

2017年2月16日

WideAngle マネージドセキュリティサービスにおいて 「プロアクティブ レスポンス」を提供開始

～インターネットなどからの不正アクセスを特定後、感染端末の通信を自動遮断～

NTT コミュニケーションズ株式会社(以下：NTT Com)は、総合リスクマネジメントサービス「WideAngle」のマネージドセキュリティサービス（MSS）において、社内システムへの不正アクセスを特定後、それにより感染した端末の通信を自動遮断するメニュー「[プロアクティブ レスポンス](#)」を、2017年2月16日から提供開始します。

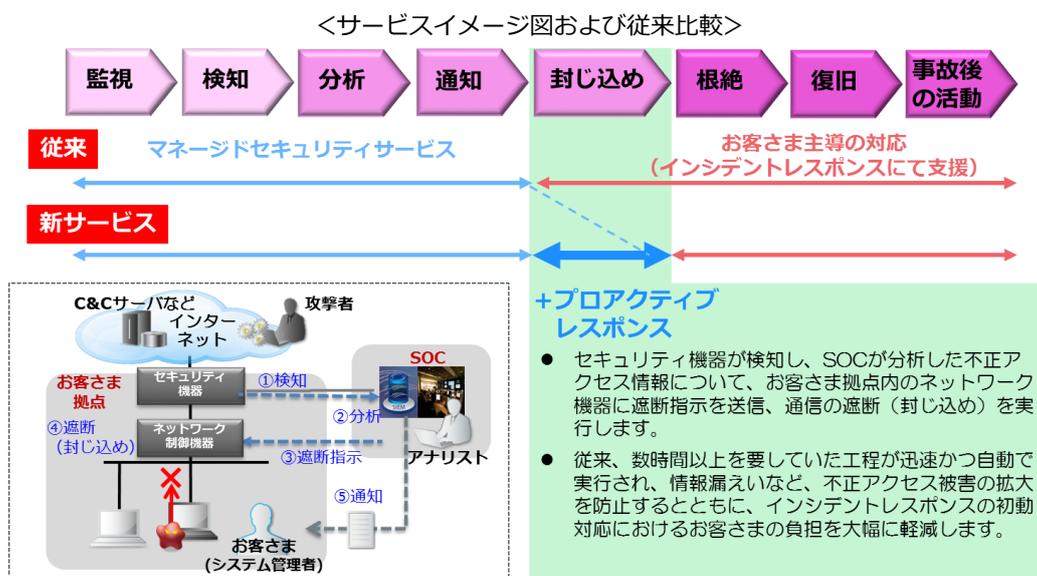
1.背景

企業の機密情報を詐取する標的型攻撃など、サイバー攻撃は巧妙化・増加の一途であり、ITセキュリティの監視業務における分析精度向上とリスクへの迅速対応は、被害を最小化するために非常に重要な要件となっています。

NTT Com はデータアナリストによるログ分析業務を支援する AI（人工知能・機械学習）を独自開発し、2015年10月よりマネージドセキュリティサービスの運用基盤（SIEM^{※1}）への搭載を進め、脅威を特定する精度の向上を進めると共に、その分析結果をもとに通信を自動遮断する機能の開発に取り組んできました。

2.概要

セキュリティオペレーションセンター（SOC）において、AI を搭載した SIEM およびアナリストにて詳細分析後、誤検知を排除した上で、特定した感染端末情報をもとに、お客さま拠点内のネットワーク制御機器に自動連携することで、感染端末の通信を迅速に自動遮断します。



(1)不正アクセス被害の拡大防止

端末単位でセキュリティ脅威を封じ込めることにより、業務全体への影響を最小限にした上で、原因・被害状況の調査や復旧対策が可能です。

(2)インシデントレスポンスのお客さま作業負担を軽減

従来、感染源情報を受領したお客さまにて速やかに実施することが求められていたインシデントレスポンスの初動対応である「封じ込め」を、SOC より迅速に実施することで、お客さま作業負担を大幅に軽減し、休日や夜間などの業務時間外における対応の遅れも回避できます。

3. 提供価格 (税抜)

初期費用 : 0 円

月額費用 : 280,000 円 (連携先ネットワーク制御機器 1 台あたりの月額費用)

※WideAngle MSS へのアドオンメニューとして提供するため、「NW セキュリティ」、もしくは「コンテンツセキュリティ」のバックメニュー契約が必要です。なお、各バックメニューのオペレーションレベルとしては、アナリスト高度分析(ナイト/スカイ)の契約が必要です。

※感染端末をより迅速に特定するため、プロキシーログを相関分析する「CLA (Correlation Log Analysis)」のアドオン契約を推奨します。

4. 提供範囲および提供開始日

日本国内にて、2017 年 2 月 16 日より提供開始予定

※連携可能なネットワーク制御機器は HPE 社製「Aruba ClearPass Policy Manager」です。

5.今後の予定

2017 年 3 月にネットワーク制御機器の対応機種ラインアップを追加予定です。また、ファイアウォールなどのセキュリティ機器との直接連携も今後予定しています。

(記載されている会社名および商品名は、各社の登録商標または商標です。)

※1 : Security Information and Event Management の略称。