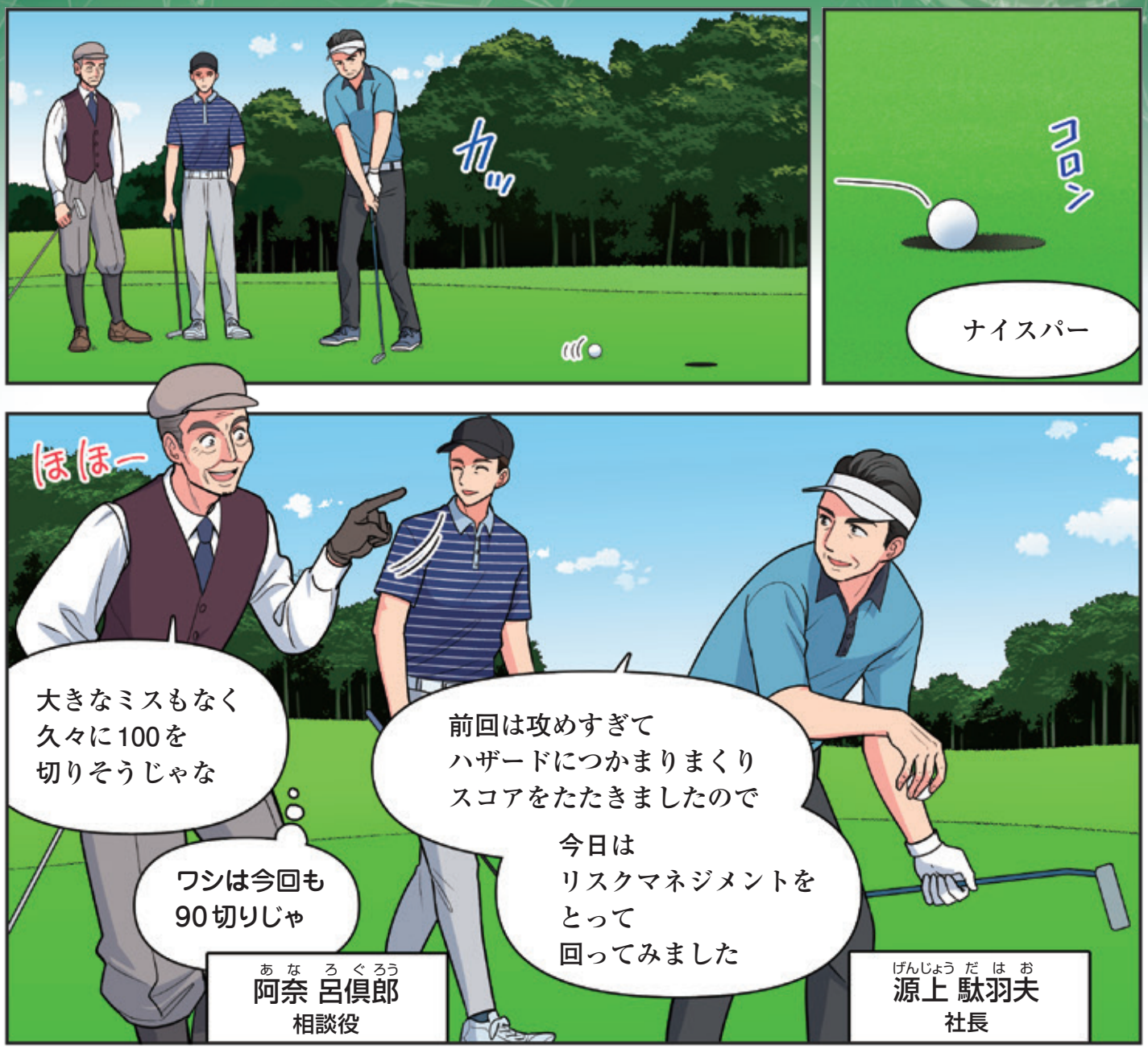
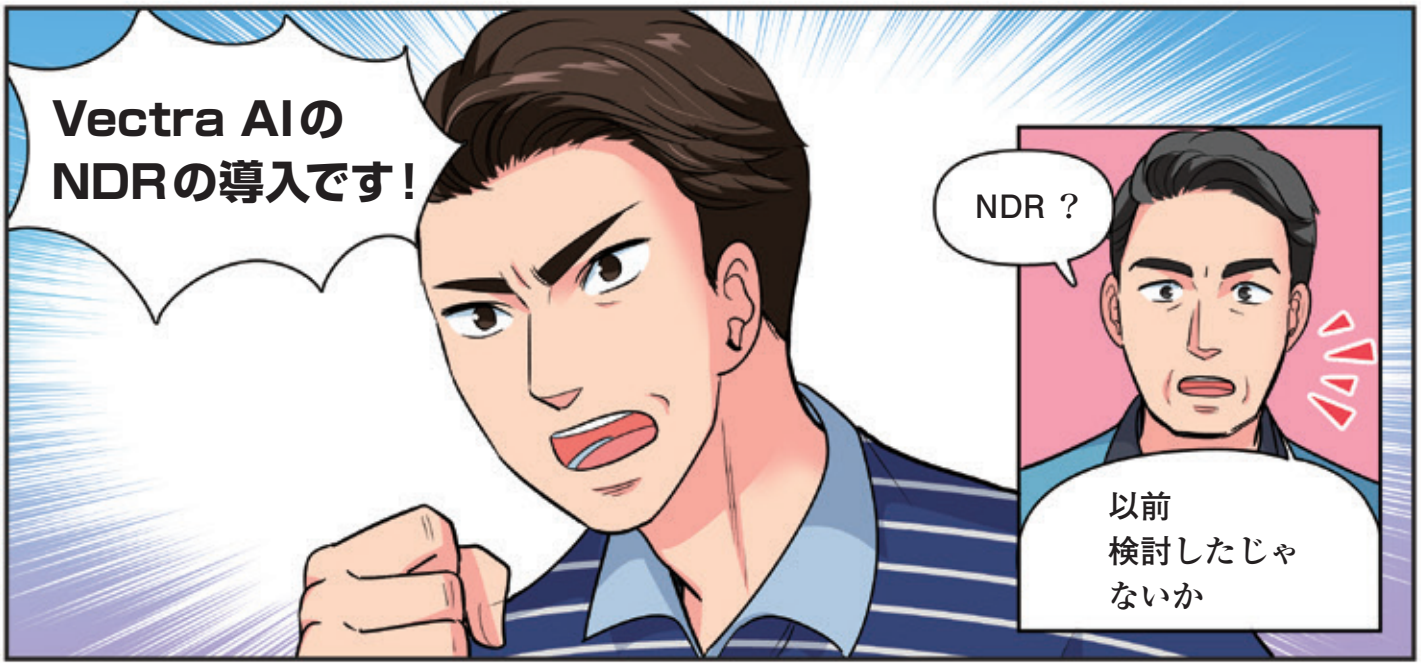
VECTRA

NDRはここまで進化した!

マンガでわかる! Vectra AI




A社がランサムウエアで
10億円の被害を
被ったのは
ご存知か思います
ネット
ニュース
ああ…
他人事ではないな
そうなんです
当社も早急に
安全策を講じる
必要があると
思います！
おいおい
うちはEDRを導入しているから
問題ないだろ？
A社もEDRを
導入していたそう
なんですが…
EDRが入っていない端末や
海外拠点から侵入された場合に
内部偵察を検知できず
感染拡大して
しまったそうです
そうなのか!?
それで今回の
被害となった
わけか…
では
どうしろと？

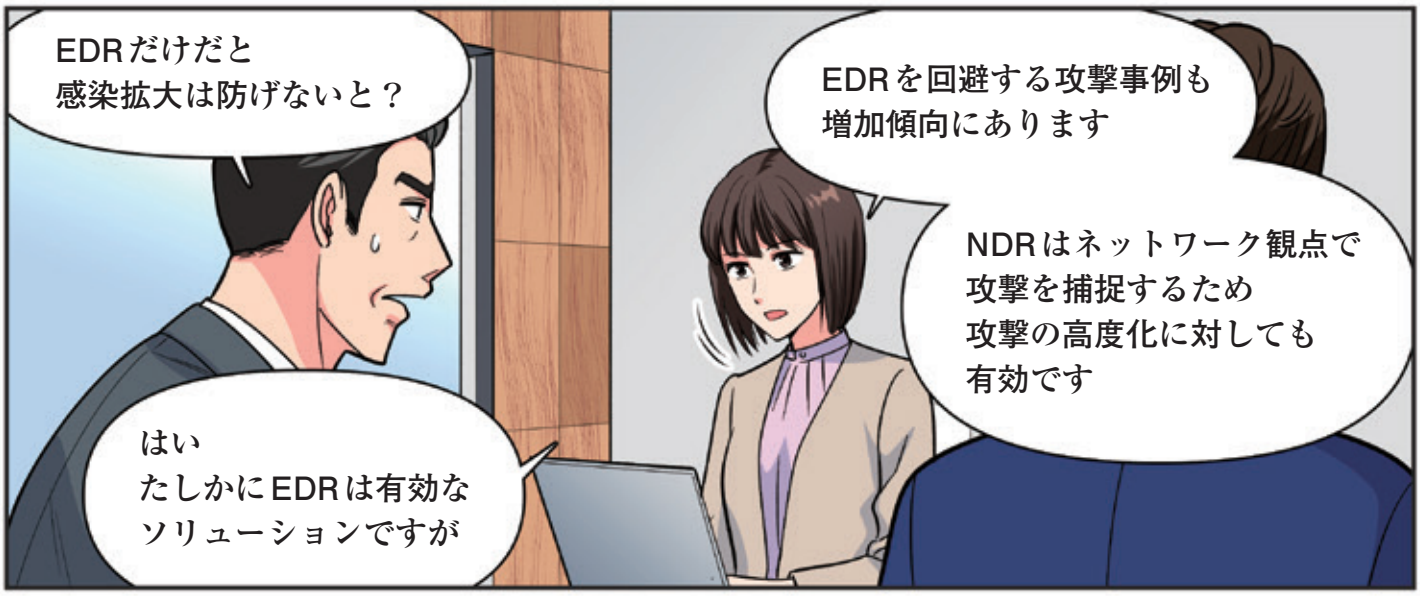

Vectra AIの
NDRの導入です！
NDR？
以前
検討したじゃ
ないか


NDRは
相当進化してます
先日
外部委託している
SOCの担当者から
ざっと説明を
受けたのですが
前回のベンダーとは違い
今回紹介されたNDRの製品
Vectra AIの性能には
正直驚かされました
う〜ん
それに
しても…
EPPの次は
EDR…
そしてNDRか…


ワシの家の
空き巣対策
みたいじゃのぉ
あ〜ん
え？


まず門を
頑丈にして
侵入を阻止
ドーン
ガッチガチ
それでも
侵入された場合に備えて
廊下に赤外線探知機を
張り巡らせておるから
ピー
それを乗り越えられて
庭や離れを
物色されても
母屋に入られないように
ドアの鍵を
二重三重にしておる
各部屋を
移動できないのじゃ！
さ…
さすがです
わかった
来週早々にも
SOCの担当者を呼んで
詳しい話を
聞かせてくれ
数日後
サイバー攻撃は
戦術面では
ターゲット企業に対して
『攻撃手法』だけでなく
『どこから攻めるか』に
ついても戦略的に
考えます
関百合 貞子
外部委託のSOC担当者

※「NDRとは何だろう」2ページより



…で
君が言っていた
Vectra AI
ってわけだな

はい

AIエンジンによる分析結果

Vectra AI 学習効果 (Brain)

Vectra AIは
脅威がみつけにくい高度な攻撃を
AIを使って防ぐ方法を提供します

だが実際に
導入するとなると

うーん…

リソース費用などあって
ハードルが高そうだな…

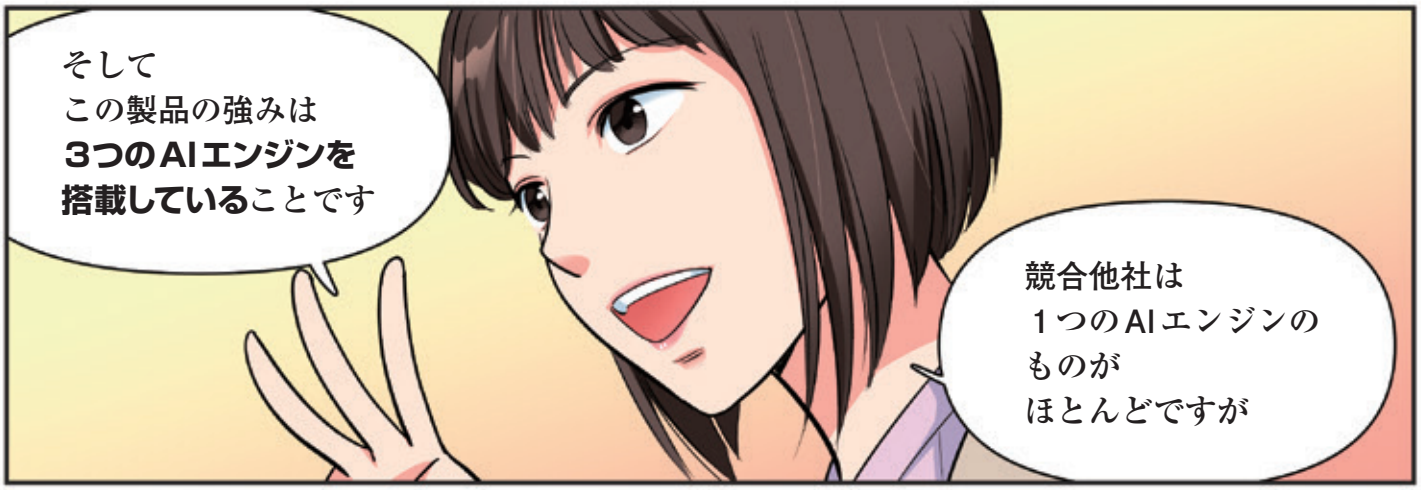
大丈夫です！

EDRは実施の端末に
エージェントを
インストール
しなければなりませんが

それに対しNDRは
コアスイッチから
通信をTAPすることで
ご利用が可能です

端末のOSや
プラットフォームに
依存することなく
監視が可能です

思っていた以上に
導入は容易だな



NDRベンダー唯一3つのAIエンジンを搭載

Vectra AI 外部脅威、内部不正対策 AI エンジン　ベンダー最多 38 特許

① MITRE ベースの グローバルラーニングエンジン

攻撃者の戦術・手法などを網羅した検知

Mitre Att & CK（マイタアタック）
客観的根拠に基づいた脅威への対策を
適宜している。

- 振る舞いにフォーカス
- Mitre Att & CK カバー率 97%
- 脅威インテリジェンス

② アノマリー検知ベースの ローカルラーニングエンジン

通常と違う振る舞いを検知

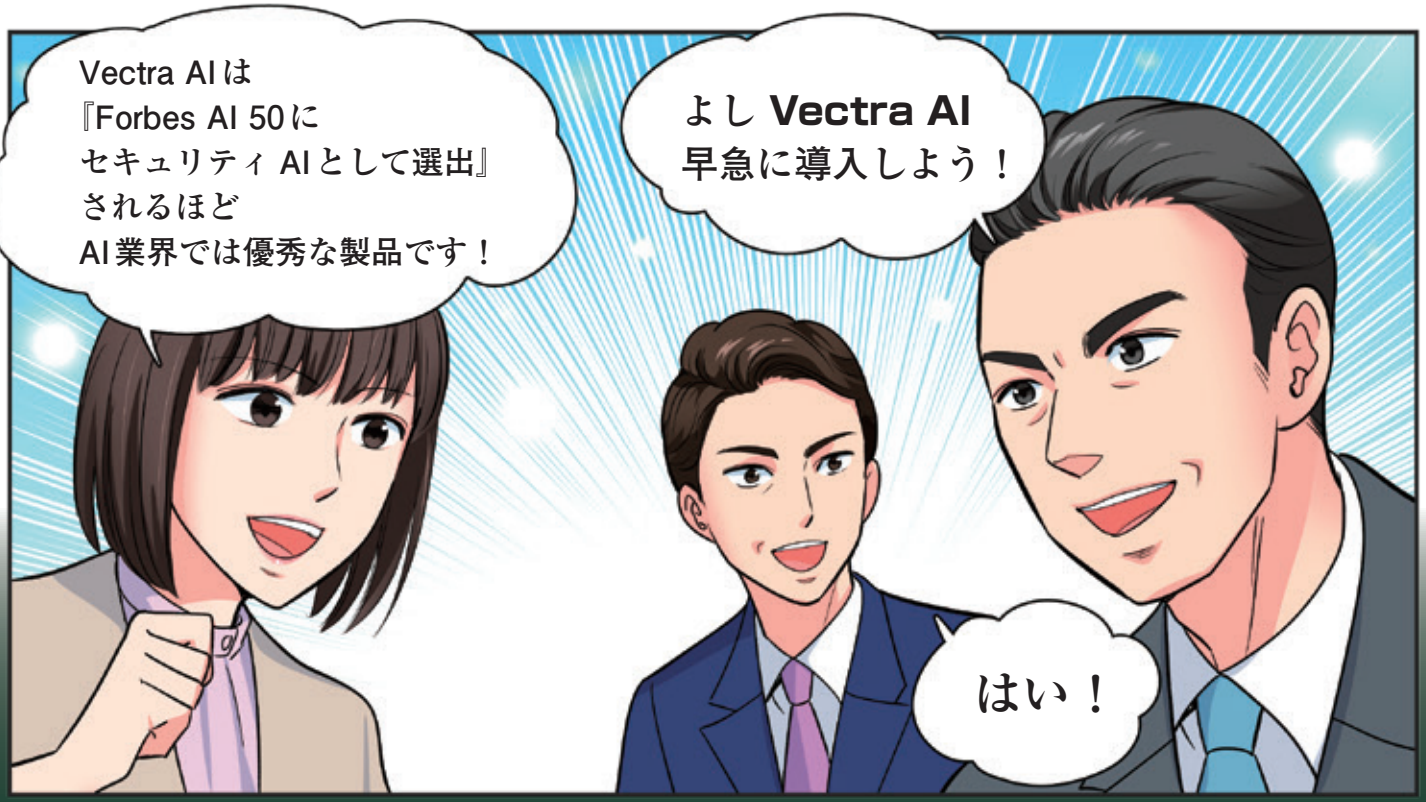
- 権限アクセス分析モデル
- ホスト、アカウント、サービス視点で分析
- 内部の不正対策にも有効

③ リアルタイム相関分析

情報統合・分析と自動化

①と②のエンジンで検知した脅威を
相関的に分析し、4 段階に対策優先順位を
つけて知らせてくれる。
①と②どちらともの情報に基づき
分析・アラートするた網羅的に検知できる。

- グローバルラーニングとローカルラーニングで検知したアラートを相関分析
- 優先順位付け（Critical 含む 4 段階）、トリアージを自動化



お問い合わせ

Vectra AI Japan株式会社

E-mail: **info-japan@vectra.ai**

VECTRA®