報道関係者各位

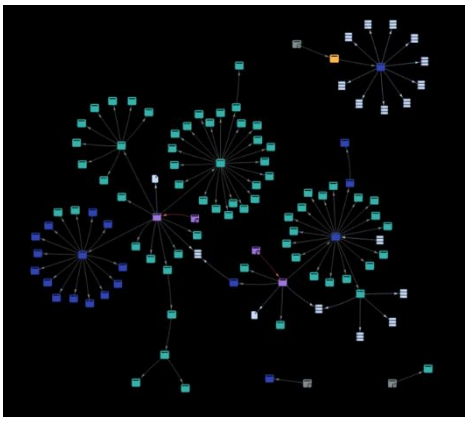
ウィズセキュア、GitHub から入手可能な オープンソースのデータ可視化ツール『Detectree』をリリース

～ インシデント発生時のデータ分析を省力化、レスポンスタイムを短縮 ～

2022 年 7 月 22 日
ウィズセキュア株式会社

セキュリティインシデントが発生した際、悪意のあるアクティビティやその影響を理解することは、多くの企業／団体にとって難しい問題です。防御側が必要とする、攻撃を封じ込めて被害を最小限に抑えるための貴重な時間とリソースが、まず理解のために使用されてしまうのです。こうしたなか、先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure（旧社名：F-Secure、本社：フィンランド・ヘルシンキ、CEO：Juhani Hintikka、日本法人：東京都港区、以下、ウィズセキュア）は、ブルーチーム（防御側）が検知した疑わしい活動の可視性を向上させるための新しいオープンソースツールである『Detectree』を発表しました。

ウィズセキュアの Managed Detection and Resposense（MDR）サービスのシニアスレットハンターである Tom Barrow（トム・バロウ）は、インシデントレスポンス担当者にとってはエンドポイント上の疑わしいイベント間の繋がりを発見することが最も重要だと説明しています。
「視認性は常に優先され、インシデント発生時には不可欠なものです。インシデントレスポンス担当者は、常に時間に翻弄されています。また、攻撃を阻止しなければならないというプレッシャー下においては、大量のテキストデータに目を通し、調査対象となる疑わしい動きとの関連付けを行うことは、問題の解決という観点からは無駄な時間なのです。」

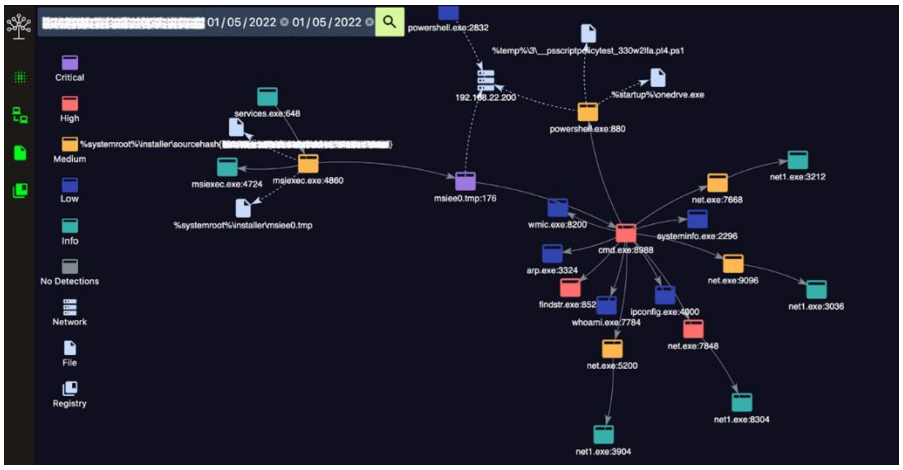


（Detectree によって、アクティビティをフォレスト／ツリーのように表して可視化）

例えば、インシデントアナリストが疑わしいプロセスの原因を探ろうとする場合、通常はログデータに目を通し、手作業でイベントの繋がりを再構築する必要があります。作業が長引くほどその管理は難しくなります。また、最近の調査[*1]によると 1 日あたり約 11,000 件とも言われる大企業のブルーチームが直面するセキュリティアラートの数を考

慮すると、このプロセスはセキュリティチームにとって大きな負荷となり、アラート疲れや燃え尽き症候群などの問題を悪化させる可能性があります。

Detectree はログデータを構造化し、検出された疑わしいアクティビティと、その検出に関連するプロセス／宛先ネットワーク／ファイル／レジストリキーとの関係を可視化することにより、ブルーチームが調査作業を省力化できるように設計されています。イベントの繋がりを再構築するためにテキストとして表現されたデータを手作業で分類するのではなく、インシデントレスポンス担当者は視覚化されたものを見て、相互作用／親子関係／プロセスインジェクションなどの繋がりだけでなく、繋がりの性質を確認することができます。可視化により、インシデントレスポンス担当者は検出された状況をすばやく確認し、そのデータをシンプルで直感的な方法で関係者と共有し、情報を必要とするすべての人がアクセスできるようにすることができます。



(インシデントレスポンス担当者が直観的に理解できるように、繋がりを視覚化)

「経験豊富な熟練のブルーチームであっても、業務の精度をより向上させるためのツールが必要となります。Detectree はシンプルなツールですが、セキュリティチームにとっては自分たちの仕事を不必要に難しくし時間を浪費させる真の問題を取り除いてくれるツールなのです。」と、Barrow は締めくくっています。

Detectree は、WithSecure Countercept の GitHub ページでダウンロードが可能です。
https://github.com/countercept/detectree
また、Detectree のデモ動画はこちらよりご覧いただけます。
https://www.withsecure.com/content/dam/with-secure/ja/resources/Detectree_demo.mp4

*1: https://www.eweek.com/security/challenges-of-the-soc-decision-intelligence/

WithSecure Web サイト:
https://www.withsecure.com/jp-ja/
WithSecure プレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure について

WithSecure™は、IT サービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちは AI を活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と

対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は 30 年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988 年に設立された WithSecure は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は www.withsecure.com をご覧ください。また、Twitter @WithSecure_JP でも情報の配信をおこなっています。