Secure SketCH

EDR 導入ガイド

Secure SketCH Books VOL.10

インシデント前提社会の最適解

インシデント対応の課題

EDR導入のベネフィットとは

製品選定のためのヒント

Secure SketCH Books VOL.10

EDR導入ガイド

目次

CHAPTER 1

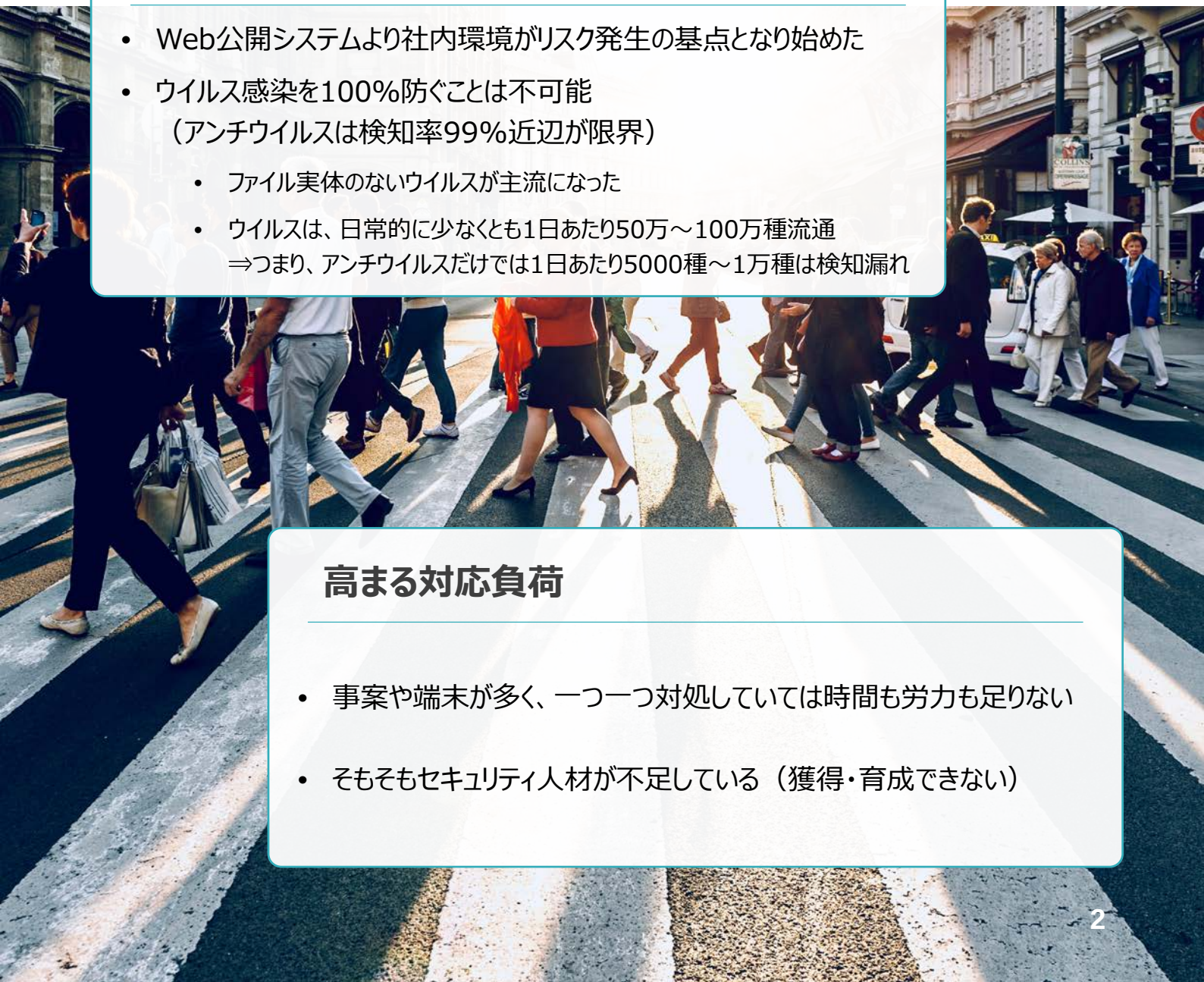
企業を取り巻く環境の変化

企業活動をとりまく環境の変化が、セキュリティに関するインシデント対応に今まで以上の困難を生んでいます。

脅威トレンドの変化に対応する人員の負荷は高まり続け、テレワーク推進、GDPR施行といった内的・外的の環境変化にも対応しなければなりません。

脅威トレンドの変化

- Web公開システムより社内環境がリスク発生の基点となり始めた
- ウイルス感染を100%防ぐことは不可能
  （アンチウイルスは検知率99%近辺が限界）
  - ファイル実体のないウイルスが主流になった
  - ウイルスは、日常的に少なくとも1日あたり50万～100万種流通
    ⇒つまり、アンチウイルスだけでは1日あたり5000種～1万種は検知漏れ



高まる対応負荷

- 事案や端末が多く、一つ一つ対処していては時間も労力も足りない
- そもそもセキュリティ人材が不足している（獲得・育成できない）

ビジネス環境の変化

- 働き方改革推進、テレワーカーや営業など、社外からのアクセス増加
- 海外拠点の対策が弱く、日本側で一括管理したい
- 企業体の統合・分割・M&A等により通信出入り口が複数あり、
  持ち株会社主体の対策が煩雑

強まる法律の要求

- セキュリティ経営に対する重要性の増加
- 経産省サイバーセキュリティ経営ガイドライン v2.0　指示5　指示8
  「防御・検知・分析・復旧を実施する体制を構築せよ」
- GDPR（EU一般データ保護規則）
  厳しい罰則(年間売上の4%か約26億円)と共に、72時間以内の
  報告責任が規定
- 働き方改革法成立
  人材不足の中、更なる残業の規制「原則月45時間・年360時間」

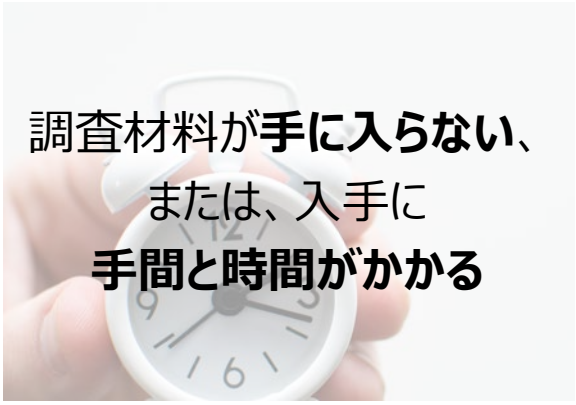
CHAPTER 2

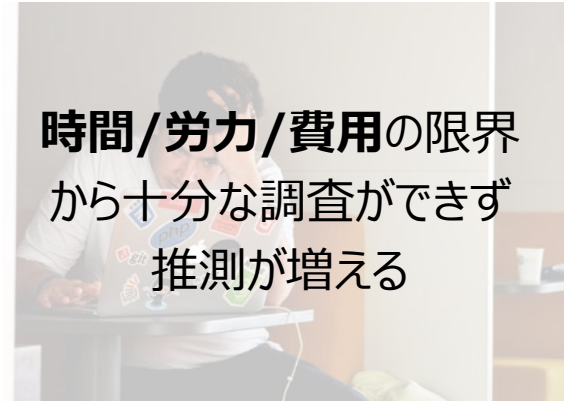
インシデント対応における課題

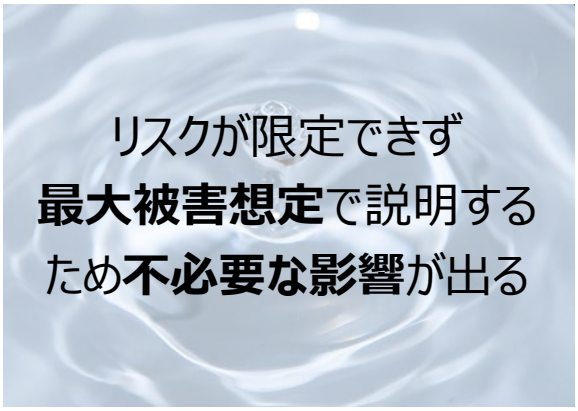
次に、インシデント対応の現場での課題を見ていきます。

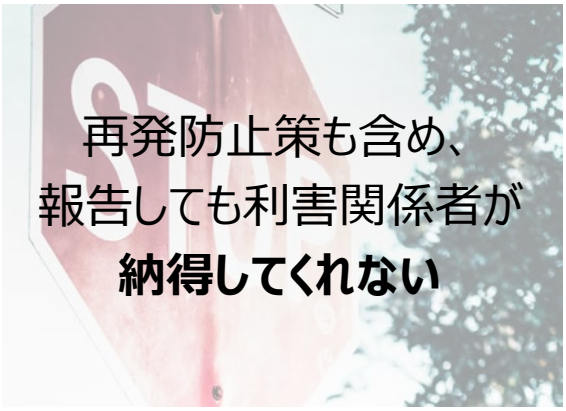
これまでも攻撃者側の手口に学び、対抗手段としての「防御・検知」の仕組みは高度化してきました。しかしながら、インシデント対応の現場では異常を発見してからの対処、すなわち「レスポンス」の質が成熟しておらず、対処能力の向上にまだまだ課題があります。

従来のインシデント対応で頻出する苦しみとして次のようなものがあげられます。









これをインシデント対応プロセスの各フェーズ毎における課題として見てみると、
次のようになります。

インシデント対応フェーズ毎の課題

検知

- 外部からの通報で気づく
- 日常的な大量アラートに埋もれて危険な事象に反応できない
- 何か検知してもそれ以上の情報がなく漠然とした不安が残る
- 監視ベンダーからの一報だけでは白黒が付けられず、対処方法が不明

初動

- ウイルス名は分かるが、どんな脅威に晒されているのか分からない
- 検知したもののみ対応すればよいと考えてしまう
- 状況を過小評価してしまい、そのまま見過ごしてしまう

被害拡大防止

- 端末の稼動を止められず、被害拡大も止まらない
- サーバの停止や端末の抜線が先行されてしまう
  （実際の大規模インシデントから強まった考え方）
- 調査が終わるまで復旧できず業務停止してしまう
- 被害抑止の範囲が不足して更なる被害が出続けてしまう

現状有姿

- ログを取っていない / 内容が不足している
- アンチウイルスでフルスキャン / 端末初期化して痕跡が消滅
- 端末が海外にあって運べない / 入手に時間がかかる

詳細調査

- 異常の痕跡が殆ど消えており、リスクを説明しきれない
- 異常がないことの証明（悪魔の証明問題）
- 説明請求を受けているが、調査に費用と時間がかかりすぎる
- 数ヶ月かけても終わりが見えない

再発防止・事象説明

- 調査結果が曖昧で、説明も曖昧になる
  最大リスクで説明せざるを得ないため、賠償が高額化し、
  再発防止策も広きに渡る
- 水に沈めてしまえそうな気になる
  例） 逆に「盗まれたという証拠もない」という論調になる
  よくある障害事案として片付けてしまいたくなる
- 自前調査では利害関係者が納得してくれない

もちろんこれで全部ではありませんが、以上がレガシーなインシデント対応で頻出する展開です。

CHAPTER 3

EDR導入のベネフィットとメリット

前章で紹介してきた企業とりまく環境の変化や、インシデント対応が抱える従来の課題を解決するソリューションとして、EDR（Endpoint Detection and Response）が注目を集めています。EDRを導入することでどんなベネフィットが得られるのでしょうか。

代表的なものとして以下の3つが挙げられます。

1. ソリューションの運用負荷、インシデント事後の対応の作業・心理負荷を下げ、**生産性の向上**に寄与する。

2. ウイルス感染が発生しても、情報漏えいなどのリスク発現を阻止し、必要十分な対処を行うことで**企業のレジリエンス**※を高める。

※困難な状況に耐える、あるいはその状況から迅速に回復する能力

3. 有事にも何が起こったのか明確にした上で利害関係者に対する説明責任を果たし、**誠実な企業イメージを形成**する。

EDR導入で獲得すべきベネフィットとは、人材、経営、顧客の三方良し、つまり会社が強くなるという状況だと考えます。

EDR導入のメリットがベネフィットを生み出す

では、ベネフィット獲得のためにEDRのどのようなメリットが有効なのでしょうか。

EDR導入のメリット

記録がとれる

過去の事象が十分に記録されており、異常を見える化できる

無力化できる

- 潜伏した脅威も能動的に発見(スレット・ハンティング)できる
- 端末が社外にあっても情報漏えいなどの致命的なリスクが発現する前に阻止できる

把握できる

影響疑義範囲について迅速に網羅的な調査を行い、的確に事象を把握できる

より楽になる

- 十分な材料を元に、説明と決断にかかる負荷を下げられる
- 維持・運用の総保有コスト(TCO)が削減できる

ちなみに初期の頃は、アンチウイルスとは別の市場としてEDR市場が形成されていましたが、現在ではアンチウイルス機能搭載がスタンダードになっています。

端末セキュリティに関して欲しい機能はアンチウイルスだけではありませんが、EDRでは端末の様々な情報を取得していますので、論理的に統合可能なソリューションが出てくると予想しています。たとえば、内部犯行抑止目線でのUBA、データに着目したDLP、端末に搭載されているアプリケーションの脆弱性管理などのIT衛生、他、ITサービスマネジメント、オーケストレーションなどです。

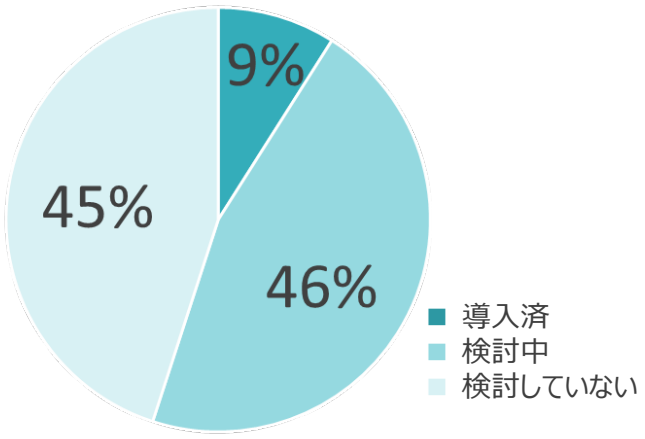
EDRは確実に拡張性、連動性のある製品に進化していくでしょう。

CHAPTER 4

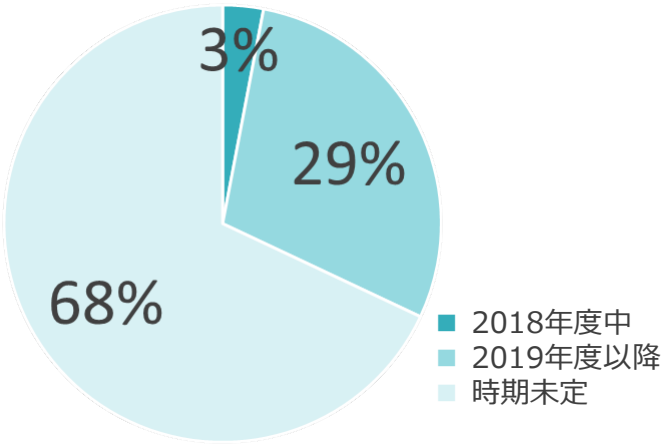
EDR製品選定のポイント

本題に入る前に、2018年8月に弊社が実施したセミナーにご参加いただいた方を対象とした、EDR導入状況についての調査結果をご紹介します。

EDRの導入を検討していますか？(n=59)

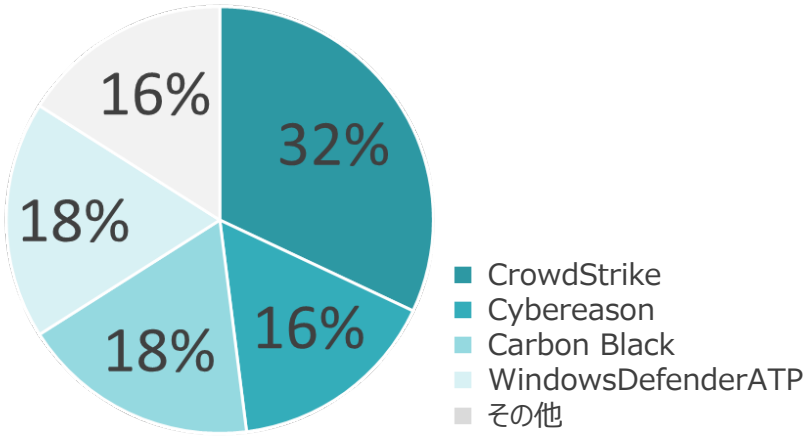


いつ頃の導入を予定していますか？(n=59)



EDR導入が終わっている企業はまだ少なく、これから検討、またはまだ検討していないという方がほとんど、という結果でした。

どの製品を検討中ですか？(n=59)



実はEDR製品は30種類以上あり、選択が悩ましい状況です。
本調査ではCrowdStrike、Cybereason、Carbon Black、Windows Defender ATPの検討多いという結果でした。

次ページからは4つの観点に分けて、EDR製品の選定ポイントを解説します。

4-1. 第三者評価の参照と価値検証

EDR製品を選定する際に外して欲しくない手順として、「**第三者評価レポートの参照**」と「**価値検証**」が挙げられます。

第三者評価レポートの参照

製品ベンダー自身がする内容は、例えば主機能の欠点を長所に言い換えていたり、導入実績が製品の良さをダイレクトに反映できていなかったりと、必ずしも買い手に必要な情報だとは限りません。
そこで、製品を客観的に評価している第三者評価レポートを参照することをおすすめします。

EDRについてはガートナーやフォレスターのレポートが参考になります。マネージドサービスや、
アンチウイルス機能の比較という点でもいくつかレポートがありますので、ご参考までに。

例）
- EDR：Gartner: Magic Quadrant for Endpoint Protection Platforms
  The Forrester Wave™: Endpoint Detection And Response
- マネージドサービス：フロスト＆サリバン：エクセレンスアワード
- アンチウイルス性能：AV-Comparatives、
  AMSTO(Anti-Malware Testing Standards Organization)

価値検証（PoV, Proof of Value）

昨今PoCというより、PoVという言い方をされ始めていますが、製品の概念を検証したいのではなくて、価値を検証するのだ、という思想です。

まず自社の既存・次期環境に導入可能なのか最低限確認してください。
また、どのように使えば現状が改善するのかイメージを作ることが必要となります。
その際、無償での試用やキャンペーン特価を活用すると良いと思います。

4-2. コストの捉え方

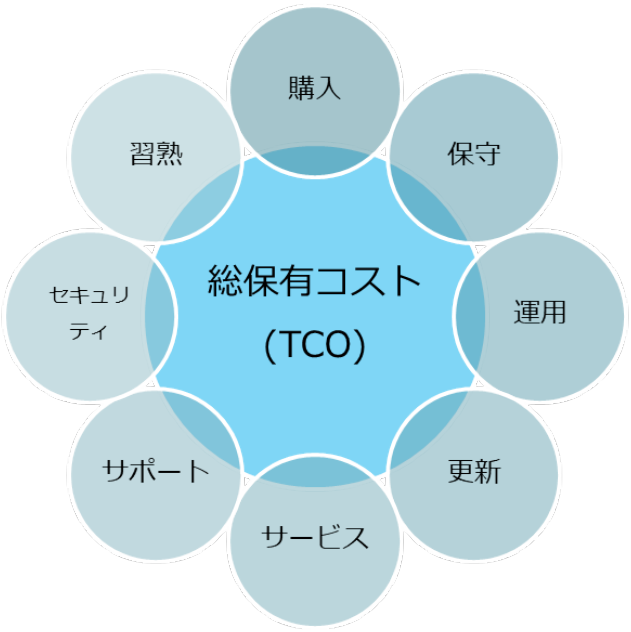
次にコスト観についてです。
新機軸のものを考えるにあたり、コスト観は広義に捉えて頂き、全体でプラスとならないか、と検討する必要があります。

たとえば、初期費とライセンス費だけで計らず、置き換えられるアンチウイルス等の費用も加味するということです。
ちなみに、アンチウイルスとEDRを別々の製品で運用するということはお勧めしません。
アンチウイルスで検知した情報をEDRに持っていって調べるという作業が必要になるからです。
これらは連動しているほうが望ましいと言えます。

また、圧縮できる費用も考えます。製品によるところもありますが、シグニチャアップデート、定期スキャンが不要だったり、状態管理も手間なし、管理サーバ不要でメンテナンス負荷もなしなどです。

さらに、日々の対応負荷がどれくらい減少するかを定量化してみるのもよいと思います。
例として、１日1人あたり10万円のコストの企業で、誤検知が月3回発生しているとします。
結果として誤検知とはいえ、2人がかりで誤検知として収束させるまでに2日かかるとすると、1440万円年間にかかる試算になります。
この対応が4分の1程度に圧縮できるのであれば、1080万は浮くので投資にまわせる、などです。

これらは一例ですが、コストについては総保有コスト（TCO）の枠済みで整理すべきと考えます。



4-3. 機能面の確認

機能面としては「**検知精度**」、「**記録量**」、「**調査のし易さ**」の3つを確認することが重要です。

また、弊社がEDR製品の性能を検証した結果をご紹介します。

検証

- アンチウイルス機能をOFFにし、純粋にEDRの性能だけを比較
- サイバーキルチェーン、つまり一連の攻撃フローを再現し、120箇所の攻撃の特徴をどれだけ多く見つけられるかを調査

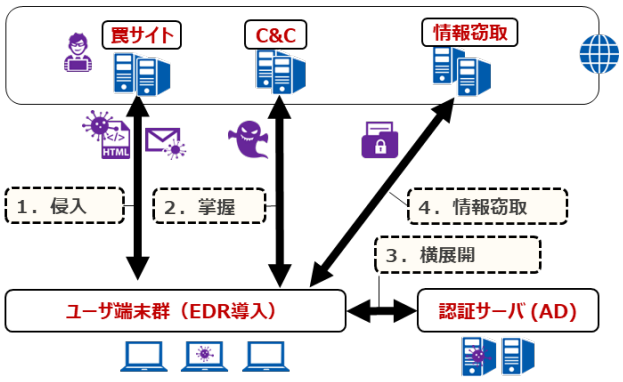
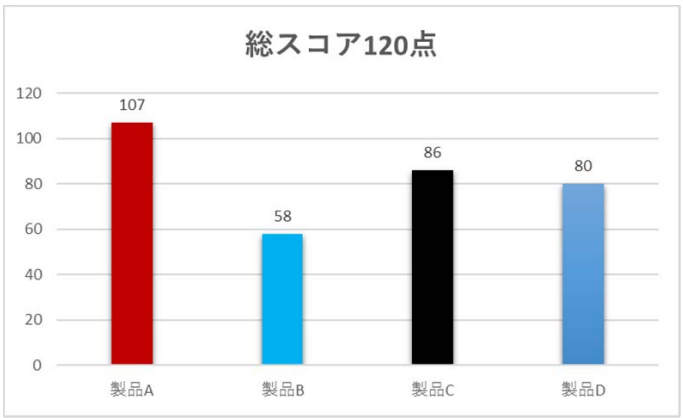


図.検証に用いた攻撃フロー



※2017/01～2018/09弊社調査時点

図.検証結果

見つけられる特徴が多いほど、リスク発現を回避できる可能性や、明確な説明ができる可能性が高まる、ということを意味します。

評価の結果、製品の重要な機能の性能にバラつきがあり、スコアに差がつきました。

良い製品や、良い製品を使うサービスを選択しないと投資損になる可能性が高いという気付きがありました。

注意の必要な仕様

1

ユーザモード動作

- 記録される情報が不十分、かつ、攻撃によって停止される可能性がある
- カーネルモードで動作する製品を選択する

2

対応OSが限定されている

- 包括的な管理の障害になる。
- Windows以外は3rdパーティ製品が必要、などの要件もネガティブ要因
- 他製品と連携というスペックは、性能が一部他製品頼みということ

3

実行ファイルしか記録していない

機密情報はドキュメントファイルにあり、その操作が記録されないため、
情報漏洩のシロクロがつけにくい

4

各端末にログが保存される

調査時に一斉に各端末にアクセスするため端末が高負荷になったり、
障害を起こしやすく、従業員の生産性に悪影響する可能性

5

OSに付属している

- 脆弱性が定期的に公表される宿命
- ウイルス被害を抑止するための製品なのに逆に感染の原因になるため
  緊急パッチ適用などの一定の負荷を覚悟することになる

6

深層学習偏重の検知エンジン

- 誤検知が多くなる傾向があり、負荷が高くなる恐れ
- なぜ異常なのかという情報が提供しにくく、状況判断や説明に困る可能性

7

何でも遠隔操作できる、ファイルの中身が閲覧し放題

コンプライアンス配慮が困難、例えば、EDR操作する人材が、役員の端末を
操作できたり機密を閲覧できるのは不適切

8

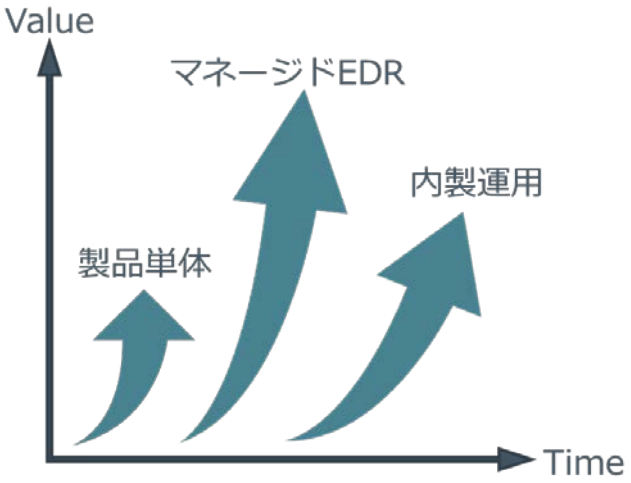
とにかく使いづらい

- 対応の速度感が改善しない、使いこなせずに終わる可能性が高まる
- 良い道具を技術者に与えないとモチベーションが上がらず、
  対応品質向上が図れない

4-4. サービス面の確認

EDRを活用することを考える際に、1つ注目したいのが「**Time To Value**」という考え方です。端的に言うと、導入から価値が生まれるまでのリードタイムが短いほどよいという考え方です。

人材不足の中、EDRの性能をフル活用し、いち早くベネフィット獲得に至るには、監視ベンダーへのアウトソースを検討するのがひとつの近道と言えます。



監視ベンダーにアウトソースを検討する際は、以下の点に注意が必要です。

レベルの低い能動的脅威探索(スレット・ハンティング)

EDRを使った能動的な脅威探索活動が可能になることは非常に有益なメリットなのですが、それを行う主体が機械的な処理だけですと、効果が出にくいと考えます。
選定の際には、人、つまりセキュリティの専門家がスレットハンティングに介在していることが重要です。

製品が検知したアラート以上の内容が提供できない

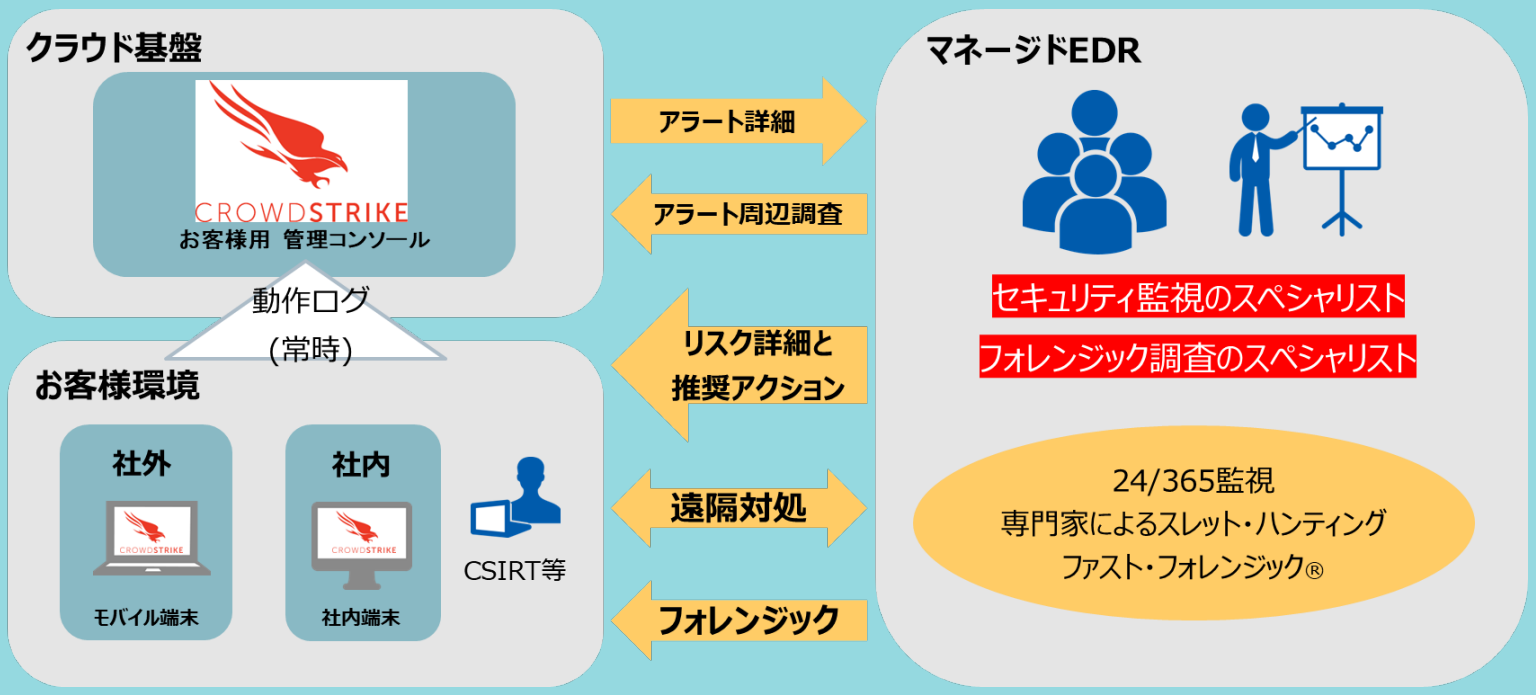
検知したアラートの解説のみで対応まで踏み込んでくれない、サービスには注意です。
MSSと区別してMDRという呼び名も出てきていますが、検知だけでなく対応まで踏み込んだサービスの方が望ましいです。

インシデント対応能力が心もとない

インシデント対応能力が最も自社に不足すると思いますが、そこをできるだけ補完できるベンダーを選ぶ必要があります。
端末知識がものをいうところもあり、フォレンジック実績のある企業が優位です。

（参考）弊社が提供するマネージドEDRサービス

弊社においても、「マネージドEDRサービス」を展開しています。



左側半分がEDRの仕組み、右側半分がサービスの仕組みです。

EDRを各端末に導入し、端末のログをクラウド基盤に吸い上げます。

吸い上げたログは自動分析されますが、そこで見つからない脅威は専門家による探索行為によって能動的に発見します。
この動作をスレット・ハンティングと呼びます。脅威を狩るという意味です。

また、異常が見つかれば遠隔で被害拡大抑止を行ったり、詳細調査を行って何が起こっているか、また、推奨アクションは何かというアドバイスを受け取る、という仕組みです。

この仕組みを持てば経営層の方々も、説明しろ、というだけでストレスなく十分な情報を得られるようになります。

おわりに

これからの時代は以前にも増して、
「ウイルス感染やサイバー攻撃は必ず発生する」
という前提に立つ必要があります。そして、

・端末で発生する脅威をより一層可視化する
・予防より事後対応に追加対策を入れ、リスクを発現させない
・遠隔で、より早く、楽に対処する

これを実現する手段がEDRであり、
早期に導入のご検討を始めていただければ幸いです。

EDR導入で会社を強くし、本業であるビジネスの競争力を高めて頂けることを願っております。

筆者略歴

NRI SECURE

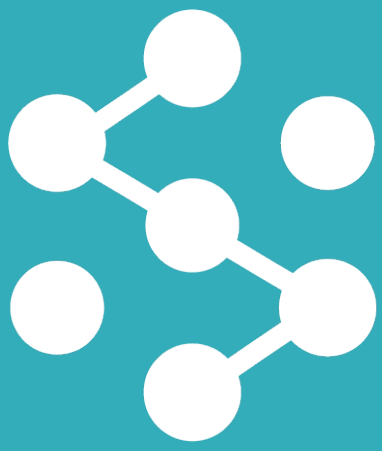
木内 雄章

2004年NRIセキュアテクノロジーズ入社。

ハッキング技術をコアコンピタンスとして事業展開し、事故対応支援、FX診断、

ブロックチェーン診断、マネージドEDR、などの立ち上げをリード。

2017年4月よりサイバーセキュリティサービス事業二部の部長。



Secure SketCH

セキュリティ経営をシンプルに

https://www.secure-sketch.com