電子ブック

IronNet™

ダイナミックな脅威に備えるダイナミックな検知

ネットワーク・ディフェンスがサイバー・リスクを軽減する方法

目次

「レフトオブブーム」の検知

サイバーリスクはビジネスリスクです。

私たちの世界がデジタルトランスフォーメーションに依存するようになったことで、サイバー脅威のリスクは広がっています。サイバーセキュリティは、この変革に不可欠なものでなければなりません。しかし、Deloitte 社の「2019 年サイバー調査の将来」において、90% 以上の C 級経営者が、サイバーセキュリティ予算の 10% 未満しかデジタル変革プロジェクトに割り当てていないことが明らかになりました。同様に、アクセンチュア・セキュリティも、企業リーダーの 79% が、「自分たちの組織は、関連するセキュリティ問題に対処するより以前に、新しい新技術を採用している」と報告していることを指摘しています。

このような予算と技術の間に大きなギャップがあると、最新の認識されていないデジタルシステムが潜在的に監視されず、保護されないというサイバーの脆弱性が生じます。**皆さまのサイバーセキュリティ戦略は、オンプレミス・ネットワーク、クラウド、ハイブリッド環境のいずれであるかを問わず、企業ネットワーク全体に対するサイバー脅威の管理方法に対応していますか？**

侵入のライフサイクル

サイバーリスクとセキュリティギャップを特定し、サイバー投資に優先順位をつけるための基準が、NIST Cybersecurity Framework（NIST サイバーセキュリティフレームワーク）であっても、マトリクスベースの MITRE ATT&CK Framework（MITRE ATT&CK フレームワーク）であっても、目的は同じです。それは、侵入のライフサイクルの可能な限り早い段階で、不正なデータアクセスやシステム操作を早期に検知して防ぐことです。ライフサイクルの他の時点での検知は、侵入発生後に追いつくためのものに過ぎないと言えるでしょう。

偵察段階（あるいはそれ以前）でハッカーの動きを止めるための機能に投資することが重要なポイントです。敵対者が侵入経路に沿って移動した後、検出された観測値を脅威の戦術にマッピングできることは、最善かつ最速の修復コースをよりよく決定するためにも不可欠です。

「レフトオブブーム」（爆発の左横）

「レフトオブブーム」（爆発の左横）とは、軍事用語で、敵が爆弾を作ったり仕掛けたりする前に反乱軍の活動を妨害することを指します。同じことがサイバー活動にもあてはまります。皆さまは敵対者が搾取や流出の段階に到達する前に阻止しなければなりません。皆さまが瞬時に行動しないかあるいはできない場合、ネットワーク侵入者に貴重な滞留時間を与えてしまい、組織のデータの窃取、ネットワーク、システムや資産の支配、金銭的資産の流出にまんまと成功させたりすることになります。未知の巧妙な脅威を検知できることは、その影響を軽減するために非常に重要であり、なぜなら侵害の平均的な滞留時間は 206 日であり、さらに 73 日平均が、封じ込めるためには必要となるためです。

皆さまはセキュリティ・オペレーション・センター（SOC）チームが、「爆発の左横」で成熟することを望まれているでしょうが、「爆発の右横」の防御も強力である必要があります。ネットワーク検出と反応 (NDR) は、固いサイバー防御を築くためにネットワークで行動をつかむ方法です。皆さまは MITRE ATT&CK® Framework（MITRE ATT&CK® フラームワーク）を使用して、これらの脅威に対する防御能力を評価することができます。

ネットワーク防御とはなにか?

皆さまは、ネットワークに侵入した脅威をどのようにして検知しますか?これらの脅威は、ファイアウォールをすり抜けたり、もしくは安全でないエンドポイントを利用してネットワークに侵入した敵対者によるものです。ネットワークに侵入すると、敵対者はそこに潜み、金銭やデータ (個人識別情報 (PII) や知的財産など) を盗むための最善の方法を決定します。そして、次には侵入ポイントからネットワーク上を横方向に移動して、ターゲットとなるシステムやデータを探すこともあります。

ネットワーク検知および対応ソリューションは、ファイアウォールやエンドポイント検知および対応 (EDR) ツールを補完して、従来のセキュリティの「名刺」や「シグネチャ」を持たないこれらのネットワーク脅威を捕捉します。場合によっては、ネットワークへのアクセス権を与えられた従業員など、インサイダーの脅威が宿敵となることもあります。

いずれにしても、皆さまの組織はネットワーク上の疑わしい行動を精査し、「爆発の左横」、あるいは最悪の場合でも、敵がネットワークを横切って移動し始めたときに、それを阻止する能力を持っていなければなりません。皆さまの目標は、敵が意図したペイロードをうまく捕捉したり、重要なシステムをリモートで乗っ取ったりする前に対応することでなければなりません。また、敵がこの時点に到達した場合 (または侵入経路を進んだ場合) には、危険な敵対的手法がネットワーク上で行われていることを検知する信頼できる方法が必要です。

目に見えないものとの戦い

暗闇の中での防御

皆さまは、目に見えないものと戦えません。ファイアウォールやエンドポイントプロテクションツールは、現在の脅威の状況において、既知の可視性とのギャップがあります。NDR ツールは、これらの空白を埋めることができ、セキュリティスタックを強化することで、脅威の全体像をより広範に把握することができます。NDR システムは、高度な行動分析を活用して、シグネチャや既知の IoC (Indicators of Compromise ＝ 侵害のインジケータ) を持たない未知の脅威を検出します。行動分析は、悪意に満ちた可能性がある活動により明るい光を当てて、シグネチャが見逃したものを検出します。

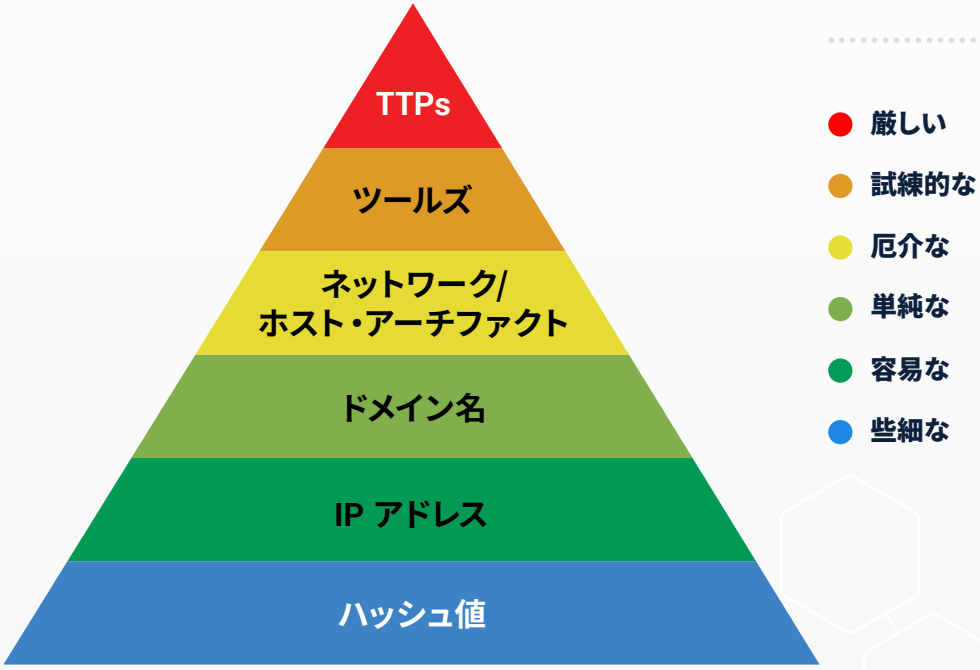
皆さまの SOC。重層的効果。

行動分析を行い、MITRE ATT&CK Framework (MITRE ATT&CK フレームワーク) などの共通のリファレンスを使用することで、皆さまの SOC チームはアラートレベルごとに対応の優先順位をつけるのに役立ちます。場合によっては、典型的な戦術、技術、手順 (TTPs) に基づいて、脅威を特定の敵グループに帰属させ、敵の動きやセクターターゲットを予測することもできます。高度な NDR ツールは、アラートの早期調査の自動化によって、アナリストがネットワーク上の脅威に対してトリアージし、迅速に対応するのに役立ちます。

詳細はこちらをご覧ください

完全な可視化の達成

なぜネットワーク防御がより強固な防御となるのか？簡単に言えば、敵対者がその TTP、すなわち行動様式をすぐに変えることは難しいということです。したがって、皆さまがサイバー攻撃者の弱体化を進めるためには、サイバーセキュリティの武器にネットワークの検出と応答を加えることで、敵が最も影響を受けやすい場所を見つけなければなりません。実際、セキュリティ研究者のデイビッド・J・ビアンコ氏が「Pyramid of Pain」（苦痛のピラミッド）と呼ぶ脅威探索フレームワークの最上位に位置するこのレベルでの防御活動が最も効果的です。



デイビッド・J・ビアンコの脅威探索フレームワーク「Pyramid of Pain」（苦痛のピラミッド）

ビアンコ氏の説明。

> 皆さまのこのレベルでの検知と対応は、敵のツールに対してではなく、敵の行動に対して直接行うことになります...純粋な有効性の観点からは、このレベルが理想的です。もし皆さまが敵の TTP に素早く対応することができれば、敵は新しい行動を習得するという、最も時間のかかることを強いられます。

皆さまはサイバーセキュリティの優先順位と投資をピラミッドの頂点に向けるべきものです。高度な行動分析を利用した NDR ツールは、サイバーディフェンスをこのレベルにまで引き上げることができます。どのようにして？それは、皆さまの SOC チームが悪意のある活動のより多くの、より早いインジケータを把握できるようになることで、これらの洗練された脅威をより早く検知し、対応できるようになるからです。

使用事例:「ついに、金融業界におけるサイバー脅威の可視化に成功」

この革新的なグローバル金融企業は、金融サービス分野で最も詳細で有能なセキュリティコントロールアーキテクチャを保有しており、行動ベースの脅威、特に APT（Advanced Persistent Threats ＝ 特に高度な持続的な脅威）を検知して対応する能力には限界があることを知っていました。

この企業が未知の脅威を検知するための能力を、どのようにして高めたかをご覧ください。

ガートナー社の SOC 可視化トライアド

NDR ソリューションは、もはや従来のサイバー・セキュリティ・スタックを補完するために「あればいい」という類いのものではなく、不可欠なものであることを念頭に置くことが重要です。NDR ツールは、EDR および SIEM の機能と合わせて、企業のサイバーセキュリティ防御において、可視性を高めるためのキーとなるものです。

これら 3 つのテクノロジーを連携させながら武装することで、企業全体を監視するために必要な包括的な可視性が得られ、特にデジタルトランスフォーメーションの取り組みが加速する中で、皆さまはサイバーリスクを軽減することができます。

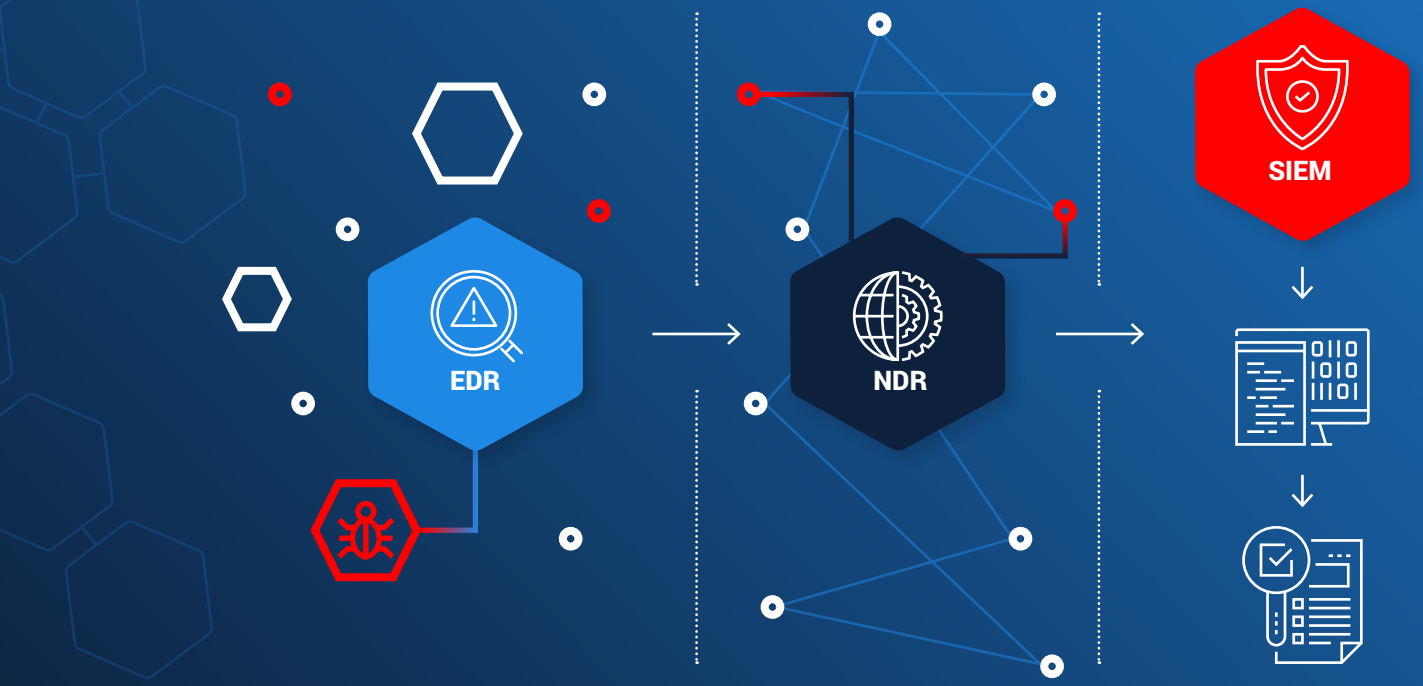
EDR は、エンドポイント・デバイス上にあるものだけを検出します。EDR は、エンドポイントでの可視化と検知のための重要な基盤となるものですが、実際には企業は無数のエンドポイントから構成されています。すべてのエンドポイントのセキュリティを確保するのは重要なことであり、エンドポイントだけのアプローチには限界があります。

今日動きある企業や組織は、パートナー、サードパーティ・サービス・サプライヤー、そしてサプライチェーン・ベンダーなど、広範囲なマトリックスに依存しているため、単なる EDR だけではすべての脅威を捉えるのに十分ではありません。エンドポイントエージェントはすべてにインストールすることはできませんし、EDR は IoT（モノのインターネット）やクラウド機能には対応していません。管理上の課題に関しては言うまでもなく対応できません。敵対者はエンドポイントを標的にし、容易に無力化することができます。

ここで NDR が非常に重要となります。要するに、真実は情報回線の中にあるということです。ネットワークがユビキタスであることを考えると、エンドポイントとの間のすべての動きはネットワークを経由しています。さらに、ネットワークは非常に広大であるため、攻撃者が自分の痕跡を完全に隠すことはほぼ不可能です。

SIEM には基本的な分析機能があり、中央のワークフローシステムとして SOC の中で重要な役割を果たしていますが、今日の世界ではそれだけでは十分ではありません。SIEM は、それが収集できるログの種類が限られているため、可視性が狭く、検知効果を高めるための分析機能が備わっていません。システムがレポート/ワークフローツールであると同時に、ハント/分析エンジンでもあることは困難なことです。

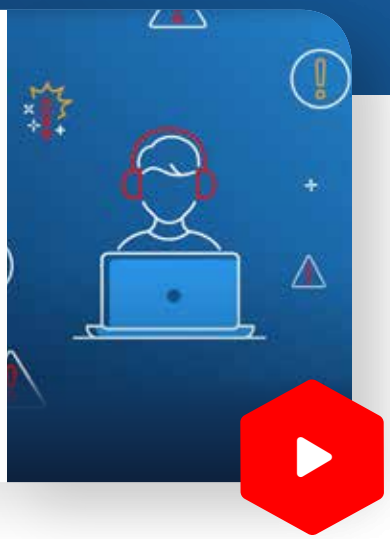
これが、企業が NDR に注目し始めている理由です。適切な人工知能（AI）／機械学習（ML）アルゴリズムを防御ポートフォリオに組み込むことで、皆さまは膨大な量のネットワークデータを処理して悪意ある行動のインジケータを検出するという課題に取り組むことができます。行動分析機能を備えた IronDefense（アイアンディフェンス）のような NDR ソリューションは、効果的なサイバー防御に必要な種類のセキュリティ toolset（ツールセット）を完成します。



皆さまの SOC チームは過負荷状態ではありませんか？

皆さまの SOC 管理者は、脅威の完全な可視化とアラーム過多の可能性のバランスについて懸念しているかもしれません。

このバランスを達成する方法についての詳細情報を知る。



ダイナミックな脅威に備えるダイナミックな検知

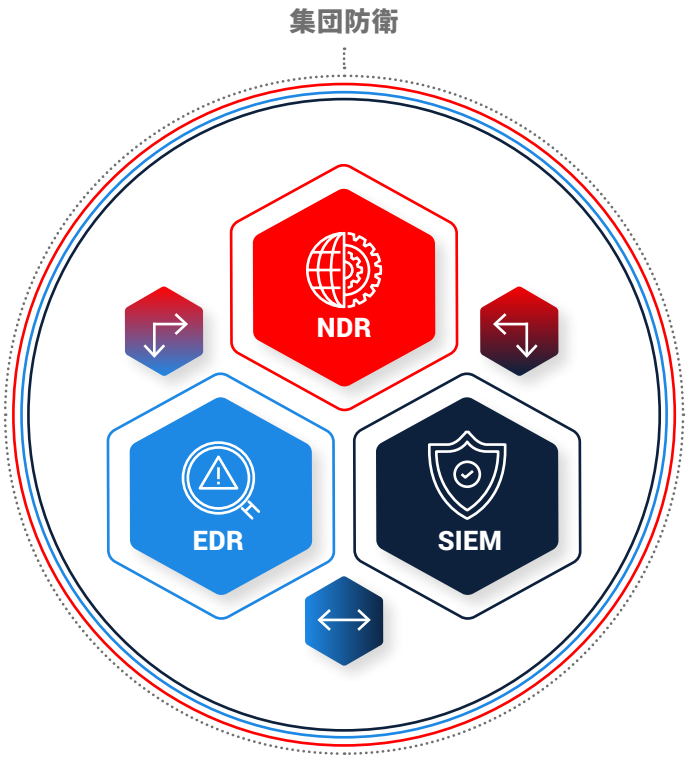
「SOC 可視化トライアド」の再検討

私たちは、NDR、EDR、および SIEM の静的トライアドを強力な適応システムとして想定するときが来ていると考えています。このシステムでは、三角形を構成する不可分な点のそれぞれが協力し合い、互いを強化することができます。

ダイナミックな検知フレームワーク

SIEM は従来、二次元トライアドの頂点に位置すると考えられてきました。なぜなら、SIEM はユーザー方向を見ながら、グループ内で唯一、データを取り込み、関連付け、分析することができるからです。しかし、SOC 可視化トライアドにさらに高いレベルの脅威インテリジェンスの洞察力を追加する方法があります。それは、トライアドのすべてのコーナーがサイバーセキュリティチームの相互接続システムに貢献することで、強固で進化し続けるピラミッド型にすることです。この協調的な検出フレームワークでは、各ノードが他のノードを強化して最強のサイバー防御態勢を形成し、サイバー上の許容誤差を集合的に削減します。これはまさにウィン - ウィンでどれにも有利なシナリオです。

皆さまが、SIEM、EDR、NDR の各ツール間でダイナミックな関係を構築するにはどうすればよいのでしょうか。その答えは、集団防衛であり、行動分析を利用しながら、共有した脅威情報をリアルタイムで、状況に応じて調整することです。アイアンネット（IronNet）のアイアンドーム（IronDome)）は、この協調的な取り組みを可能にするプラットフォームであり、SOC の可視性化トライアドをダイナミックなピラミッド型に変えるエンジンとなります。各ポイントはまさにマシンスピードで相互に通信し、常に相互に連携して、脅威の全体像を完全に把握できるように強化します。

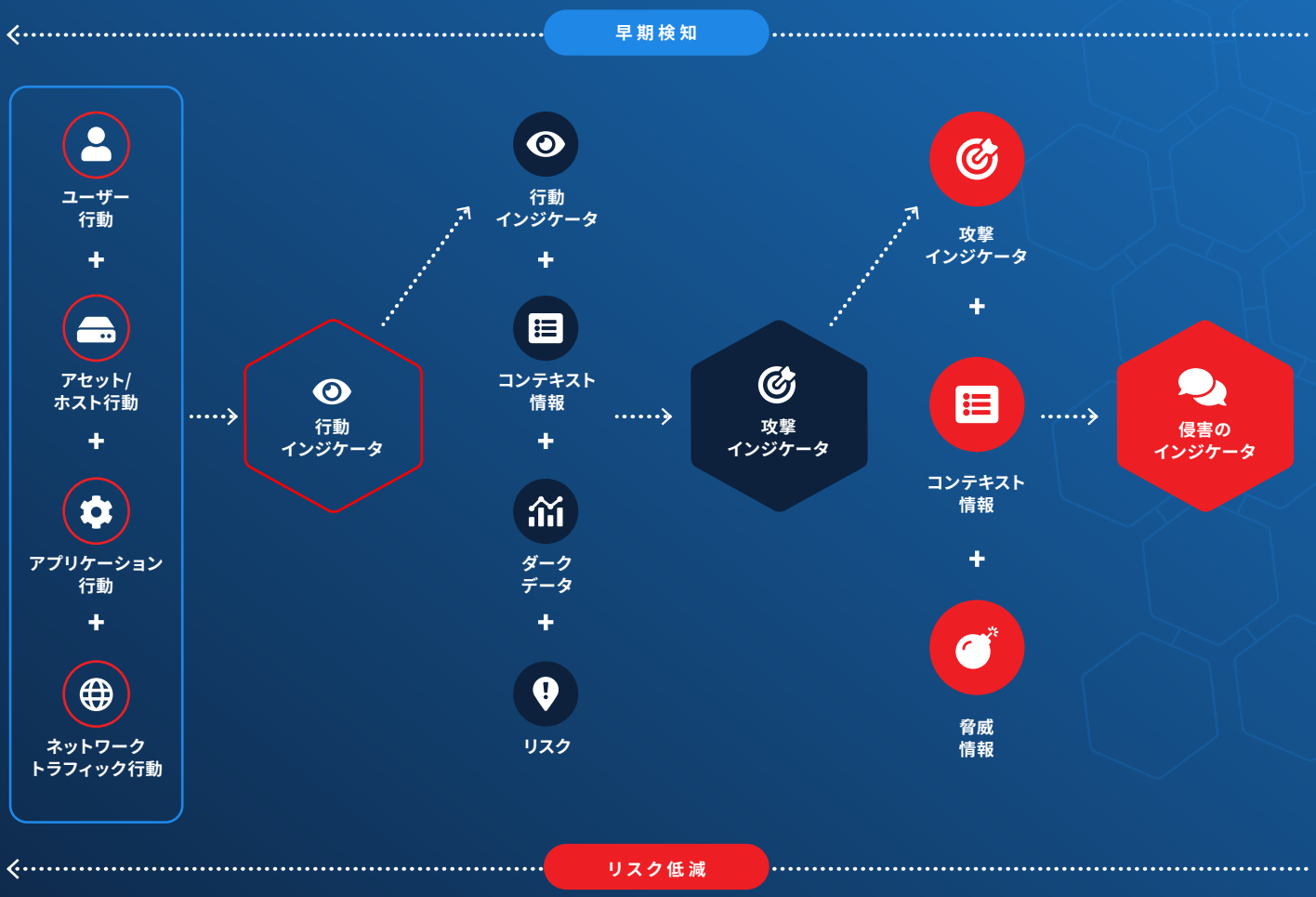


検知の段階：針を動かす

企業のセキュリティを確保しようとする組織が、ログベースの検知を長い間 SIEM のみの機能として扱ってきたことは理解できます。しかし、IronDefense（アイアンディフェンス）のような高度な行動分析を用いた NDR ソリューションは、妥協案を示すインジケータとしてのみならず、行動を示すインジケータ（IoB）に重点を置くことで、この概念に挑戦し、変えようとしています。簡単に言えば、侵害の兆候インジケータだけを検知しても、侵入サイクルの中でリスクを最小化するには遅すぎます。検知が早ければ早いほど、リスクが軽減されます。

行動インジケータとは何ですか？

ユーザー、ホスト、アプリケーション、ネットワーク全体の行動インジケータにより、内在的な IoC が変化しても TTP を検知することが可能です。行動分析により、内部または外部のアクターによる攻撃のステージングにおける潜在的な試みを識別することができます。



アイアンディフェンス（IronDefense）によるネットワーク防御の強化

アイアンネット（IronNet）は、IronDefense（アイアンディフェンス）の脅威アラートを侵入サイクルにマッピングするのに役立つという独自の行動分析と、IronDome Collective Defense platform（アイアンドーム集団防衛プラットフォーム）を備えており、皆さまの SOC チームが真に動的な防御を採用することが可能となります。一般的に NDR は最高の隠れ場所のように見られますが、アイアンネット（IronNet）の分析は、より多くの情報を得ているためより賢く、フラットな個別のトライアドを連結されたピラミッドに変えているためより強力で、新しい脅威情報にリアルタイムですばやく対応できます。

脅威セキュリティ分析、運用分析、および脅威検知を統合している結果、脅威のあらゆる段階で検知と分析が可能になります。このようにして、皆さまはサイバーリスクプロファイルを成熟させて「レフトオブブーム」（爆発の左横）に限りなく近づけながら、「ライトオブブーム」（爆発の右横）の防御態勢を強固で即応性あるものに維持することができるのです。

アイアンネットドットコム（IronNet.com）にアクセスして、schedule a live demo（当社のライブデモ）視聴予約をとってくださいダイナミックな脅威に対するダイナミックな検知機能。

IronNet™