kaspersky

侵入されたとき、何分で気付けますか？

Kaspersky MDRで実現する24時間365日の脅威監視

攻撃者は攻撃を成功させるため、侵入経路に公開サーバー・VPNに加えて
開発者環境・サプライチェーンへと多角化させています。
さらに、検出を回避するための正規ツール悪用やBYOVDによるセキュリティツールの
無効化など、攻撃手法は洗練され、従来の対策では検知が難しくなっています。
現在のサイバー攻撃において、重要なのは「侵入に完全に防ぐこと」だけではなく、
不審な兆候を早期検出するための継続的な監視・調査・分析が求められています。





24時間365日の
監視の実現



AIによるインシデントの
フィルタリング



エキスパートによる
専門的な調査

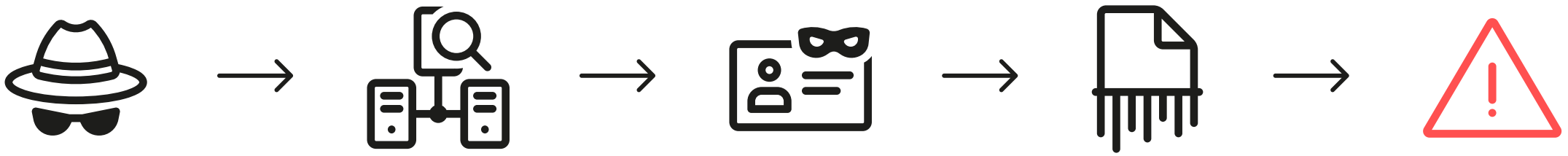


レスポンスの
即時実行

01 今求められるMDRの役割

kaspersky

- 攻撃者は侵入後、正規ツール・正規アカウントを悪用して横展開や権限昇格を実施
  日常業務に利用される正規ツールの悪用はEPP単体で判定することが難しい
- 侵入経路も従来の公開サービス・VPNなどの脆弱性悪用に加えてサプライチェーン攻撃など多角化



初期侵入
内部偵察

横展開

権限昇格
認証情報窃取

情報流出

目的の達成
（ランサムウェア配布など）

■ 課題

- サイバーセキュリティ担当者不在の深夜帯・休日の対応が決まっていない
- EDR導入済みだが、アラートを精査するスキルに課題
- インシデント発生時の対応・判断が属人化している

攻撃者の「侵入後」にいかに早く気付けるかが、
被害が深刻化するかどうかのポイントになります。

Copyright © 2026 Kaspersky Lab. All rights reserved.

02 Kaspersky MDRで解決できる4つのこと

- Kaspersky MDRはAI x エキスパートによる調査・分析で24時間365日を実現し、
  高度な攻撃の早期検出とインシデント発生時の対応を支援します。

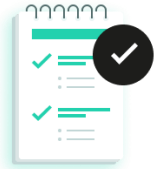
01 24時間365日の監視を実現

- お客様環境で発生したイベントを24時間365日
  継続監視
- インシデント発見時に、インシデントの詳細と
  レスポンスおよび推奨の対応策を提供；
  レスポンス：ネットワーク分離・対象ファイル取得など
  推奨の対応策：スキャン実行、各製品の設定調整など



02 検出ロジック・AIを活用したインシデント処理

- 収集したテレメトリを脅威ハンティングルール・
  AIによってリアルタイムで処理、機械的に偽陽性の
  フィルタリング・優先順位付けを行うことで
  攻撃の検知からお客様への報告まで時間短縮を実現
- 2025年、重大度の高いインシデントの報告時間：平均42分



03 エキスパートによる高度な分析

- 脅威ハンティングルール・AIが脅威判定した場合、
  エキスパートによる脅威ハンティングを実施
  エキスパートも脅威と判定したインシデントのみ
  お客様へ報告
- さらに、エキスパートは能動的にテレメトリを調査
  検出ロジック・AIが見逃す高度な攻撃を検出



04 「自動承認機能」で初動対応の自動化を実現

- 自動承認機能を有効にすることで、管理者の
  承認無しでレスポンスを自動実行
- 深夜・休日時間帯を狙うランサムウェアなどに
  対する対象端末のネットワーク分離や調査・分析に
  必要な検体の自動取得が可能



Copyright © 2026 Kaspersky Lab. All rights reserved.

03 MDR：チェックリスト

以下のチェックリストで現在の体制を振り返りましょう。

チェック項目	はい	いいえ	不明
夜間・休日もアラートを確認できる体制がある	☐	☐	☐
EDRのアラートを分析できる担当者がいる	☐	☐	☐
誤検知・過検知を判断する基準がある	☐	☐	☐
正規ツール悪用を検知するツールが導入済み	☐	☐	☐
インシデント発生時の対応が決まっている	☐	☐	☐



1つでも「はい」に
チェックが入らなかった場合、
Kaspersky MDRによる
監視・調査・分析が
有効な選択肢です。



詳しいご説明・デモ・検証のご相談はこちら

株式会社カスペルスキー　セールス営業本部　jp-sales@kaspersky.com