SB C&S

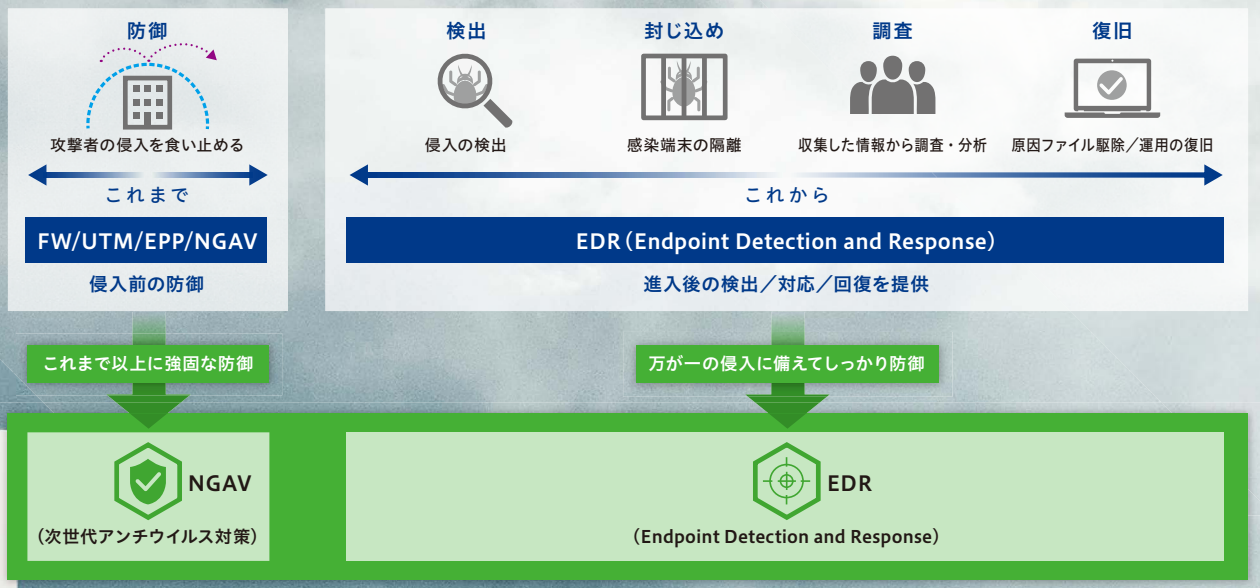
悩みの尽きないエンドポイントセキュリティ

EDRのトレンドがわかる！

製品選定における
3つの視点

「100%防ぎ切れない」を前提に侵入後対策を強化するEDR

昨今、メモリ上で動作するファイルレス攻撃や、進入時に回避行動を取るランサムウェア、凶悪な未知のマルウェアなど、既存の対策ソフトでは検知が困難な攻撃が増加しています。しかも、モバイルワークの加速やクラウドサービスの活用を背景に、パソコンやタブレットを含むエンドポイントが侵入ルートになりつつあり、もはや脅威の侵入を食い止めるための対策だけではセキュリティーを守り切れません。これからは「攻撃は100%防ぎ切れない」という前提に立ち、侵入後の対策を強化していく必要があります。これが、エンドポイント対策としてEDR（Endpoint Detection and Response）と呼ばれるソリューションが注目される理由です。



検知

- ✓ 多様化するデバイスの利用状況を把握しきれない
- ✓ 取得できる情報が少なく限定的である
- ✓ 感染が疑われるデバイスの特定に時間がかかる
- ✓ 侵入の痕跡から既知の攻撃との類似点を特定している
- ✓ 最新の脅威を検知できない

分析

- ✓ 膨大な量のログを人海戦術で調査している
- ✓ 分析に必要な詳細な可視化が不十分である
- ✓ 攻撃テクニックの解析が不足しており付加情報も少ない
- ✓ 詳細な分析は結局人の判断に委ねられている
- ✓ リスクを正確に把握できず的確な状況判断ができない

侵入後対策、できていますか？

運用性

- ✓ アラートが膨大かつ複雑すぎて対応しきれない
- ✓ アクティビティの相関性を把握できず効果的に対処できない
- ✓ 迅速にレスポンス可能なインシデント情報が不足している
- ✓ 分析結果が英語でわかりにくく時間と労力がかかる

EDR 製品選定における 3 つの視点

1：検知

網羅的に攻撃の検出が可能？

さまざまな脅威に対抗していくためには、検知能力が高いに越したことはありません。
非マルウェアや未知のマルウェアなど、巧妙化する最新の脅威を検知できるかどうかも重要なポイントです。

Point 「カーネルモード」で動作

一般的なアンチウイルス製品は、OS からより多くの情報を取得しマルウェアの攻撃を効果的に防御する目的で、カーネルモードで動作するものがほとんどです。これに対し、EDR 製品にはユーザーモードで動作するものがあります。この場合、解析に必要な十分なログを収集できず、不審な挙動が見つかっても不正を見逃してしまう可能性があります。ユーザーモードは導入が容易な反面、収集できる情報量が少なく、インシデントへのレスポンス機能が低下するため注意が必要です。

Point 遡り分析が可能なログの取得

EDR 製品の目的は、そもそもブラックなログを見つけることではありません。過去を遡ると、以前侵入された痕跡が見つかったり、事態がさらに悪化しつつあることが判明したりすることがあります。したがって、機械では見つけられないような振る舞いにも注目し、脅威ハンティングを行うための十分な情報が必要です。これが、クリーンログと呼ばれるような通常ログまでを残すことの重要性です。しかし、フルクラウドモデルのソリューションの場合、全ログは収集しない、クリーンログは 1 週間しか残さないといった製品がほとんどです。

Point 調査のための十分な情報量

EDR 製品が登場した背景の一つに、企業のセキュリティー対策においてエンドポイントの情報が圧倒的に不足しているという課題があります。それでもクラウドにリソースを持つベンダーを中心に、グレーなログやブラックなログのみを分析する製品が少なくありません。
全ログを収集できる製品は、オンプレミスモデルもしくはオンプレミスとクラウドのハイブリッドモデルに多く見られますが、管理サーバーを自社内に設置する必要があるほか、改ざんのリスクが高まる上に痕跡を消しやすいといったデメリットが残ります。この点で注意が必要なものの、既知の攻撃と未知の攻撃の両方を阻止するためには、フィルタリングされない正確なエンドポイントデータが必要です。何が疑わしいかわからないからこそ、全ログを収集できるのが理想です。

Unbiased Data
—全ての情報を余さず収集—

保持期間
- Alert に関連したイベント：6 か月
- Alert に関連しないイベント：1 か月

何が疑わしいか分からないからこそ EDR が必要

用語解説

■**レトロスペクティブ**　日本語で「振り返り」。セキュリティー業界では、過去のログに遡って脅威を検知することを意味する。感染経路や原因を可視化したり、被害の拡大を阻止したりするために必要な機能である。

EDR 製品選定における 3 つの視点

2：分析

適切な分析結果が提供される？

分析機能は、検知した脅威への対処に影響する重要なプロセスです。速やかに原因を特定すると同時に、侵入経路や被害状況、優先順位などを包括的かつわかりやすく可視化し、効果的な対応につなげる仕組みが必要です。

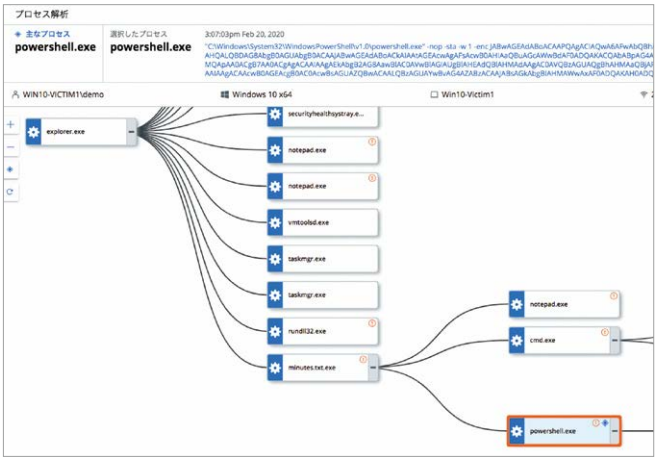
Point 攻撃全体の可視化

従来型のアンチウイルスは、すべての機能が縦割りで提供されています。多層防御をうたっているアンチウイルスソフトであっても「点での防御」の組み合わせであることがほとんどです。あるエンジンをすり抜けてしまった攻撃は、他のエンジンが検出してくれるはずもなく、そのままエンドポイントに着弾することになります。

これを防ぐためには、攻撃全体の流れを理解した上で、その結果の中から止めるべきところを止めるという考え方が重要です。したがって、脅威であるかどうかに関わらず、エンドポイントでの動きをすべて記録し、可視化する仕組みが必要になります。

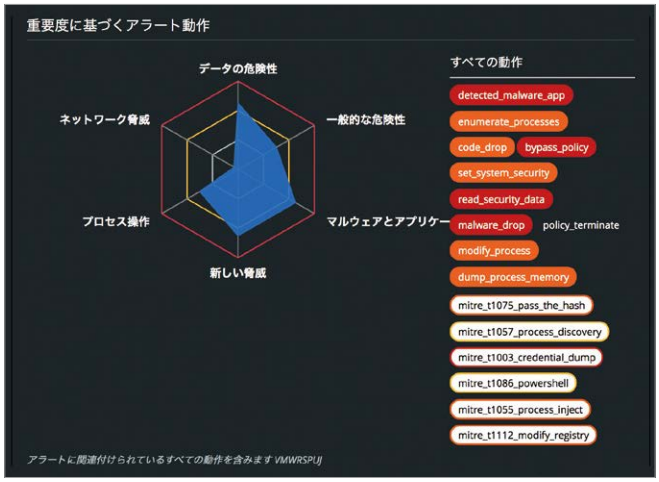
Point 挙動ごとの評価

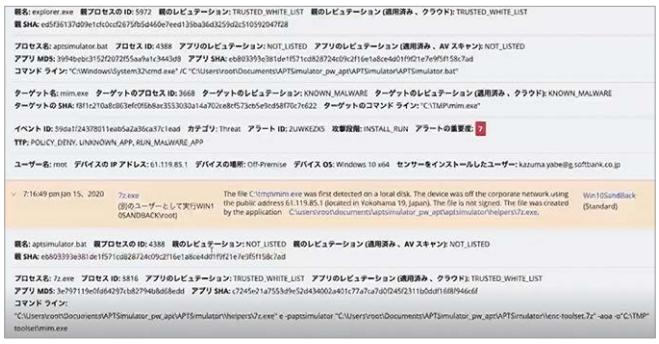
ファイルレス攻撃や環境寄生型攻撃（Living off the Land）に対応するためには、挙動ごとの評価が重要です。たとえば、PowerShellが悪用された場合にも、どのアプリケーションを起因にPowerShellが立ち上がったのか、PowerShellが何をしたのかなど、アプリケーションの親子関係を一つひとつ追跡していく必要があります。EDR製品においては、攻撃の流れ（攻撃者の戦術、技術、手順）を示すTTP（Tactics, Techniques, and Procedures）やプロセスツリーなどを通じて、一つひとつの挙動に分析結果を提供するベンダーが増えています。



Point ユーザーが把握可能な提供方法

エンドポイントでの動きを可視化する際、攻撃テクニックの付加情報としてMITRE ATT&CK※の番号のみ提示するEDR製品がありますが、本当に重要なのは「具体的に何をされたのか」であり、分析結果の提示方法としては望ましくありません。今後は、独自のTTPタグを利用するなどして、ユーザーが把握しやすい形で情報が提供されることが求められます。





ライトユーザーとアナリストそれぞれに必要な情報を提供

用語解説

■MITRE ATT&CK（マイター アタック）フレームワーク

米国の非営利団体MITRE（マイター）社が提供している攻撃手法や戦術を段階的に定義したセキュリティーのフレームワーク。標的型攻撃における攻撃者の行動を分解した「サイバーキルチェーン（Cyber Kill Chain）」より、具体的なセキュリティー対策に落とし込めるとして利用されている。

EDR 製品選定における 3 つの視点

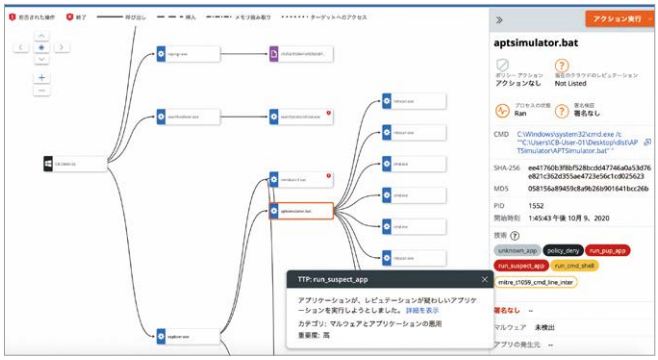
3: 運用性

速やかに対処できる？

ほとんどのエンドポイント セキュリティープログラムでは、複数のサイロ化されたシステムが必要となるため、エンドユーザーに負担がかかり、管理が困難になっています。運用を簡素化し、重要な業務に集中できる環境が求められます。

Point アラートの集約

従来の製品はイベントごとにアラートを上げていましたが、アラートが膨大に上がってくると運用が回らなくなるため、昨今はイベントごとのアラートをインシデント単位で集約する製品が増えています。これらの製品では、複数の疑わしいイベントを検知した場合にそれらの相関分析を行い、一連の攻撃の流れをまとめた上で、対応が必要なインシデントとして提供されます。膨大なアラートを 1 から分析することなく、迅速な対応が可能になります。



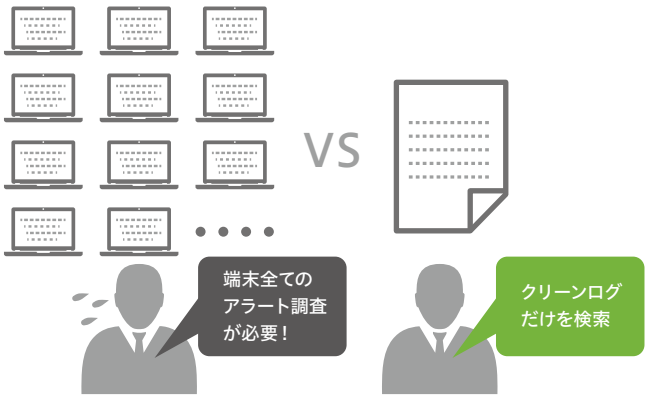
複数の疑わしいイベントを検知した場合、相関分析を行い一連の攻撃の流れをまとめた上で、対応が必要なインシデントとして提供

Point 日本語対応&日本のデータセンター

ユーザーフレンドリーなインターフェースの提供は、運用効率を向上させる重要な要素です。英語に不安がある場合には、管理コンソールや解析結果の表示が日本語対応していない製品はあまりおすすめできません。実際に何が起こっているのか、具体的に何をされたのかを把握しにくいからです。また、事業の特性上海外にログデータを保管したくないというニーズに対しては、コンプライアンスの観点から国内のデータセンターを使ったサービスも提供されています。

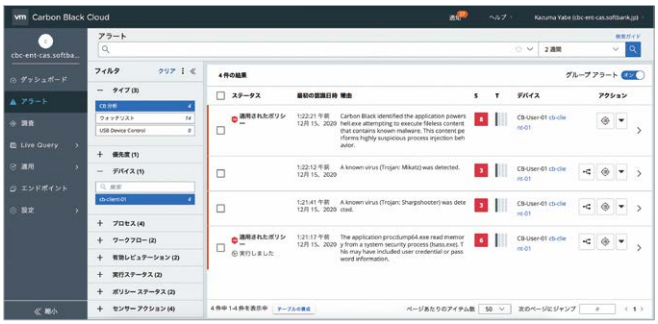
Point 簡単ですばやい検索

フルクラウドの EDR 製品は、アラートに関係のないクリーンログを平均して 3 日から 1 週間しか残しません。たとえば、一定期間に USB を差した端末を特定したい場合、クリーンログが残っていないとなると、端末を直接調査する必要があります。端末の台数が多くなればなるほど調査には時間を要し、数時間～一日かかることになります。一方、全ログを取得できている場合は、ログを検索するだけです。



Point アラートの進行度の可視化

アラートの内容はリアルタイムに変化していきます。たとえば、攻撃が進行して情報収集段階の攻撃からラテラルムーブメント（感染拡大）に移行したとなると、セキュリティーの緊急度が一気に高まります。この緊急度の変化がアラートにも反映され、わかりやすく表示されることが重要です。



緊急度の変化がアラートにも反映され、わかりやすく表示

よりシンプルに、より堅牢に・・・

今後もサイバー攻撃が減ることはなく、むしろ複雑さや巧妙さが増し
対応の難易度も高まっていくとなると、より網羅的に防御能力を高めつつ
シンプルで負荷の少ない運用環境の実現が求められます。
この点を踏まえ、EDR製品選定における3つの視点「検知」「分析」「運用性」に
さらに2つの視点「防御策」「拡張性」を加えることをお勧めします。

＋防御策

EDRさえあれば従来のアンチウイルスが不要になるというわけではありません。アンチウイルスをすべてEDRに置き換えてしまうと、EDR側でのアラートが膨らみ過ぎて対応が追い付かなくなる可能性があるため、防御策としては依然として必要です。
「防げるものは未然に防ぐ」という考え方に基づき、既知の脅威は次世代アンチウイルス（Next Generation Anti-Virus：NGAV）で防御策を強化し、さらに侵入後の可視化および対応をEDRで強化します。
また、EDRで発見された脅威情報はクラウドに集約され、既知の脅威としてNGAVでの防御に反映されるのが望ましいです。

防御策の強化

次世代アンチウイルス
NGAV

＋

侵入後の可視化／対応

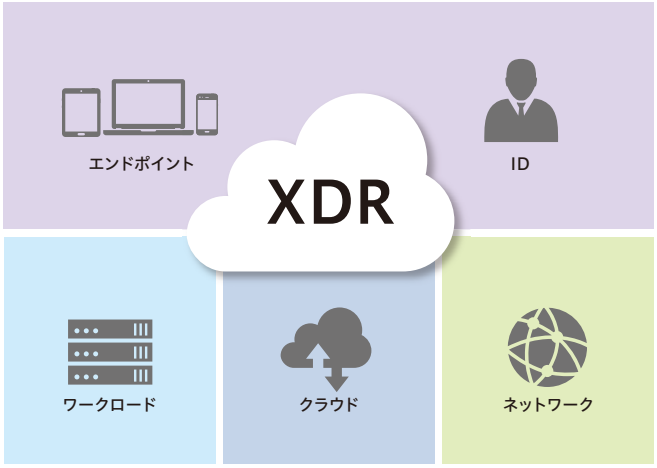
Endpoint Detection and Response
EDR

＋拡張性

EDR製品は今後も急速にカタチを変えていき、次世代のエンドポイントセキュリティとされるXDR（eXtended Detection and Response）へとシフトしていくと考えられます。XDRは、よりシンプルに高度化する脅威に対応していくための統合的なアプローチです。
つまり、EDRはエンドポイントの情報だけを活用するものではなく、ID、ネットワーク、ワークロード、クラウドなどをすべて統合したシングルプラットフォームとして提供されるようになっていくと予測されます。
したがって、これらのプラットフォームと親和性の高い製品であること、インフラ全体を網羅するセキュリティエコシステムを提供できることがアドバンテージになります。

EDRからXDRへ

Networkの情報取り込みだけではない、
プラットフォーム全体の脅威分析と対応

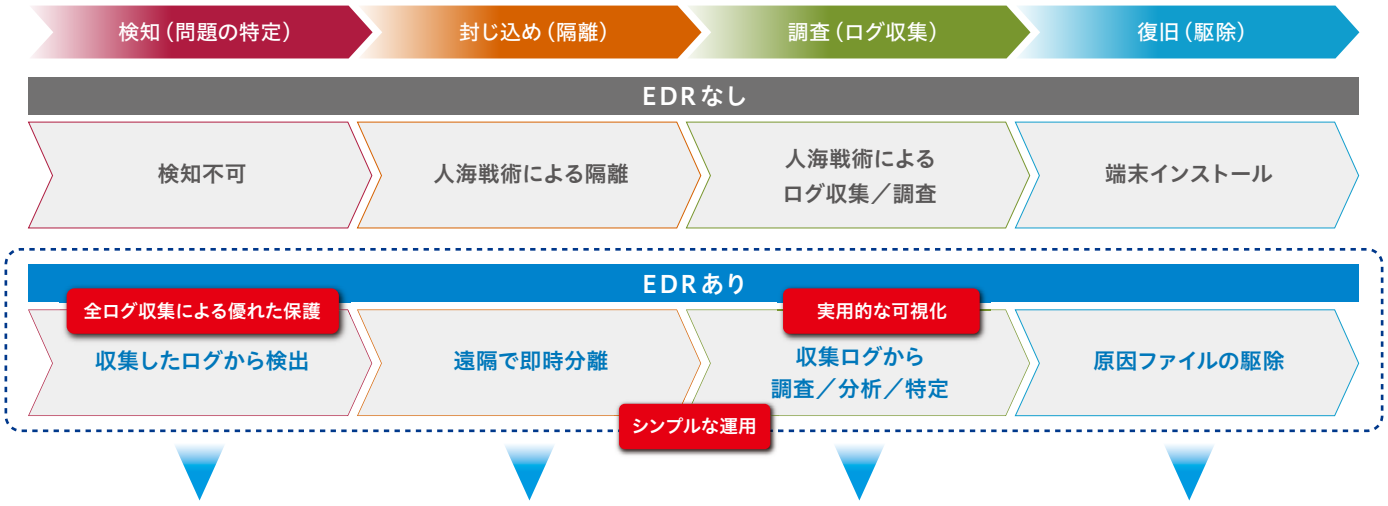


まとめ

3つの視点がもたらすメリット

セキュリティーインシデントが発生した際、さまざまなログの調査を行う上で決定的に足りないのがエンドポイントのログです。EDRがない場合、周辺のログからのアラートでエンドポイントを探すため、ログの収集や端末の特定に時間がかかり、復旧やデータの保護が手遅れになる危険性があります。EDR を導入すると、怪しい動きをするエンドポイントを特定してから影響範囲を調査するというように脅威への対応方法が変わります。

さらに、EDR製品の選定において「検知」「分析」「運用性」の3つの視点を重視することで、未知の脅威に対してより優れた防御力を発揮できるようになると共に、不審な挙動の特徴を瞬時に把握し速やかに対処できるようになります。
脅威への対応方法を最適化できれば、万一の侵入後も感染したデバイスの迅速な特定や隔離を実現し、セキュリティー被害や影響範囲を最小限に抑えることが可能です。



サイバー攻撃への迅速な対応による被害の最小化

検　知

各エンドポイントの振る舞いを監視することで侵入した脅威の検出が可能。
侵入を迅速に検知することで迅速に対応でき、被害を最小限に。

分　析

平常時から各種ログを収集・分析しているため、調査に必要なログだけを迅速に抽出・調査。脅威の侵入検知がそのまま影響範囲や被害情報の調査へと直結しているため、事態の収束に向けてすぐにアクションできる。

運用性

日本語化されたUIや日本国内サーバーでの運用、
コンソールやエージェントの統一により、セキュリティーの一元管理を実現できる。

SB C&S が提供するEDR製品

VMware Carbon Black Cloud™ ができること

VMware Carbon Black Cloudは、侵入前対策としての次世代型アンチウイルス機能とEDRによる侵入後の対策を兼ね備えた、サイバー脅威の検出、分析、セキュリティーの運用性のすべてにおいて高い水準の性能を提供する、これからの企業や組織に必要な次世代のセキュリティー製品です。もともと脅威ハンティングを目的に開発された製品であることから、すべての挙動を丸裸にし、その一つひとつに対して分析結果を提示できる点が大きな強みとなっています。

VMware Carbon Black Cloudの情報はこちらをご参照ください。

優れた防御能力

NGAVを搭載。既知および日々変化する未知の攻撃からも防御

市場をリードする検知と対応

アンフィルターデータをリアルタイムに分析
迅速な調査と復旧が可能

運用のスリム化

シングルエージェント、シングルコンソール
フルクラウドモデル

VMware Carbon Black Cloud の機能比較

名称	機能	説明	VMware Carbon Black Cloud				旧CarbonBlack製品名称
			Prevention	Endpoint Standard	Endpoint Advanced	Endpoint Enterprise	
Endpoint Standard	Next-Generation Antivirus	未知の脅威を検知する次世代のウイルス対策	●	●	●	●	CB Defense
	Behavioral EDR	エンドポイント上の挙動を分析する EDR 機能		●	●	●	
Audit and Remediation	Live Response	個別のエンドポイント調査		●	●	●	CB LiveOps
	Live Query	すべてのエンドポイントへのリアルタイム検索			●	●	
脆弱性管理	Vulnerability Management for Endpoints	リスクの可視化と分析		Add-on	●	●	
Enterprise EDR	Enterprise EDR	脅威のハンティングとインシデント対応				●	CB ThreatHunter

SB C&S Carbon Black セキュリティ監視サービス
監視センターとセキュリティのプロが高度なEDRツールをフル活用して、セキュアでシンプルな EDR 運用をサポートします。

SB C&Sがおすすめする VMwareソリューションはこちら

SB C&S

SB C&S株式会社

〒105-7529 東京都港区海岸一丁目７番１号 東京ポートシティ竹芝オフィスタワー
https://cas.softbank.jp/

vmware PARTNER DISTRIBUTOR

お問い合わせ先

2022/06