教師なし学習・数学的アプローチで検知
—「Interset UEBA」で実現する、内部脅威対策

雇用の流動化やリモートワークの導入を背景に、内部不正による情報漏洩のリスクが高まっている。内部脅威を防ぐために、組織内のPCやシステムの操作ログを分析するツールとしてSecurity Information and Event Management（セキュリティ情報イベント管理、以下SIEM）を導入する企業も多いが、それだけでは検出が難しい場合もある。Micro Focusの「Interset UEBA」（以下Interset）は、教師なし学習によってユーザーの行動を分析し、異常を検知するソリューション。SIEMと併せて利用することで、セキュリティチームの生産性向上を実現できるという。Intersetの特徴について、マイクロフォーカスエンタープライズの担当者に聞いた。

内部脅威対策のため、UEBAへの関心が高まっている

User and Entity Behavior Analytics（以下UEBA）とは、人物や端末などの振る舞いを分析して、異常な行動やリスクを検知する技術。膨大なログデータを機械学習なども活用しながら分析することで、より的確な検知ができるテクノロジであり、Intersetもそのひとつである。

マイクロフォーカスエンタープライズ プリセールス統括本部 ソリューションコンサルタントの宮崎 功氏に、企業のUEBAへの関心について聞くと「この数年で、日本国内においていくつも重大な内部不正事件があり、大きなニュースになりました。こういった背景を受けて注目度は急上昇しています。IPA（独立行政法人 情報処理推進機構）が発表した『情報セキュリティ10大脅威 2020』では、『内部不正による情報漏えい』が2位となりました。前年は5位でしたので、こういった点からも関心の高まりがわかります。また、内部不正の特徴として、解決まで時間がかかること、犯行が明らかになっても被害金額は多くの場合取り戻せないことがあります」と語った。

雇用の流動化やDXの推進がその背景にあり、転職時の情報持ち出しが増えている等が理由として挙げられるという。企業にとって重要情報である営業秘密情報や商品設計図などのファイルが漏洩した場合、それに投資した時間やコストを鑑みるとダメージが甚大なのは一目瞭然だ。しかしこのような被害が拡大する一方で、内部脅威にフォーカスしているセキュリティソリューションはあまり多くないのが実情だという。

Intersetは、内部脅威、未知の脅威、情報漏洩の3つにフォーカスしたソリューションで、これは現在企業が抱えている課題でもあり、かつ既存のセキュリティソリューションが苦手としている領域でもある。宮崎氏に特徴を聞くと、「内部不正を見つけるのに、一般化された外部の脅威情報などは有効ではありません。必要なのはその組織自身とそこに所属する人の特徴です。そこで、Intersetはその『組織専用』の通常状態を学習し、そこからの異常の大きさを捉えるというアプローチをします。しかし、限られた視点からでは見つけるのは難しく、異常検知特有の誤検知にもなる。そこで、Intersetは450の機械学習によるモデルを用いて様々な観点からの通常状態の定義と異常

マイクロフォーカスエンタープライズ株式会社
情報セキュリティ&ガバナンス技術本部
プリセールスコンサルタント
宮崎 功 氏

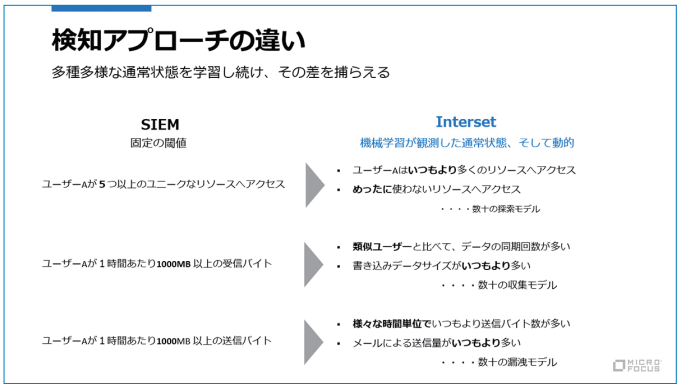
の大きさ検知をします。そして、最終的にそれらを総合的に評価し、内部不正を見つけます」と述べた。

評価の元となるのが、ユーザーや端末の動作ログだ。Intersetは、ログを「教師なし学習」と「数学的アプローチ」によって分析して異常を検知する。マイクロフォーカスエンタープライズ プリセールス統括本部 統括本部長の福田 慎氏は「教師あり学習の場合は、一般的で共通な既知の情報を元にした検知となります。それ以外の異常は捉えにくいので、個々の組織のコンテキストが必要な内部脅威やこれまで経験していない脅威を捉える目的ではあまり有効ではありません」と学習方法の違いを説明した。

既存・他社のSIEM製品と組み合わせることでお互い補える関係に

組織内の端末やシステムの操作ログを分析するツールとしてはSIEM製品が普及しているが、Intersetとは機能が異なるという。SIEMは、既知の脅威に対するリアルタイム検知のために使われ、脅威情報との照合や、想定内セキュリティシナリオでの検知に役立つ。

一方でSIEMを含む既存のセキュリティソリューションが苦手なのが内部不正、未知の脅威、そして情報漏洩だ。特に情報漏洩に関しては、SIEMを導入している企業でも漏洩事件が起こっていることから、既存のセキュリティソリューションだけでは情報漏洩のリスクを十分に低減しきれていないことがわかる。

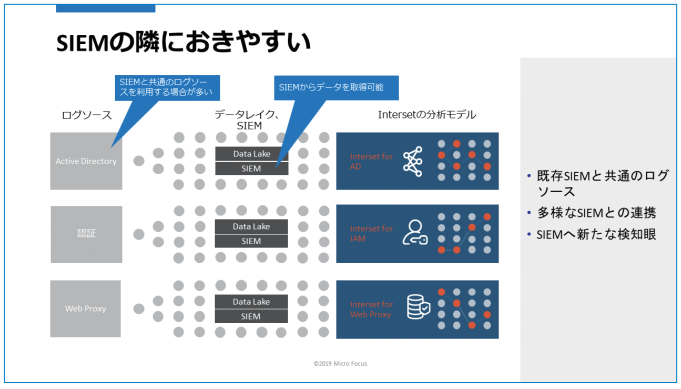


Intersetの分析結果から、脅威リスクの高いユーザーや端末を0から100までのスコアの高い順にリストアップした優先度リストが提供される。宮崎氏は、「Intersetの優先度リストは非常に実用的です。高品質でユーザーが実際に使えるリストを提供します。例えば、SOC(Security Operation Center)ではこれを使うことで、一次分析などの業務負担を大幅に削減することができます。初動が非常に明確になるのです」

またIntersetの重要なコンセプトは、余計なチューニングを利用者に強いず、チューニングを施さなくても十分な価値を出すということだという。先の優先度リストがチューニングレスであるとともに、検知モデルで使われるグループ比較の定義なども、教師なし学習などを使いチューニングレスであるという。

探索・収集・漏洩と、あらゆる段階・条件での異常を検出

では、Intersetはどのような場面での異常検知ができるのだろうか。宮崎氏は、まず転職を機に内部不正の情報漏洩をおこなうケースを例に説明した。「情報漏洩一つをとっても、いくつか段階を踏んで行われます。悪意のある従業員は、まず

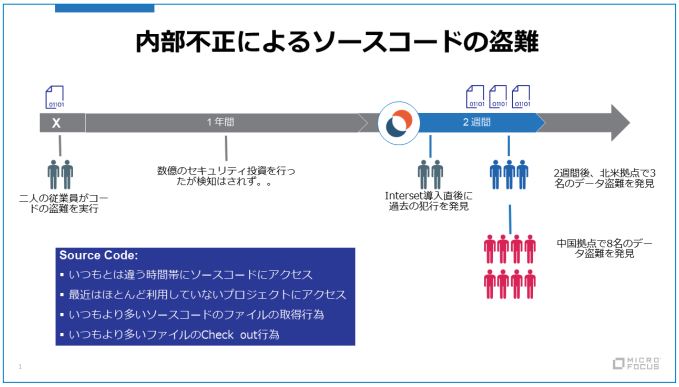


共有ドライブを徘徊するような行為を行います。多くのドライブやフォルダにアクセスするだけではなく、実質休眠しているようなフォルダや、他部署のフォルダなど様々な物色を行います。次に、自分の端末に目的のファイルを移すなどします。ここまで情報漏洩の準備段階で、探索、収集といった段階ですが、Intersetはこれら準備段階を捕らえるためのモデルがそれぞれ数十含まれています。多くの場合、ここで気づくことができますが、仮に次の情報漏洩の段階までいっても見逃しません。Intersetは情報漏洩を短期、中期、長期のように様々な時間単位で検知を行っています。例えば、数ヶ月かけてゆっくり抜き出すような不正の検知も可能です。Low and Slowな行動や情報漏えいは多くのセキュリティソリューションが苦手とするところですが、Intersetでは検知が可能です」

他のセキュリティ製品では発見不可、Intersetだからこそ即発見

さらに宮崎氏は、他のセキュリティ製品では見つからなかった内部不正が、Intersetを導入したことで即発見につながった象徴的な事例も紹介した。

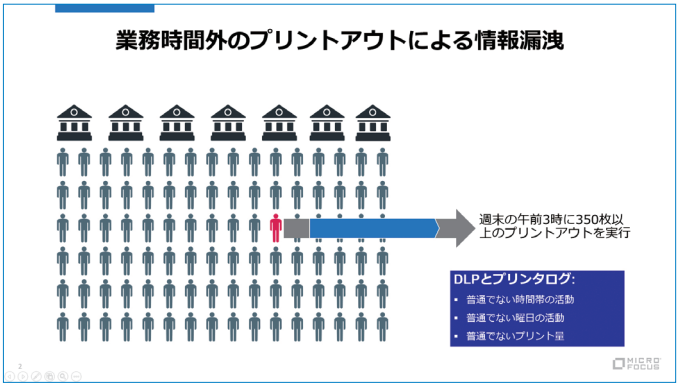
「あるお客様の事例で、Intersetを導入したことで、今まで全く気づいていなかった内部不正を発見した例があります。Intersetを導入して、過去に2名の従業員による私的な情報資産の盗難があったことを、即座に発見しました。実はこのお客様はIntersetを導入する前に数億円を投じて、様々なセキュリティソリューションを導入してきたようなのですが、そういったものではこのインシデントを発見することができ

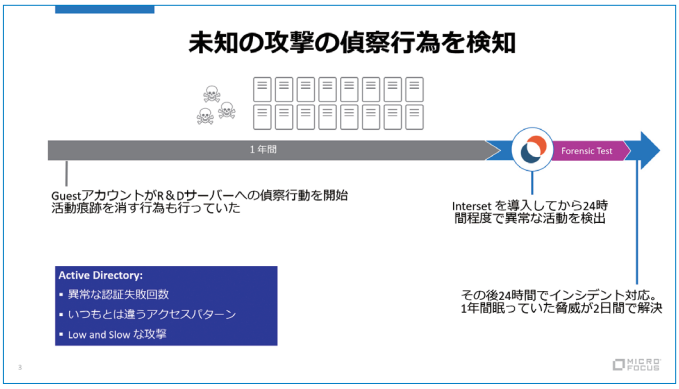


ませんでした。結果的にインシデント発生からIntersetが導入されるまでの約1年間、全く情報資産の盗難に気づいていなかったそうです。この事例では、Interset導入直後に過去ログを利用しています。過去ログを利用することで、導入から非常に短時間でIntersetの検知効果を実感できるケースがあります。またこのお客様は、運用を継続することで、2週間後にも従業員による類似した情報資産の盗難を、複数発見したのです」

新型コロナウイルスの影響で在宅勤務が増えているが、そこでもIntersetは有効だという。例えば、データモデルにVPNに関する検知モデルも用意されているため、社外からの利用についても監視は有効だ。また、宮崎氏は「CrowdStrikeなどのEDR（Endpoint Detection and Response）製品とIntersetの組み合わせはテレワーク環境の監視に非常に相性が良いです。EDRがインターネット経由でログを直接収集し、それをIntersetが分析することができます。EDRはログソースとして非常に優秀で、1つのログソースとしては、かなり広範囲の検知ができる場合があることを確認しています」と説明した。

マイクロフォーカスエンタープライズ株式会社
プリセールス統括本部 統括本部長
福田 慎 氏





データモデルを増やし、ほかの製品との連携機能強化も推進

リスクの高い行動をいち早く見つけて対処を促せるInterset。今後も検知強化のため、データモデルを追加していくという。今後について宮崎氏は「ビルドインのモデルだけでなく、高度なニーズに向けた機能も提供する予定です。たとえば、自社のデータサイエンスチームが作った検知モデルを利用できる『BYOM（Bring Your Own Model）』です。運用面では、弊社で提供しているビッグデータの分析基盤であるVertica Analytics Platform（ヴァーティカ、以下 Vertica）の実装や、ArcSightという非常に歴史あるSIEM製品をもっているのですが、その製品との連携強化を予定しております」と構想を語った。

最後に福田氏は「Intersetは非常に個性ある製品なので、単独の製品としてプッシュしていきます。一方で、弊社は一般的なセキュリティベンダーと違って運用面も含めたソリューションを展開していますので、その点も差別化できるポイントと考えています。脅威の検知だけでなく、管理対象への確認を促す、パッチを適用する、ネットワークから外すなどの連携を提案できます」と、同社の幅広い製品ラインナップによるメリットをアピールした。

詳しくはこちら：
www.microfocus-enterprise.co.jp/products/interset-ueba/

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