電子ブック

IronNet™

集団防衛:
レーダーのような視点で
サイバー脅威を把握

サイバーセキュリティに関しては、「問題領域全体に可視性を有する単一の組織は存在しません。そのため、グローバルなエコシステムが個々人から集団へとサイバーレジリエンスを高めていくためには、コラボレーションと情報共有が不可欠となります。」

—世界経済フォーラム、2020 年 10 月

アイアンネットは、世界経済フォーラムの呼びかけに応えて、サイバー防御への協力体制に取り組んでいます。私たちはこのアプローチを「集団防衛」と呼んでいます。これは、セクター、サプライチェーン、国から構成される組織が、脅威情報を安全かつリアルタイムに共有し、すべてのメンバーに潜在的な攻撃の早期警告システムを提供する能力を意味するものです。

この電子ブックでは、集団防衛がどのように機能するかを説明します。

1. 業界やセクターを超えた、脅威の状況へのより明確な可視化が可能です。
2. SOC チームとサイバーセキュリティへの投資効率を高めます。
3. 偶発的事故への対応と復旧までの平均時間が短縮されます。

適切なアプローチを取るためには、主として以下のような適切な質問をすることから始まります。

- **私たちの組織は、新しい脅威に対応するために**適切なサイバー防御に投資しているのか、それとも、既知の脅威のみを識別できる従来と同じ技術を買い増しているだけなのか？
- **私はどうすれば、組織の手の届く範囲内に強力な防御を取得し、**その運用に必要な資源を確保できるのか？
- 脅威行動参加者間での連携が進む中で、**これらの脅威に正面から対応するために、**限られた予算の中でセキュリティチームを拡大し、こうした脅威に正面から対応するにはどうすればよいのか？

課題

サイバーセキュリティ技術と人材に何百万ドルもの投資をしているにもかかわらず、依然としてあらゆる業界や公共部門の組織が攻撃を受けています。その理由は何ですか？

例えば SolarWinds/SUNBURST や Microsoft Exchange へのサーバー攻撃が露出した際には、相手は脅威検出カバレッジの僅かなすき間を見つけていました。相手方は、ファイアウォールやエンドポイント検出ツールをすり抜けて、業界やセクターを超えて広く相互に接続されたエコシステムやサプライチェーンに侵入しています。

個別対象への攻撃は、急速に全体的への攻撃になりつつあります。これまでのシグネチャベースツールでは、ネットワークに向かっている敵対者や、すでにネットワーク上にいる敵対者を検知することはできませんし、手動のコミュニケーションに依存する従来の脅威共有システムでは、敵対者が検知された後に十分な速度での行動をとることはできません。言うまでもなく、ネットワーク上の膨大量の変則的な異常に対応できる SOC アナリストは不足しています。

行動分析機能を備えたネットワークの検知および応答（NDR）は、脅威の状況の可視性を幅広くするものです。

詳しくは NDR 電子ブックをご覧ください。

サイバーセキュリティの現状

315 日 悪意のある侵害を特定して封じ込めるまでの平均時間 (IBM/ポネモン・インスティテュート調べ)

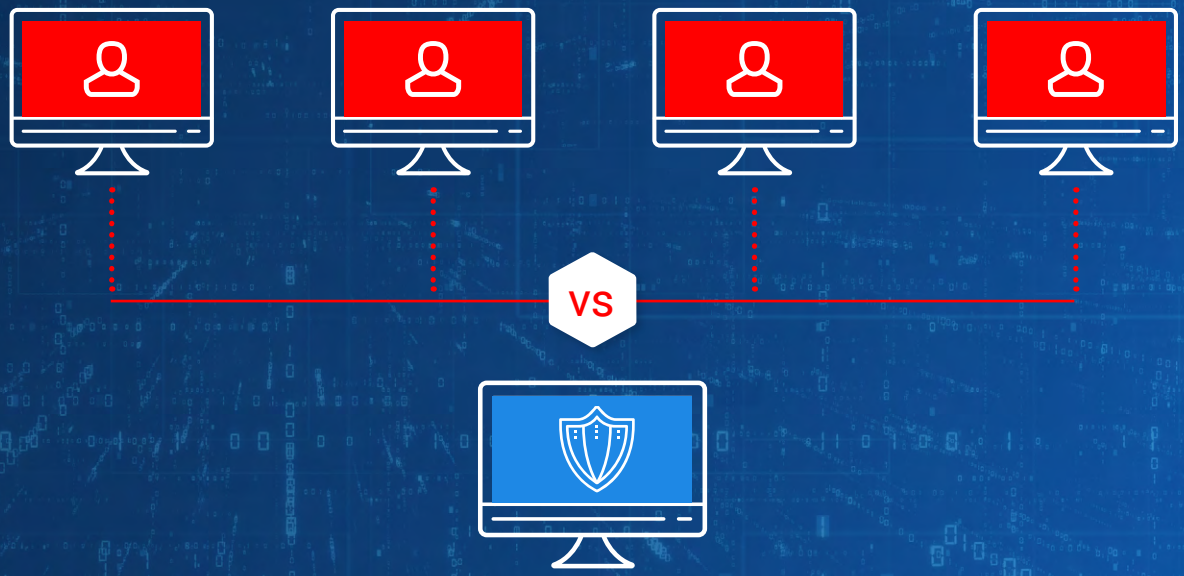
4.43 百万ドル 国家が関与していると推定される侵害による平均損害額 (IBM/ポネモン・インスティテュート調べ)

40% はサプライチェーンの弱いリンクに対するサイバー攻撃 (アクセンチュア調べ)

あなたは積極的に行動するのに十分対応できていますか？

数年前までは積極的なサイバーセキュリティと考えられていたことも、もはや十分ではありません。組織は、誰もがパッチ適用、ソフトウェア更新、ファイアウォール、およびその他の責任ある手段を実装する必要がある一方で、これらだけでは十分ではないことを認識しなければなりません。**脅威の可視化にはすき間があり、攻撃者の侵入を許すことになります。**

サイバー攻撃者たちは協力し合っています。**では、なぜ私たちも一緒になって防衛しないのでしょうか？**



攻撃者がより強力になってきているのは、コラボレーション、つまり「集団的攻撃」が増えてきたことが一因です。簡単に言えば、悪意ある攻撃者はこれまで以上に迅速に、効果的に、そして有益に連携しております — ダークウェブ上でのデータや不具合利用ツールの共有の増加から、侵害の成功、国家機関によるサイバー犯罪のアウトソーシング、さまざまな家内工業的な「サイバー傭兵」グループの台頭に至るまで。今日の高度な攻撃者の多くは、従来のサイバーセキュリティツールを回避するように設計された標的型技術を活用しています。

このような状況を背景にして、公共機関、フォーチュン 500 企業、中小企業、サプライチェーンのサービスプロバイダーなど、あらゆる規模の組織が同じ状況に置かれていますが、この問題に対処するためのリソースのレベルはそれぞれ相違しています。デジタルで相互に接続された世界において、個々のサイロを守るためにますます多くの費用を費やすという現在の対処方向は、持続不可能です。結果として、サイバー脅威に遅れず対応するための、新たなサイバー防御戦略が必要なのです。**私たちには「集団防衛」が必要です。**

簡単に言えば、悪意ある攻撃者はこれまで以上に迅速に、効果的に、そして有益に連携しております — ダークウェブ上でのデータや不具合利用ツールの共有の増加から、侵害の成功、国家機関によるサイバー犯罪のアウトソーシング、さまざまな家内工業的な「サイバー傭兵」グループの台頭に至るまで。

解決策

防御におけるスケールメリット

「米国政府と産業界は、サイバースペースにおける国家の安全を確保するために、責任を共有する新たな社会契約にまで到達する必要がある。このサイバースペースにおける「集団防衛」においては、官民が真に状況認識を共有し、それぞれが独自の比較優位性を共通の防衛のために活用することが必要である。」

— 米国サイバースペースソラリウム委員会報告書

企業は従来以上に他者と相互に結びついています。そのため、サプライチェーン、パートナー、ゲストのアクセスは、サイバー攻撃者にとって大きな脅威のベクトルとなっています。SolarWinds や Microsoft Exchange への攻撃で明らかになったように、エコシステム全体のサイバーリスクは、手遅れになるまで知られないことが多いのです。

すべての人のためにサイバーセキュリティを強化する最善の方法は、セキュリティアナリストの判断力とデータサイエンティストの行動分析力を組み合わせた協調的なアプローチを採用して、マシンスピードで脅威を検知することです。それによって、集団防衛エコシステムへの参加者は、業界の枠を超えて仲間と協力することができます。これは本質的に、脅威の先を行くための「防衛の経済的スケールメリット」と言えるでしょう。

このアプローチは、同じことを再度繰り返すのではありません、代わりに、既存の人材、リソース、ツールをより効果的に活用するものです。

ステップ 1: 行動検出の高度化

昨日までの既知の脅威に焦点を当てたシグネチャベースの検知方法から、システムの悪用やデータの流出を阻止するには遅すぎる最終的な「標的に対するアクション」のステップだけでなく、侵入サイクル全体にわたってネットワーク上の未知の脅威の根本的な動作をプロアクティブに識別する動作ベースの検出機能へと移行します。

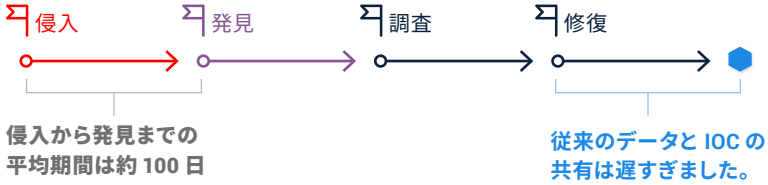
ステップ 2: リアルタイムでの脅威の共有

脅威の洞察を共有し、受信することで、サイバースペースでのレーダーのような早期警報システムを創造します。集団防衛エコシステムにおいて、参加者は官民の仲間のコミュニティ全体で匿名化された個々のサイバー異常をマシンスピードで積極的に共有することができます。このクラウドソース利用による脅威の共有機能により、企業は攻撃サイクルの早い段階で、敵対的手法の多くが一企業での検知閾値を下回った時に、ステルス攻撃者を特定することができます。

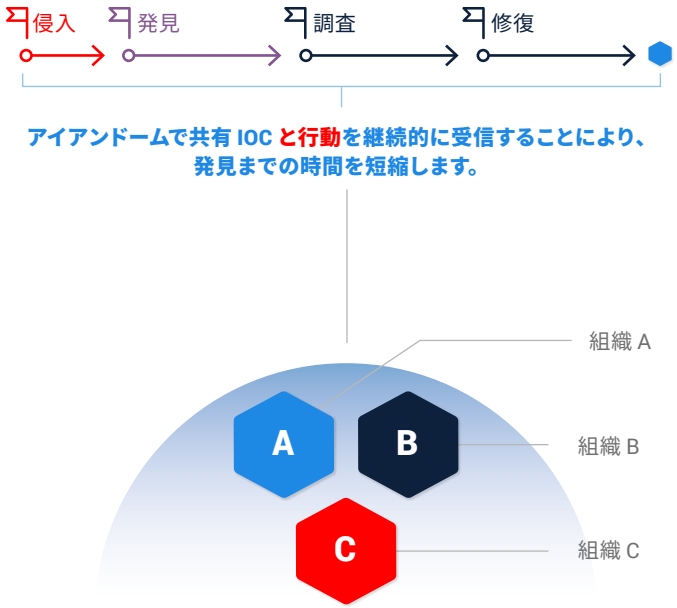
ステップ 3: 仲間との協力

リアルタイムフィードバックに基づいた選別と反応の洞察のためにコミュニティに参加することで、リアルタイムのフィードバックに基づいたトリアージや対応策を得ることができ、これにより参加者はアクティブな脅威を軽減するために迅速に行動を起こすことができます。集団防衛の参加者が団結して一丸となることで、すべての参加者は、リソースを最適化して「防衛経済のスケールメリット」を達成することができます。

伝統的なデータ共有では、サイバー脅威を回避するには遅すぎ事態が発生しました

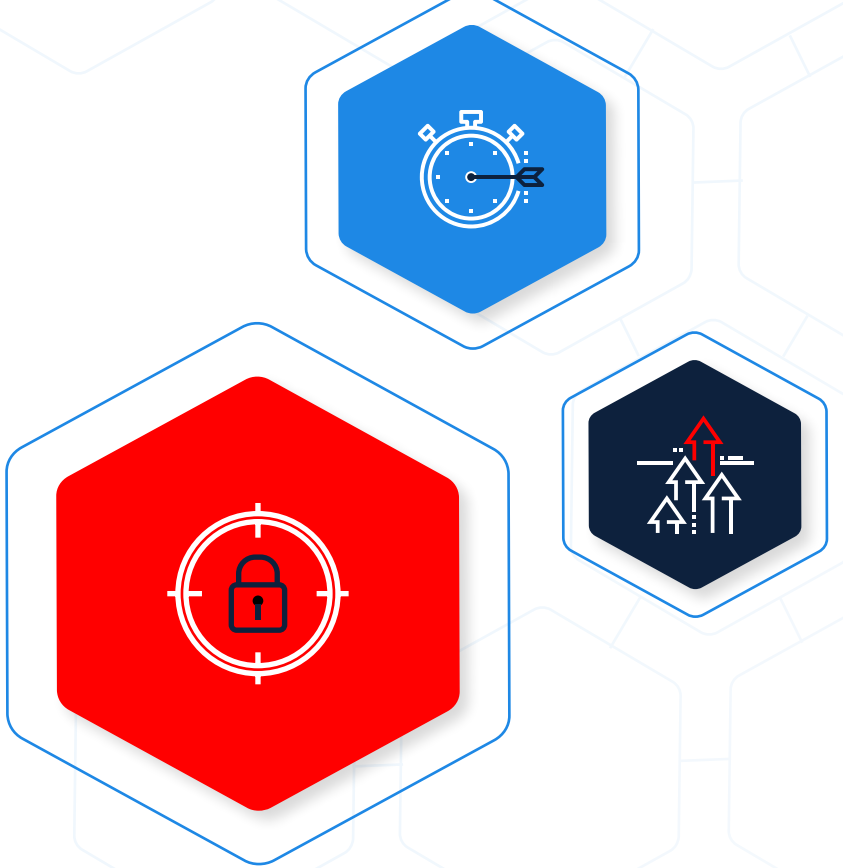


集団防衛データと行動の共有は、リアルタイムで継続的に行われ、滞留時間が短縮されます



メリット

- 既存のシグネチャベースのツール、エンドポイント検出および対応ツール、ファイアウォールでは気づかれることがない異常なネットワーク活動をより正確に検出することができます。
- 匿名化された脅威を共有することで、既知および未知のサイバー脅威をリアルタイムでさらに明確に可視化できます。
- 自治体や州、連邦政府機関、民間企業セクターを標的とした脅威の早期警告できます。
- ネットワーク速度で洞察力を共有することにより、SOCチームの有効性が向上し、サイバーリソースが最適化されます。
- 統一勢力として協力することで、より迅速なトリアージと強力な対応能力を実現。



18,000 SolarWinds の攻撃により侵入された公共機関および民間企業の数

もし、これらの企業のセキュリティアナリストが、異常や行動をリアルタイムで共有できていたらと想像してみてください、攻撃を数か月前に停止できていたはずです。

SolarWinds/SUNBURST に対するアイアンネットの対応については、こちらをご覧ください。

データのプライバシーが心配ですか？

集団防衛のエコシステムでデータ・プライバシー・コンプライアンスを維持する方法の具体的説明が得られます。

ホワイトペーパーを参照してください。

結論

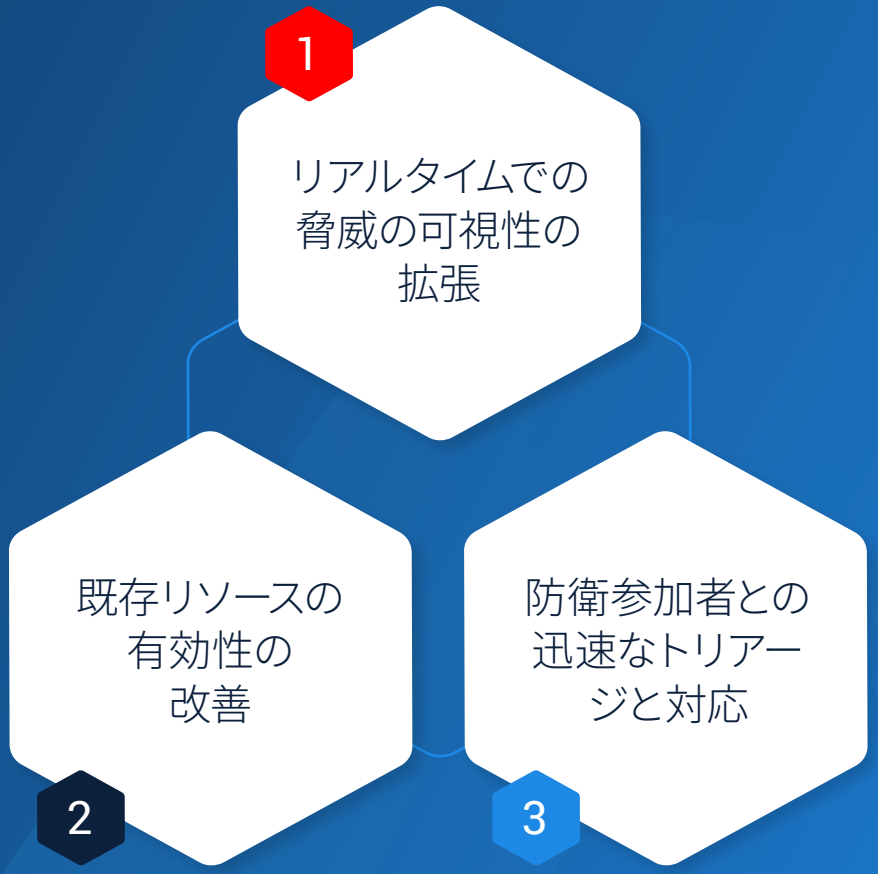
「当社の目標は、脅威の状況を常に最も広い視野で把握できることです。これが、最初にアイアンネットと契約した理由の 1 つであり、高品質で自動化された状況認識を取得して、手動に依存する方法から脱却するためです。」

— トム・ウィルソン
Southern Company 社 副社長兼 CISO
ケーススタディをお読みください。

集団防衛によるサイバーセキュリティの変革

アイアンネットの集団防衛プラットフォームは次のもので構成されています。

- アイアンディフェンスは、高度なネットワーク検出および応答 (NDR) ソリューションであり、ネットワークレベルで動作ベースの AI 駆動型分析を提供して、個々の企業の異常なアクティビティを検出し、企業のネットワークで最も高い脅威に優先順位を付けます。
- アイアンドームは、クラウドソーシングのような環境を促進する脅威共有ソリューションであり、個々の企業によるアイアンディフェンスの検出結果は、自動的かつ匿名でリアルタイムに共有され、より迅速なトリアージと対応のために、自発的な参加者の洞察力が得られます。



集団防衛の実戦行動を参照してください。**デモンストレーションをリクエストしてください。**

IronNet™