ALog × cybereason

SIEM × EDR

で実現する
サイバー攻撃対策

AMIYA

目次

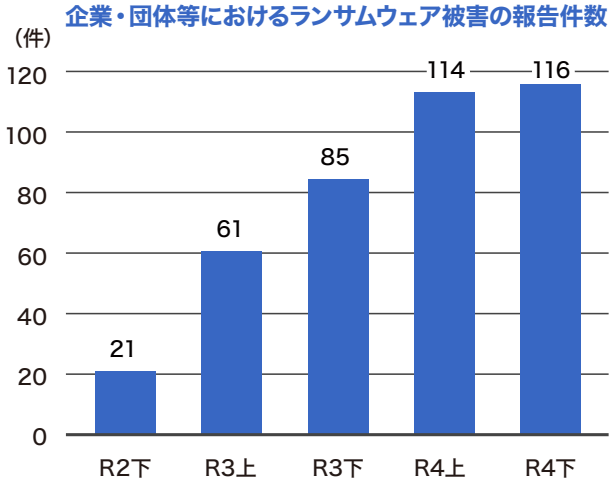
はじめに：境界型防御の限界 ・・・

はじめに

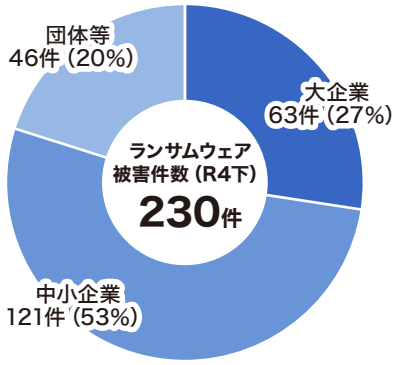
境界型防御の限界

サイバー攻撃が猛威を振るっています。警視庁が発表した「令和４年におけるサイバー空間をめぐる脅威の情勢等について」によると、ランサムウェア被害件数は右肩上がりで被害企業の規模や業種も多岐に渡り、あらゆる企業がターゲットとなり得ることが明らかとなっています。また、最近のランサムウェアウェア攻撃は従来型と比べて被害範囲が広く、事業継続を揺るがす大きなリスクとなっています。

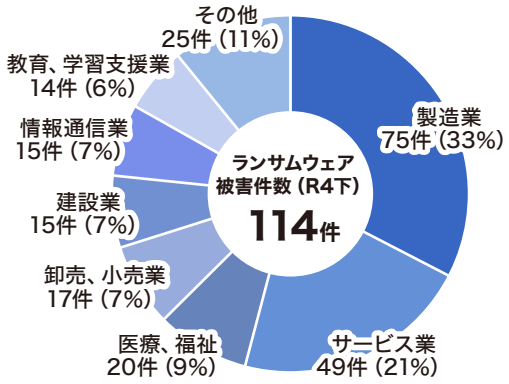
企業・団体等におけるランサムウェア被害の報告件数



ランサムウェア被害の企業・団体等の規模別報告件数

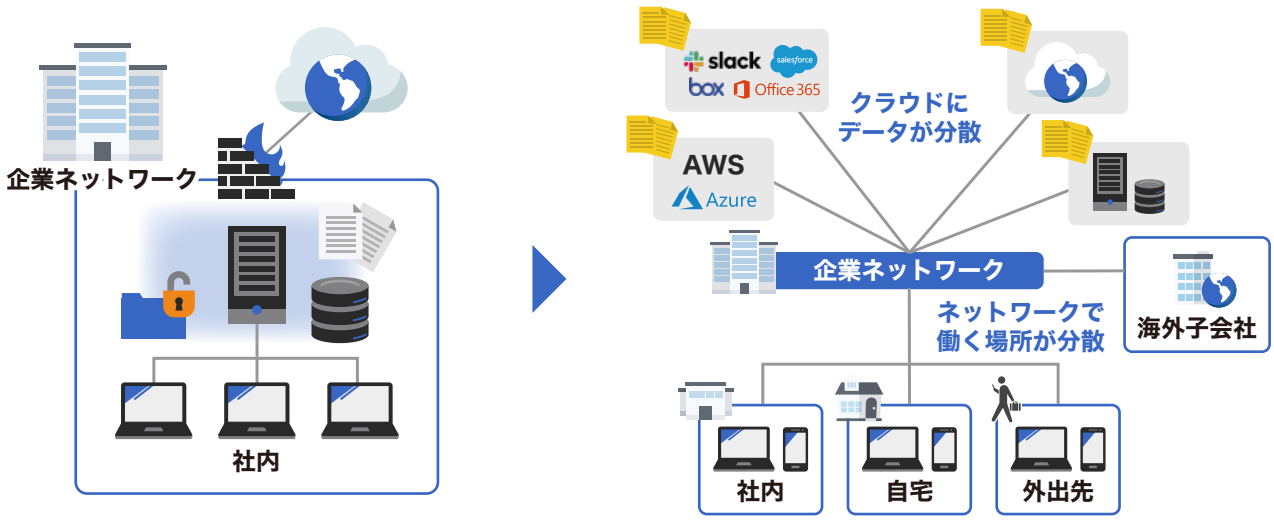


ランサムウェア被害の被害企業・団体等の業種別報告件数



注：図中の割合は小数第一位以下を四捨五入しているため、総計が必ずしも100にならない。

出展：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf



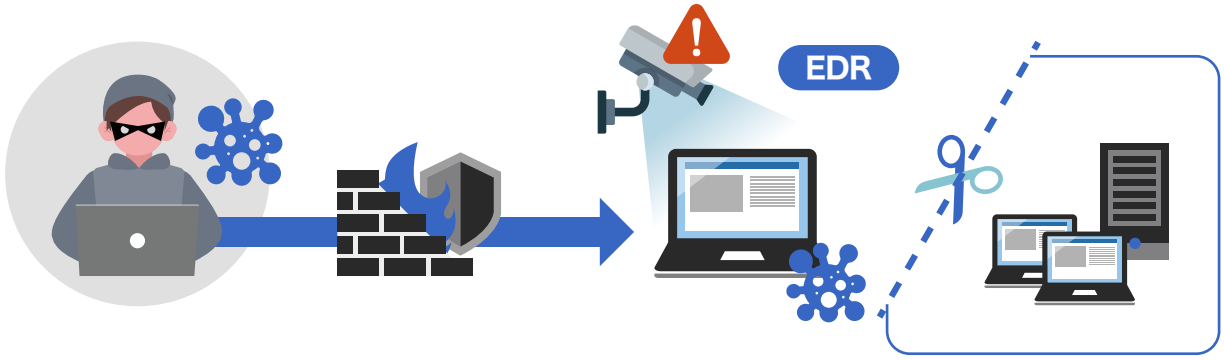
さらには、近年急速に進むテレワークの拡大やクラウド化により守るべき資産があちこちに分散していることに加え、サイバー攻撃の多様化・巧妙化により社内ネットワークへの侵入を完全に防ぎきることが難しくなってきています。そのため、社内ネットワークの入口で侵入を防ぐ境界型防御のみでは資産を守り切れない状況です。

EDRとSIEM

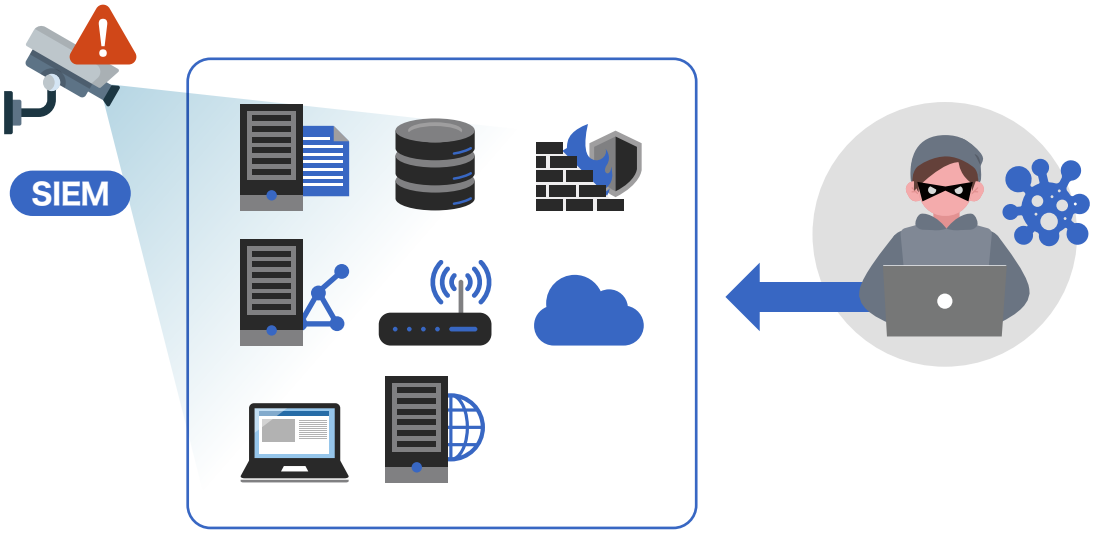
このような状況下で、全ての攻撃を防ぎきることができるセキュリティ対策はない、という前提に立ち、侵入された際に「被害を最小限に抑えるための対策」を講じる必要に迫られることになりました。

サイバー攻撃などの被害を最小限に食い止めるためには、初動でいかに迅速に適切な対応を取れるかが肝心になります。そのため、防御重視だったセキュリティ対策は検知・対応・復旧等のインシデント対応を重視するようになっています。迅速なインシデント対応の支援を目的としたソリューションとして、注目を浴びているのがEDR（Endpoint Detection and Response）とSIEM（Security Information and Event Management）です。

EDRは、組織内のネットワークに接続されているPCやサーバなどのエンドポイントの状況を監視し、不審なふるまいの検知や対処をするためのソリューションです。EDRの基本的な機能は、エンドポイントで発生するイベントと操作に関するデータを収集し、悪意のある振る舞いを検知することです。異常を検知した際には、被害が拡大しないように遠隔で通信制御等を行うことができ、素早い初動対応により被害を最小限に抑えることも可能になります。



一方SIEMは、ネットワーク機器やサーバなどあらゆるIT機器からログを収集・加工・分析し、異常を検知するためのソリューションです。SIEMのメイン機能は相関分析です。複数のログデータを相関分析することで、セキュリティインシデントの予兆や痕跡を発見し、管理者に通知します。それにより、迅速な対応が可能となり、また、コンプライアンス対応やレポーティング機能によって監査報告の際にも活用することができます。



機能比較

EDRとSIEM両者とも、侵入されることを前提として検知・対応・復旧を重視し、サイバー攻撃の被害を最小限に抑えることを目的としている点は同じです。しかし、それぞれが得意とする部分は以下のような違いがあります。

NISTサイバーセキュリティフレームワーク

現状把握	防御	検知	対応	復旧
脆弱性診断 など	次世代 アンチウイルス など			

EDR		
◎ エンドポイントの リアルタイム監視による 不審なふるまいの 検知が可能	◎ リアルタイム検知により 迅速な初動対応が可能	○ エンドポイントを除く 複数の環境にまたがる インシデント調査には 向かない

SIEM		
◎ システム環境全体の ログの相関分析による 異常の検知が可能	○ 検知内容をもとに ユーザーでの対応が必要	◎ ログからインシデントを 詳細に事後調査できる

EDRとSIEMのどちらを導入すべきか、悩まれる方も多いかと思います。EDRはエンドポイントをリアルタイムで監視しているため、即座にセキュリティインシデントを検知することができます。さらに、EDRには対処機能があるため、早期の段階でインシデントを未然に防ぐことも可能です。

しかし、サイバー攻撃は様々なITシステムを標的にします。昨今では、VPNの脆弱性などを悪用したサイバー攻撃を受けるケースも増加しているため、PC端末やサーバといったエンドポイントだけでなく、アプリケーション、ネットワークといった複合的なレイヤーを監視し、どのシステムがサイバー攻撃にあったとしても、検知が行えるようなアプローチも重要です。

上の図のように、どちらも得意とする分野が異なり、２つは相互に補完し合う関係にあることから、長期的にはどちらも導入して万全を期すことが理想的です。しかし、どちらを先に導入するかは、導入の目的や環境に合わせて優先順位をつけ、決めるとよいでしょう。

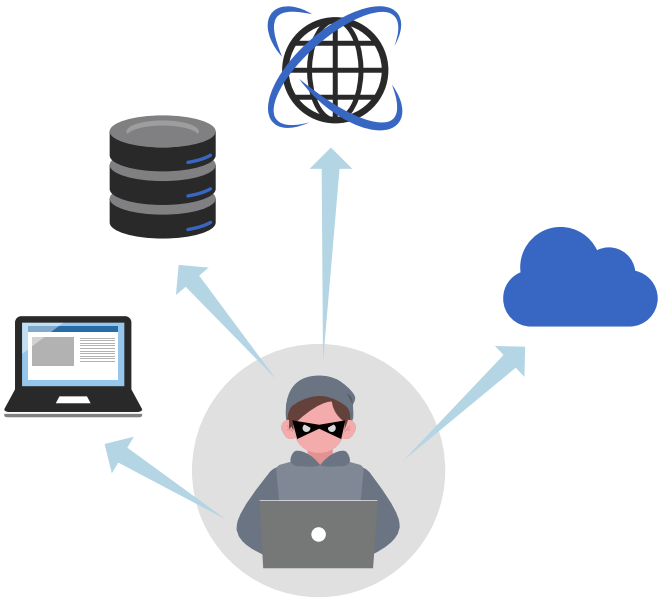
EDR×SIEM 連携で実現するサイバー攻撃対策

前述のとおり、EDRとSIEMは相互に機能を補完し合う関係にあることから、
連携をすることで強固なセキュリティ対策を実現することができます。連携の効果は主に次の２つが挙げれらます。

1. 監視対象の拡大と適切な対応

EDRとSIEMを連携することにより、お互いの弱点を補い合うことができます。EDRは前述の通り、エンドポイントの情報を吸い上げるため、SIEMでVPNやネットワーク機器なども監視すれば、ユーザーのIT環境を包括的に可視化することが可能になります。

一方で、SIEMのみでは検知の難しい不審な動きはEDRで検知し、その際には適切なアプローチで対応することができるため、サイバー攻撃の被害を最小限に抑えることも可能です。



2. 詳細なインシデント調査

EDRのログをSIEMへ連携することにより、更に詳細なインシデント調査が可能となります。

EDRでインシデントを検知した際、本当にサイバー攻撃かどうかを判断する必要があります。SIEMに集めたEDRを含む各システムからのログを総合的に確認することにより、インシデントの全体像を把握し、精度高く判断できます。

網屋のALog

網屋のALogシリーズなら、EDRと連携してサイバー攻撃対策を強化することができます。ALogは、多様なITシステムのログをエージェントレスで自動集約・運用監視するログマネジメントソリューション。特許を取得したログ翻訳変換・整形技術をはじめとした国産ならではのこだわりで、ログ管理の「むずかしいをカンタンに」。専門知識やノウハウがなくとも強固なセキュリティ対策を実現できます。

むずかしいをカンタンにする4つの特徴

機能が多く使いこなすことが難しいSIEM。
ALogなら、SIEMに必要な機能を絞ってあるため、SIEMによるログ管理の「むずかしいをカンタンに」します。

特許取得の翻訳変換技術

データアクセスの記録を複雑で膨大なシステムログから抽出し、
特許(第6501159号)取得のログの翻訳変換技術を使って、見やすい「アクセスログ」にまとめます。

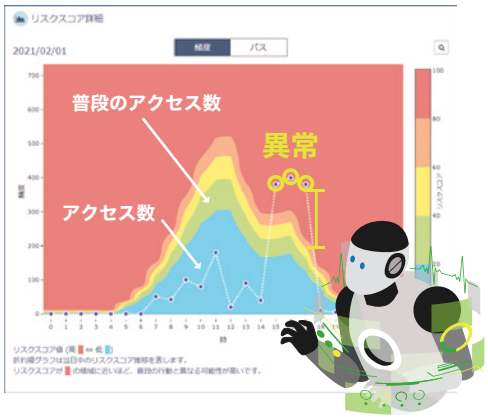
日時	ユーザー	サーバ	ファイル	操作
2022/09/29 15:44:19.825	amya Sasaki	amyfs001	D:\fsvol1\営業部\重要顧客リスト.xls	READ
2022/09/28 23:43:21.422	amya Yamada	amyfs001	D:\fsvol1\企画部\FY13事業計画.doc	WRITE
2022/09/28 12:45:02.259	amya\Sato	amyfs003	D:\fsvol1\経理部\給与明細_田中.xls	DELETE
2022/09/27 02:38:12.245	amya Akagi	amyfs002	D:\fsvol1\営業部\製品別購入者一覧.xls	WRITE

効果的なレポート・アラートルール

効果的な監視と異常を自動検知する
レポート・アラートルールをアドオン。
複雑な要件定義は不要で、
導入したその日からログ活用をスタートできます。

AIが異常を自動検知

ユーザーごとの行動傾向をAIが自動学習。
いつもと違う行動を危険度に応じてスコアリングし、
不正や攻撃の予兆を検知します。



オンプレからクラウドまで、ログデータを収集

オンプレのサーバ、ネットワーク機器、などの様々なログを自動取得するためのテンプレートを準備。
クラウドサービスは、収集プラグインが実装されているので、カンタンに取り込むことができます。

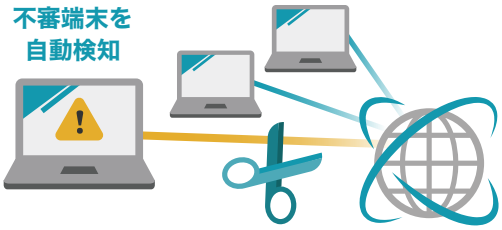
連携事例
Cybereason×ALog

ALogは、EDR国内シェアNo.1※のCybereasonとの連携をしております。Cybereasonのログに加えて、様々なシステムを集約することで、エンドポイント以外の影響調査や不正の予兆検知が可能です。国内シェアNo.1メーカー同士の連携ソリューションを活用し、包括的且つ、容易にセキュアなIT環境を実現しましょう。

※出典：株式会社富士キメラ総研 2022年11月17日発行「2022 ネットワークセキュリティビジネス調査総覧（市場編）＜2021年度＞

cybereason

マルウェアの検知と隔離遮断



検知ログをSyslog受信

EDRアラート / NGAVアラート情報

ALog

様々なシステムのログを統合

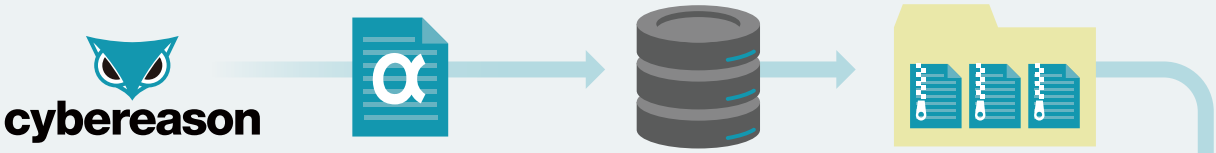
Cybereason検知ログ

各管理者操作ログ
個人情報へのアクセス操作ログ
クラウドサービス利用ログ等

不正・危険の監視

レポート / 検索　AI検知　異常の検知

カンタン4STEP連携



1. Syslog出力

ALog Syslog Receiver にてSyslogを受信。
取り込み用のCSVデータを生成。

2. Syslog受信

Cybereasonより、各種検知ログをSyslog形式で
出力するための設定を実施。

3. 取り込み

Cybereason専用のログ取り込み用テンプレートを
ALogにセットしてインポート処理。

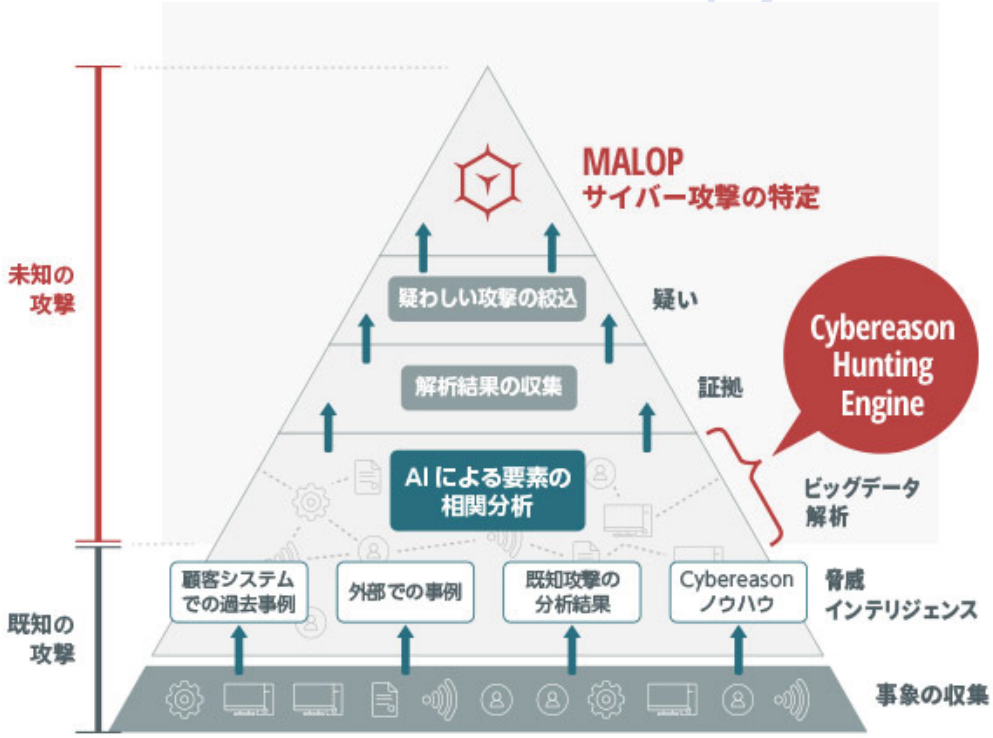
4. レポートセット

Cybereason専用のレポート / アラートテンプレートを
ALogにセットして自動レポート作成。

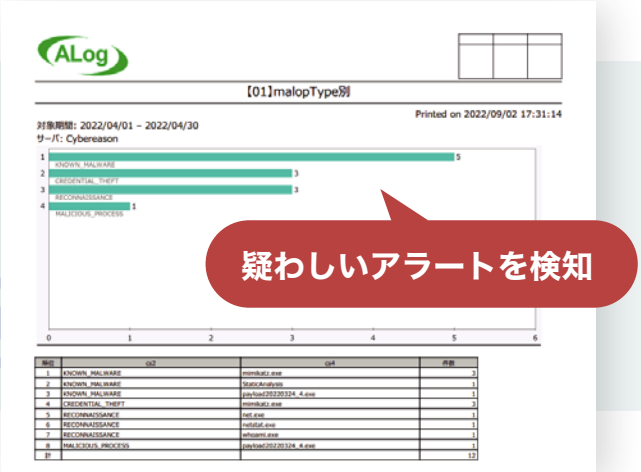
Cybereason×ALog
活用事例

疑わしいアラートから被害を特定

CybereasonのEDRは、独自の分析エンジンで取得したデータを横断的に分析し、異常な行動を発見します。
それらの異常な行動を「証拠」として集め、関連する「証拠」の集まりを「不審事項」として監視後、
攻撃性の高いものを「MALOP」(malicious operation: 悪意ある操作)として特定します。



出典：Cybereason EDR の分析エンジン　https://www.cybereason.co.jp/products/edr/



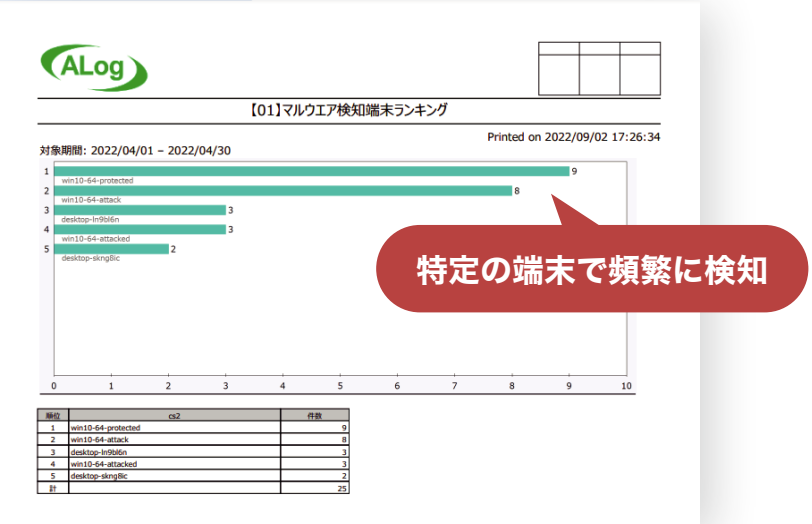
EDRにおける脅威度が高くないものや、Malopまでの判定をするには材料が足りなかった不審事項など、放置するには怪しいと考えられるログをAlogに連携し、様々なログをトリガーにエンドポイント以外の環境も包括的に監視することで、より広範囲のセキュリティを実現することができます。

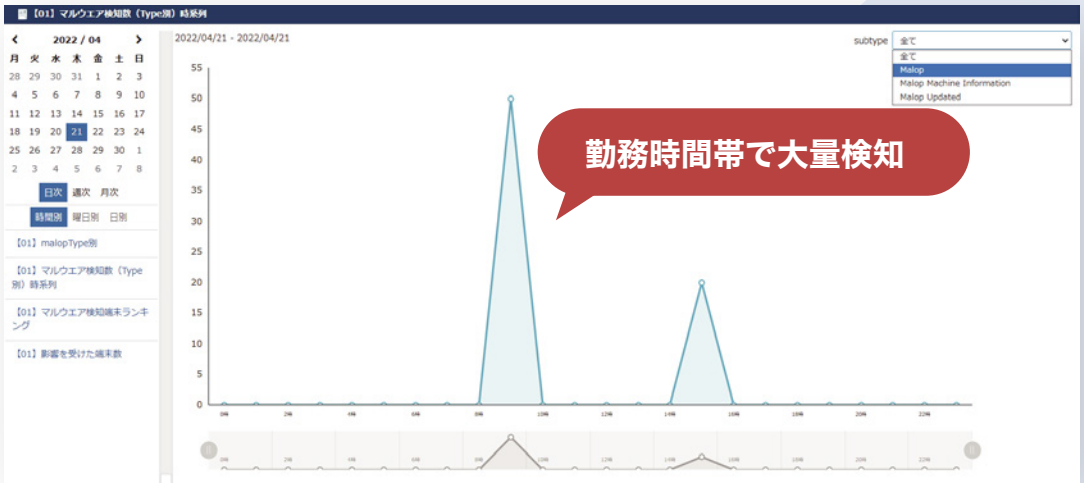
Cybereason×ALog
活用事例

端末のアクセス傾向を把握

CybereasonのEDRとALogを連携することで、マルウェアを頻繁に検知したエンドポイントをランキング化して、上位の端末の感染前後の挙動などをレポートと検索結果でトレースすることもできます。

例えば、マルウェアの検知回数を時間軸で統計してみると日中の作業時間が多いことが判明し、
さらにWebプロキシなどに検索範囲を拡大すると安全でないサイトへのアクセスが目立ち、
その結果ウイルスを頻繁に持ち帰っていることがわかる、
というようなユーザーのアクセス傾向を分析することができます。
それにより、個々の社員のセキュリティリテラシーの実態の把握にも繋がります。

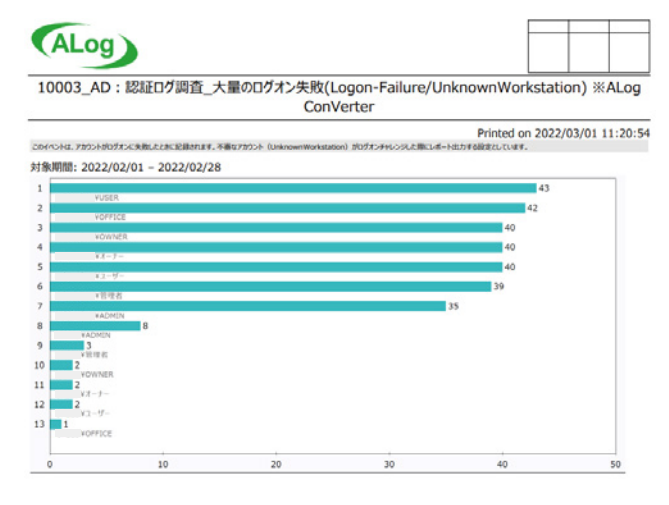




Cybereason×ALog
活用事例

Active Directoryへの侵入を検知

CybereasonのEDRから受け取った検知ログをALogで端末をキーに検索すると、
Active Directory(AD)にその不審な行動と関連する攻撃の痕跡が残っている可能性があります。
ADの管理者アカウントは、ADの管理配下にある全てのリソースにアクセス可能な権限を持っているため、
攻撃者も優先的にADを攻撃する傾向にあります。



例えば、ADを掌握してグループポリシーを悪用すれば、検知システムを停止させ、効率的にウイルスを拡散させることが可能になります。

ADへの侵入の試行として、総当たり攻撃によってパスワードの割り出しを行っている場合、ALogに短時間で大量のログオン失敗が記録されます。ADへの侵入試行をいち早く検知することで、被害を拡大させないための策を講じることができます。

大量に発生する不自然なログオン失敗
/ Unknown Workstation /

ありがちなアカウント名を語ったログオンチャレンジ

順位	ユーザー	件数
1	¥USER	43
2	¥OFFICE	42
3	¥OWNER	40
4	¥オーナー	40
5	¥ユーザー	40
6	¥管理者	39
7	¥ADMIN	35
8	¥ADMIN	8
9	¥管理者	3
10	¥OWNER	2
11	¥オーナー	2
12	¥ユーザー	2
13	¥OFFICE	1
計		297

おわりに

セキュリティ人材不足に

本書では、EDRとSIEMの連携により、強固なセキュリティ対策が実現できることを紹介してきました。冒頭でも述べた通り、日本企業は今かつてない規模のサイバー脅威にさらされています。最近のトレンドとしては、セキュリティが強固な大企業を直接狙うのではなく、比較的セキュリティ対策が不十分な中堅・中小企業を経由し、その企業グループに侵入するような攻撃が増加しています。

こうした状況下で、中堅・中小企業におけるサイバーセキュリティ対策が急がれる一方で、現状、セキュリティ人材は中堅・中小企業で特に顕著に不足しており、EDRやSIEMを導入しても、人材不足を理由にその運用まで手が回らないことも多く見受けられます。

クラウドCSIRTサービス「セキュサポ」

そこでご紹介したいのが、クラウドCSIRTサービス「セキュサポ」です。「セキュサポ」は、セキュリティ対策の導入から事故時の対応までを月額固定でワンストップ提供する、セキュリティ代行サービスです。

サイバーセキュリティの専門チームが、セキュリティツールの導入・設計から、インシデント対応までを一貫して実施。EDRのログ活用やSIEMの運用を代行し、中堅・中小企業でも大手企業レベルのセキュリティ対策を実現できます。

サイバー攻撃対策
お客様環境に検知システムを常設。外部攻撃を常時監視

内部不正対策
内部不正の兆候をAIを使って常時監視

脆弱性対策
公開サイトを脆弱性検査し、脆弱性の発見と改善を実施

強化レポート
対策を証明する各種レポートを定期で提出

インシデントレスポンス
事故発生時には、インシデントレスポンスを実施
（原因や影響範囲の調査など）

サイバー保険
インシデントレスポンス費用をサイバー保険でカバーリング。原則無償対応を実現

＼さらに！／

セキュリティ相談窓口
不審なメールの安全確認など、日常のCSIRT対応を代行

セキュサポ

ALog

ログマネジメントソリューション「ALogシリーズ」は、
サーバアクセス監視パッケージ別シェアで、16年連続トップシェアを獲得。※
多様な情報システムのログをエージェントレスで自動集約・運用監視します。
独自のログ翻訳変換技術とAIの不正予兆検知により、
専門知識やノウハウがなくとも、高度なログ活用を実現。
内部不正やサイバー攻撃対策、監査報告など、あらゆるビジネスの課題を解決します。

※出典：https://mic-r.co.jp/mr/02620/ デロイト トーマツ ミック経済研究所「内部脅威対策ソリューション市場の現状と将来展望 2022年度」2023年01月発刊

詳しい製品概要資料をご覧になりたい方はこちら

製品概要資料ダウンロード（無料）

詳しい製品のご紹介や、無料トライアル体験をご希望の方は以下にお問い合わせください

電話でのお問い合わせ
03-6822-9996

メールでのお問い合わせ
bv-sales@amiya.co.jp

株式会社網屋 データセキュリティ事業部

Secure the Success.

網屋の事業は、セキュリティ。

セキュリティ製品やサービスを自ら開発・製造・販売する、セキュリティの総合プロバイダです。

サイバー攻撃は、経済的余裕度に関係なく、全ての事業法人がターゲットになります。

サイバー攻撃の脅威を「セキュリティの自動化」で解決し、

高水準のセキュリティを誰でも享受できる社会を創りたい。

それが私たちのアイデンティティです。

AMIYA

ALog 開発元

株式会社 網屋

https://www.amiya.co.jp/

〒103-0007
東京都中央区日本橋浜町3-3-2
トルナーレ日本橋浜町 11F
TEL: 03-6822-9999
FAX: 03-6822-9998

ALog は株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため
予告なく変更される場合があります。
このホワイトペーパーの内容の一部、
またはすべての複写・転用・転載等を
株式会社網屋に無断で行った場合、
著作権の侵害になります。