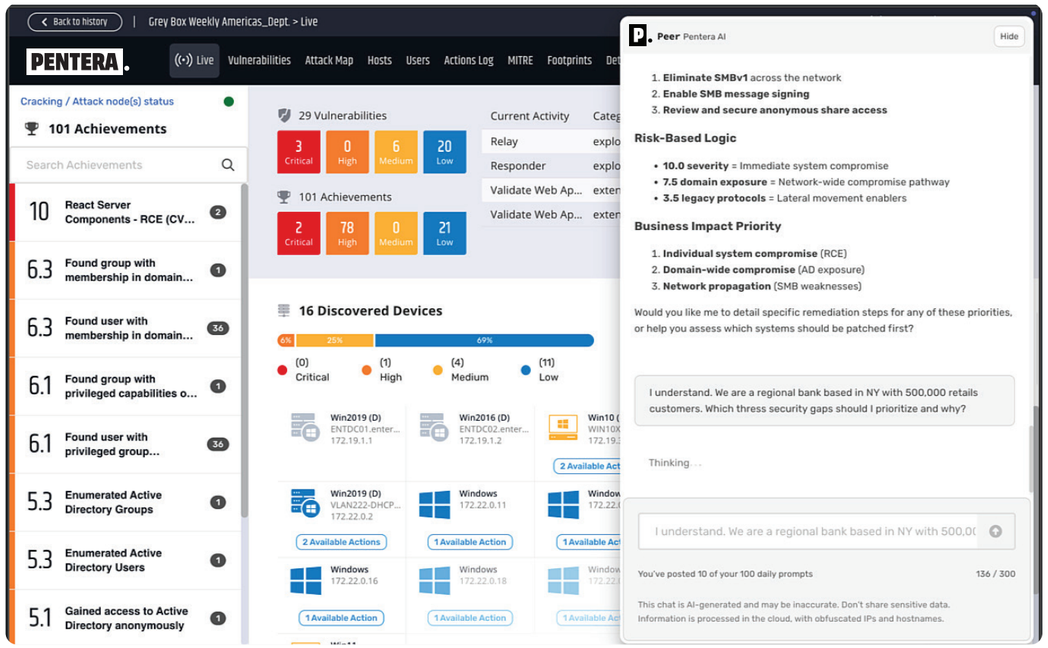
自律型の敵対的テスト



ビジネスに沿った分析
役割、業界、コンプライアンスのニーズに基づいて、検証済みの指摘事項を、明確かつビジネスに関連した優先事項に変換します。

リアルタイムの優先順位付け
アクティブなテストのデータを、修正の優先順位に合わせた即時の行動計画に変換します。

Penteraについて

PenteraはAIを活用したセキュリティ検証市場のリーダーであり、最新のサイバー攻撃に対するあらゆるサイバーセキュリティ管理策を積極的なテストするためのプラットフォームを企業に提供しています。Penteraは、攻撃表面全体の真のリスクを特定し、露出を効果的に削減するための修正ワークフローを自動的に編成します。Penteraのセキュリティ検証は、継続的脅威露出管理（CTEM）運用に不可欠なものです。世界中の何千名ものセキュリティ専門家がPenteraに信頼を寄せ、脅威アクターに悪用される前にセキュリティの隙間を解消しています。

PENTERA. データシート | プラットフォーム

PENTERA PLATFORM

検証済みのサイバーリスクを測定可能な露出削減に変革

AIを活用した本番環境での敵対的テストにより、内部ネットワーク、外部資産、クラウド環境とハイブリッド環境をまたいでサイバー露出を削減します。実証済みのビジネスへの影響度に基づいて優先順位付けされた悪用可能なセキュリティの隙間を修正します。継続的な再テストと、経営陣やコンプライアンス部門に向けた監査対応可能な証明により、露出の削減を実証します。

セキュリティ対策を強化

攻撃者と同じような動的テスト

お客様の環境に適応する敵対的テストを含むオンデマンドのテストにより、悪用可能な構成不備、資格情報、特権昇格のリスクを明らかにします。

判明している影響に基づいて優先順位付け

動的にデータを照会し、資産の重要度、ビジネスへの影響、業界、地域に応じてリスクを文脈化することにより、最大のリスクを特定します。

正確に修正

ネイティブに既存のSecOpsツールに明確な修正ステップを提供するAI駆動型のワークフローにより、修正を動員し、MTTR（平均解決時間）を削減します。

リスク削減を検証

修正の進捗を追跡し、問題の完全な解決を確認するために修正を再テストして、時系列でセキュリティ態勢の改善を実証します。

詳しくは **www.pentera.io** をご覧ください。
© 2026 Pentera. All rights reserved.

Penteraで露出管理を運用可能に

実際の敵対者に対する積極的なテストを行い、本当に悪用可能なものを特定し、発見から修正までの修正作業を編成します。

発見
AIを活用した偵察と100以上のネイティブ統合機能により、内部、外部、クラウドの資産を継続的に発見してマッピングします。

評価
組織の露出を高めてしまう、悪用可能な脆弱性、構成不備、衛生管理の隙間を特定します。

テスト
資格情報の侵害、特権昇格、横展開、データアクセスなど、本番環境において多段階の攻撃経路をエミュレートします。

検証
実際の敵対者のTTP（戦術、技術、手順）とIoC（侵入の痕跡）に対する本番環境のエンドポイント、ID、クラウド、データのセキュリティ管理策の強靭性を確認します。

優先順位付け
ビジネスへの影響、実証済みの悪用可能性、アクティブな脅威インテリジェンス、コンプライアンス要件に基づいて、修正の優先順位を調整します。

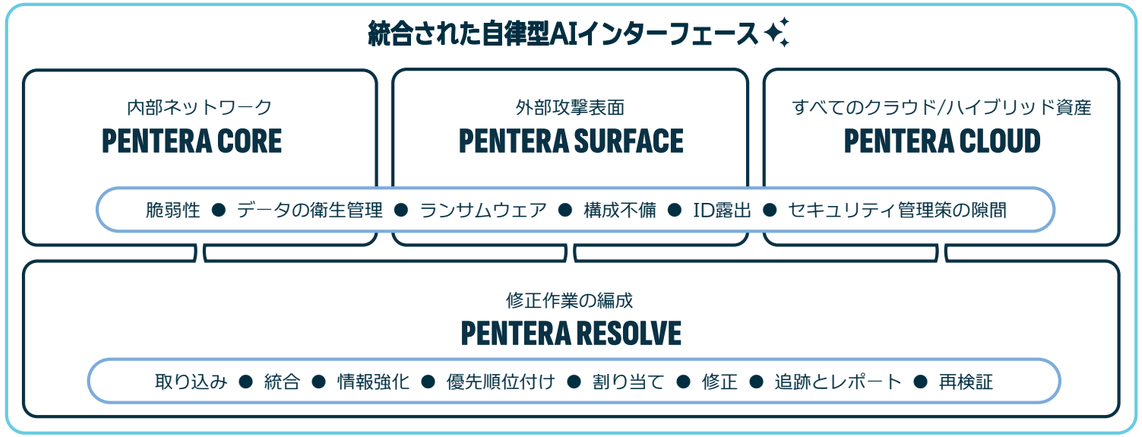
動員
AI駆動型の編成により、既存の運用ワークフロー内で修正タスクを自動トリガーし、適切な担当者に割り当てます。

レポート
経営陣やコンプライアンス関係者向けの監査対応可能なレポートにより、測定可能なリスク削減を追跡し、実証します。

再テスト
修正を自動的に検証することにより、修正作業が効果的に露出を削減していることを確認します。

PENTERA. データシート | プラットフォーム

統合された露出検証プラットフォーム



エンタープライズ規模で敵対的テストを

- **真の敵対的エミュレーション** - 決定論的なロジックと自律的な適応性を用いて、完全な攻撃チェーン全体で実際の攻撃者の振る舞いに対する防御を検証します。
- **攻撃表面を完全にカバー** - 悪用可能な隙間を特定し、企業の攻撃表面全体にわたってセキュリティ管理策の出来映えを評価します。
- **エンタープライズ規模のテスト** - 人員を増やすことなく、脅威インテリジェンス、コンプライアンス、ビジネス上の要因に合わせてテストを拡張し、適応させられます。

リスク削減を運用可能に

- **文脈駆動型の優先順位付け** - 検証済みの攻撃経路により情報強化され、セキュリティファブリック全体から統合されたデータを使用して、修正作業を優先順位付けします。
- **自動的に修正作業を編成** - 既存のITSM（ITサービス管理）システムと統合されたAIを活用した修正ワークフローにより、修正までの時間を短縮します。
- **露出と成績のレポート** - 明確なトレンドベースのレポートにより、MTTR（解決までの所要時間）を短縮し、組織の露出を時間とともに削減します。

Penteraを選択する理由

敵対的テストから解決まで**AIを活用したセキュリティ検証**

ハイブリッド環境と分散IT環境をまたいだ**エンタープライズグレードのテスト**とガバナンス

SecOpsチームが既に使用しているワークフローにネイティブ統合できる**修正機能**

稼動時間や安定性などの業務影響を生じさせずに実環境で**安全に攻撃エミュレーション**

メンテナンス負荷や運用上の摩擦が生じない**エージェントレス配備**

詳しくは **www.pentera.io** をご覧ください。

© 2026 Pentera. All rights reserved.