービスの特長：次世代サイバーセキュリティ対策

プロティビティは、パートナーのCYFIRMA社が提供する外部脅威情勢管理プラットフォーム「DeCYFIR」のサイバー脅威インテリジェンスと、プロティビティが培ってきたサイバーセキュリティ強化のノウハウや技術的専門知識を活用し、脆弱性の根本原因の特定や洞察、短期的・長期的な改善策の提言を提供します。改善策の提言にあたっては、主要なソリューションやプロバイダーとのパートナーシップから、当該製品の専門家とともに、最適な改善策を導出します。

DeCYFIR：外部脅威情勢管理プラットフォームが提供する7つのインテリジェンス

攻撃者から見える自組織のリスクの把握

Attack Surface Discovery

外部攻撃対象領域の調査と把握

- 侵入口となりえる公開資産を調査・把握
- 未認識のシャドーIT、脆弱な高リスク資産を調査・把握

Brand Intelligence

ブランドに関するインテリジェンス

- 攻撃を受ける可能性のブランド・ドメイン調査
- 危険な類似ドメイン・SNSなりすましを特定

Digital Risk Discovery

デジタルリスクの認識

- 攻撃者に悪用される可能性がある情報漏洩、データ侵害、不適切なデータ露出を把握

Third Party Intelligence

サードパーティインテリジェンス

- 重要な取引先に関するアタックサーフェスやデジタルリスクを把握

自組織にとっての攻撃者の特定と理解

Situational Awareness

脅威情勢の認識

- 特定の国、業界に対する最新の脅威動向や攻撃シナリオを理解

Vulnerability Intelligence

脆弱性に関するインテリジェンス

- 特定の脆弱性を悪用する攻撃者、攻撃キャンペーン、ツールなどの洞察
- ゼロデイ脆弱性のニュース

Cyber Intelligence

CYFIRMA独自のサイバーインテリジェンス

- 特定業界や組織に対する攻撃者の攻撃キャンペーン、目的、TTP、インフラ等に関する洞察

サイバー脅威インテリジェンス関連サービス

		ご要望(例)	サービス内容	期間
01	**サイバー脅威インテリジェンスヘルスチェック**	• 攻撃者から見える自社の状況把握 • 優先すべき対策の特定	• インタビューおよびDeCYFIRのインテリジェンスにより企業の環境を分析 • 推奨するセキュリティ対策や優先度を付加したレポートを提示	2か月程度
02	**サイバー脅威インテリジェンス定期診断**	• 攻撃者から見える自社の状況把握 • 緊急対策の導入 • 改善状況の定期的な確認 • 委託先環境のセキュリティ評価	• インタビューおよびDeCYFIRのインテリジェンスにより企業の環境を1か月間分析し、レポートを提示 • 予め設定した期間で継続評価し、改善状況のレポートを提示 • オプションで委託先の分析レポートの提示も可能	1年以上 (四半期毎、または半期毎)
03	**サイバー脅威インテリジェンス継続モニタリング**	• 継続的なサイバー脅威インテリジェンスの活用 • 導入や運用に関するセキュリティ要員の不足	• サイバー脅威インテリジェンスの活用を導入から運用まで、要員を含め包括的に提供 • サマリーレポート(月次)、企業の環境・状況を踏まえた経営層(CISO)向けレポート(四半期毎)を作成 • 予兆を捉えたリアルタイムアラート発信	1年以上

CYFIRMA DECODING THREATS

プロティビティは、外部脅威情勢管理とサイバー脅威インテリジェンスのリーダーであるCYFIRMA社(サイファーマ社)と戦略的パートナーシップを締結しています。CYFIRMAのインテリジェンス主導のアプローチにより、プロティビティはサイバー脅威から保護するだけでなく、ビジネスのイノベーションと発展を促進するサイバーセキュリティ戦略をクライアントに提供します。

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。25ヶ国、85を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、デジタル、オペレーション、人材・組織、データ分析におけるコンサルティングサービスを提供しています。プロティビティは、米国フォーチュン誌の2023年働きがいのある会社ベスト100に選出され、Fortune 100の80％以上、Fortune 500の約80％の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティは、1948年に設立され現在S&P500の一社であるRobert Half International (RHI)の100％子会社です。

プロティビティLLC protiviti.jp

〒100-0004 東京都千代田区大手町2-6-4 TOKYO TORCH 常盤橋タワー 24F Tel. 03-4577-3980
〒530-0001 大阪市北区梅田2-2-2 ヒルトンプラザウエストオフィスタワー 18F Tel. 06-6450-9367

protiviti®