アンラボ・セキュリティレター

Press Ahn

2019.10　Vol.70

アンラボ EDR の基準『F.O.C.U.S』

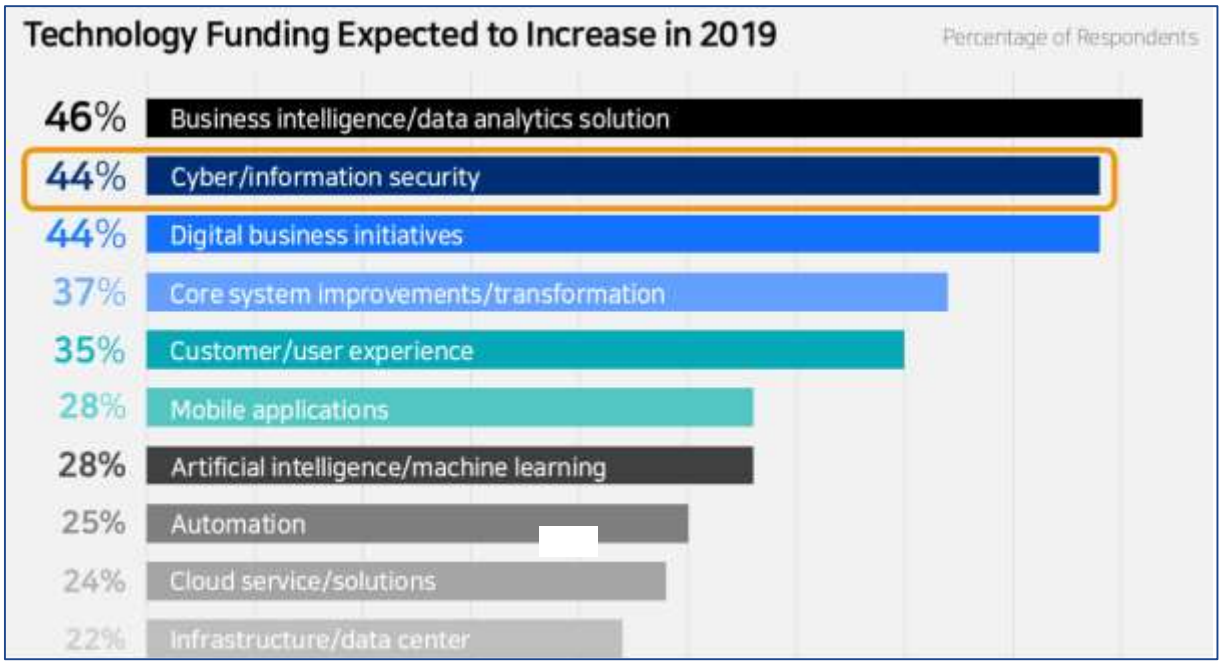
セキュリティにおける「Response」について

アンラボ EDR の基準『F.O.C.U.S』

最近 EPPと EDR市場の融合により、顧客は製品へのアプローチ方法を図りかねているようだ。EDRは従来のセキュリティソリューションに代わる万能薬ではなくエンドポイントの可視性=見える化(Visibility)を提供するツールであることを忘れてはならない。
今回のプレスアンでは顧客とのコミュニケーションで感じた EDRへの誤解と真実、セキュリティ業界のこれからの『対応(Response)』の行方について紹介し、EDR導入を検討する際に考慮すべき 5つの基準を提案した。

デジタルトランスフォーメーション時代のセキュリティ：Security still matters

デジタルトランスフォーメーションション(Digital Transformation)は全産業分野における重要なアジェンダーであり、年を追うごとにその重要性が高まっている。企業は収益(Revenue)と成長(Business Growth)が重要だがこれを実現するためのデジタルトランスフォーメーションをどのように適用するかが差別化ポイントになる。その鍵とされる技術に「人工知能(Artificial Intelligence)」、「ビジネスインテリジェンス(Business Intelligence)」、「データーアナリティックス(Data Analytics)」などがある。これらの技術がビジネスに組み込まれる中でセキュリティが重要な課題として浮上している。すべての情報がデジタル化され IT-OT-IoTが繋がり、データーと資産を守る保護の役割がさらに重要になったのだ。



[図1] 2019年の予算増加が予測される技術トップ10 (*出典：Gatmer、2018.10)

3 つのキーワード : Better、Malware、Behavior

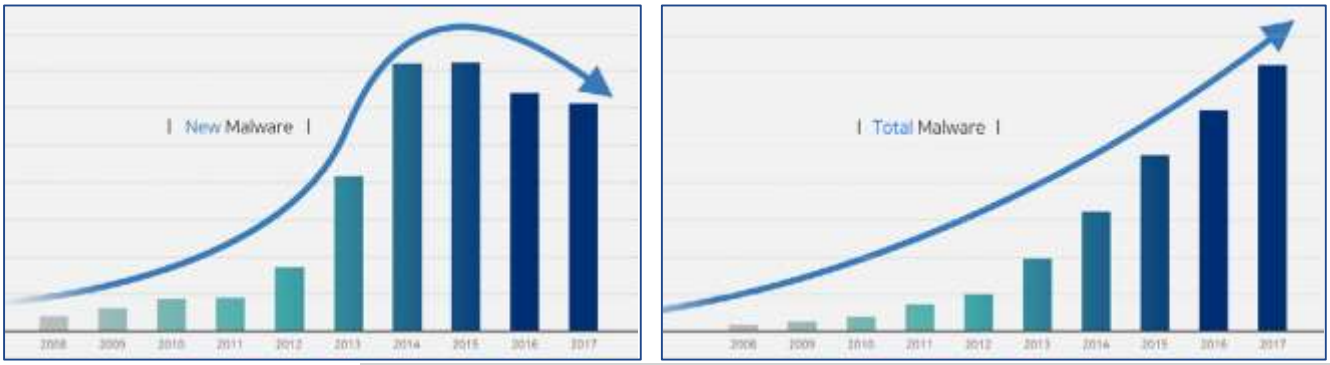
次に情報セキュリティにおいて不変の重要キーワードについて説明する。

第一は「より良い(Better)」である。RSAカンファレンス(RSA Conference、以下RSAC)2019のスローガンは『より良い世界のためのセキュリティ』だった。これは、RSAC2018のスローガン「今大事なのは(Now Matters)」と繋げると次のように解釈できる。

『より良くなるためにトライするならば、より悪しきことを選択してみることだ。なぜなら、より悪い状況が来ないようにするためである』

上記メッセージは重い内容を含めているがキーワードそのものはシンプルだ。アンラボはこれに合わせて「完璧を実現するために、より良いものを(Better for the perfect !)」をベースに『顧客と共により良いセキュリティソリューション』を提案していく。

第二は「マルウェア(Malware)」である。グローバルテスト機関 AV-TESTによると、直近 5年間新たに出現したマルウェアは減少したがマルウェアの総数はいまだ急増中だ。このような傾向の原因は変種にある。変種は自己複製レベルの変種(Variant)からより悪質な行為と回避手法で武装した変種(Divergent)に至るまでその領域を拡げている。
また攻撃者は LOLBins(Living Off the Land Binaries)のような正常プログラムをも悪意を持って利用する自給自足型攻撃を試みている。

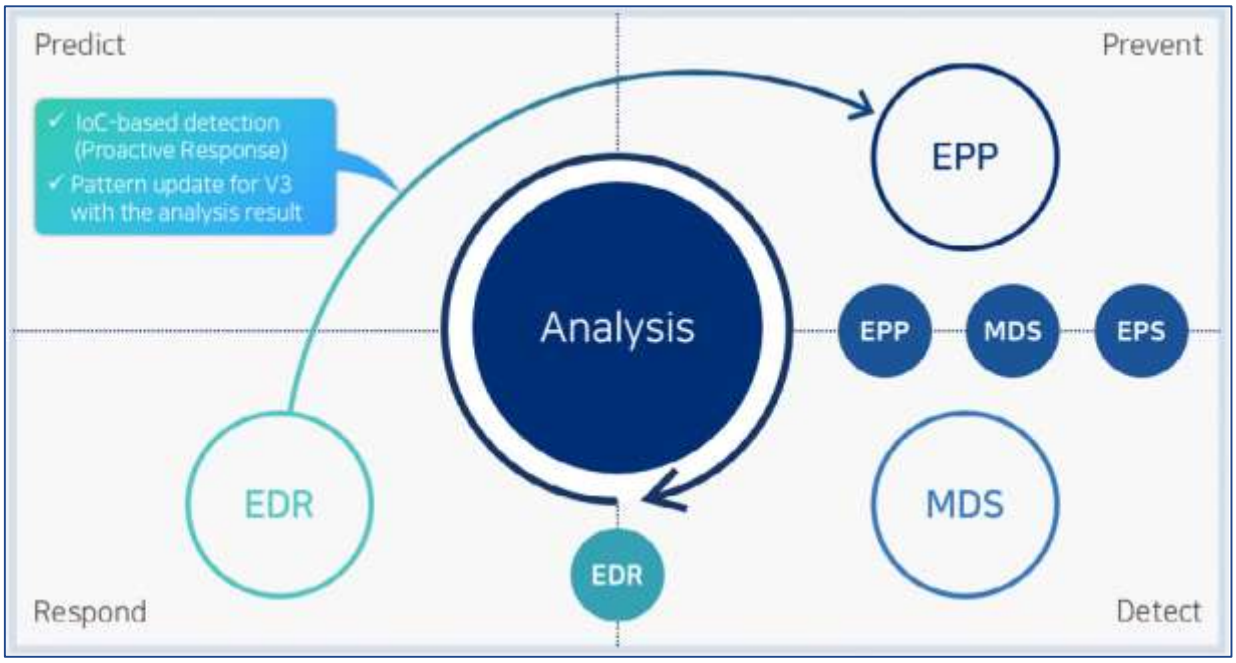


[図2] 過去10年間の新種のマルウェア数(左) vs. 全てのマルウェア数(右) (*出典 : AV-TEST、2018.10)

第三は「行為(Behavior)」だ。情報セキュリティではよくお城(Castle)に例えて『守備者は攻撃者の視点(View point)で見なければならない』と説明するが、マルウェアの複雑さ(Complexity)がますます進化しているため攻撃と防御についてさらに深く考察しなければならない。最近攻撃者の行為は大きく 2つに区分できる。まずは攻撃場所を確保するために長期に渡って調べること。そしてその痕跡を消そうとすることである。
では逆の立場からはどうか。我々が攻撃を防ぐために必死に努力するものの些細な歪みから問題が生じるように、攻撃者も自分の痕跡を完全に消し去ることはそう簡単ではない。消去しきれなかった痕跡から攻撃者の行為を辿って推定できるようになり、逆にこちらの脆弱性が明らかになる。
このトレース方法論がまさに脅威狩り(Threat Hunting)なのだ。

これは「より良い(Better)」を目指すため、問題の原因となる「マルウェア(Malware)」とそのマルウェアによる「行為(Behavior)」の3つのキーワードをどのように解釈するかによってインテリジェントな攻撃に対する効果的な対策を立てられることを意味する。

アンラボのセキュリティ対応領域 : Adaptive Security Architecture by AhnLab



[図3]アンラボの適応型セキュリティアーキテクチャ

アンラボは「既知(Known)の脅威」、「未知(Unknown)の脅威」、「不可視(Invisible)脅威」への対応という3つのキーワードでソリューションをマッピングして市場に提供してきた。アンラボの最終目標は攻撃の表面を最小限に抑えることにある。そのため 4年前からグローバルガイドラインを遵守して適応型セキュリティアーキテクチャ(Adaptive Security Architecture)のためのソリューション領域をプラットフォームマップとして完成させた。またそれぞれのポジション別に「EPP(Endpoint Protection Platform)」とネットワーク上のサンドボックスソリューションの「MDS」、「EDR(Endpoint Detection&Response)」の各領域を設定して相互補完する構造を作った。ソリューションを提供することに加えてアンラボの技術が適用されたサービスも一緒に提供している。

この適応型セキュリティアーキテクチャは、継続的な可視性(Visibility)の確保と有効性(Validation)検証を目標にしており、すべては『分析』に帰結する。アンラボの強み ー『マルウェアを最もよく分析・対応する』という観点からソリューションを整えてサービスを改善を進めている。

EDRとは : EDR focus on Visibility

アンラボは 2018年4月「AhnLab EDR」をリリースし、EPP、MDSに続いて脅威の事前防御・検知・対応のポートフォリオを完成させた。

一部では EDRさえあれば既存のエンドポイントセキュリティソリューションの領域が必要ないものと誤解するようだが EDRはエンドポイント領域をすべてカバーできるものではない。

EPPの代表的なソリューションであるアンチウイルスを例に挙げてみよう。アンチウイルスはシステムにマルウェアが侵入すると、既知のものであれば自動的に検知して駆除する。未知のファイルが侵入すると脅威対応ソリューション MDSがシステムで検知して同ファイルの実行を保留させた後、隔離されたサンドボックスの仮想環境で先に実行して悪性かどうか判断する。

なら EDRの役割は何か。EDRはエンドポイントシステムの行為を記録・保存するソリューションであり、多様なデーター分析技術を利用して疑わしいシステム動作を検知・状況情報を提供するソリューションなのだ。つまり EDRがあればその日の痕跡と、先週この場で何があったのか、1か月前にはどんなことがあったか情報が取れるようになる。EPPソリューションが自動処置した内容と MDSが実行保留した内容を含むエンドポイントのすべての情報を記録して、管理者はいつでも確認できるうえに、同情報をベースに不正行為を防止して感染システムを復元するための方法を提案することが EDRの役割だ。市場ではこのような点が強調され、EDRが自動で遮断・対応して情報を表示する万能薬として誤解される傾向がある。

EDRの可視性 : What happened here ?

EDRはエンドポイントの可視性(Visibility)を提供するツールとされるが、ならば「可視性」とは何だろうか。情報が一枚レポートとしてうまくまとめられて自身のヒューマンインテリジェンスと結合できることと説明する者もいれば、X線のように透視機能がついていて見えない領域まで見せてくれることを可視化と言う者もいる。しかしすべての部分をさらけ出したとしてそれをきちんと理解できるかどうかはまた別問題ではないか。

ここでは EDRの可視性を『ここで何が起こったのか。(What happened here ?)』を見える化するものと定義したい。今日このエンドポイントで 1ヶ月前、2ヶ月前、1年前に何があったのか、その痕跡を保存して仮説を証明する根拠を示してくれることこそ EDRの役割なのだ。

つまりマルウェアがシステムに侵入して突然悪意ある行為を起動した瞬間に診断・遮断するソリューションではなく、過去に何が起こったのか証明することをサポートするツールなのだ。エンドポイントのアンチウイルス製品が過去のある時点で何をしたか表示し、その時に NACソリューションがどんな役割をしたか証明することも EDRの成すことだ。EDRはマルウェアを遮断して駆除するのではなく現場を中心に攻撃者の行為と継続的な侵害活動データーの蓄積を行う。同データーの見える化によってセキュリティイベントの妥当性を検証し、インシデントが発生する前後の領域で優先順位を決める可視性の提供こそが EDRの役割である。

EDRへの誤解と真実 : EDR concerns and benefits

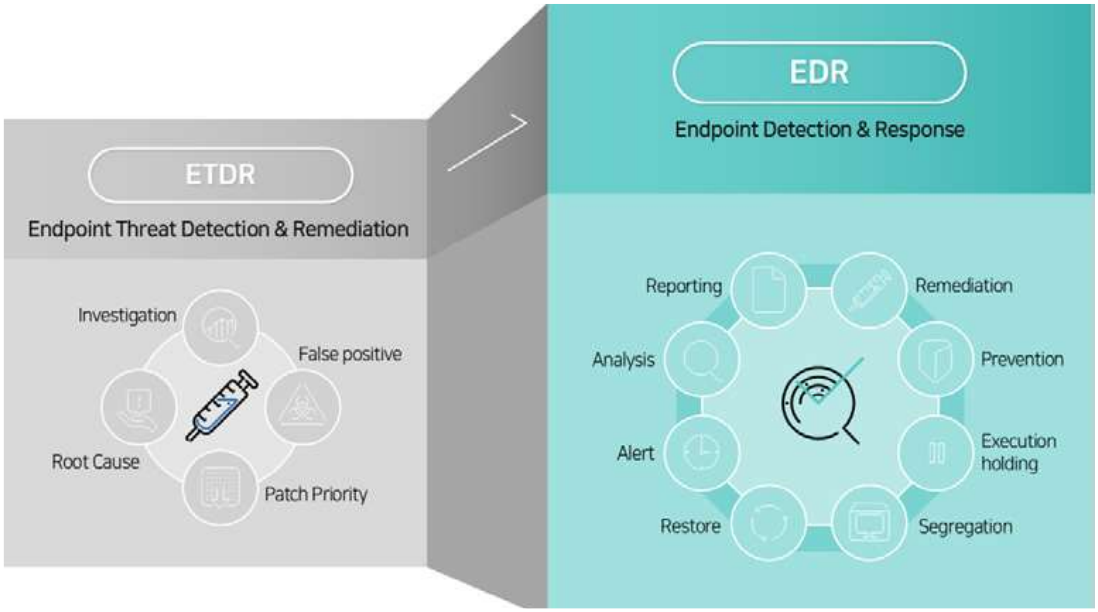
EDR(Endpoint Detection&Response)は、4年前の ETDR(Endpoint Threat Detection&Remediation)から始まった。ここで重要な概念は駆除(Remediation)であり、ソリューションが自動で遮断するのもよいが依然としてインシデントが発生していたため、顧客が自ら調べて定義して直接駆除までできたらどうか ー という観点から ETDRソリューションの必要性が台頭した。

このような市場のニーズを汲んで欧米を中心に多くの企業が登場した。一部企業は次世代 AV(Next Generation Anti-Virus)を前面に出して従来のアンチウィルスを否定し、またある企業はクラウドサービスさえあればより大きなボリュームをさらに速く分析して最小のエージェントとして提供できるため EPPソリューションすら導入する必要がないと主張した。しかし 4年が経過した今、多くの企業で EPPと EDRを一緒に提供している。特に EDR専門会社としてスタートした企業は M&Aや ODMを通じて EPPエージェントを活用したり連動中であることをアピールしている。

ならばなぜ ETDRから EDRに変化したのか。なぜ顧客が駆除(Remediation)機能を正しく実装できなかったのか。

その理由は4つ挙げることができる。まずは顧客が確保した情報を信頼することが難しく、誤検知(False positive)の可能性が高かった。さらに誤検知によってパッチの優先順位(Patch Priority)を決めることが難しかった。原因を解明(Root Cause)するための多角的な証明ができなかったため、調査(Investigation)の一貫性を示すことができなかった。

このような限界性を抱えたまま駆除行為にまで辿り着けないとすれば、一層のこと最終目標値までの段階をより詳細に表示し、多様な方法で分割したほうが良いという認識から駆除→対応(Response)領域に変化したのである。



[図4] ETDRからの領域拡大

不確実性に基づく駆除よりはユーザーがより多様な行為を選択できるように、より多くの機能を搭載した「対応(Response)」の意味を拡張したのである。『治療(Remediation)』、『遮断(Prevention)』、『実行保留(Execution holding)』およびシステムに問題が生じた際に『隔離(Segregation)』したり、隔離されたシステムを『復元(Restore)』してセキュリティ上の『警告(Alert)』を受信し、『分析(Analysis)』して『報告(Reporting)』する 8つの活動を含めて、顧客がより能動的に対応できる EDRに再定義した。ただし EDRの 8つの活動のうち「駆除(Remediation)」は現 EDRツールにおいて最も微々たる機能であり、単純な脅威遮断レベルに過ぎない。

このような点で EDRが提供する可視性と様々な対応(Response)方法により万能薬と誤解されることもある。

しかし EDRが提供する膨大な情報は適切にマッピングされないと情報として活用することが難しい。それに数多くの他のセキュリティソリューションに代わるほど EDRがすべての領域をカバーするとなると、EDR本来の性能を十分発揮できるだろうか。

[図5] EDRの可視性側面から考慮すべき基準

アンラボは、現在市場で議論されている EDRへの誤解と真実、そして本来の EDRの役割について以下のように再定義した。

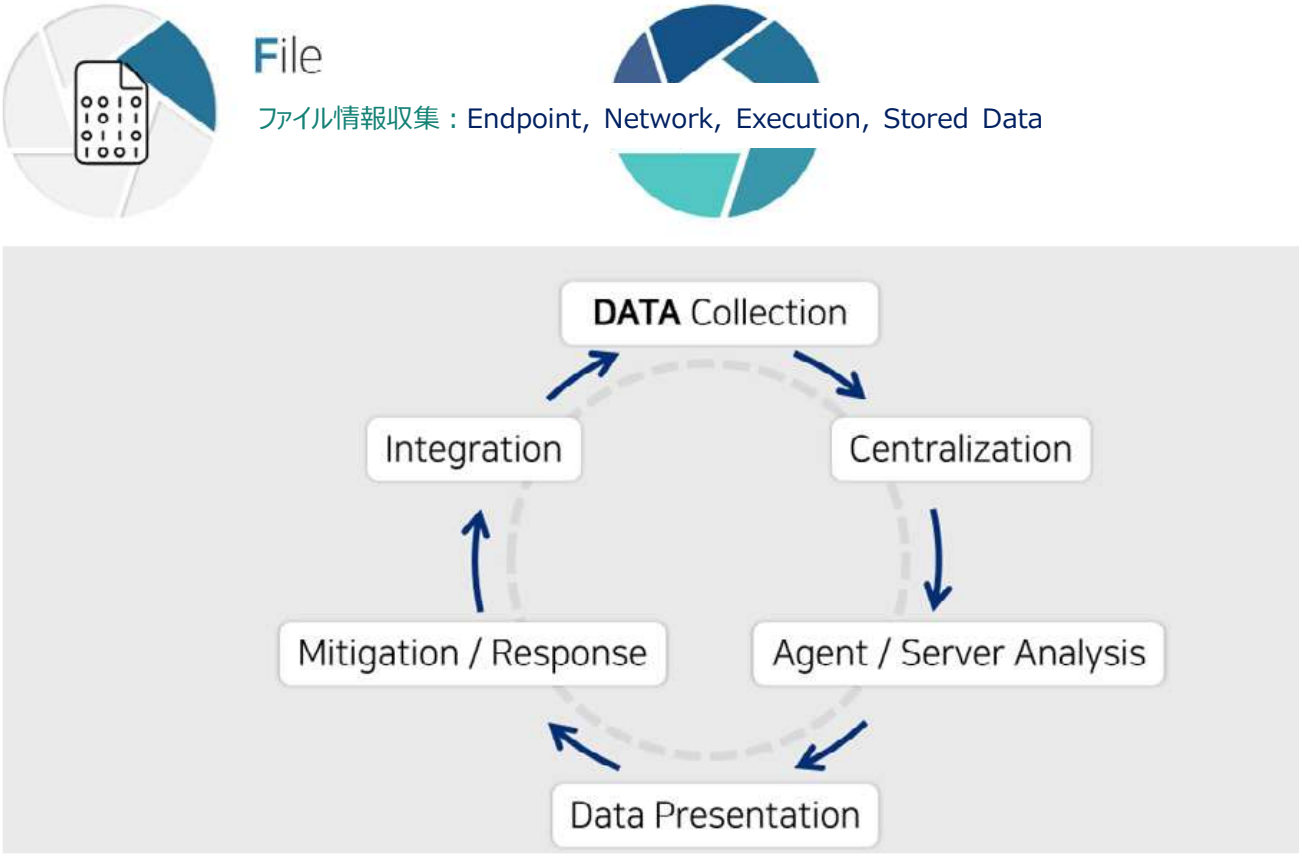
EDRは、▲フォレンジック(Forensic)ツールではない、▲ログを分析する SIEM(Security Information and Event Management)分析ツールではない、▲ユーザーの行為やキーボード入力(Keystroke)を監視する UEBA(User and Entity Behavior Analytics)ソリューションではない、▲アンチウイルスや攻撃者に対抗するために導入するエンドポイントセキュリティ・プラットフォームの他のソリューションに代わるものではない。

EDRは前述した 3つのキーワード「より良い(Better)」、「マルウェア(Malware)」、「行為(Behavior)」の観点から見た場合、インシデント発生時に物理・管理・技術的なコストを最小化できるソリューションであり、より良い事前・事後検知領域を通じて証拠を集められるように、正しく有効な可視性を提供するツールなのである。まとめると ▲インシデント発生によるコストを削減し、▲エンドポイントから脅威の検知をよりうまくできるようにし、▲エンドポイントの脅威検証のために可視性を提供するツールと定義付けできる。

次に、EDRを効果的に使用するために必要な概念として『F.O.C.U.S』を提唱したい。

これは「ファイル(File)」、「運用性(Operation)」、「互換性(Compatibility)」、「統合管理(Unified Management)」、「サービス(Service)」の 5つを意味する。EDR導入を考慮するならばこの5つの領域をしっかりとサポートするかどうか判断基準としなければならない。

ファイル「File: Incident data search」



[図6] EDRのデーター収集の好循環構造

F.O.C.U.S 1. ファイル(File)にフォーカスせよ

EDRはデーター収集が簡単で内容も充実したものを探索できなければならない。EDRは構造的にデーター収集から始まり、その後で中央で一旦まとめて(Centralization)してエージェントやサーバーで分析とデータープレゼンテーション(Presentation)し、再現による再発防止策を用意して再度追加データーを収集する循環構造を持つ。同データーはエンドポイント、ネットワーク、および実行中のデーター、保存型データーなどのすべてのプロパティを保存する。例えば単純なメタデーター以外に、ユーザーがブラウザをクリックしたメタデーター、ネットワーク分析を通じてフィルタリングされたデーター等、これらすべてを保存してそのまま表示するか、或いは優先順位を設定して表示するか取り決めなければならない。

アンラボEDRがフォーカスを当てたのはファイル実行に関するデーターだった。これを基準にデーターを分類してシステムを整えてこそ、探索が容易になる。またファイルのボリュームよりプロパティが重要だ。特に最近は攻撃者が自分の痕跡を消してマーク(Foot point)を残さない Fileless攻撃が主流となっている。これらの攻撃に対応するためにはビヘイビアベース分析による侵害の痕跡(Indicator of Compromise、IOC)だけでなく、侵害の意図(Indicator of Attacks、IOA)まで推測できなければならない。ファイル収集にフォーカスしてファイルのプロパティを把握してこそビヘイビアを確認でき、これにより能動的なインシデント対応が可能になる。

確かなことはすべてのファイルを保持しているとして全部を見るわけではない。何を収集して確認するか、優先順位を決めることが大事だ。

オペレーション「Operation: Activity blocking and containment」

Operation

悪意ある行為の遮断および防御するためのオペレーションシステム

Interoperation : EPP + EDR

: 相互補完(Complementary)により脅威対応シナリオへのシナジー効果最大化

[図7] EPPと EDRの相互補完オペレーティングシステム

F.O.C.U.S 2. 操作(Operation)にフォーカスせよ

エンドポイントセキュリティはいくつかの領域が存在する。これまでエンドポイントセキュリティは EPP(Endpoint Protection Platform)領域で検知・遮断・防御する役目を担当していた。しかしこれだけでは不十分な部分があるため、さらに積極的に収集して視覚化することにフォーカスを当てたのが EDRである。脅威が発生した際に EPPエージェント領域で対応することが多いため、積極的に防ぐ役割は EPPにしてもらう必要がある。

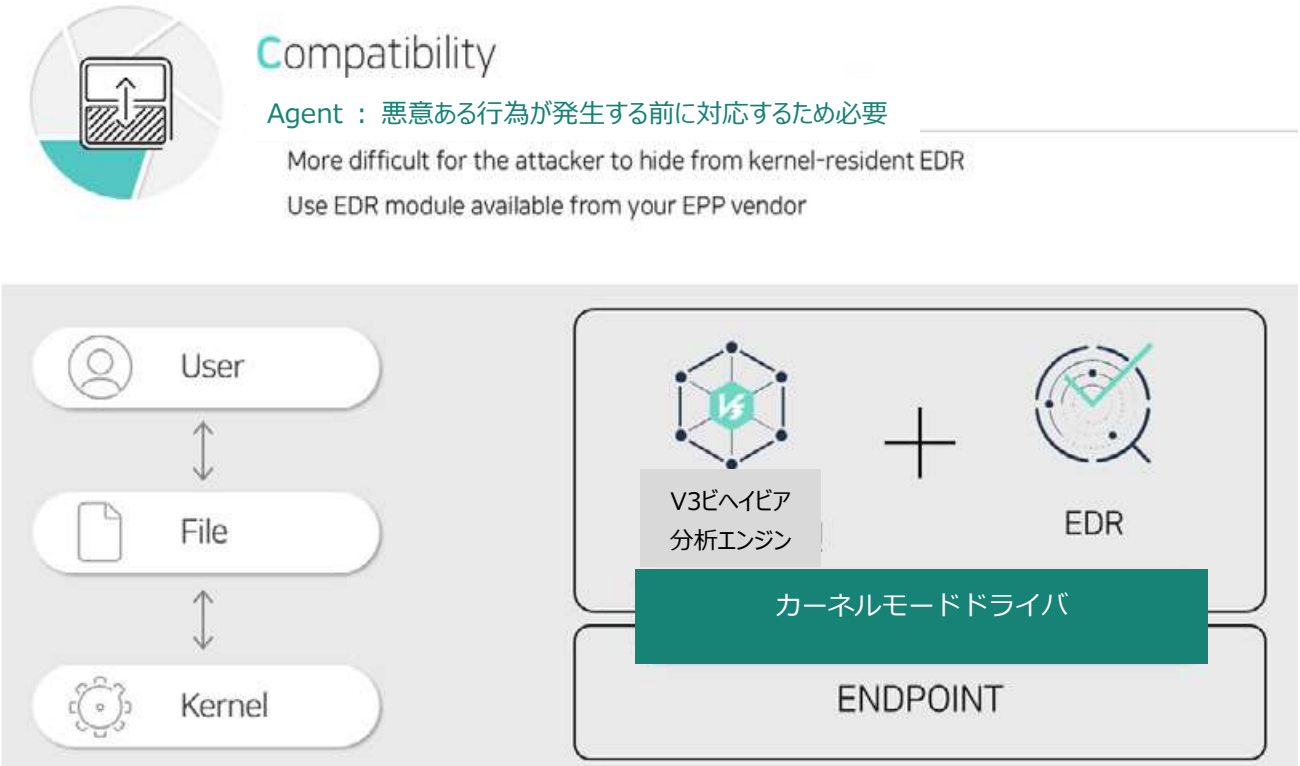
これを EDRに任せると EDR固有の機能をスムーズに実行することができなくなる。例えば収集・分析が必要なときにより多くの要件をタイムリーに提供することが EDRにおける対応(Response)機能だが、マルウェアを遮断・駆除してレポートをエクスポートして再遮断する役目まで遂行するようになってしまうと EDR本来の力を発揮できなくなる可能性が大きい。EPPとEDRは、お互いに役割が異なるため取って代わるものではなく、相互補完(Complementary)的なものとして運用してこそシナジー効果が得られる。前述のように EDR専用ソリューションからスタートした企業らが EPPメーカーを合併したり、ODM方式で EPPソリューションを提供する動きがその証である。

また EDRは運用面における監視、IR(Incident Response)との連携プロセスもサポートする。セキュリティ監視サービスで重要な SIEMは非常に多くのイベントを発生させるため、これを効果的に運用する SOAR(Security Orchestration、Automation、and Response)が生まれた。しかし SIEMと SOARがお互いの活動範囲を減らして準備を整える役割はするものの、いまだ多くのセキュリティイベントが発生させているのも事実だ。

EDRを通じて確かな情報をベースにイベントをフィルタリングしてインテリジェントな基準となる値を持ってデーター収集レベルを調整し、オンタイムで対応してこそ効果的なセキュリティ監視対応が可能になる。

EDRはエンドポイントとサービス領域において、監視とインシデント発生時の緊急対応(Triage)を判断する可視性を提供してくれるだろう。

互換性「Compatibility: Deployment with Agent resistance」



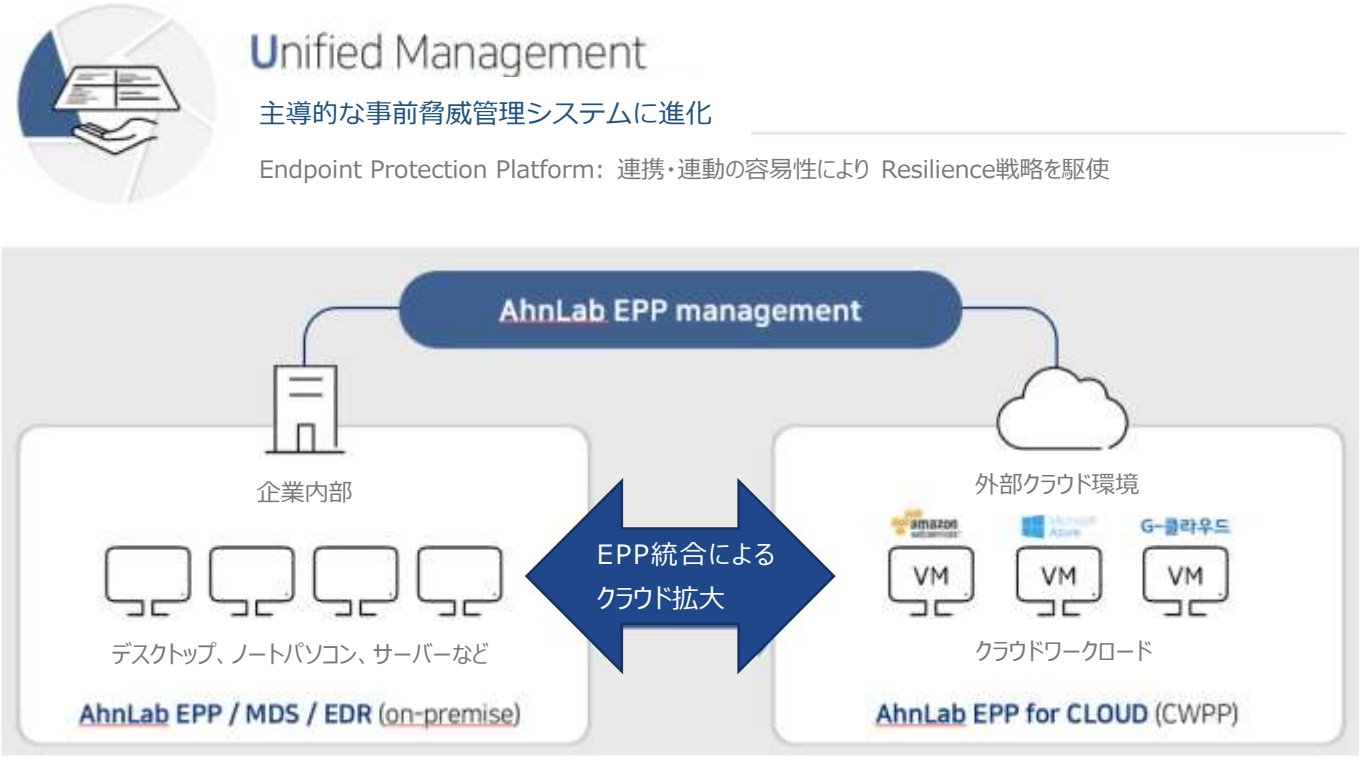
[図8] EDRはカーネルモードドライバレベルのサポートが必須

F.O.C.U.S 3. 互換性(Compatibility)にフォーカスせよ

ソリューション導入の際に新たなエージェントをインストールすることに対する拒否感がある。しかしセキュリティ問題は常に予期しない状況で発生するため、エージェントがないと対応しきれないことが多い。なぜなら突発的に起こったインシデントに対する緊急処置リクエストを受信するエージェントがあってこそ処置の遂行が可能になるからだ。もちろんエージェントレスでもできる部分があるが、これはインシデント発生時に「このようなことが起こる」ということをすでに学習済みのエージェントレスタイプであり、臨機応変に有効なコマンドを実行する(Action)ためのリクエストまでは受信できない。さらに攻撃者はユーザーモードだけでなくカーネルモードドライバまで侵入して攻撃を仕掛けるため、同レベルまでカバーできるエージェントを入れてすべての攻撃活動、証拠、スナップショットを収集・保存する必要がある。よってEDRソリューションベンダー選定時、単にカーネルレベルをサポートするかどうかではなく互換性をカバーする技術力と経験を備えたベンダーを選ぶことが非常に重要だ。

アンラボは 30年に渡り V3、パッチ管理ソリューション、脆弱性チェックソリューションなどエージェントを使用したエンドポイントセキュリティ製品を市場に提供し、多くの技術開発とフィードバック、リファレンスを蓄積してカーネルレベルの技術とノウハウを保有している。

統合管理「Unified Management: Evolution to the proactive management」



[図9] オンプレミスとクラウド統合管理をサポートする EPP Management ロードマップ

F.O.C.U.S 4. 統合管理(Unified Management)にフォーカスせよ

韓国はまだオンプレミス(On-premise)環境がほとんどであるが多くの企業でクラウド導入を検討し始め、クラウドへの移行は逆らえない流れになっている。クラウドで重要なのはやはりシングルマネジメント(Single Management)だろう。統合マネジメントソリューションを選択し、オンプレミスとクラウドの連携・連動によって回復性(Resilience)戦略を確保する方針である。

アンラボは 2018年に EPPと EDR製品をリリースし、今年は仮想化バージョンをリリースしている。2020年上半期に「AhnLab EPP for Cloud (仮)」リリースを予定しており、統合型 EPPマネジメントプラットフォームを構築する予定だ。

サービス「Service: Deployment with professional service」- 1

[図10] EDR活用を最大化するアンラボプロフェッショナルサービス

F.O.C.U.S 5.　サービス(Service)にフォーカスせよ

EDRは自動化ツールではなく十分に活用するために顧客やサプライヤーが一緒に作り上げていくツールである。

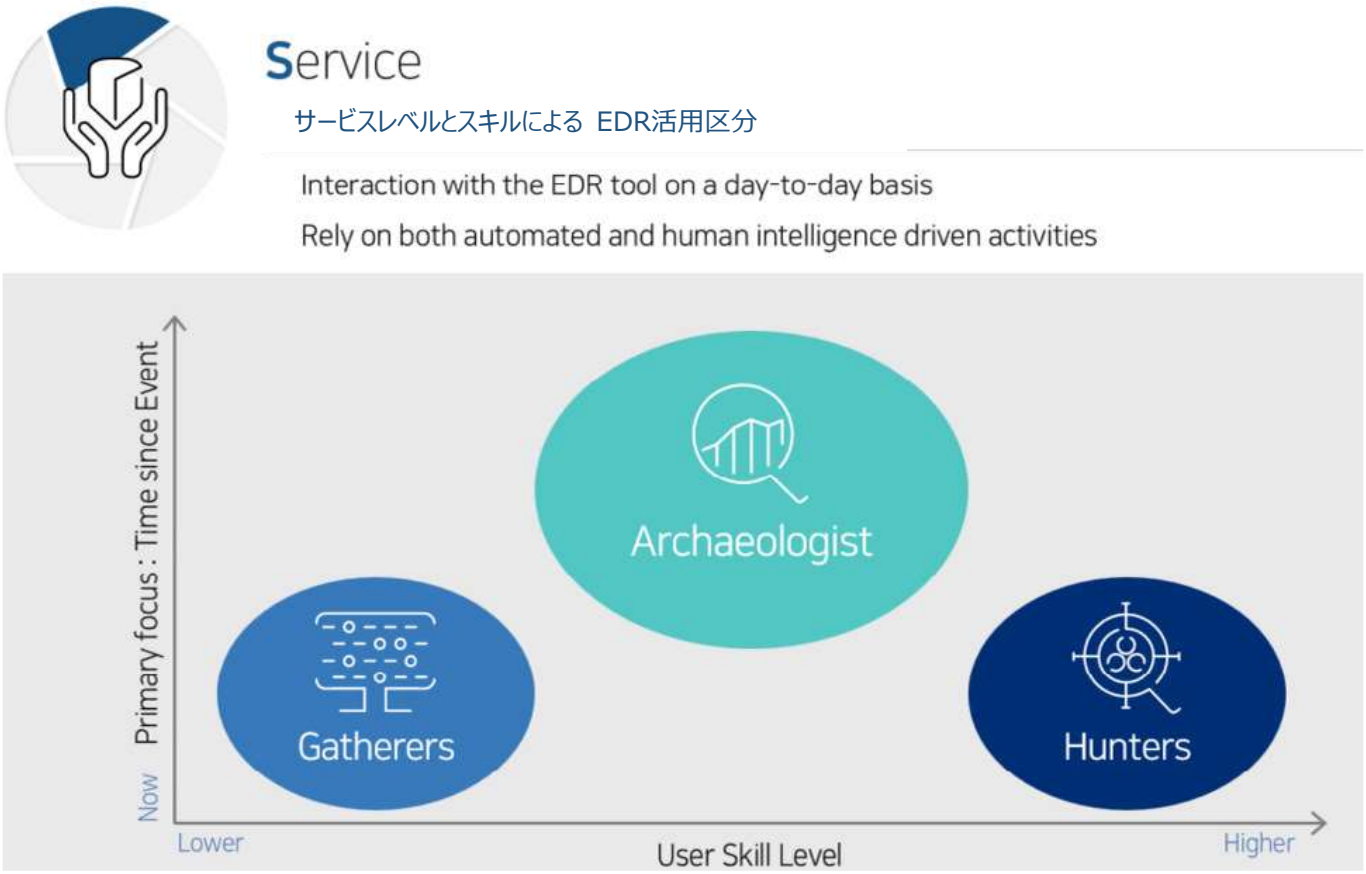
なら誰にガイドをもらえばよいのか。もちろんそのソリューションを提供した企業のプロフェッショナルサービスを利用することが有効だ。

ソリューションを正しくインストールするためにはどの部分を基準にするか正確な目的を設定することが大事であり、例えば IR(Incident Response)基準の複雑さを解決することを優先するか、またはフォレンジック専門家のサービスモデルをより減らしたいのか、それとも内部 IR対応プロセスのサポートをより強化して新たな持続可能型 IRサービスを作り上げるのか、など目的を明確化する。

これによりターゲットシステムの範囲(Scope)、データーのポーリング(Polling)サイクル、データの保持(Retention)期間が異なってくる。

顧客の要求事項をベースにして EDRをシステムに実装するには、ベンダーが提供するプロフェッショナルサービスを効率的に活用する戦略が求められる。

サービス「Service: Deployment with professional service」- 2



[図11] EDRを活用するためのユーザースキルアップ

EDR導入後にうまく運用するためにはサプライヤーのプロフェッショナルサービスを活用することに加えて、内部のスキル(Human intelligence&Skill-set)アップもしっかりと行う。セキュリティ監視サービスの場合、1~2年目の初級『コレクター(Gatherers)』、10~15年経歴の直感と経験を持つハイレベル専門家『ハンター(Hunter)』がある。

コレクターやハンターにしっかりと情報を提供できればより効率的に運用できるようになる。この役割を果たすのが EDRツールであり、このような中間サポートを『デジタル考古学者(Archaeologist)』と命名できるだろう。

つまり考古学者(EDR)によって 5ヶ月前、1年前に何があったのか追跡・分析し、日常的にもハンターとコレクターが判断材料にできるようにデーターの精度を高めて提供する。そうなればハンターは効率的に獲物を狩ることができるようになる。仮説による再現の成功から攻撃を推測するだけでなく、明確な証拠や痕跡から攻撃を辿るハンティングの土台作りこそが、まさにこのデジタル考古学者の役割なのだ。

顧客が EDRを正しく活用するためには、サプライヤーのプロフェッショナルサービスによるガイド、準拠によって顧客の基準を作成し、内部でもスキルアップしてデジタル考古学者を育成し、コレクターとハンターのためのサービスモデルを作っていく必要がある。

EDR is ... Not set up It's Build up

顧客とベンダーの二人三脚ビルドアップソリューション

EDRは顧客やサプライヤーが一緒に作り発展させていくツールだが、顧客側もインシデントに備えて対応力を高めるために様々な遡及分析(Analysis in Retrospective)を通じてこれまで見えなかった脅威を探し続けなければならない。そのためにまずはシステムで発生するすべてのデーターを収集して優先順位に基づく学習を通して分析・対応を継続的に進めていく。

長い間情報セキュリティ分野は攻撃者と防御において防御側に不利な戦いだった。一度些細な穴でも開いてしまうと即防御の敗北に繋がる。

だが防御側が追跡能力を持てばこの構図は変わるはずだ。攻撃者はすべての痕跡を徹底的に消さなければならなくなり、ハンターにたった一つでも痕跡が見つかれば今度は逆に攻撃者が追い込まれる立場になる。いよいよ防御側が勝利する時代が来たのだ。

これを可能にするのが脅威狩り(Threat Hunting)であり、現在最も効果的な脅威狩りツールはまさにEDRといえる。

EDRは完成されたセットアップ(Set-up)ソリューションではなく、一つのツールに過ぎない。防御側が一般的な対応を越えて創意的な攻撃手法、トレース手法、ハンティング方法を習得し、顧客とベンダーが一緒に能動的かつ有機的にビルドアップ(build-up)するソリューションなのだ。

長い企業の歴史から、アンラボは新たなデジタル時代においてもセキュリティ対策とツールをどのように改善・ビルドアップすればよいのか短時間で把握し、お客様との学習を通してパフォーマンスを導き出している。今後もより良い検知・領域・セキュリティ対策を提供し、顧客の資産を保護するために努力していくだろう。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)