未来を拓くチカラと技術。

NTT AT

News Release

2021 年 1 月 28 日
NTTアドバンステクノロジ株式会社

標的型攻撃シミュレーションサービスを提供開始

ー標的型攻撃の脅威を感じているお客様や重要インフラ／顧客情報を扱うお客様向けー
～標的型攻撃（侵入から内部感染まで）の防御の成否をシミュレーションで事前に把握しセキュリティ対策の有効性を判断～

NTT アドバンステクノロジ株式会社（以下：NTT-AT、本社：神奈川県川崎市、代表取締役社長：木村丈治）は、Cymulate Ltd.（以下：Cymulate 社、本社：イスラエル、CEO：Eyal Wachsman）と代理店契約を締結し、Cymulate 社のサイバー攻撃シミュレーションプラットフォーム*1 を利用した標的型攻撃シミュレーションサービスの提供を 2021 年 2 月 1 日から開始します。

NTT-AT は、セキュリティビジネスを重点分野の一つと位置づけており、Web 診断、ペネトレーションテスト等の脆弱性診断サービスを提供してきましたが、標的型攻撃を実際に受けた際のセキュリティ対策の有効性評価や、内部侵入を受けた後の感染拡大フェーズにおける攻撃に関する診断までカバーできていませんでした。このたび、Cymulate 社のプラットフォームを利用した標的型攻撃シミュレーションサービスをラインナップに追加することにより、高度かつ多様なセキュリティ攻撃に対する診断の領域を拡大し、侵入から内部感染までをカバーしたセキュリティ対策の有効性評価を提供することができるようになりました。これにより既存のセキュリティ商材と組み合わせた更に高度なセキュリティソリューションの提供が可能となります。

今回 NTT-AT が提供を開始する標的型攻撃シミュレーションサービスでは、これまで NTT-AT が培ってきたインシデント対応／フォレンジック調査*2 の技術やノウハウ、Web 診断、ペネトレーションテスト、SOC サービス*3 における経験等を活かし、お客様のセキュリティ対策に対する NTT-AT 独自の目線でシミュレーション結果のフィードバックを行い、お客様が実施しているセキュリティ対策への指針を提示いたします。本サービスは、検査結果に対する評価の妥当性への疑問、検査までの長いリードタイム、発見されたばかりのセキュリティ脅威への対応の不安、セキュリティ要員の不足といったお客様が抱えるさまざまな課題解決に貢献します。

1. 背景

企業へのセキュリティ攻撃が増え続けている中で、多種多様なセキュリティ製品・ソリューションが世の中へ提供されています。しかしそれらの製品・ソリューションを適切に利用し設定しても、次々と発生する新たなセキュリティ脅威への対処は、手を緩めることはできません。

既存のセキュリティ診断（表 1）には、脆弱性の発見に重きを置く脆弱性診断や、お客様ごとにシナリオを作成し実際に侵入まで確認する脅威ベースのペネトレーションテスト、レッドチーム演習などがありますが、評価の目的によって取捨選択されているのが現状です。昨今のセキュリティ攻撃は高度化／多様化してきており、既存のセキュリティ診断をしておくだけでは十分とはいえない状況となってきています。また侵入経路や侵入手口ごとに網羅的に検査するのは多くの金銭的・人的・時間的コストがかかります。

表1　主なセキュリティ診断の概要と課題

	概要	課題
脆弱性診断	Web サイトや IP アドレスを対象に存在する脆弱性等を網羅的に検証	侵入後の影響については把握できない。
ペネトレーションテスト	実践的なサイバー攻撃手法を模して侵入を試み、脆弱性の確認と影響を検証	実践的なサイバー攻撃手法の準備等を行える人的リソースの確保が難しい。
レッドチーム演習	人／システム／施設を対象に事前に設定した目的を達成できるか総合演習で評価	準備負担が最も大きく、実施時に環境/サービスへの影響も懸念される。

2. 標的型攻撃シミュレーションサービスの概要と特長

NTT-AT が提供する標的型攻撃シミュレーションサービスは、お客様の社内システムに対して疑似的に攻撃を仕掛け、その成否をシミュレーションします。標的型攻撃の範囲は、侵入から内部感染の攻撃まで広く対応しています。NTT-AT では、攻撃シミュレーションにより得られるレポートをベースにこれまで培ってきたインシデント対応／フォレンジック調査の技術やノウハウ、SOC サービスにおける経験等を活かしてフィードバックを行い、お客様の今後のセキュリティ対策への指針を提示します。標的型攻撃の脅威を感じているお客様や重要インフラ／顧客情報を扱うお客様向けのサービスとなっています。

本サービスの概要および特長は次のとおりです。

(1) 多様な侵入経路に対して標的型の疑似攻撃を網羅的に仕掛け、お客様が実施しているセキュリティ対策の有効性を確認することができます。

(2) 仮に侵入を許してしまった際に、内部感染フェーズにおける内部からの攻撃に対するセキュリティ対策の有効性を確認することができます。

(3) シミュレーションによる検査結果は経営層向けのエグゼクティブサマリにより、現状のセキュリティ対策に関する投資効果や追加投資の判断にご利用いただけます。またセキュリティ部門向けの技術レポートによりセキュリティ軽減施策の適格性の継続的な評価にご利用いただけます。

(4) 自動化されたプラットフォームによるサービス提供のため、お客様の企業規模によらずご利用いただけます。また検査要員のスキルに依存しないため、技術水準を同一に担保して継続的な評価にもお使いいただけます。継続的な評価を希望されるお客様に対しては、サブスクリプション型での提供も可能です。

(5) 検査実施までのリードタイムを大幅に短縮することができます。また最新のセキュリティ脅威への対応が求められている中、その検査を短期間で評価することができることはお客様の大きな安心材料となります。

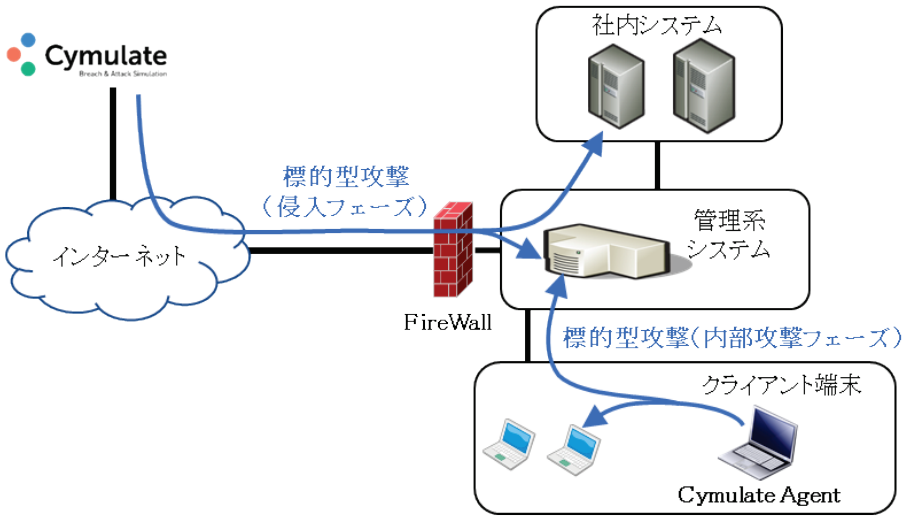

図1　標的型攻撃シミュレーションのイメージ

3. 提供開始日

2021 年 2 月 1 日

4. 提供価格

お客様のネットワーク環境やエンドポイント数などに合わせて最適なサービスを提案いたします。提案価格はその都度お見積りさせていただきます。また、詳細なレポートを所望されるお客様へのレポーティングサービスや初期導入支援サービスを提供いたします。

またサービス提供開始を記念し、2021 年 9 月末までのキャンペーンとして、特別価格で提供いたします。

参考：182 万円（500 エンドポイント数、4 回分のアセスメント）；　キャンペーン価格：145 万円（20% Off）

5. 今後の展開

NTT-AT では、国内セキュリティ市場、IoT 市場においても同様のニーズが潜在している現状を踏まえ、一般の企業様はもちろんのこと、金融・保険、製造、重要インフラ分野も含め、サイバー攻撃を遮断しなければならない多くのシーンに、本サービスを提供していく予定です。

■Cymulate 社について

Cymulate 社は、共同創設者兼 CEO の Eyal Wachsman と共同創設者兼 CTO の AvihaiBen Yossef によって 2016 年にイスラエルで設立されました。Cymulate 社の継続的なセキュリティ検証により、進化するセキュリティ脅威に対して、簡易かつ継続的に評価、最適化することができます。Cymulate 社の BAS（Breach and Attack Simulation）プラットフォームは簡単に使用でき、リスク評価に基づいた専門的な脅威インテリジェンスを提供します。また、お客様の環境やセキュリティポリシーに合わせて調整されたセキュリティ保証プログラムやホワイトハッカーにより作成され自動化されたレッドチーム演習を実現するオープンフレームワークも提供します。Cymulate 社は、セキュリティの専門家が動的な環境を把握して制御するのに役立ちます。

***1 サイバー攻撃シミュレーションプラットフォーム**

攻撃者が用いるさまざまな切り口のサイバー攻撃を自動化した BAS と呼ばれる攻撃シミュレーションプラットフォームです。高度セキュリティ人材不足の解消やテスト準備時間の短縮化を目的としており、侵入準備から侵入後までの一連のアセスメントについて非破壊的な検査を繰り返し実行することができます。

***2 フォレンジック調査**

発生したインシデントに対し、PC・HDD・スマホといった電子機器や記録媒体等から、サイバー攻撃や不正アクセスなどの被害状況を割り出す調査手法。

***3 SOC サービス**

Security Operation Center の略。24 時間 365 日体制でネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行うサービス。

※記載されている会社名および製品名等は、各社の商標または登録商標です。

【本件に関するお問い合わせ先】

NTTアドバンステクノロジ株式会社
セキュリティ事業本部
セキュリティサービス＆ソリューションビジネスユニット
BAS担当
https://www.ntt-at.co.jp/product/penetration_cymulate