IOC（Indicators of Compromise）活用のススメ

IOC（侵害指標）の代表的な例

- 異常な送信パターンのネットワークトラフィック
- 特権ユーザーアカウントのアクティビティの異常
- ログインとアクセスパターンの地理的な不規則性
- ログインの失敗や存在しないアカウントでのログイン
- データベースへのアクセス量の異常な増加
- HTML の応答サイズの増大
- 人間の行動らしくない動きの Web トラフィック
- DDos アクティビティの兆候
- 同一ファイルに対する膨大なリクエスト
- アプリケーションのポート使用トラフィックの不一致
- 疑わしいレジストリまたはシステムファイルの変更
- DNS リクエストの急増やパターンの監視
- レジストリやシステムファイルの意図しない変更
- システムへの突然のパッチ適用

セキュリティ対策を検討する場合、世の中にはたくさんの高価なセキュリティツールが存在します。
しかし、それを導入することがベストな選択と言えるでしょうか？
堅牢なセキュリティを保つために多くの企業が、メーカーが提供するソリューションをセキュリティ対策として導入しておりますが、ハイレベルなセキュリティツールの運用をするためには、コストのみならず人的、およびシステムのリソースに多大な負荷がかかります。
一方、既に発生したセキュリティのインシデントに関しては、入手可能な IOC（indicator of compromise）など様々な外部のインテリジェンスを利用して、ある程度自社で仕組みを作り脅威から守ることが可能です。
IOC とは、マルウェアなどのセキュリティ違反となるアクティビティを特定できる可能性があるフォレンジックデータです。IOC のデータは、不審なインシデント、セキュリティイベント、またはネットワークからの予期しない呼び出しなどに起因して、集められます。
IOC のデータを利用して、異常なアクテビティや脆弱性を検出するために、定期的にチェックしたり、疑わしいファイルやデータを見つけて隔離するような仕組みを、自社でも開発することができます。
IOC の代表例としては、送信のネットワークトラフィックの異常なアクテビティや、特権ユーザの異常なアクテビティ、レジストリやシステムファイルに対する異常なアクセスなどの指標があり、その指標は、セキュリティイベントと、侵害の検出はもちろん、攻撃を封じ込めて停止させるために、攻撃者が何をしようとしているのか意図を推測するのに役立ちます。そうして得られた情報は、社内のセキュリティチームが、侵入を阻止するために、攻撃者が次のステップで何をしようとしているのかを知ることで優位に立つことができます。
また、セキュリティチームが侵害の兆候に注意を払うことにより、セキュリティイベントの検出と対応のパフォーマンスを向上させることができ、IOC の情報も活用することによって、他のセキュリティツールでは検出できなかった疑わしいアクティビティも特定できるようになります。
社内で、IOC のデータを活用することにより、セキュリティチームは、情報に基づいた意思決定をより迅速にかつ正確に行うことができるので、有害な侵害を拡散する前に攻撃を封じ込め、迅速に対応することが可能になります。