会社概要

サイバーセキュリティーを再定義する

アイアンネットが導入するのは、第一線の自動化されたコラボレーションプラットフォームです。高度な分析により、互いに関連性のある検出事例を報告し、匿名のメタデータをリアルタイムで共有することができます。これぞ集団防衛です。

> 米国政府と業界は……
> サイバースペースにおける国防を担うため、責任を分かち合い、新たな社会契約を結ぶ必要があります。サイバースペースにおける、この新たな「集団防衛」を機能させるには、公的機関と民間企業が、状況認識を文字どおり共有する場を持ち、共通の防衛目的のため、それぞれ、自らの立場に与えられた比較優位を活かす必要があります。
>
> *サイバースペース・ソラリウム委員会*
> *報告書、96 ページ*

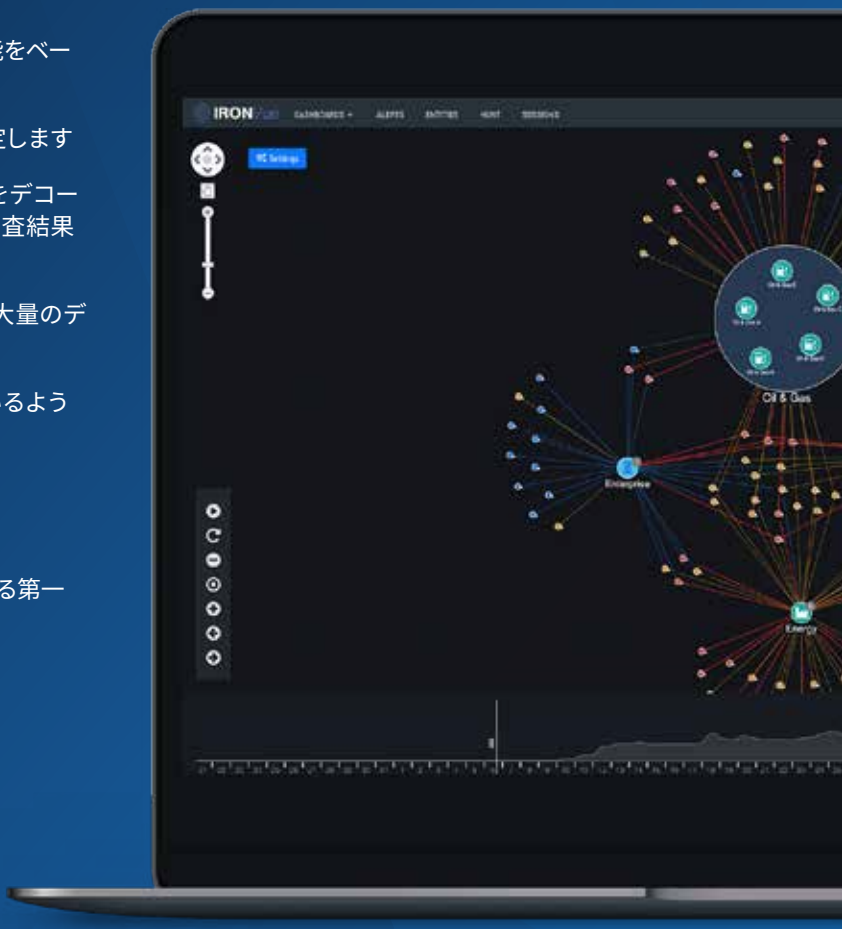
アイアンネットについて

アイアンネットサイバーセキュリティーは、アメリカ国家安全保障局（NSA）長官やアメリカサイバー軍の司令官を歴任したキース・アレクサンダー退役陸軍大将が設立した会社で、高度標的型攻撃（APT 攻撃）を特定し、その被害を軽減することができる包括的な多層防御ソリューションを提供いたしております。アイアンネットは、機械学習を活用し、世界クラスのデータサイエンティストの手になる分析技術を展開しており、これまでの業務実績のなかで培ってきた知識や経験（トレードクラフト）も活かしつつ、重要インフラ、各産業分野、州政府、連邦政府を、お守りしています。

サイバーセキュリティに関する課題	アイアンネットのソリューション
• 国家が絡む攻撃の前には、個別的な防禦は無力で、機能しません	• 共通の脅威に対抗できる集団防衛をリアルタイムで実現するコミュニティベースのプラットフォームを提供いたします
• 民間企業と政府は、国益を守るため、コミュニケーションを取りあい、一丸となって協力する必要があります	• 互いに関連性のある検出事例と、アナリストによる調査結果を、コミュニティ全体で匿名で共有できます
• 地球規模で行われる脅威キャンペーンを検出できるようにするため、民間企業のネットワークの可視性が求められています	• 共通の脅威を可視化することで、御社が被害に遭うまえに、キャンペーンや攻撃を検出します
• マルウェアやツールの変化が早いため、シグネチャ型の検出は無力化しつつあります	• 高度な行動分析を展開しており、ほとんどのサイバーセキュリティ企業が見落としている脅威も検出できます
• 検出が遅すぎ、すでにネットワークへの侵入を許し、データが盗まれたあとだった、ということが頻繁に発生しています	• 集団防衛インフラ、および、セキュリティ情報・イベント管理（SIEM）とセキュリティオーケストレーション・自動化・応答（SOAR）の統合により、実用的な対応を迅速に提供いたします
• セキュリティ業界では、脅威を特定し、その被害を軽減できる、訓練を積んだサイバーセキュリティアナリストの不足が深刻です	• これまでの業務実績のなかで培ってきた知識や経験（トレードクラフト）をエキスパートシステムに組み込んでおり、アナリストのワークフローのうち、いくつかの手順を自動化しています

アイアンディフェンス

- ネットワークの典型的な動作を学習して逸脱を報告する分析機能をベースにして構築された高度なネットワーク検出および応答
- エキスパートシステムの計算ルールを適用し、リスクスコアを決定します
- DNS トンネリングを検出し、アナリストが、盗み出されたデータをデコードし、パケットキャプチャ（PCAP）ファイルをダウンロードし、調査結果を共有できるようにします
- HTTP、HTTPS/TLS、DNS プロトコルを通してネットワークから大量のデータが盗まれた場合、即座にアラートを発出します
- ランサムウェア攻撃を識別するほか、ネットワーク上で急増しているようなフィッシング攻撃をユーザーがクリックした際も、識別します



アイアンドーム

- 商用データからの脅威検出をリアルタイムで共有することができる第一線の集団防衛自動化プラットフォームです
- IT-ISAC（情報技術―情報共有分析センター）のような脅威インテリジェンスフィードではありません
- セキュリティ侵害インジケーター（IoC）のうち、互いに関連性のある匿名のメタデータを、迅速に共有することができます
- アイアンネットがアマゾンウェブサービス（AWS）の中に設けているプライベートクラウドから展開するため、セキュリティと信頼性に優れています
- アナリストは、集団防衛ポータルまたは Splunk や Qradar などの SIEM を通して、調査結果やコメントをコミュニティと共有したり、コミュニティの力を借りてアラートを評価したりすることができます

アイアンディフェンスは、世界クラスの検出を維持するため、日々増え続けている行動分析のうち、以下を使用しています。

リカバリー管理データ・セット (RECON)

- 外部 IP スキャン
- 外部ポートスキャン
- 内部 IP スキャン
- 内部ポートスキャン

アクセス

- フィッシング HTTPS
- クレデンシャルフィッシング
- 個人を特定できる情報 (PII) データの紛失
- 一連の横展開
- 疑わしいファイルのダウンロード

コマンド&コントロール (C2)

- DNS トンネリング
- ドメイン生成アルゴリズム（DGA）
- ドメイン分析 HTTP/TLS
- 定期的に Web ビーコンを使用している HTTP
- 一貫した Web ビーコン使用
- 暗号化通信

アクション

- 極端な値
- 極端な値を示す TLS 通信
- 通常とは異なる 1 日の動き
- DoS 攻撃

その他

- 脅威インテリジェンスルールの一致
- 無効な TLS 証明書チェーン
- Tor トラフィック
- レアな ASN (ActiveService Network)

集団防衛を体験する

アイアンネットのコミュニティにご参加いただき、集団防衛の力を直接ご体験ください。アイアンネットは、包括的な価値実証（PoV）プログラムを提供しており、御社が現在運用されているサイバーセキュリティソリューションの有効性を評価いたします。これにより、既存のシステムから出発して、高度な行動分析や集団防衛を実現するに至るまでの手順や方法を決定することができます。

今すぐ始めましょう。アイアンネットの営業担当者にお電話いただくか、info@IronNet.com までメールをお送りください。