MICRO FOCUS

データシート

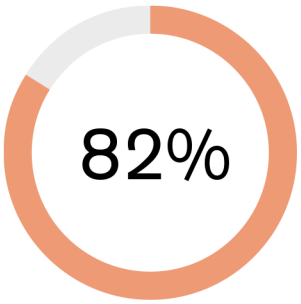
Security ArcSight User Behavior Analytics (UBA)

ArcSight User Behavior Analytics

Micro Focus® Security ArcSight User Behavior Analytics (UBA) を使用すると、セキュリティアナリストは、サイバー攻撃のリスクと影響をリアルタイムで最小化できます。ArcSight UBAは、イベントとログデータだけに注目するのではなく、専用のセキュリティ分析を通じて未知の脅威を検出します。そのために、ユーザーとエンティティの通常の動作のベースラインを作成し、異常が発生した場合に特定します。ArcSight UBAは、アクティビティと、セキュリティ侵害の複数のインジケーターを集計することで、資格情報が正当であっても、リスクが高いユーザーやエンティティを明らかにすることができます。

セキュリティ環境の拡大と進化とともに、企業のセキュリティプロフェッショナルが直面する脅威は、ますます深刻かつ複雑になっています。特に懸念が高まっているのが、内部者による脅威です。悪意のあるユーザーやエンティティが正当な資格情報を持っている場合、発見は困難です。不正なアカウントや侵害されたアカウントによってインストールされたマルウェアが何か月も見つからずに活動し、機密情報を盗み出したり重要な資産を破壊したりするおそれがあります。セキュリティチームが侵害の影響を効果的に抑制するためには、このような脅威の検出、調査、対応の速度と正確さが重要です。ただし、今日の企業が直面する進化した持続的な脅威に対処するには、従来のセキュリティソリューションでは不十分な場合が多くなっています。

SIEM (Security Information and Event Management) プラットフォームのようなルールベースのツールもまだ使用されてはいますが、最新の脅威に対しては多くの場合は力不足です。Verizonの最近のセキュリティ調査によると、調査対象の侵害の82%で、攻撃者のアクティビティの証拠がセキュリティログファイルに残っていました[1]。従来のツールは疑わしい活動について企業に警告はしますが、セキュリティチームが侵害に気づいて、イベントを調査し、その有効性を評価して、コンテキストに関連するソリューションで対応するころには、すでに敵対者は深刻な損害を与えてしまっています。さらに、セキュリティプロフェッショナルは、このような大量のログデータを調べる一方で、規制要件の変化への対応やコストの管理にも取り組まなければなりません。



1 Ross, Joan.(2016年8月25日)。Making the Most of Limited Security Resources (Webブログ投稿)。securityblog.verizonenterprise.com/?p=7578より取得

概要

- 攻撃への可視性を高め、疑わしいアクティビティや行動をリアルタイムで警告
- 直観的なワークベンチを表示することで、セキュリティリスクの即時の理解を可能にし、調査を合理化し、生産性向上を実現
- すべてのユーザーとエンティティの中から最も疑わしい異常なアクティビティを見つけ出し、リスクによる脅威のランク付けを表示
- 正当な資格情報が使用されている場合でもサイバー攻撃や内部者による脅威を検出できるので、重要な損害が発生する前に敵対者を発見可能

製品ハイライト

ArcSight UBAを使用すれば、ユーザーやエンティティから生じる高度な脅威を検出できます。また、インストールされているMicro Focus Security ArcSight SIEMと組み合わせることで、現在の運用チーム、データフィード、インシデント対応プロセスをそのまま利用できます。これにより、調査の効率が上がり、運用コストを節約できます。

主なメリット

図2をご覧ください。

- 攻撃への可視性を高め、ユーザーやエンティティの疑わしいアクティビティや行動をリアルタイムで警告
- 直観的なワークベンチを表示することで、セキュリティリスクの即時の理解を可能にし、調査を合理化し、生産性向上を実現
- すべてのユーザーとエンティティの中から最も疑わしい異常なアクティビティを見つけ出し、リスクによる脅威のランク付けを表示
- 正当な資格情報が使用されている場合でもサイバー攻撃や内部者による脅威を検出できるので、重要な損害が発生する前に敵対者を発見可能
- サポートされるユースケースは数百種類におよび、さまざまな脅威状況を対象とした調査活動に利用可能

主な特長

ユーザー行動およびエンティティ分析による高度な脅威検出

ArcSight UBAは、機械学習と高度な異常検出技法/アルゴリズムの最新の進歩を組み合わせることで、シグネチャ、ポリシー、ルールだけに頼らずに、既知と未知の両方の脅威を迅速に検出します。ArcSight UBAは、ピアグループ分析によって、異常な行動や前例のないイベントを特定します。ArcSight UBAは、ユーザーやエンティティのグループを比較することで、行動を比較し、ベースラインから外れた行動を、たとえ1回しか行われなかった場合でも検出できます。ユーザーやエンティティの異常な行動を、豊富なコンテキストに支えられたインテリジェンスで相関付けることにより、誤検知が減り、セキュリティチームは組織に対する真の高リスクの脅威に集中できます。これには、マルウェアのビーコン送信の検出や、疑わしいサイトへのトラフィックの異常な量や回数など、ネットワークに関連するシナリオも含まれます。ArcSight UBAを使用すれば、高リスクのデータ引き出しや、特権アカウント/サービスアカウントの悪用を特定し、高度で持続的な脅威を検出することができます。

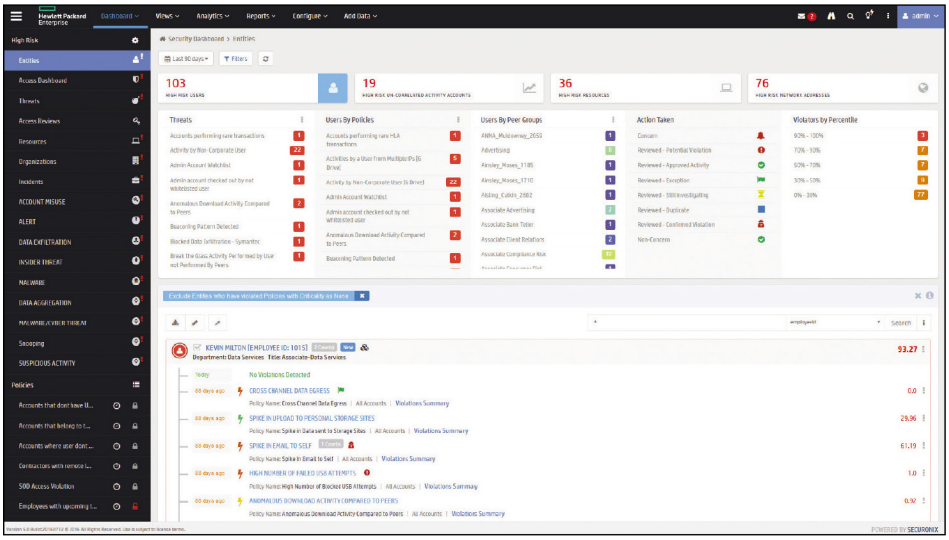


図2: ArcSight UBAでは、ユーザーやエンティティから生じる高度な脅威をリアルタイムで検出できます。

よりプロアクティブな敵対者探索による侵害の影響の軽減

ArcSight UBAは、ユーザー ID管理とアクセス情報を、データベース、ファイル、ユーザー中心のアクティビティと組み合わせ、権限を持つユーザーのアクションにリスクを伴うアクティビティや普段と異なるアクティビティがないかを能動的に監視します。この結果、異常な行動が早期に検出されるため、サイバー攻撃のリスクと影響が低減します。これには、高度な標的型の攻撃の識別、IDの相関、インサイダーの脅威の識別と調査、権限を持つアカウントの不正使用の検知が含まれます。この情報は、組織が攻撃者をより迅速に発見するために役立つ方法で可視化されます。

調査と意思決定の速度と正確さの向上

整備されたユーザーインターフェイスにより、調査の効率をあげ、有効な意思決定が可能となります。マルチエンティティ調査ワークベンチにより、異なる種類のソースから収集された大量のデータを精製し、ビジネスに関連するコンテキストでセキュリティ情報に優先順位を付けることができます。ダッシュボード、違反タイムライン、ポイントアンドクリックフィルタリング、検索などの機能により、ホスト名、IPアドレス、リスクスコアといった意味のある情報だけをデータやログからすばやく抽出し、真の脅威を特定することができます。リスクブーストやダッシュボードアクションにより、サイバーディフェンスセンターの人的要素が維持されます。

状況把握の改善による脅威へのインテリジェントな対応

ArcSight UBAの脅威ライブラリには、数百種類の高度なユースケースが収録されており、個々の企業のニーズに合わせた設定が可能です。サ

イバーディフェンスセンターでは、ArcSight UBAの脅威ライブラリを使用することで、ユーザーやエンティティの行動分析、データ損失の防止、エンタープライズ/クラウドアプリケーション、デバイスに対するサイバー脅威といったさまざまな脅威状況をターゲットとしたアクティビティを実行できます。何百種類ものユースケースがサポートされているので、単なる異常の発見に留まらず、脅威をより正確に認識し、誤検知を減らすことができます。

効率的で効果的なイベント解決
専用のセキュリティ分析とインテリジェンスによってイベント解決を迅速化できます。インテリジェンスによってSIEM情報のマイニング、充実化、変換が行われ、ユーザーやエンティティの詳細な可視化を実現することでIT環境全体に対する既知および未知の脅威にすぐに利用できるインテリジェンスが作り出されるため、脅威を発生前に軽減できます。

IPアドレスからユーザーマッピングへの移行
プロキシなどの重要なシステムのログの多くでは、記録されるのはIPアドレスのみで、ユーザー行動情報は記録されません。これらのシステム上でユーザーアクティビティを調査するには、特定の時間にユーザーがどのIPアドレスを使用していたかを知る必要があります。UBAでは、ID相関を使用することでこの問題を解決しています。ID相関は、未認証のアクティビティと個別ユーザーを結びつけるため、アドレス指定方式間のデータを相関させるプロセスです。

詳細情報
https://software.microfocus.com/software/siem-big-data-security-analytics

www.microfocus.com

Micro Focus
英国本社
United Kingdom
+44 (0) 1635 565200

米国本社
Rockville, Maryland
+1 301 838 5000
+1 877 772 4450

www.microfocus.com

マイクロフォーカスエンタープライズ株式会社
0120 923 333

www.microfocus-enterprise.co.jp

360-000042-001 | 4AA5-8223 | H | MM | 11/17 | © 2017 Micro Focus.All rights reserved.Micro FocusおよびMicro Focusロゴは、英国、米国、およびその他の国におけるMicro Focusまたはその子会社または関連会社の商標または登録商標です。その他の商標については、それぞれの所有者が権利を有しています。