その対策、本当に防げますか？
ランサムウェアやサイバー攻撃へのAI活用状況から考える、実効性あるセキュリティ対策とは

～AIも活用した攻撃者視点のセキュリティ検証で真のリスクを特定～

東京エレクトロン デバイス株式会社

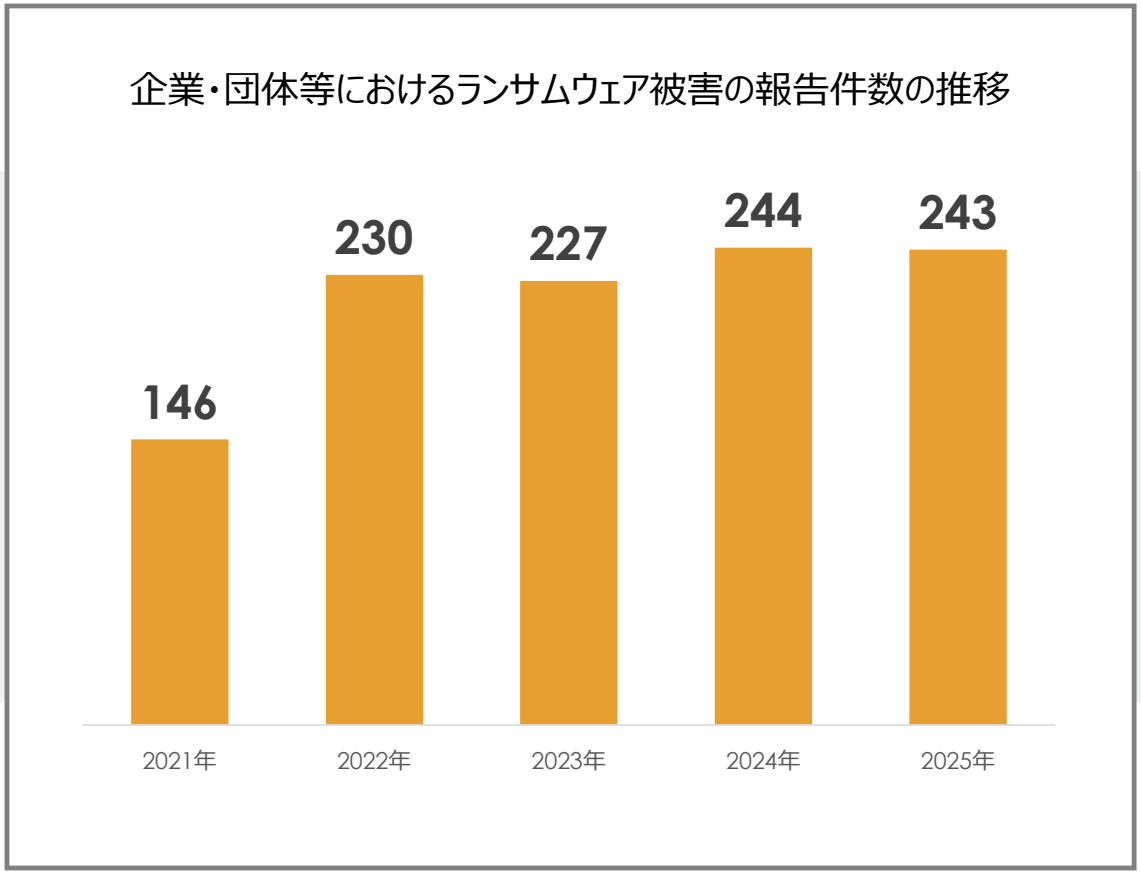
Pentera Security Ltd.

目次

- なぜランサムウェア被害は後を絶たないのか
- AIによるサイバー攻撃の高度化・高速化
- 攻撃者視点のセキュリティ評価を可能にする「Pentera」
- Penteraは何を実現するのか
- Penteraデモ
- まとめ

なぜランサムウェア被害は後を絶たないのか

ランサムウェアの最新被害状況



2022年以降

高い水準で推移

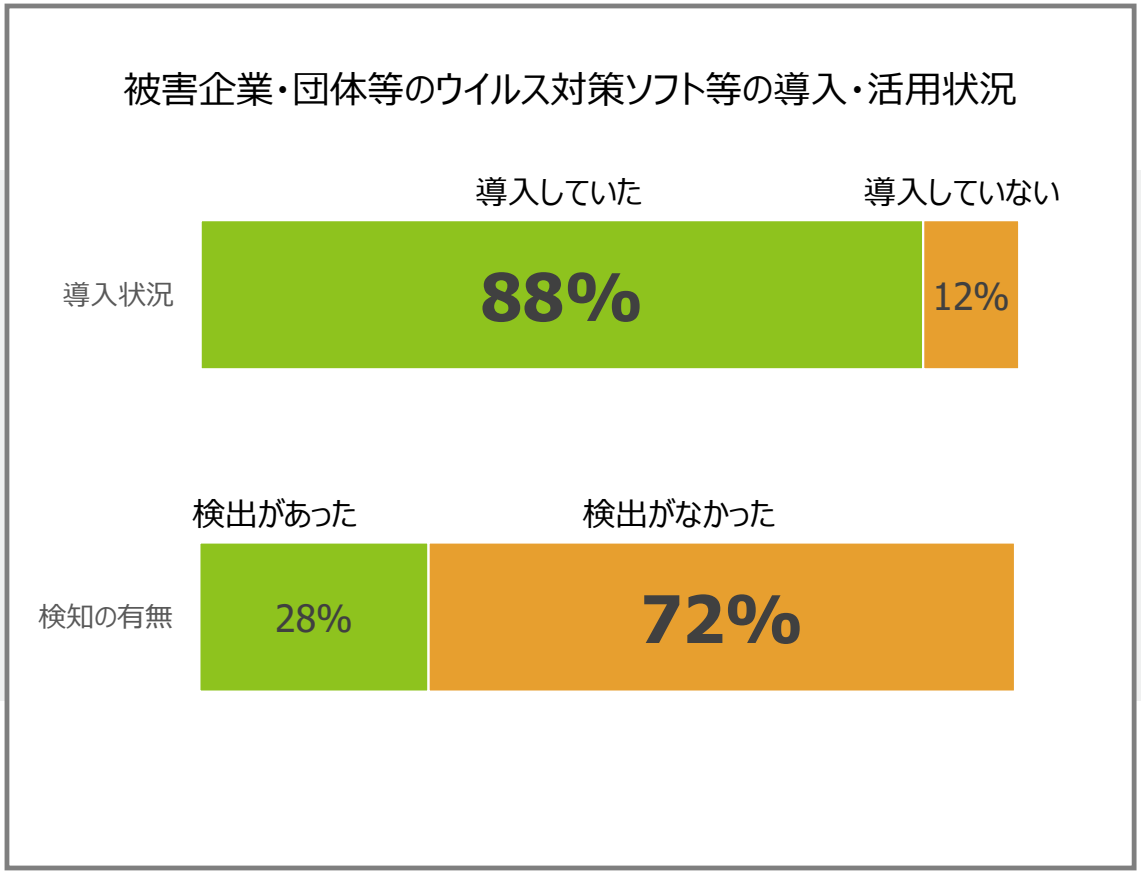
IPAが公表する情報セキュリティ10大脅威*でも

11年連続1位

出典：令和7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（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

*情報セキュリティ10大脅威 2026（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/10threats/10threats2026.html

被害企業団体のウイルス対策ソフトの導入状況

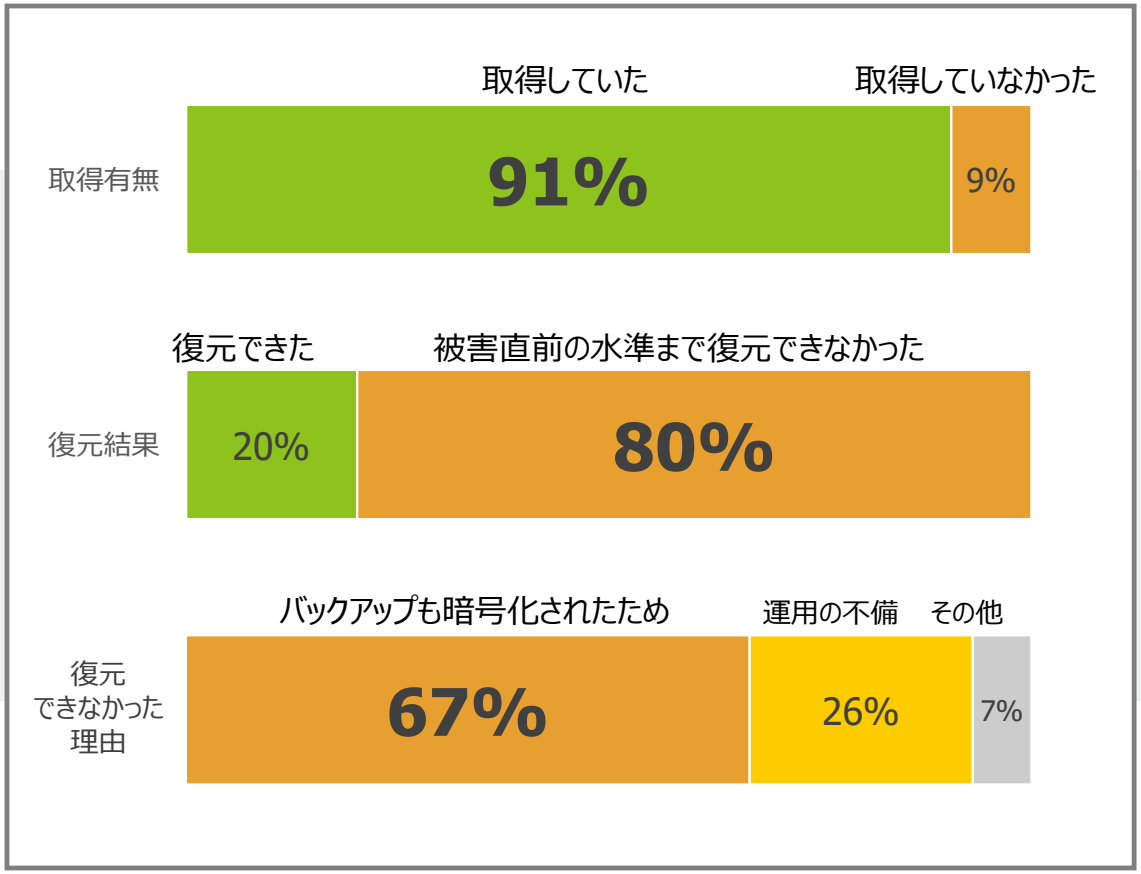


対策ソフトを導入していながら検出できず 72%

ランサムウェア攻撃を受けた際、EDRが検知できるかの検証が必要

出典：令和7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（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

バックアップの取得・活用状況



バックアップを取得していても
復元できなかった **80%**

ランサムウェア攻撃を受けた際、
バックアップ復元可能性の検証が必要

出典：令和7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（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

なぜこのような状態が続いているのか？

なぜランサムウェア被害は減らないのか

- 何らかの対策は導入しているが、**その対策が有効に機能するかどうか**は把握できていない
- 防御側の視点で「このような対策が必要だろう」「必要な対策はできているはず」ではなく、
  攻撃者の視点で「ランサムウェア攻撃は成功するか」「どんな対策が必要か」を考えることが重要

どこまで攻撃が広がるかを確かめるには

攻撃者と同じ手口で攻撃してみることが一番

AIによるサイバー攻撃の高度化・高速化

Claude Mythosの登場

- Claude Mythos（クロード ミュトス）とは
  - Anthropic社が2026年4月7日に発表したセキュリティタスクにおいて驚異的な能力を発揮するモデル
  - 非常に強力なサイバー攻撃能力を有し、危険すぎて一般公開できないという異例の判断
  - 「Project Glasswing」という国際的なサイバーセキュリティ連合を立ち上げ、限定公開

- なぜClaude Mythosは衝撃を与えたのか？
  - **大量の脆弱性の自律的発見と悪用：**
    主要なOSやブラウザの未知の脆弱性を自律的に発見、
    中には16年間誰も気づかなかったソフトウェアの欠陥なども含まれる
  - **複雑な攻撃チェーンの構築：**
    単一の脆弱性を突くだけでなく、複数の脆弱性を組み合わせた高度な攻撃を生成する能力も有する
  - **攻撃の高速化とコストの劇的な低下：**
    人間であれば数週間かかる高度なエクスプロイト開発を、数時間レベルで完了させることができる

セキュリティを守る立場としてどう考えるべきか

MythosのようなAIによって

- 脆弱性の発見を高速化
- 悪用コードの生成を加速
- 攻撃パターンの作成を高度化

自社環境において

- どの脆弱性が悪用され得るか
- どのような攻撃経路が存在するか
- どの脆弱性から優先的に対処すべきか

必要なのは

「本当に成立する攻撃経路を特定すること」

「自社にとっての対策優先順位を付けること」

攻撃者視点のセキュリティ評価を可能にする「Pentera」

Penteraとは

PENTERA.

Automated Security Validation（自動セキュリティ検証プラットフォーム）

攻撃者の視点で自社のセキュリティリスクを確かめる

- **脆弱性の一覧ではなく、実際にどこまで進めるかを検証**
- **「問題があるか」ではなく「どれだけ現実的な脅威か」を可視化**
- **本番環境で安全に、繰り返し実行できる**

会社概要

PENTERA.

ペネトレーションテストの手法を用いて攻撃者視点での継続的なセキュリティリスクの可視化と改善を実現する自動セキュリティ検証プラットフォーム

本社	ボストン
販売・サポート拠点	イスラエル、トロント、ロンドン、APAC（シンガポール、日本、オーストラリア）
従業員数	450名以上
Pentera Labs	イスラエル国防軍エリートサイバー部隊出身者による強力なリサーチチーム
Gartner社によるカテゴリー	Adversarial Exposure Validation（攻撃者視点の露出検証） 攻撃者が実際に悪用可能な脆弱性を検証する手法

Connect Beyond

導入実績

グローバル：

- 65か国1300社以上への導入実績
- 銀行、保険、リテール、法律事務所、ヘルスケア、政府系など多種多様な業界での採用

日本国内：

- 金融系、官公庁、エンタープライズでの採用実績

各種受賞

RED HERRING EUROPE WINNER 100

FROST & SULLIVAN 2019 BEST PRACTICES AWARD

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019

2019 FORTRESS CYBER SECURITY AWARD

CYBERSECURITY BREAKTHROUGH AWARDS

準拠

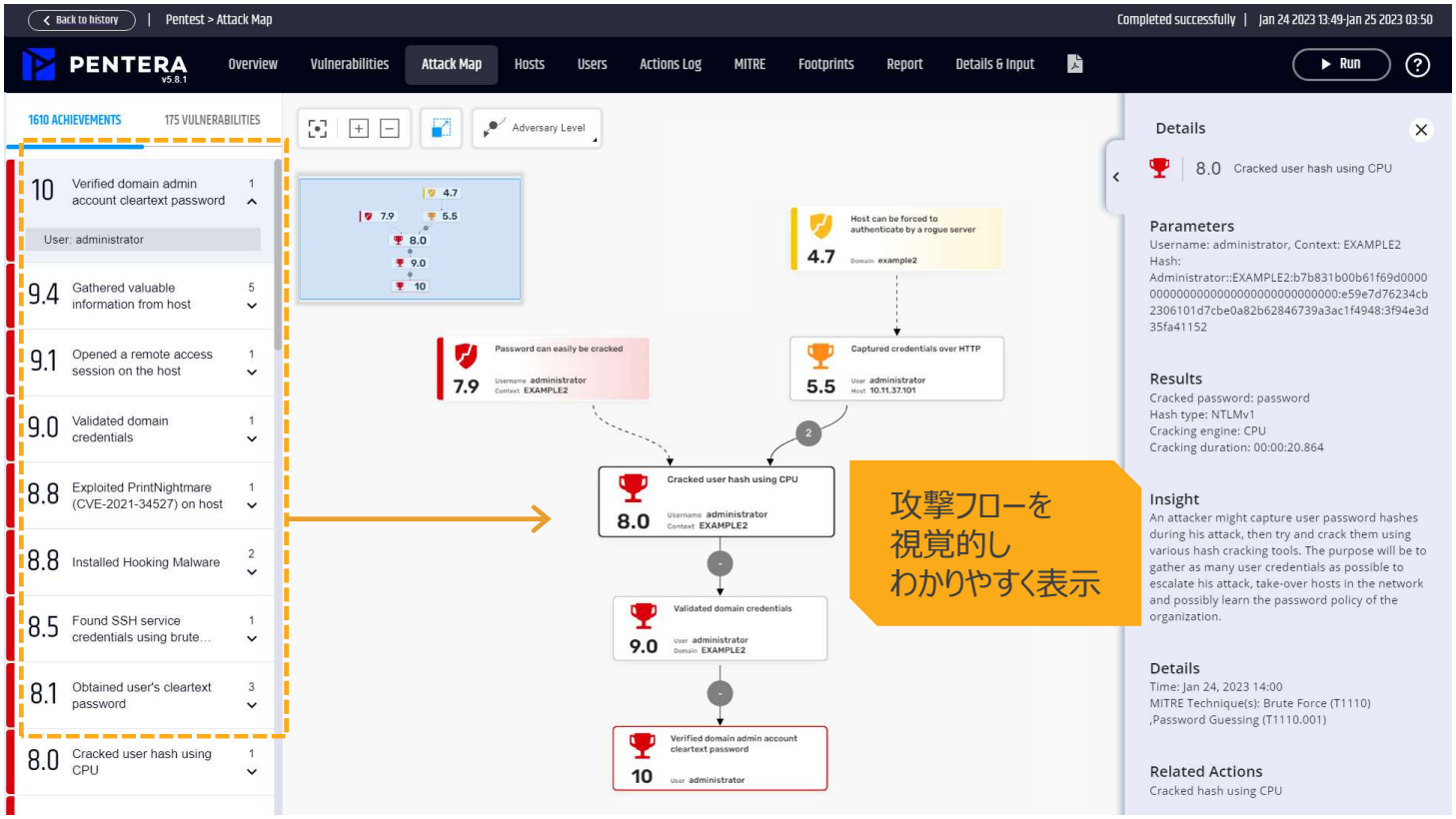
Information Security Management ISO 27001 Certified

PENTERA FROST & SULLIVAN BEST PRACTICES AWARD GLOBAL BAS MARKET LEADERSHIP 2022

Penteraは何を実現するのか

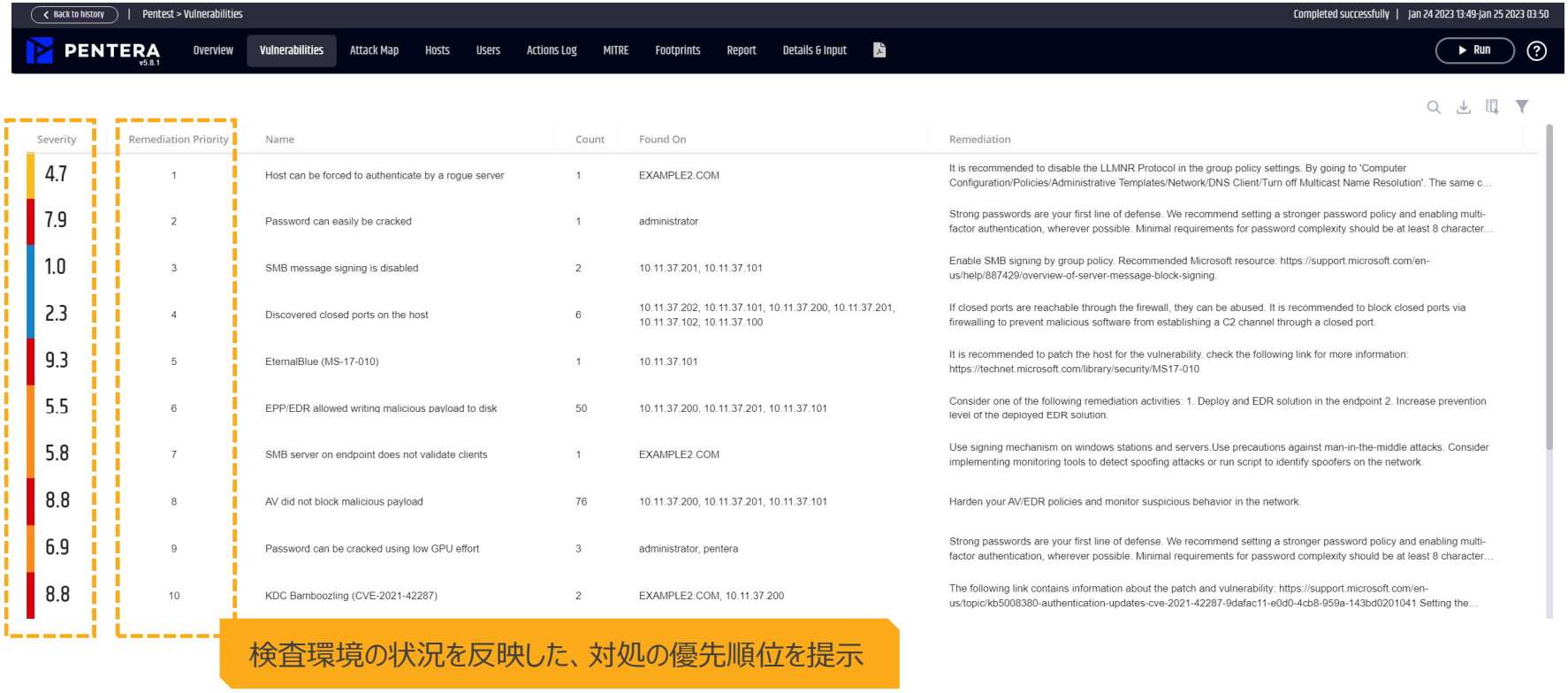
攻撃者視点でセキュリティリスクを可視化する

- 攻撃者目線で達成した攻撃経路を可視化
- 悪用され得る脆弱性とその結果起こり得る被害を把握



攻撃の影響度をもとに優先順位を付ける

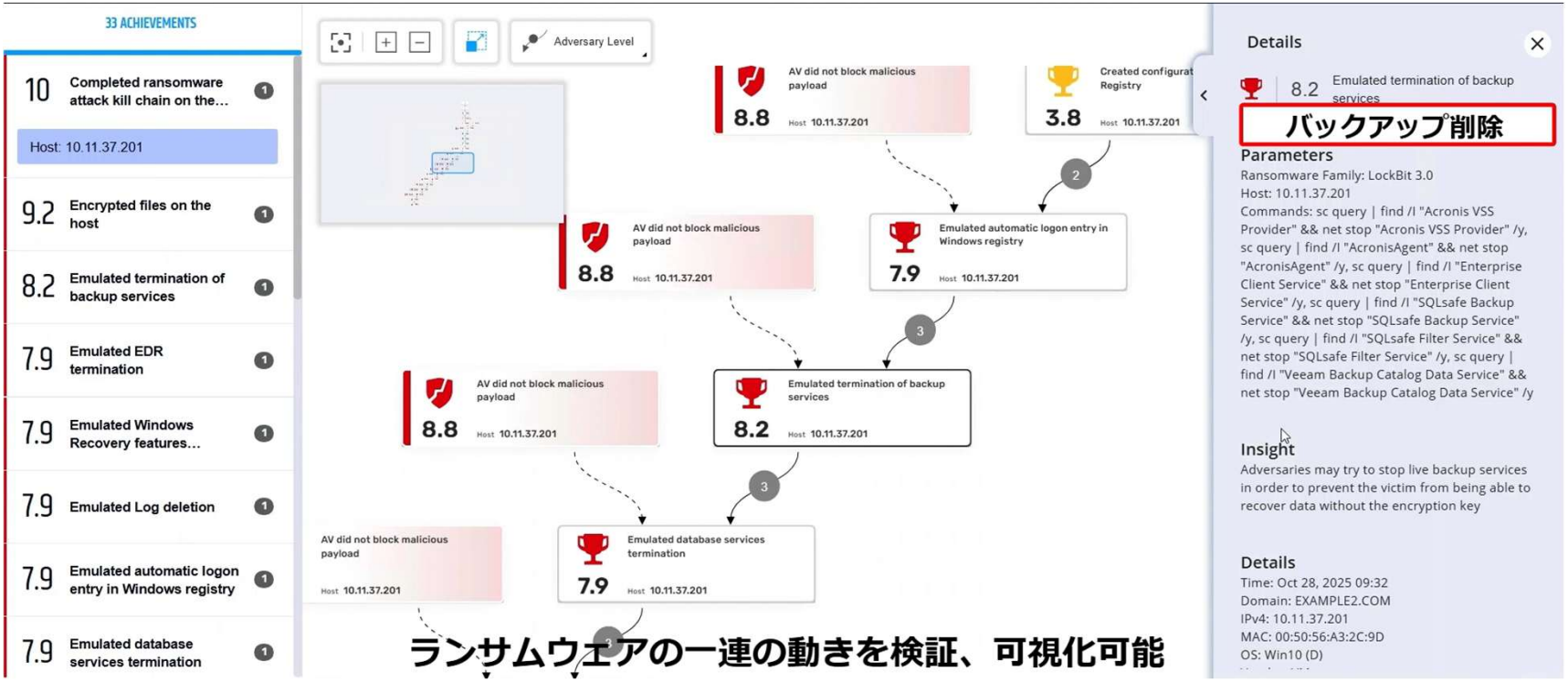
- CVSSのスコアが高いかどうかではなく、攻撃の成立可能性、影響を基に優先順位付け



検査環境の状況を反映した、対処の優先順位を提示

導入している対策が“有効に機能しているか”の確認

- 実際のランサムウェア攻撃に対してEDRやバックアップ等が機能するかを検証、可視化



AIを活用した運用の高度化

- **AI インサイトレポート**
  - 複数回のテスト結果の分析
  - セキュリティ状態の主な傾向を特定・表示
  - 効果的な改善策の提案

推奨事項

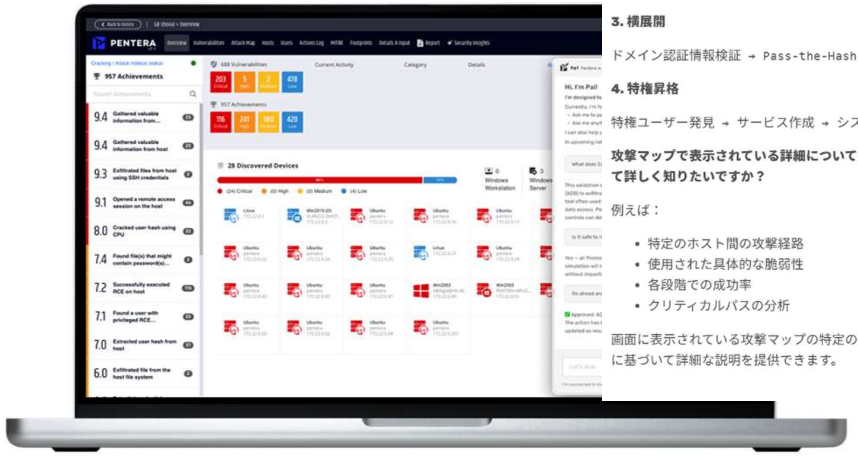
🚨 最も緊急に修復すべき脆弱性

- **ホストは不正なサーバーによって認証を強制される可能性がある（深刻度4.7、発生件数1件）**
  - **リスク：**中間者攻撃による認証情報の盗難および不正アクセス
  - **対策：**グループポリシー設定を使用して、LLMNR、NetBIOS-NS、およびmDNSプロトコルを無効にします。
- **パスワードは、GPU負荷の低い方法で解読可能です（深刻度6.9、発生回数1回）。**
  - **リスク：**脆弱なパスワードによる不正アクセス
  - **対策：**強力なパスワードポリシー（8文字以上、複雑性要件）を導入し、多要素認証（MFA）を有効にする。
- **ZeroLogon (CVE-2020-1472) (深刻度 10.0、発生件数 1)**
  - **リスク：**ドメインの完全な侵害とドメインコントローラーへの権限昇格
  - **対応策：** CVE-2020-1472に対するマイクロソフトのセキュリティパッチを直ちに適用してください。
  - **サンプルホスト:** 192.168.103.2

🔑 重点分野

- **パッチ未適用ソフトウェア：**重要なセキュリティパッチは直ちに適用し、ドメインコントローラーを優先的に適用し、定期的なパッチ管理サイクルを確立してください。
- **脆弱な認証情報：**強力なパスワードポリシーを徹底し、すべてのサービスで多要素認証（MFA）を導入し、パスワードの強

- **Pentera Peer（AI ユーザーインターフェース）**
  - 自然言語で対話できるインターフェースを提供
  - テスト設定・結果探索・是正ガイダンスの取得等をAIが支援



攻撃フロー（データベースの結果より）

初期段階 → 認証情報獲得 → 横展開 → 特権昇格

1. 初期侵入

ネットワークスキャン → 脆弱性発見 → PrintNightmare悪用 → 初期RCE

2. 認証情報ハーベスト

ローカル情報収集 → ドメイン管理者パスワード発見 → Kerberoasting → ハッシュ

3. 横展開

ドメイン認証情報検証 → Pass-the-Hash → SMBリレー → 複数ホストへアクセス

4. 特権昇格

特権ユーザー発見 → サービス作成 → システム権限取得 → ドメイン管理者権限

攻撃マップで表示されている詳細について説明いたします。どの特定の部分について詳しく知りたいですか？

例えば：

- 特定のホスト間の攻撃経路
- 使用された具体的な脆弱性
- 各段階での成功率
- クリティカルパスの分析

画面に表示されている攻撃マップの特定の箇所を指していただければ、そのデータに基づいて詳細な説明を提供できます。

PENTERA.

Mythosを活かすセキュリティ対策

本当に危険な攻撃経路への早期対策

Claude Mythos

Good Points	高速な脆弱性の発見による必要対策箇所の早期特定
Bad Points	高速な脆弱性の発見による攻撃ターゲットの早期特定

必要な取組み

- 対策優先順位付け
- 攻撃経路の特定

PENTERA.

- 網羅的・継続的に実施可能なTLPT
- システムを破壊しない安全な手法
- 自社環境で成功する攻撃経路の可視化
- テスト結果に基づいた優先順位と対策の提示

Penteraデモ

デモで見ていただきたいポイント

- どのように攻撃経路を可視化できるのか
- 対策の優先順位をどのように把握できるのか
- ランサムウェア攻撃を安全に再現し、自社のセキュリティ耐性をどのように評価できるのか

まとめ

まとめ

- ランサムウェア対策はEDRやバックアップを導入していても十分とは限らない。
  →対策を入れているかではなく、**実際の攻撃に対して有効に機能するかを確認する**ことが重要。

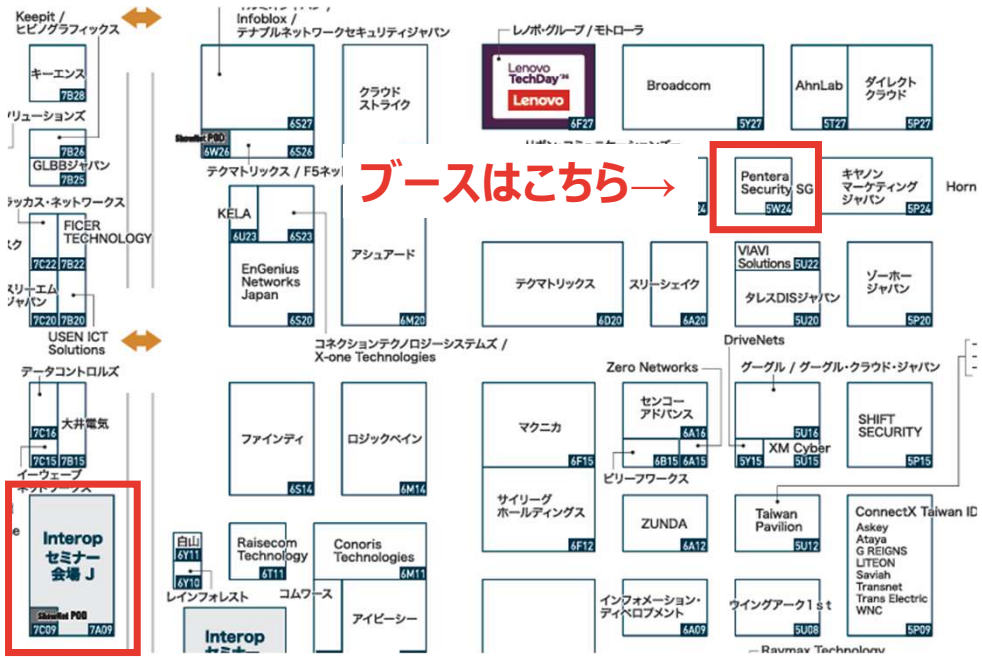
- AIの進化により、脆弱性の発見・悪用はさらに高速化している。
  →だからこそ**自社で本当に悪用され得る脆弱性と攻撃経路を把握する**必要がある。

- Penteraは、攻撃者視点のセキュリティ検証を安全に実施することにより、
  成立する攻撃経路の可視化、対策の優先順位付け、ランサムウェア対策の有効性確認を実現します。

攻撃が高度化、高速化する今だからこそPenteraが必要

ブースにもぜひお越しください

- 小間位置：5W24
- ブースでは以下のようなお話もできます
  - より詳しい機能紹介
  - 実際の画面を用いた詳細なデモ
  - 実際のユーザー様の活用方法



アンケートと無料ハンズオンのご案内

本セミナーアンケート
【回答者特典資料付き】

アンケートにご回答いただいた方には
以下特典資料を提供（PDF）
・本セミナーの投影資料
・カタログ/データシート

回答後すぐに資料がご覧いただけます

無料ハンズオン申し込み
【7月3日開催 複数社限定】

Penteraをラボ環境で実際に触ることができます
・日程：7月3日(金)13:30-16:00
・場所：東京エレクトロンデバイス渋谷本社
（渋谷サクラステージ SHIBUYAタワー35階）

このようなお悩みをお持ちの方におすすめです
・自社にどのような攻撃リスクが存在するのか把握しきれていない
・脆弱性が多く、どこから対応すべきか判断できない
・セキュリティ対策の優先順位付けに時間がかかる