ArcSight Intelligence により 国家レベルの高度な実力を持ったレッドチームからの攻撃を検知

Micro Focus ArcSight Intelligence の UEBA は、既存のエンドポイントデータを利用して未知の脅威を検知することができます。ある大手消費財企業のレッドチーム演習において、UEBA とエンドポイントの組み合わせは、高度に洗練された攻撃の数々を検知できることが実証されました。

Micro Focus ArcSight Intelligence の UEBA は、既存のエンドポイントデータを利用して、未知の脅威を検知することができます。ArcSight Intelligence を Endpoint Detection and Response (エンドポイントでの検出と対応、EDR) プラットフォームと組み合わせることにより、多数のイベントを分析して危険性の高い行動を発見し、調査を要する脅威リードをセキュリティチームに提供します。

ArcSight Intelligence による大手企業のレッドチーム攻撃の発見

ハンターとインシデント対応者のスキルをテストできるレッドチームは、効果的なサイバーセキュリティ戦略には不可欠です。このような攻撃の予兆を検出することにより、現実の攻撃を検出する体制が整います。

ある大手消費財企業では、ArcSight Intelligence により豊富なエンドポイントデータ (プロセス、ユーザー、マシンの行動) を活用して、国家レベルの高度な実力を持ったレッドチーム攻撃を検知しました。ArcSight Intelligence は攻撃を示す行動をただちに発見し、攻撃ライフサイクル全体を明らかにして、攻撃への対応に必要なコンテキストを企業のセキュリティチームに提供しました。

ArcSight Intelligence は、次のような攻撃について、質の高いセキュリティリードを脅威ハンターとインシデント対応者に提供しました。

OWA プロファイリング	攻撃者は Outlook Web Access (OWA) タイミング攻撃により有効なユーザーアカウントを発見しました。この攻撃によって平文のパスワードが急激に増加したため、この OWA サーバーとログオンタイプに対する異常なログイン活動として検知されました。
リモートの脆弱性攻撃	リモート攻撃ツール Mimikatz および CrackMapExec を既知の管理サーバーに対して使用したところ、通常、このサーバーでは実行されていないプロセスとして検知されました。
偵察	セキュリティ侵害を受けた管理者アカウントで管理権限のあるノートパソコンにログインし、他のマシンのディレクトリに対してパスワードの記録されたファイルの検索を行いました。非表示の共有に対する結果が各マシンから送信され、ローカルのレジストリハイブが管理者のノートパソコンから抽出されました。これらのイベントは、異常な共有行動と 1 時間あたりの処理量の異常として検知されました。
ラテラルムーブメント (侵入後の攻撃)	セキュリティ侵害を受けたアカウントが関連サーバーに対してラテラルムーブメントを実施し、多数の偵察攻撃を仕掛けました。管理者アカウントに対する異常なログインと、他のマシンでの異常なプロセスの利用が検知されました。
パスワードの推測	第二の攻撃は、初期パスワードの使用をテストするものです。この攻撃では、Python スクリプトにより、各ユーザー名のユーザードライブと初期パスワードをマッピングしました。これにより大量のプロセスと多数の認証試行エラーが発生しました。
IP アドレスと攻撃ツール	最後の攻撃は、複数のサーバーに対する、長期にわたる一連の Windows Management Instrumentation (WMI) 攻撃でした。これは、攻撃されているサーバーでの通常は見られないプロセスおよび攻撃側マシンでの異常な量のプロセスの実行として検知されました。ArcSight Intelligence は、イベントの生データを保管して、最初のセキュリティ侵害に使用された攻撃ツールと IP アドレスを特定しました。

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
www.microfocus-enterprise.co.jp