onnect Beyond

TED × PenTera 共同webinar

東京エレクトロン デバイス株式会社

東京エレクトロン デバイス

PENTERA

弊社ご紹介

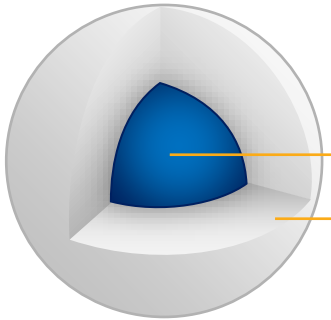
PENTERA

攻撃対象となる環境全体の
セキュリティを確かなものに

ミッション

Assure security readiness across your complete attack surface

- 設立　2015年　ユニコーン企業
- 従業員数　>330人
- 導入実績
  - 56ヵ国
  - >800社



TOTAL ATTACK SURFACE COVERAGE

One platform for all your security validation operations

東京エレクトロン デバイス

TED×PenTera 攻撃者から見た効果的な対策シリーズ

7月	ランサムウェア対策
9月	継続的な脅威エクスポージャーマネージメントとその実装
11月	脆弱性とASM（Attack Surface Management）による対策
12月	2023年のKey learning、2024に向けて

PENTERA

セキュリティ人材なら知っている 今話題の用語CTEM （継続的な脅威エクスポージャーマネージメント） とその実装

2023年9月

柴崎　恵美
Sales Engineer Japan

PENTERA

組織のサイバーセキュリティや
脆弱性管理に
自信がありますか?

PENTERA

継続的な脅威エクスポージャーマネージメント
Continuous Threat Exposure Management (**CTEM**)

エクスポージャーマネージメント

組織がITリスクやサイバー攻撃にさらされている程度を計測し、改善していくプロセス

エクスポージャー（露出）= 組織サイバー攻撃にさらされているリスク
マネージメント = 管理

アタックサーフェス

攻撃者がアクセスできる
対象や範囲

脆弱性

OSやアプリケーションの
脆弱性

漏洩したクレデンシャル

過去に漏洩した
ユーザーID/パスワード情報

PENTERA

Gartner

継続的な脅威エクスポージャーマネージメント
Continuous Threat Exposure Management (**CTEM**)

継続的なエクスポージャーマネージメントをもとに優先順位付けしてセキュリティ投資を行う組織は、 2026 年までに侵害に苦しむ可能性が 3 分の 1 に減少すると予想されます。

By 2026, organizations that **prioritize** their security investments based on a **continuous exposure** management program will be 3x less likely to suffer a breach

Source: Gartner, "How to Manage Cybersecurity Threats, Not Episodes", August 21, 2023

PENTERA

組織の視点と攻撃者視点

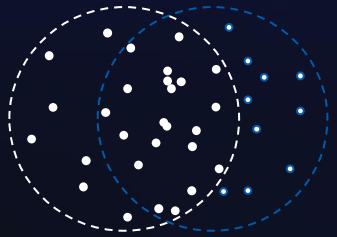
組織側の視点

転換が必要

攻撃者側の視点

見えるものの違い

組織が把握していること



攻撃者から見えること

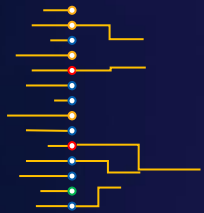
優先順位付けの違い

CVSSにもとづき
対処を優先順位付け

攻撃のできるものを攻撃対象

検証方法の違い

脆弱性を確認



影響や攻撃の成果を確認

PENTERA

Validation（検証）とは

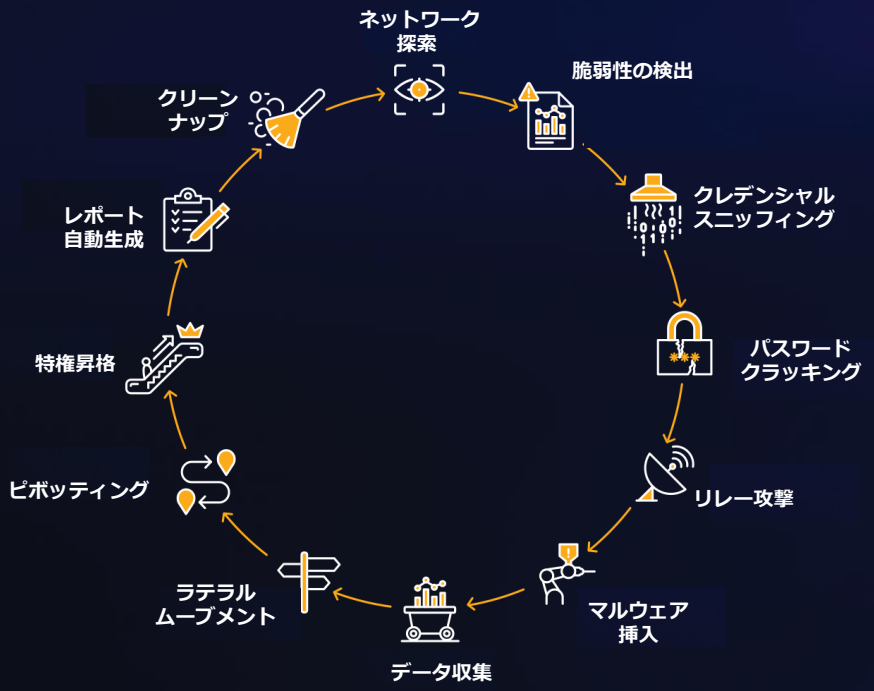
攻撃者の視点から色々な攻撃手法を用いてテストを行い、サイバー攻撃を受ける危険性があるのかを検証すること

		VALIDATION
脆弱性の発見	→	**脆弱性をついた攻撃が可能か**
クレデンシャルの奪取	→	そのクレデンシャルを使ってログイン可能か
疑わしいファイルの有無	→	マルウェアが実行できC2C通信が確立できるか

VALIDATION

PENTERA

Penteraのご紹介



ASV
Automated Security Validation

自動化

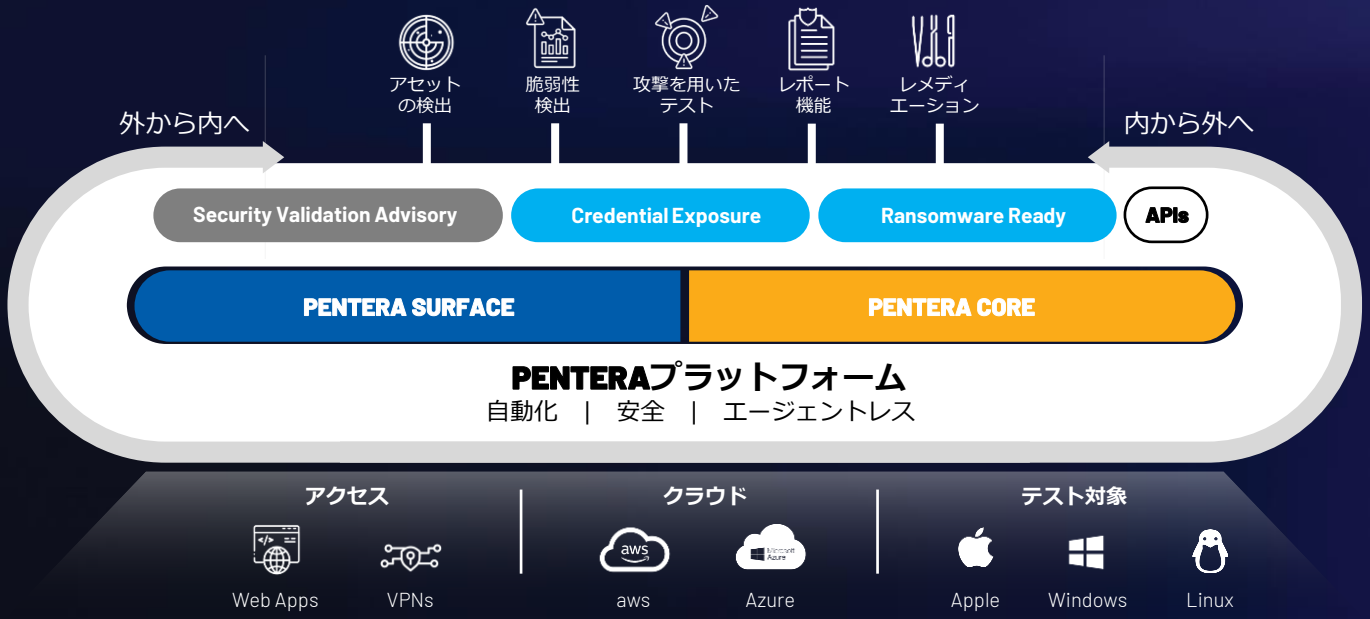
実際の攻撃と同様のテスト

エージェント不要

安全

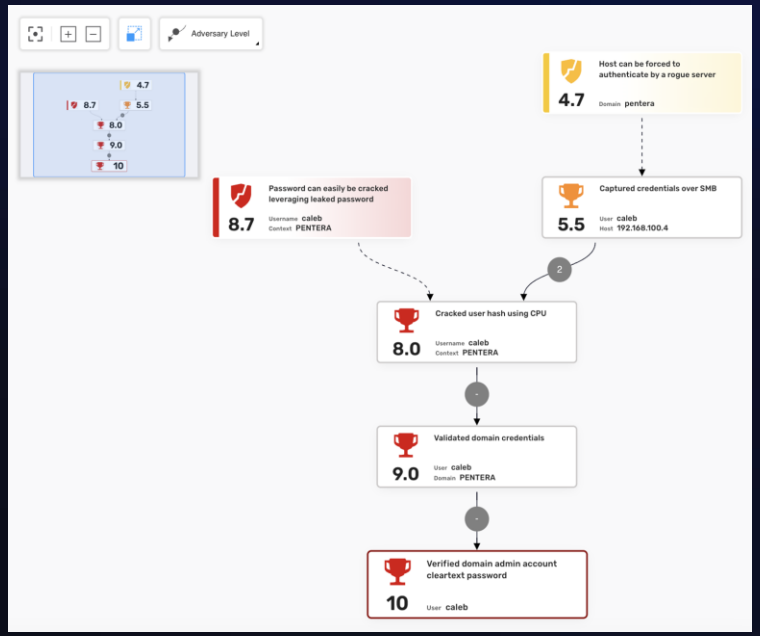
PENTERA

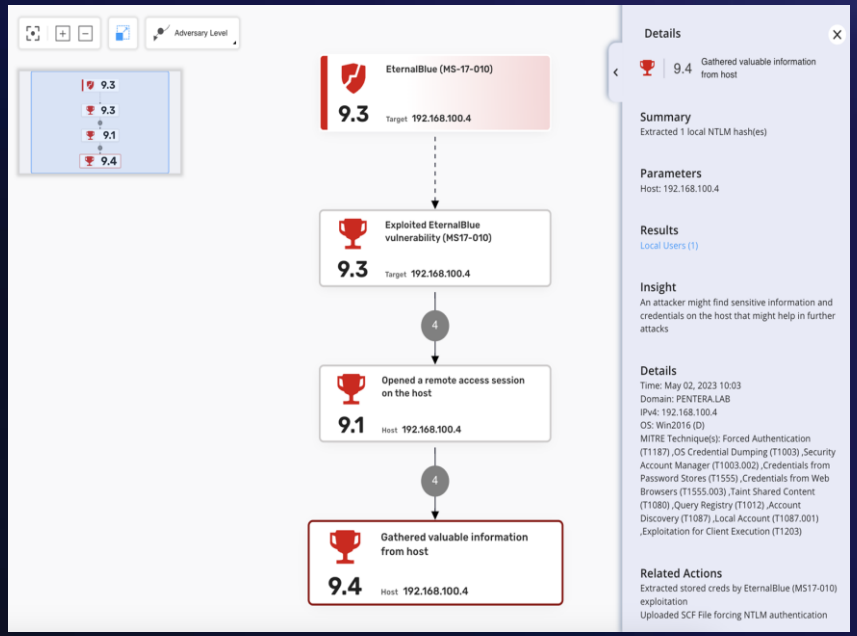
Penteraのプラットフォームの構成



PENTERA

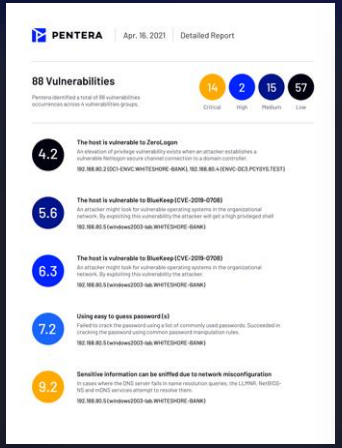
テスト結果例

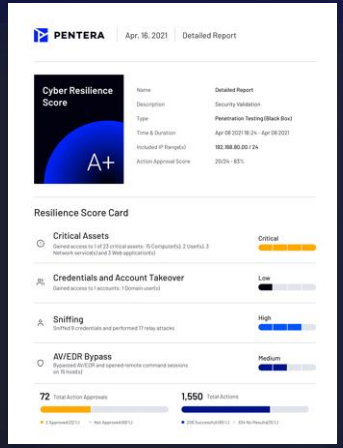


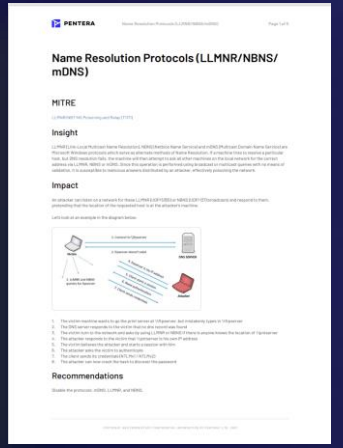


PENTERA

自動レポート生成







PENTERA

Penteraによる継続的なエクスポージャーマネージメント

発見

- アセットの検出
- 脆弱性検出
- 攻撃者視点

Validation

- 自動化
- エージェントレス
- 本物に近い攻撃手法

優先順位付けと対処

- 根本的な脆弱性の発見
- サイバー攻撃への準備
- 対処方法の案内

PENTERA

まとめ

- CTEM（継続的な脅威エクスポージャーマネージメント）は、継続的に優先順位付けすることで、効率的に実施できます。
- 優先順位付けは、攻撃者の視点から行うことが重要です。
- Penteraのご利用により、攻撃者の視点からリスク検証を行い、セキュリティ対策の優先順位付けと継続的なCTEMが可能です。

PENTERA

Thank You