



ランサムウェアに備えるには

東京エレクトロンデバイス株式会社

- 最近のランサムウェアの状況
- ランサムウェアへの対策
- セキュリティ対策の有効性可視化
- Pentera RansomwareReady™

名古屋港統一ターミナルシステム（NUTS）における被害

2023年7月4日、名古屋港統一ターミナルシステム（NUTS）においてシステム障害が発生し、約2日間に渡ってターミナルの機能がストップし、物流に大きな影響が出ました。

この原因はランサムウェアによる攻撃である事が判明しており、一般のニュースでも日本初のランサムウェアによる重要インフラの大規模被害として大きく取り上げられました。

感染経路としてはシステムに接続している事業者側からである事が示唆されています。

IPAの「情報セキュリティ10大脅威」の1位、2位に該当？

順位	組織における脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃

NHK名古屋のおすすめ

NHK名古屋 > 名古屋のおすすめ > 名古屋港にサイバー攻撃？ランサムウェアの被害とは？

名古屋港にサイバー攻撃？ランサムウェアの被害とは？

2023年07月05日

#おすすり #WEB特集 #まるっと1



名古屋港のコンテナターミナルで4日からシステム障害が発生し、コンテナの積み降ろしができなくなりました。システムを管理する協会は、身代金要求型のコンピューターウイルス「ランサムウェア」の感染が確認されたと発表。何者かによるサイバー攻撃を受けたとみている。サイバー攻撃によって国内の港湾施設の運営がストップするのは今回が初めてとみられる。貨物の取扱量が全国一の名古屋港で何が起きたのか。



名古屋港のシステム障害 名古屋港運協会は身代金支払わず ロシアのハッカー集団がランサムウェア使用か

経済 地域 暮らし・生活 企業 2023年7月6日 18:55



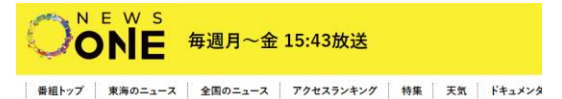
記者「5日はトラックの動きが見えなかったのですが、6日は多くのトラックが列を作っています」

名古屋港の貨物を一元管理するシステムがサイバー攻撃を受けた問題で、システムの復旧は当初予定していた7月5日夜から6日朝7時半に大機にずれ込みました。

システムを管理する名古屋港運協会によりますと、データの安全性の確保に務めたことがあったということです。

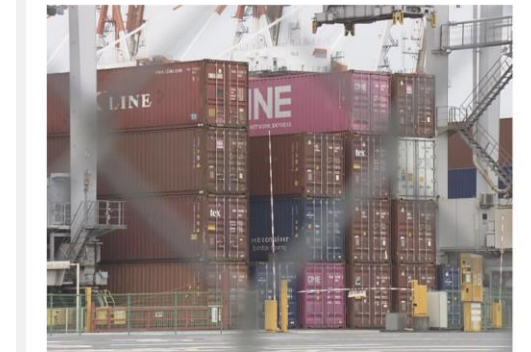
テレビ愛知 愛知のニュースより
<https://news.tv-aichi.co.jp/single.php?id=2303>

NHK名古屋放送局より
<https://www.nhk.or.jp/nagoya/lreport/article/001/44/>



貨物取扱量は日本一…名古屋港の情報管理システムが「ランサムウェア」に感染 障害による物流への影響続く

2023/07/05 17:47配信



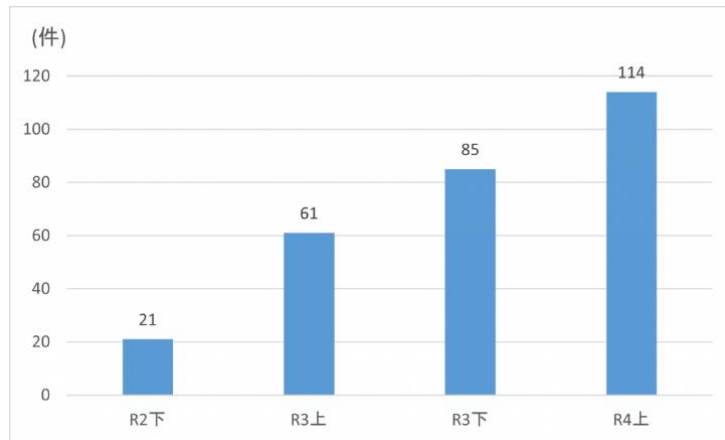
名古屋港でシステム障害が発生し、物流への大きな影響が懸念されています。

貨物の取扱量が日本一の名古屋港。5日、そのコンテナターミナル周辺には、トレーラーが行列をなしていました。

貨物の取扱量「日本一」の名古屋港で、4日午前6時半ごろから続くシステム障害。

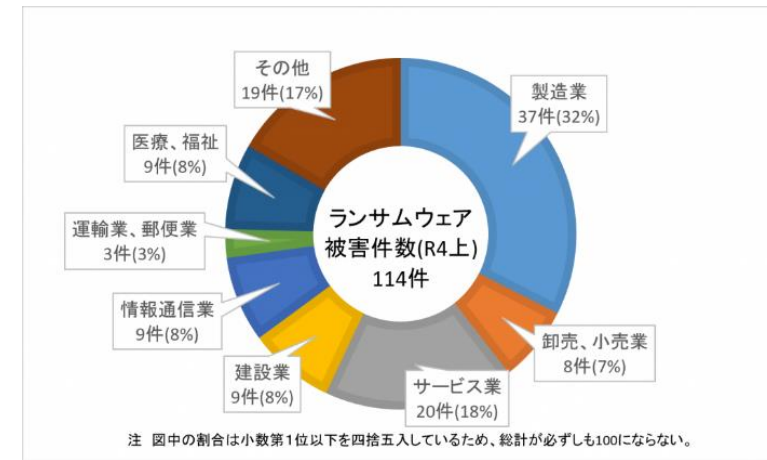
東海テレビ NEWS ONEより
https://www.tokai-tv.com/tokainews/feature/article_20230705_28607

ランサムウェア被害は毎年右肩上がり



企業・団体等におけるランサムウェア被害の報告件数の推移(2022年9月)
出展：警視庁「令和4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」

被害に遭う企業、団体も様々



ランサムウェア被害の被害企業・団体等の業種別報告件数(2022年9月)
出展：警視庁「令和4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」

業種、規模を問わず被害を受ける可能性があり、そのリスクは年々上昇してきています。

例えば、トレンドマイクロは以下のような対策を提案しています。

- 総合的、多面的な対策を導入するとともに、侵入を前提とした対策を行う
- エンドポイントやサーバには総合的なセキュリティソフトを導入する
- メールサーバにおいて攻撃メールを検出するソリューションを導入する
- 外部への不正なネットワーク通信・接続を検出するソリューションを導入する
- ネットワーク内部の監視と不審な挙動を可視化するためのソリューションを導入する
- セキュリティポリシーを策定し、管理者権限の管理やシステムの脆弱性管理を適切に行う
- 「3-2-1ルール」に則り、データの冗長性を十分に担保できるようなバックアップポリシーを策定する
- インシデント対応体制を構築する
- 従業員に対するセキュリティ教育、注意喚起を実施する

トレンドマイクロ 脅威解説「ランサムウェア」より

https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/ransomware.html

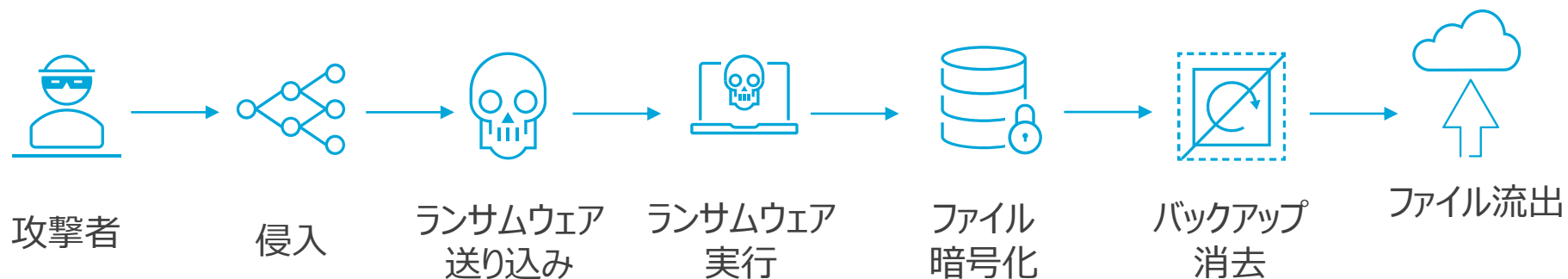
一つ重要なポイントが欠けていませんか？

セキュリティソフトの導入、不正な通信、挙動を検知するソリューションの導入、脆弱性管理の徹底・・・

その対策は本当に有効なのでしょうか？

セキュリティ対策の有効性を検証する事は必要不可欠です。

ランサムウェアの攻撃手法

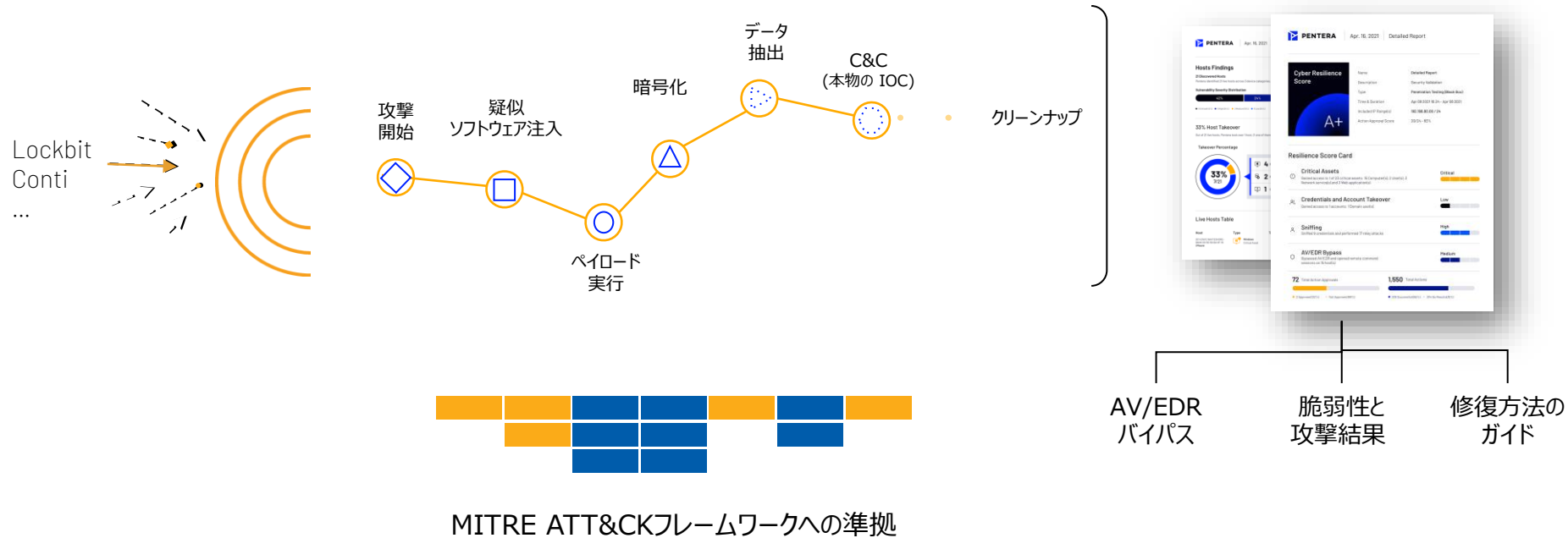


ランサムウェアの攻撃は単なるファイル暗号化だけではなく、一連の攻撃プロセスです。

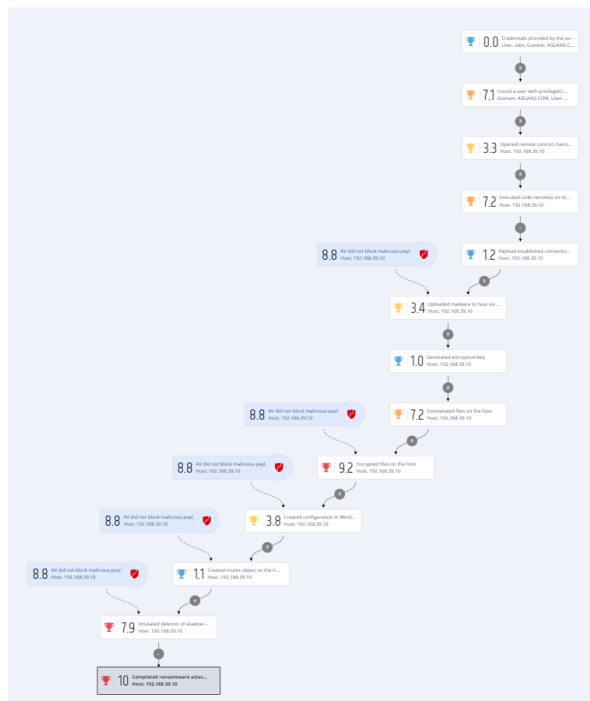
ランサムウェアの攻撃を再現しないと、有効性の検証は出来ません。

RansomwareReady™による対策

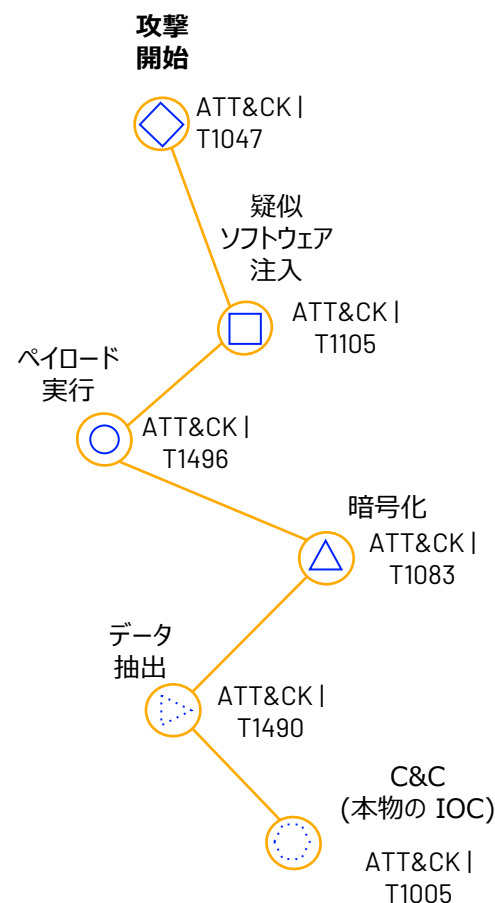
Pentera RansomwareReady™は実在のRansomwareの挙動を忠実に再現し、自動的に検査を実施し、問題点を可視化します。



自律的検証

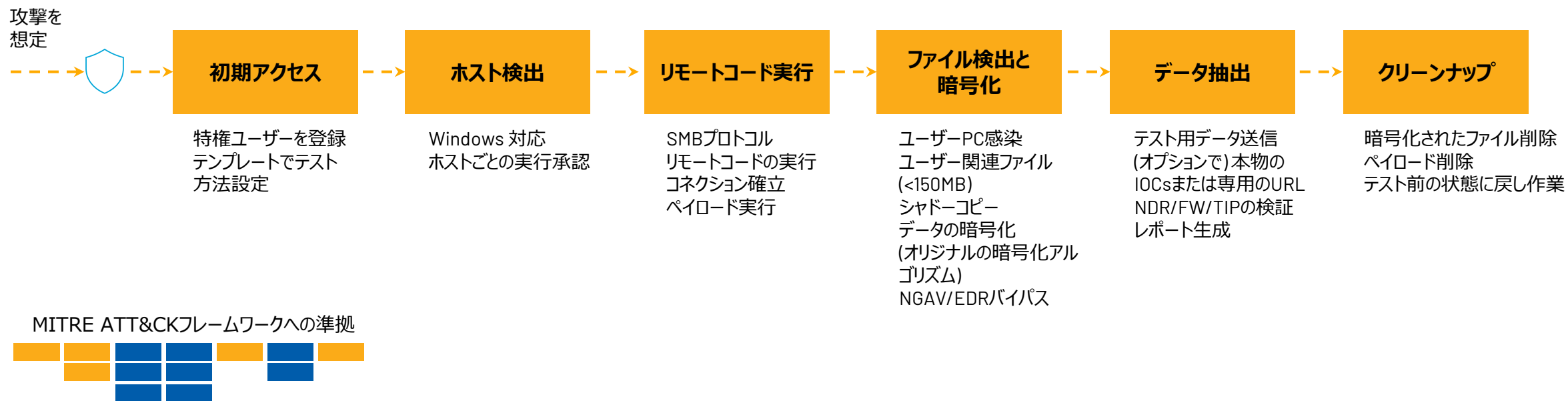


実在のランサムウェアに対応: Maze, Revil, Conti, LockBit 2.0

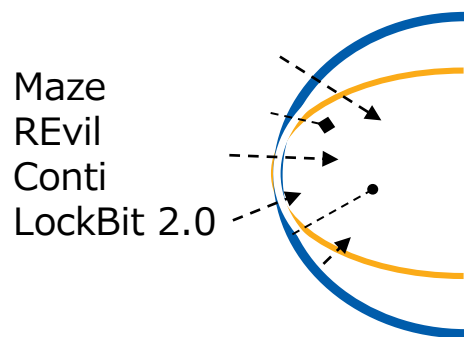


- エンドツーエンドのランサムウェア攻撃作
- MITRE ATT&CKフレームワークとの連携
- 実際の暗号化アルゴリズム
- シャドーコピーを用いたテスト
- 安全な実行
- データ流出シミュレーション

ランサムウェアLockBitを用いたテストの例



ワンクリックでテスト開始



Penetration Testing (Black Box)
Full stack automated penetration testing which includes all product capabilities. No initial credentials required to run this test.

Targeted Testing
Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options.

What-if (Gray Box)
Run granular penetration testing scenarios with specific starting point and end-goal definition.

Vulnerability Assessment
Assesses and identifies the vulnerabilities in the network based on CVSS scoring.

- Info
- Ranges
- Attack Interface Selection
- Target Domain
- Settings
- Scheduling and Duration
- Notifications

Max Criticality

Ransomware Emulation NEW

Execute end-to-end attack flows of the most notorious ransomware campaigns on a sample of hosts to validate AV & EDR tools deployed in your network.

10

エージェントレス

本物に近い攻撃

安全な検査

RansomwareReady™による評価レポート



優先付け

リスクから
攻撃結果を
スコアリング



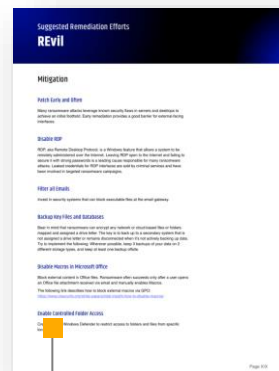
MITRE ATT&CK 充実した内容

テスト結果を
戦術やテクニックに
マッピング



修復方法

リスクやインパクトを
解説



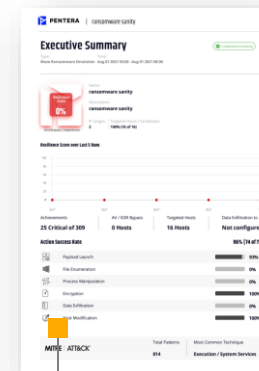
感染情報

今後の対策方法を
アドバイス



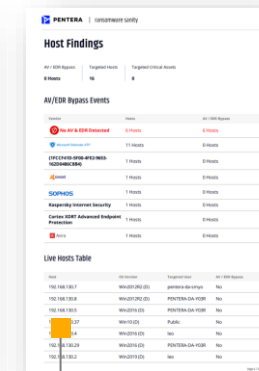
スコアを採点

ランサムウェア攻撃
に成功したホスト
情報



エンドポイント

検出されたエンド
ポイントとAV/EDR
バイパス情報



1. ランサムウェア攻撃を受けた際に想定される被害範囲、被害内容
2. ランサムウェアの被害を受けた際の復旧可能性（バックアップ、スナップショットの有効性）
3. AV製品、ファイヤウォール、IDS/IPS、ネットワーク監視といったセキュリティ製品の有効性
4. ランサムウェア攻撃に利用された脆弱性や設定ミス等の問題点、及び対処方法
5. MITRE ATT&CKの基準に基づいたセキュリティ評価

今の備えで十分でしょうか？皆さんの組織でも確認してみてください。

RansomwareReady™も含めたPentera Core製品の特長

- アセットディスカバリー**
 - ワークステーション/サーバー/ネットワーク機器
 - Windows / Linux
 - Azure クラウド
- アセットの内容検出**
- 攻撃の実施**
 - 実攻撃と同様の攻撃
 - 運用やシステムへの影響なし
 - 安全なエクスプロイト
 - 攻撃前に事前承認
- レポート**
 - スコアカード
 - エグゼクティブサマリーレポート
 - MITRE ATT&CKマッピング
 - 脆弱性や修復の優先順位付け
- 影響の解析と修復対応**
 - 修復対応のガイダンス
- ビジネスへの配慮**
 - 可検知なし
 - スケーラブル
 - 悪影響なし / 安全性
 - 自動スケジューリング機能
 - 複数のセグメント / ドメイン / サイト
- テストの種類**
 - ブラックボックステスト
 - グレーボックステスト
 - 優先順位付けされたアチーブメント
- セキュリティ評価**
 - 防御 / 検知の検証 (EPP, EDR, SASE, NDR...)
 - インフラのポリシー設定 (FW, Zero Trust)
 - セキュリティ設定
 - ブルーチーム / インシデント対応の予行練習
 - データ衛生
- パスワードマネージメント**
 - パスワード強度診断
 - パスワードポリシー
 - パスワードクラッキング
- 脆弱性マネージメント**
 - 静的脆弱性スキャン
 - 脆弱性の優先順位付け
- RansomwareReady™**
 - 検証のコントロール
 - データ暗号化
 - データ抽出
 - ランサムウェアのリスクと影響
 - 根本的な脆弱性