マネージドセキュリティサービス最前線
第8回 ー 実例ベースで考える ー

未知の脅威を検知する
～独自開発の SIEM エンジン＋リスクアナリストによる相関分析～

NTT コミュニケーションズ㈱　経営企画部
マネージドセキュリティサービス推進室長
与沢 和紀

NTT コムセキュリティ㈱
オペレーション＆コンサルティング部
本橋 孝祐

連載 8 回目となる今回は、今年 6 月に報道発表を行った弊社 WideAngle マネージドセキュリティサービスにおけるセキュリティ脅威の検知率大幅向上について、運用実績を交えて紹介する。

従来のマネージドセキュリティサービス（MSS）の限界

突然ですが、あなたが不審人物を目撃したとする。その人物は如何にも怪しい装いにサングラス、派手な刺青でキョロキョロと周りをうかがいながら、あなたの隣人の家に侵入していった。もちろんあなたは警戒する。「110 番すべきか?」と迷うでしょう。しかし、本当に通報すべきでしょうか？

この場合、もし通報したとすると、それは「見た目」「玄関前での挙動」があなたの認識する「不審人物」のパターンと一致したということだ。

しかし、挙動不審な善人もいれば、装い正しく堂々とした犯罪者もいる。本当に危険な人物かどうかは、外見だけでは判断できない。

MSS も同じである。

一見怪しそうに見える正常通信、怪しそうにない不正通信は多々あり、その見極めの精度を高めるには多くの分析の視点が必要だ。しかし従来の MSS では、IDS/IPS のシグネチャやウイルスのパターンファイル、つまりセキュリティ機器が危険と判断したものに分析を依存していた。そのため、

①実際には危険だが脅威レベルが低いと判断されてしまった攻撃通信を無視しがち

②セキュリティ機器では検知できない未知の脅威は見逃してしまう

③逆に多くの怪しそうな通信に対するセキュリティ機器からの通知に振り回され、真の脅威の通知があっても見逃してしまう

など、機械的に行われる分析によって生まれる膨大な誤検知、それによる非効率な対応という問題があった。これらの 3 点が、従来の MSS の限界だと言える。

次世代 MSS、WideAngle による限界突破

では逆に、これらの課題を解決した理想の MSS とはどういうものであろうか？

それは、セキュリティ機器のつける危険度のみに過度に依存せず、セキュリ機器以外の Proxy サーバや認証サーバなどの動作ログも総合的に分析し、本当に脅威であるものだけを対応方法も含めて通知する MSS であると考える。それを実現するために我々がとったアプローチは、日々進化する検知ロジックを容易に実装可能な SIEM エンジンの開発と、リスクアナリストによる分析体制である。

では、具体的にどのようなアプローチを行ったのか、現場の実例をまじえて紹介する。

限界①：実際には危険だが脅威レベルが低いと判断

されてしまった攻撃通信を無視しがち

我々のセキュリティ運用基盤（SIEM エンジン）の特長は

・現場の現役リスクアナリストの経験（日々蓄積される攻撃パターンのロジック）を還元したルールセット
・NTT 研究所独自のマルウェア解析研究結果
・NTT Com 独自ハニーポット産のブラックリスト

など、セキュリティベンダの持っていない独自ルールを Dev-Ops 体制*で実現している点だ。

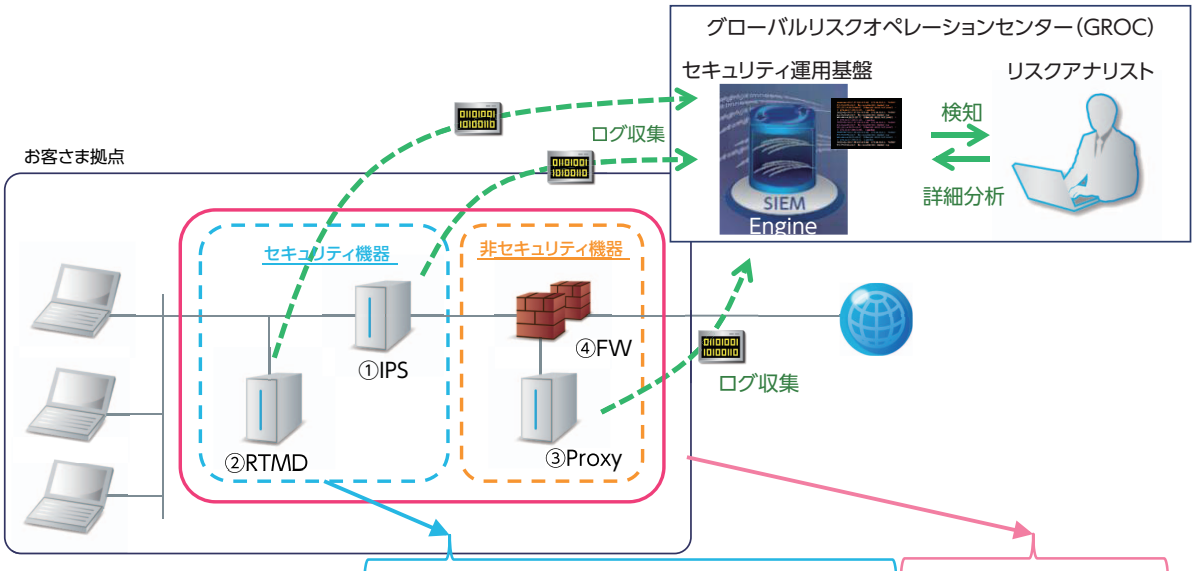
このようにベンダシグネチャ／パターンファイル以外に複数の分析観点を加えることで、危険な通信がハイライトされてリスクアナリストに届くようになる。

図 1 にあるように、現在 WideAngle を導入しているある顧客を例にあげると、Serious/Critical なセキュリティインシデント 39 件（50 日間）のうち、NTT Com 独自開発のセキュリティ運用基盤（SIEM エンジン）による検知をトリガーとしてリスクアナリストが分析したものは 33%にのぼる。

なお、NTT Com 独自開発のセキュリティ運用基盤による検知（33%）の内訳は、リスクアナリストの知見に基づき Dev-Ops で作成された「NTT Com 独自ルールセット」による検知が約半分の 54% を占め、「NTT 研究所独自ルール」の検知が 31%、「NTT Com 独自のブラックリスト」による検知が 15% という結果であった。

限界②：セキュリティ機器では検知できない未知の脅威は見逃してしまう

WideAngle では非セキュリティ機器を監視・分析



検知トリガー	①IPS	②RTMD	①②③④相関分析
Critical/Serious 脅威検知件数　39 件	21%	46%	33%

相関分析トリガー　内訳	NTT Com 独自ロジック	NTT 研究所 独自ロジック	NTT Com 独自ブラックリスト
Critical/Serious 脅威検知件数	54%	31%	15%

図 1　相関分析を用いたセキュリティ脅威分析の効果

マネージドセキュリティサービス 最前線

第8回 ー 実例ベースで考える ー

対象にすることを重視し、上述の「NTT Com 独自ルールセット」がそれを実現している。実際には、セキュリティと関わりのない膨大なログを避けるため、脅威につながるログをその独自ルールでピックアップし、IDS/IPS などのセキュリティ機器と非セキュリティ機器を流れるトラフィック並びに動作ログの相関分析が可能としている。

参考までに、対応事例の中から具体的な分析経過を以下に紹介する。

(1) ある顧客の社員が疑わしいサイトへアクセスし、実行ファイルをダウンロードしたことが SIEM エンジンによりアナリストへ通知

(2) リスクアナリストがその社員の PC のログを注視していると、2 分後、攻撃者の設置した C&C サーバであるとしてブラックリストに登録されているサイトへ通信を開始

(3) SIEM エンジンがさらに攻撃用マルウェアのダウンロードを確認し、リスクアナリストがその中身まで確認し、リアルタイムに攻撃内容・対策をまとめ、お客さまへ通知

このような非セキュリティ機器のログをトリガーとした重大なインシデント通知は全体の約 30% にのぼる。

限界③：膨大な誤検知と、それによる非効率な対応

誤検知は、SIEM エンジン、そしてリスクアナリストによって排除している。そしてお客さまへは対応すべき脅威となるインシデントのみ通知する。ある顧客の 1 カ月のセキュリティ運用実績では、監視対象デバイスから収集される 100 億件のアラートから、SIEM エンジンによる自動分析、リスクアナリストによる高度分析を経て、30 件のインシデント報告がなされている。

我々のインシデント報告レポートの特徴は、「何が起こったか」の説明ではなく、「お客さまは次に何をすべきか」が一番に分かりやすくなっている点である。どれも同じに見えるログを精査し、分析し、正しい推奨対策を導くのは容易なことではないが、それをお客さまの代わりに行うのがリスクアナリストの価値だと考えている。

未知のセキュリティ脅威との戦い

前回の連載（8 月号）では、自社の公開 Web サーバやイントラサーバの脆弱性を一元管理できる「情報セキュリティ管理プラットフォーム（ISMP)」を紹介したが、それは、アプリケーションの脆弱性が公表されてから数時間でその弱点を悪用した攻撃が開始される状況への対策である。前々回（6 月号）では Sandbox 技術による未知のマルウェア解析（サービス名：リアルタイムマルウェア検知〔RTMD〕)、そして今月号では、過去の実績をベースにしたパターンファイルやシグネチャでの検知のみに頼るのではなく、独自の分析エンジンとリスクアナリストにて未知の脅威をリアルタイムに検知する取組みに触れた。

SIEM エンジンそのものも市販製品は存在する。しかしながら、攻撃は日々変化し、かつ新たな脆弱性を突いた攻撃が発生しており、あらゆる攻撃手法を熟知し、短時間で内容を確認し対策まで提示できるリスクアナリストの育成及びレベルの維持は非常に困難なことであり、多くの実例を日々ハンドリングしている専門業者へ委任することも考慮すべきである。今回紹介した実例はどの企業でも起こっていることであり、SIEM とリスクアナリストがセットとなった我々の WideAngle マネージドセキュリティサービスの採用もご検討頂けると幸いである。

＊ DevOps は、開発担当者と運用担当者が連携して協力する開発手法。開発 (Development) と運用 (Operations) を組み合わせた用語。

お問い合わせ先
NTT コミュニケーションズ㈱
経営企画部 マネージドセキュリティサービス推進室
E-mail：mss-sp-cp@ntt.com