Core レポート

2026 年 9 月 1 日　東京エレクトロンデバイス（株）

目次

1 エグゼクティブサマリー 5

1.1 評価概要 5

1.2 対象範囲 5

検出された資産 5

2 評価方法 6

2.1 テストシナリオ詳細 6

2.1.1 ブラックボックス 6

2.1.2 グレーボックス 7

2.2 グレーボックス追加項目 8

2.3 Pentera 評価アプローチ 9

2.4 ファイル痕跡 10

3 テスト結果サマリー 12

3.1 検出結果サマリー：ブラックボックステストシナリオ 12

3.2 検出結果サマリー：グレーボックステストシナリオ 13

4 ブラックボックステスト結果 14

4.1 技術的所見 14

4.1.1 **ブラックボックス TF-001：SMB メッセージ署名が無効** 14

4.1.2 **ブラックボックス TF-002：ホストが不正サーバーへの認証を強制される可能性** 14

4.1.3 **ブラックボックス TF-003：パスワードが容易に解析可能** 15

4.1.4 ブラックボックス TF-003：PrintNightmare（CVE-2021-34527） 15

5 グレーボックステスト結果 16

5.1 技術的所見 16

5.1.1 **グレーボックス TF-001：AV/EDR が暗号資産マイニングのペイロードをブロックしなかった** 16

5.1.2 **グレーボックス TF-002：ドメインユーザーが複数ホストでリモートコード実行権限を保持**... 16
5.1.3 **グレーボックス TF-003：空のパスワードを使用** 16
5.1.4 **グレーボックス TF-004：ホストからファイルを持ち出し可能** 17
5.1.5 **グレーボックス TF-005：スクリプトファイルに平文認証情報が保存されている可能性** 17
5.1.6 **グレーボックス TF-006：データベーススクリプトファイルに平文認証情報が保存されている可能性** 17
5.1.7 **グレーボックス TF-007：ユーザーアカウントに「パスワードを無期限にする」属性が設定** .. 17
5.1.8 **グレーボックス TF-008：ホスト上で閉じたポートを検出** 18
5.1.9 **グレーボックス TF-009：許可されるパスワード有効期間が長すぎる** 18
5.1.10 **グレーボックス TF-0010：Security Account Manager Remote Protocol（SAMRPC）が有効** 18
5.1.11 **グレーボックス TF-0011：EPP/EDR が悪意あるペイロードのディスク書込みを許可** 19
5.1.12 **グレーボックス TF-0012：SMB メッセージ署名が無効** 19
5.1.13 **グレーボックス TF-0013：AV が悪意あるペイロードをブロックしなかった** 19
6 クロス分析（グレーボックス実施時） 20
6.1 ブラックボックス／グレーボックス クロス分析 20
7 主要課題／是正優先度とお客様の次の対応 21
7.1 ブラックボックステストシナリオ 21
7.1.1 主要課題 21
7.1.2 是正対応 21
7.2 グレーボックステストシナリオ 30
7.2.1 主要課題 30
7.2.2 是正対応 30
8 レッドチーム分析と攻撃者視点 36
9 付録 38

検出されたデバイス 38
ホスト 38
ホスト侵害 38
ユーザー 38
レジリエンス・スコアカード 39
AV バイパス 39

1　エグゼクティブサマリー

1.1 評価概要

当社のペネトレーションテストチームは、定義された評価範囲のセキュリティ態勢を評価するため、Pentera Automated Security Validation プラットフォームを使用して内部自動ペネトレーションテストを実施しました。テストは［ブラックボックス／グレーボックス］の観点から行い、環境侵害に悪用される可能性がある脆弱性、セキュリティ制御の弱点、攻撃経路を特定・検証しました。

評価対象は［対象ネットワーク／ドメイン／資産］で、［評価日］に実施しました。Pentera は［検出件数］件の脆弱性を［深刻度レベル数］段階で検出し、［重要な結果の概要（例：ホスト侵害、認証情報漏えい、リモートコード実行、セキュリティ制御回避）］を実証しました。

評価結果に基づき、主に対応が必要な領域は［主要セキュリティ領域 1］、［主要セキュリティ領域 2］、［主要セキュリティ領域 3］です。Pentera の推奨する是正優先度に従い、特に攻撃経路の成立や侵害につながった弱点を優先して対応してください。

是正は Pentera の推奨優先順位に従い、［最優先課題／制御領域］から開始してください。初期対応では［対応 1］、［対応 2］、［対応 3］を優先し、その後［セキュリティ領域］全体を強化します。推奨対応の実施後は、影響を受けたシステムと実証済みの攻撃経路を再テストし、特定された弱点が有効に解消されたことを確認してください。

1.2 対象範囲

本評価後に特定された資産は、外部 IP アドレス 1 件、内部ネットワーク範囲 2 件、domain.sample.com の ActiveDirectory ドメイン、および内部ネットワークへのアクセスを取得した場合に検出される Sample Customer 所有のその他の Active Directory ドメインです。

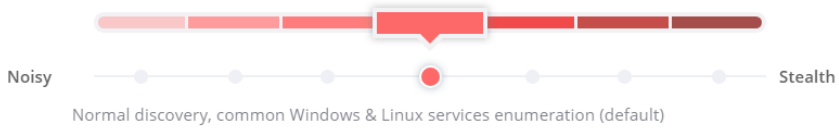
検出された資産

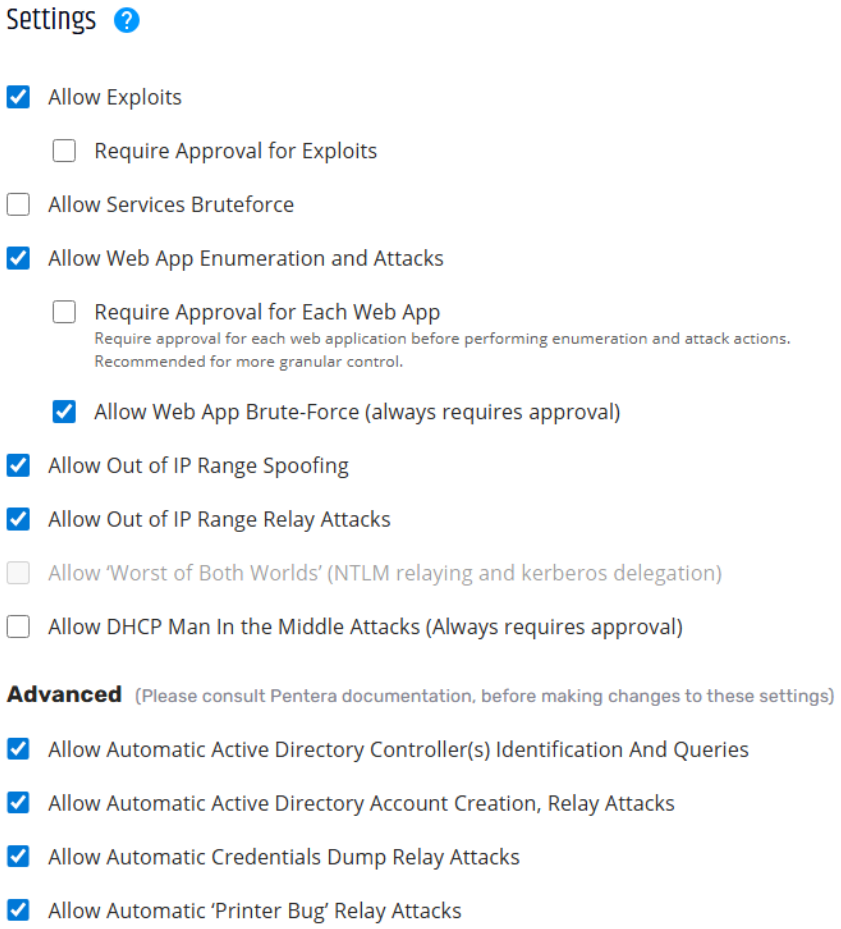
ホスト／URL／IP アドレス	説明
10.129.X.X	お客様内部ネットワーク
10.129.X.X	ドメインコントローラー
10.129.X.X	お客様内部ネットワーク
10.129.X.X	Web サーバー
10.129.X.X	お客様内部ネットワーク

2　評価方法

2.1 テストシナリオ詳細

2.1.1　　ブラックボックス

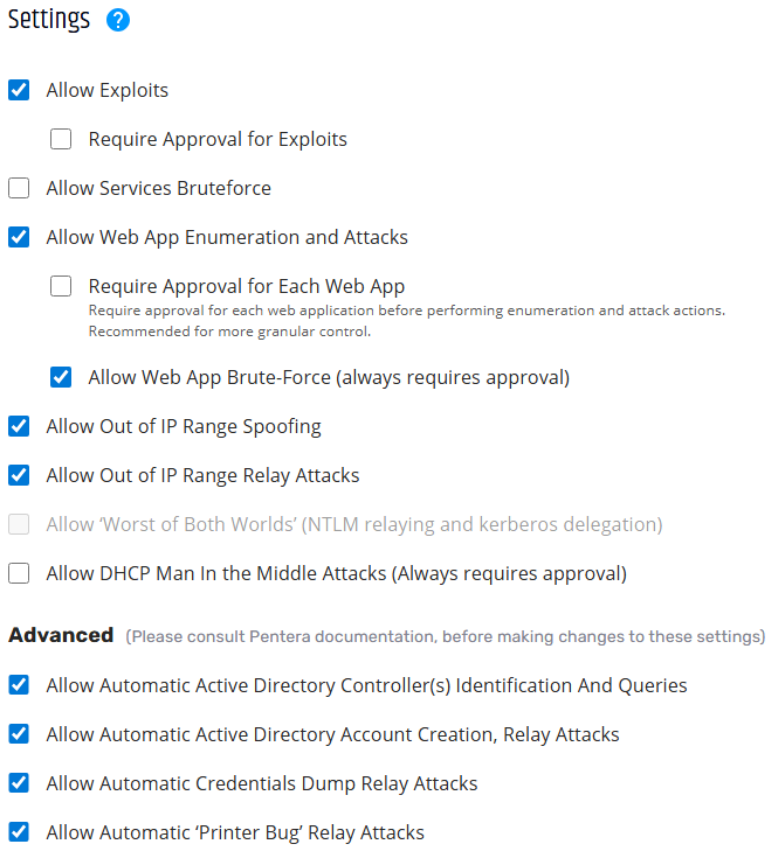
項目	内容
テスト名	miyashita_Insight_test
テスト種別	ペネトレーションテスト（ブラックボックス）
Pentera バージョン	v8.1.3
テスト日時	2026/7/23 17:08 - 2026/7/24 09:17（レポート記載時刻）
対象	10.11.37.100-102、10.11.37.200、10.11.37.202
除外対象	10.11.37.201
完了ステータス	承認なしで完了
承認	0/10 承認、10/10 未承認
ステルスレベル	 Normal discovery, common Windows & Linux services enumeration (default)

項目	内容
設定	

2.1.2 グレーボックス

検出数が限られていたため、有効なドメインユーザー認証情報を用いてグレーボックスシナリオを実施しました。

項目	内容
テスト名	グレーボックステスト 5 - Rayven
テスト種別	What-if（グレーボックス）
Pentera バージョン	v8.1.3
テスト日時	2026/7/23 17:08 - 2026/7/24 09:17（レポート記載時刻）
対象	10.20.1.94, 10.20.1.125, 10.20.1.23,
除外対象	N/A
完了ステータス	正常に完了

項目	内容
承認	68 / 68 , 100%
ステルスレベル	
設定	

2.2 グレーボックス追加項目

Pentera グレーボックステストシナリオ用に提供された追加項目です。

項目	内容
ドメイン認証情報	ユーザー： flatwhite、パスワード： ********、ドメイン： CAFFEINEOPS.LOCAL ユーザー： doubleshot、パスワード： ********、ドメイン： CAFFEINEOPS.LOCAL

項目	内容
	ユーザー： sqlservice、パスワード： ********、ドメイン： CAFFEINEOPS.LOCAL ユーザー： blackcoffee、パスワード： ********、ドメイン： CAFFEINEOPS.LOCAL
重要ファイル	ファイル名： Important-Liberica-Passwords.txt ファイル名： Important-Robusta-Passwords.txt
ファイル内キーワード	キーワード： Credentials

［Pentera／結果／詳細と入力］

2.3 Pentera 評価アプローチ

Pentera は、到達可能な資産、サービス、ドメイン情報、潜在的な攻撃機会を検出し、対象範囲の環境を動的に評価しました。特定された脆弱性とアクセス経路は、適用可能な悪用手法で検証し、アクセス成功により追加テストが可能な場合は、認証情報アクセス、リモート実行、ラテラルムーブメント、侵害後活動を続けて実施しました。また、代表的な悪意ある活動とペイロード実行を試行し、既存セキュリティ制御の有効性も評価しました。したがって本結果は、定義された評価範囲内で Pentera が特定・検証できたセキュリティ上の弱点と攻撃経路を示します。

フェーズ	評価目的	アクションログで確認された活動
1. 環境ディスカバリ	到達可能なシステム、サービス、ドメイン、潜在的な攻撃面を特定	稼働ホスト探索、ポートスキャン、DNS/DC 探索、mDNS 列挙、メールサーバー列挙、未認証のシステム情報収集
2. ID／アクセス探索	ドメイン情報、ユーザー、認証情報、利用可能な認証経路を特定	AD 列挙、LDAP/SMB ユーザー検証、認証情報検証、Responder 活動
3. 脆弱性／露出検証	検出したシステムとサービスに悪用可能な弱点があるか確認	CVE スキャン、Web 脆弱性テスト、サービス固有の脆弱性確認、安全でない設定の検証

フェーズ	評価目的	アクションログで確認された活動
4. 悪用・実行	特定した弱点で実際にコード実行またはアクセス取得できるか検証	PsExec、WMI、WinRM、PowerShell／MSBuild 実行、Web 悪用、その他の実行手法
5. 認証情報アクセス	アクセス取得後に追加の認証情報を取得できるか確認	SAM ダンプ、メモリ内認証情報抽出、ファイル内パスワード検索、安全でない保存領域からの認証情報取得
6. ラテラルムーブメント／攻撃拡大	取得したアクセスや認証情報で追加システムを侵害できるか確認	リモートサービス実行、SMB ベース実行、認証情報再利用、追加ホストへの接続
7. セキュリティ制御検証	エンドポイント保護が代表的な悪意ある活動を阻止するか確認	悪意あるペイロードのアップロード、悪性静的シグネチャバイナリ、暗号資産マイニングペイロード実行、ランサムウェア模擬
8. 影響の検証	侵害成功後に攻撃者が実行可能な影響を確認	ファイル／データ持ち出し、リモートマルウェア接続、リソース乗っ取り、その他の侵害後活動

2.4 ファイル痕跡

本セクションでは、評価中に Pentera が使用したファイルとオブジェクトの詳細を示します。各オブジェクトに関連するイベント時刻、ホスト、ホスト名、ユーザー、ファイルパス、ファイル名、SHA-256 ハッシュを含みます。

ホスト	ファイル名	SHA256	注入方法	操作
10.20.1.1	mimikatz_trunk.zi	9e998c589777a04f21e3af959c8cea8eae45b924bdebe836df070	Smb	注入
10.20.1.243	curl.exe	04aa05d63e3639f90995afc0e635dad45e57afc858a88ac10ede7	Smb	注入
10.20.1.1	curl.exe	04aa05d63e3639f90995afc0e635dad45e57afc858a88ac10ede7	Smb	注入

10.20.1.243	mimikatz_trunk.zi	9e998c589777a04f21e3af959c8cea8eae45b924bdebe836df070	Smb	注入
10.20.1.243	curl.exe	04aa05d63e3639f90995afc0e635dad45e57afc858a88ac10ede7	Smb	注入
10.20.1.243	mimikatz_trunk.zi	9e998c589777a04f21e3af959c8cea8eae45b924bdebe836df070	Smb	注入
10.20.1.243	GNFKTGRewj.cspr	b6e60abbe15167b5f3f2fe2cbe9c750dbe237a6f9a888b55c67ea	Smb	注入
10.20.1.243	SZOIHSwsHK.cspr	9fa69fdf9ddd1a9222f87f222d9d66ee10ee48570c74260c2b972c	Smb	注入
10.20.1.1	kwlJAcKAoC.cspro	fc7be11c9a93652fa450d1f491322285f23f11d2a659a9be5bd413	Smb	注入
10.20.1.243	DPXUNLpmlX.cspr	70a0c5b54d59f695f8366386be7ceb731478d486daaeeb27a079	Smb	注入
10.20.1.1	FzfNOLnGce.cspr	84011abd251f67094ebcf2d2fc9d465df99e18a62e75328e67a8cf	Smb	注入
10.20.1.243	utlzcBJvzt.csproj	3b7f3000b7ad07b100ec747322e88011c358799004e69e1132ca	Smb	注入
10.20.1.243	mKmBVSKQCh.cs	81f6d9e394c5336c0e3d7094f5e280c46309bda0d288b1769121	Smb	注入
10.20.1.1	iztEJmnubM.cspro	354f2f0fc91a46df9773fdcad07104c5070d5481f9e10365b6bca0	Smb	注入
10.20.1.243	TIkVzNsDVq.exe	d22b65453c1f7162a28fd3932dd389a1cf375bdc659dad8a72ffc4	Smb	注入
10.20.1.243	zKMbYKIput.csproj	c8b3b100351efd64474f937930355c3dabe56e8652cad29890f31	Smb	注入
10.20.1.243	hviGSDaPiN.cspro	d50ba0749380f4dad1ea4752b24a406f723fa0569140ce8095318	Smb	注入
10.20.1.1	AOUQWhMcuW.c	8162817449279ecb4007068224f0854173456294efe1489ac2f24	Smb	注入
10.20.1.243	RdmuDGfxma.exe	6b946671a458635a9994a067b17c4563e47f6f591a5138e54651f	Smb	注入
10.20.1.243	BRxKVUBndN.cspr	d579c0d61ffc463a439f3ac244b48f0b5ec9585a52b83fb9133429	Smb	注入

10.20.1.243	ZbrGyCxXHA.cspr	08caa5b9fd85f1c731f3a5ab9ac31fb4c76ae21de8db03fbc88cac	Smb	注入
10.20.1.1	VAlPSDommr.cspr	be2b40f08f57b6c271a4e84afd4921e2f8199676041fe8cd5403b8	Smb	注入
10.20.1.243	sCicHInMQf.cspro	007bc57f097dd4ecc86a774ff7f438e471a6142ca083eac11cbad	Smb	注入
10.20.1.1	JJBdMwWmak.csp	a2edb7d90ac54c026728a81d161fa657ff885ab5329fe943413e3	Smb	注入
10.20.1.243	wCCHeiRFyR.cspr	bd5d4f080637b20894d4b93a14ed02804832967554480c2380e3	Smb	注入

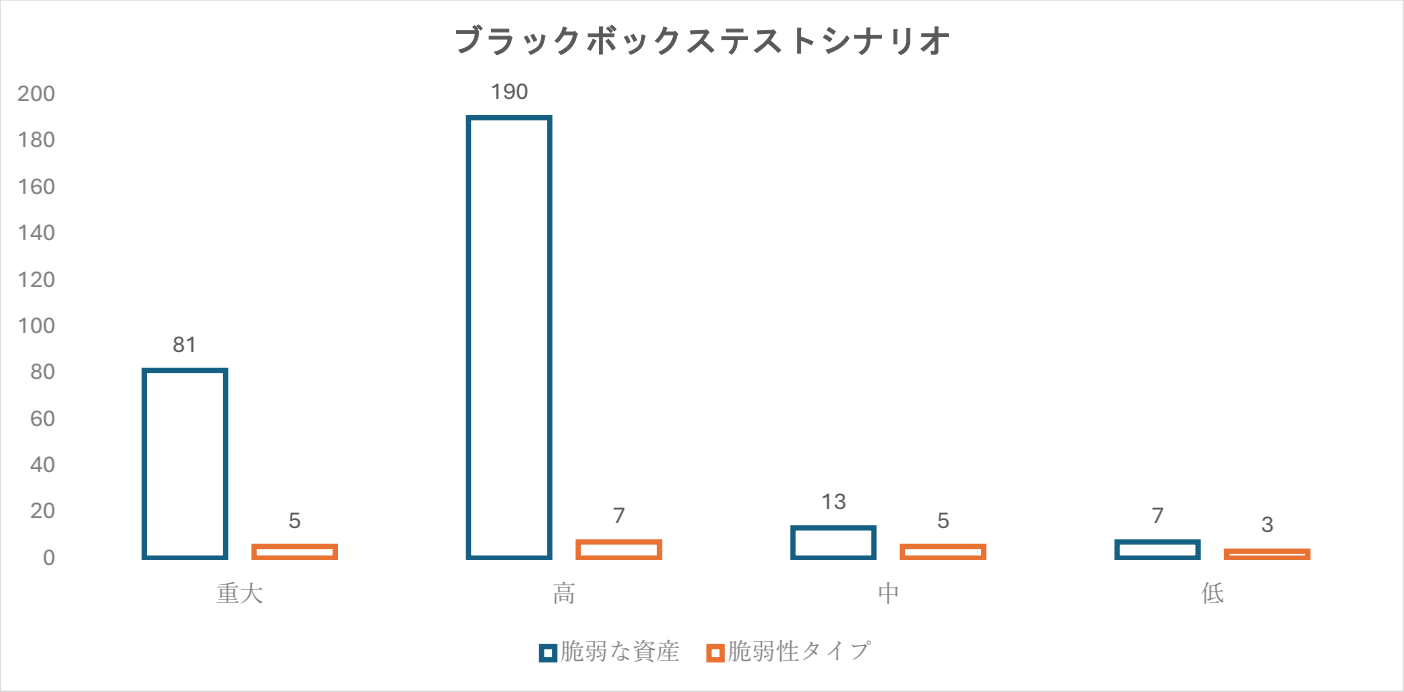
［Pentera／結果／痕跡／ファイル］

［時刻、ホスト、ホスト名、ユーザー、パス、ファイル名、SHA256］

3　テスト結果サマリー

3.1 検出結果サマリー：ブラックボックステストシナリオ

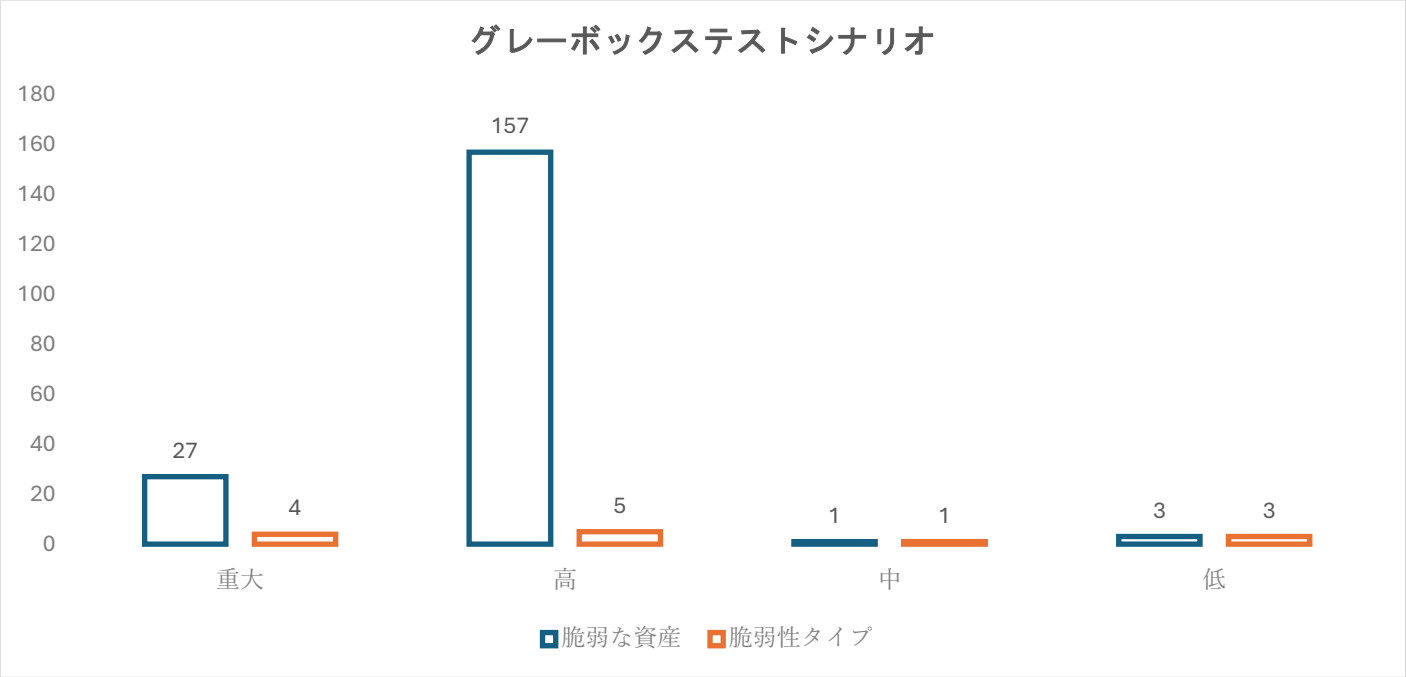
ブラックボックステストシナリオで、Pentera は 4 段階の深刻度にわたり合計 291 件の脆弱性を特定しました。すべて認証情報を使用しないテストで検出されたものです。以下のグラフに深刻度別の結果を示します。



3.2 検出結果サマリー：グレーボックステストシナリオ

ブラックボックス評価で十分な侵入または評価範囲を確保できない場合に、グレーボックステストを実施します。有効な認証情報を投入して Pentera に認証済みアクセスを与え、未認証の観点では評価できなかった攻撃機会を追加評価します。

グレーボックステストシナリオで、Pentera は 4 段階の深刻度にわたり合計 188 件の脆弱性を特定しました。すべて認証情報を使用したテストで検出されたものです。以下のグラフに深刻度別の結果を示します。



4 ブラックボックステスト結果

4.1 技術的所見

4.1.1 ブラックボックス TF-001：SMB メッセージ署名が無効

深刻度	影響を受ける資産
1.0	10.11.37.101 (TGT-WIN10V-3.example2.com)

所見
攻撃者は署名なし SMB サーバーを悪用し、他ホストからの NTLM チャレンジを中継してシェルアクセスを取得できる可能性があります。

4.1.2 ブラックボックス TF-002：ホストが不正サーバーへの認証を強制される可能性

深刻度	影響を受ける資産
4.7	tgt-win10v-10, tgt-win10v-3, tgt-win10v-6, example2, tgt-win10v-9 tgt-win10v-4

所見

DNS サーバーが名前解決に失敗すると、LLMNR、NetBIOS-NS、mDNS サービスが解決を試みます。これらはブロードキャストプロトコルのため、誰でも照会へ応答できます。攻撃者は中間者攻撃により要求を自ら管理する端末へ誘導し、ユーザー名やパスワードハッシュなどの機密情報を取得できる可能性があります。

4.1.3 ブラックボックス TF-003：パスワードが容易に解析可能

深刻度	影響を受ける資産
7.9	administrator, pentera

所見
多くのパスワード解析ツールは辞書ルールセットを使用するため、Aa123456 や P@ssw0rd などの一般的なパスワードや、加工していない辞書語の使用は避けてください。意図的で独自の綴り違い、または頭字語の使用が推奨されます。Pentera のカスタム辞書へ独自ワードリストをアップロードして再テストすると、ソーシャルエンジニアリングを用い対象を熟知した攻撃者が予測・推測できるパスワードを追加検出できます。

4.1.4 ブラックボックス TF-003：PrintNightmare（CVE-2021-34527）

深刻度	影響を受ける資産
8.8	10.11.37.200 (ADSERVER2.EXAMPLE2.COM), 10.11.37.100 (ADSERVER1.example.com)

所見
Windows Print Spooler サービスが特権ファイル操作を不適切に実行すると、リモートコード実行の脆弱性が生じます。悪用に成功した攻撃者は SYSTEM 権限で任意コードを実行でき、プログラムのインストール、データの閲覧・変更・削除、完全なユーザー権限を持つ新規アカウントの作成が可能になります。

5 グレーボックステスト結果

5.1 技術的所見

5.1.1 グレーボックス TF-001：AV/EDR が暗号資産マイニングのペイロードをブロックしなかった

深刻度	影響を受ける資産
8.8	10.20.1.243 (EC2AMAZ-ARABICA-DC.CaffeineOps.local) 10.20.1.125 (EC2-LIBERICA.CaffeineOps.local) 10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)

所見
暗号資産マイニング(Cryptojacking)ペイロードとは、被害者の同意なくコンピューティングリソースを利用して暗号資産を採掘するマルウェアまたは不要なソフトウェアを指します。このマルウェアは感染したコンピューターや Web ブラウザーのバックグラウンドで動作し、その処理能力を利用してブロックチェーン上の取引を検証する複雑な計算を行います。検証に成功すると、攻撃者のデジタルウォレットへ暗号資産の報酬が直接付与されます。暗号資産マイニングペイロードは大量の処理能力と電力を消費するため、システムの顕著な低速化、性能低下、電力コスト増加につながることがあります。

5.1.2 グレーボックス TF-002：ドメインユーザーが複数ホストでリモートコード実行権限を保持

深刻度	影響を受ける資産
7.7	CAFFEINEOPS.LOCAL

所見
ホストへのアクセス取得後、攻撃者は侵害した認証情報を使ってネットワーク内を横展開する可能性があります。

5.1.3 グレーボックス TF-003：空のパスワードを使用

深刻度	影響を受ける資産
8.6	guest

所見
空のパスワードを使用してパスワード解析に成功しました。

5.1.4 グレーボックス TF-004：ホストからファイルを持ち出し可能

深刻度	影響を受ける資産
6.0	10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)

所見

5.1.5 グレーボックス TF-005：スクリプトファイルに平文認証情報が保存されている可能性

深刻度	影響を受ける資産
6.0	10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)

所見
攻撃者は、攻撃を継続するため、ネットワーク内のコンピューターにあるスクリプトから機密情報や保存済み認証情報を探索する可能性があります。スクリプトは高い権限で実行され、重要サービスに使用されることが多いため、組織への潜在リスクが高まります。

5.1.6 グレーボックス TF-006：データベーススクリプトファイルに平文認証情報が保存されている可能性

深刻度	影響を受ける資産
5.5	10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)

所見
攻撃者はネットワーク内のコンピューターにあるファイルや文書からパスワードを探索する可能性があります。データベーススクリプトには、データベース自体へのアクセスを許し、高機密情報の収集・操作を可能にする認証情報が保存されている場合があります。

5.1.7 グレーボックス TF-007：ユーザーアカウントに「パスワードを無期限にする」属性が設定

深刻度	影響を受ける資産
2.3	CAFFEINEOPS.LOCAL

所見
「パスワードを無期限にする」属性は通常、サービスアカウントとして使用するユーザーアカウントに設定します。多くのセキュリティポリシーでは一定期間内のパスワード変更を求めるため、その他のユーザーには設定しないでください。多くの組織では少なくとも 90 日ごとの変更が必要です。

5.1.8 グレーボックス TF-008：ホスト上で閉じたポートを検出

深刻度	影響を受ける資産
2.3	10.20.1.243 (EC2AMAZ-ARABICA-DC.CaffeineOps.local)

所見
ホスト上で閉じたポートを検出しました（ファイアウォールなしで到達可能）。

5.1.9 グレーボックス TF-009：許可されるパスワード有効期間が長すぎる

深刻度	影響を受ける資産
2.5	CAFFEINEOPS.LOCAL

所見

5.1.10 グレーボックス TF-0010：Security Account Manager Remote Protocol（SAMRPC）が有効

深刻度	影響を受ける資産
1.0	CAFFEINEOPS.LOCAL

所見
SAMRPC プロトコルにより、低権限ユーザーでも SMB 経由でネットワーク上の端末へデータ照会できます。たとえば SAMRPC を使用すると、ローカル管理者やドメイン管理者などの特権アカウントを含むユーザー、ローカル SAM および Active Directory のグループや所属関係を列挙できます。この情報は重要な状況把握に役立ち、攻撃者がドメインやネットワーク環境を侵害する起点になる可能性があります。

5.1.11 グレーボックス TF-0011：EPP/EDR が悪意あるペイロードのディスク書込みを許可

深刻度	影響を受ける資産
5.5	10.20.1.243 (EC2AMAZ-ARABICA-DC.CaffeineOps.local) 10.20.1.125 (EC2-LIBERICA.CaffeineOps.local) 10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)

所見
攻撃者は、侵害済みホストで永続性を確保するため、マルウェアをディスクへ書き込む可能性があります。ディスクへの書込みは感染成立の一歩手前です。そのマルウェアは情報収集、ファイル暗号化、バックドア通信など、攻撃者が望むさまざまな動作を実行できます。

5.1.12 グレーボックス TF-0012：SMB メッセージ署名が無効

深刻度	影響を受ける資産
1.0	10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)

所見
攻撃者は署名なし SMB サーバーを悪用し、他ホストからの NTLM チャレンジを中継してシェルアクセスを取得できる可能性があります。

5.1.13 グレーボックス TF-0013：AV が悪意あるペイロードをブロックしなかった

深刻度	影響を受ける資産
8.8	10.20.1.243 (EC2AMAZ-ARABICA-DC.CaffeineOps.local) 10.20.1.125 (EC2-LIBERICA.CaffeineOps.local) 10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)

所見
攻撃者は、コマンド実行やさまざまな形でホストを制御するためにマルウェアを注入する可能性があります。ネットワークの安全性を確保するには、最新かつ十分な機能を備えた AV/EDR セキュリティ構成が必要です。

6　クロス分析（グレーボックス実施時）

6.1 ブラックボックス／グレーボックス クロス分析

評価項目	ブラックボックス	グレーボックス	差異
開始時の認証情報	なし	有効なユーザー認証情報	認証情報を投入
検出ホスト	10.11.37.200 (ADSERVER2.EXAMPLE2.COM), 10.11.37.100 (ADSERVER1.example.com)	10.11.37.200 (ADSERVER2.EXAMPLE2.COM), 10.11.37.100 (ADSERVER1.example.com) 10.20.1.243 (EC2AMAZ-ARABICA-DC.CaffeineOps.local) 10.20.1.125 (EC2-LIBERICA.CaffeineOps.local) 10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)	追加端末を検出
ホスト侵害	10.11.37.200 (ADSERVER2.EXAMPLE2.COM), 10.11.37.100 (ADSERVER1.example.com)	10.11.37.200 (ADSERVER2.EXAMPLE2.COM), 10.11.37.100 (ADSERVER1.example.com) 10.20.1.243 (EC2AMAZ-ARABICA-DC.CaffeineOps.local) 10.20.1.125 (EC2-LIBERICA.CaffeineOps.local) 10.20.1.23 (EC2AMAZ-ROBUSTA.CaffeineOps.local)	追加エンドポイントを侵害
認証情報取得	［有効なユーザー認証情報 16 件］	［有効なユーザー認証情報 30 件］	［追加の有効なユーザー認証情報 14 件］
脆弱性悪用	[20]	[33]	［追加で悪用された脆弱性 13 件］
特権アカウント侵害	[6]	[7]	［追加の EnterpriseAdmin アカウント 1 件］
ラテラルムーブメント	達成	達成	両方で達成

ドメイン侵害	未達成	達成	新たに達成
Pentera 達成項目	1709	2264	新規達成項目 555 件

7　主要課題／是正優先度とお客様の次の対応

7.1 ブラックボックステストシナリオ

7.1.1　主要課題

Pentera は 4 段階の深刻度にわたり合計 291 件の脆弱性を特定しました。これらは 20 種類の脆弱性タイプに関連しています。Pentera は検出結果に基づき、各セキュリティ課題へ対応すべき推奨順序を示す是正優先度を提示します。

7.1.2　是正対応

#1	1.0	SMB メッセージ署名が無効
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#2	4.7	不正サーバーによりホストへ認証を強制可能
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#3	7.9	パスワードが容易に解析可能
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#4	8.8	PrintNightmare（CVE-2021-34527）
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#5	8.8	KDC Bamboozling（CVE-2021-42287）
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#6	6.9	低い GPU 負荷でパスワード解析可能
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。

3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#7	8.6	空のパスワードを使用
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#8	4.9	高い GPU 負荷でパスワード解析可能
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#9	5.3	匿名 FTP ログインが許可

是正優先度　深刻度

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#10	5.8	エンドポイントの SMB サーバーがクライアントを検証しない

是正優先度　深刻度

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#11	5.5	ユーザーアカウントに「パスワードを無期限にする」属性が設定

是正優先度　深刻度

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#12	5.0	管理者／一般ユーザーのパスワードが同一
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#13	5.3	未認証のプリンター登録（CVE-2024-47176）
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。

3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#14	2.3	ホスト上で閉じたポートを検出
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#15	3.3	ホストが NTLMv1 認証を使用
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#16	3.5	ホストが SMBv1 プロトコルをサポート
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#17	5.5	EPP/EDR が悪意あるペイロードのディスク書込みを許可
是正優先度	深刻度	

是正／推奨事項

1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。

#18	3.2	ネットワークホスト上で開いているセッションが多すぎる可能性のあるユーザーを検出
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#19	1.0	Security Account Manager Remote Protocol（SAMRPC）が有効
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

#20	8.8	AV が悪意あるペイロードをブロックしなかった
是正優先度	深刻度	

是正／推奨事項

推奨事項例:1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。

3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。
4. 脆弱性の緩和には、[ツール/製品/セキュリティソリューション例]などの利用を推奨します。

7.2 グレーボックステストシナリオ

7.2.1 主要課題

Pentera は 4 段階の深刻度にわたり合計 188 件の脆弱性を特定しました。これらは 13 種類の脆弱性タイプに関連しています。Pentera は検出結果に基づき、各セキュリティ課題へ対応すべき推奨順序を示す是正優先度を提示します。

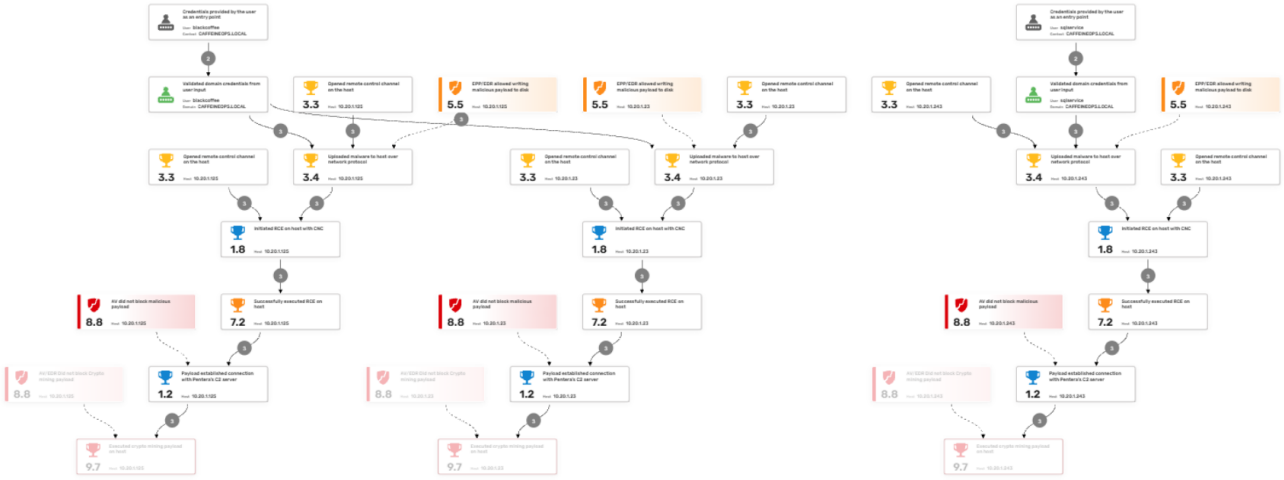
7.2.2 是正対応

#1	8.8	AV/EDR が暗号資産マイニングのペイロードをブロックしなかった
是正優先度	深刻度	

是正／推奨事項

1. AV および EDR ソリューションを全端末に展開し、最新のシグネチャに更新するとともに、すべての振る舞い検知機能を有効化してください。
2. 可能であれば、過剰なリソース使用など暗号資産マイニング活動に関連する異常な挙動パターンを識別できる高度な EDR ソリューションを利用してください。
3. 既知の暗号資産マイニングプールへの接続など、通常と異なる通信パターンを検出するネットワーク監視ツールを導入してください。ネットワークセグメンテーションによりマルウェアの拡散を抑え、重要リソースへのアクセスを制限してください。

修正シミュレーション



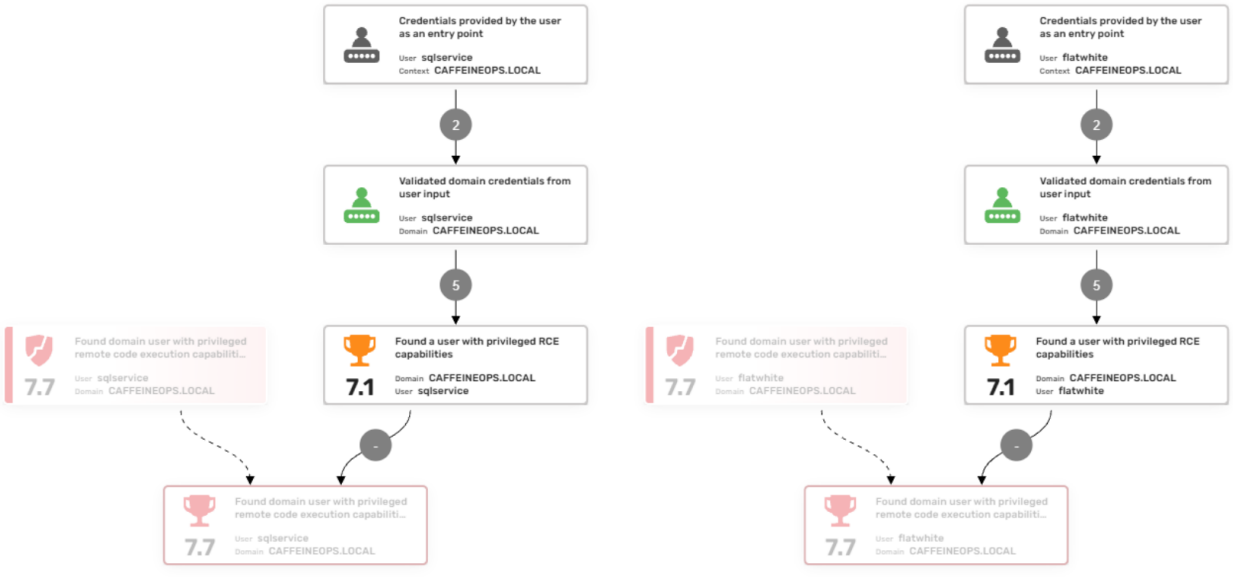
#2	7.7	ドメインユーザーが複数ホストでリモートコード実行権限を保持

是正優先度　　深刻度

是正／推奨事項

ネットワーク全体でユーザーのアクセス範囲を制限し、高権限ユーザーの人数も制限することを検討してください。

修正シミュレーション



#3	8.6	空のパスワードを使用

是正優先度　深刻度

是正／推奨事項

認証を必要とするすべてのユーザーまたはサービスに対し、特権アカウントを特に重視した強固なパスワードポリシーを設定してください。最低要件は次のとおりです。A. 8 文字以上。B. 英大文字、英小文字、数字をそれぞれ 1 文字以上含む。C. Aa123456 や P@ssw0rd など一般的なパスワードは使用しない。

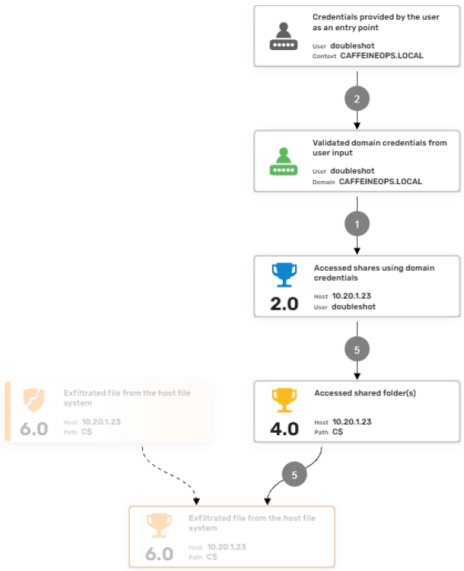
#4	6.0	ホストからファイルを持ち出し可能

是正優先度　深刻度

是正／推奨事項

影響を受けるホスト上の SMB ベースのファイル転送を確認・監視し、不正または異常なファイルの持ち出し／持込みを検出してください。必要に応じて SMB アクセスを許可済みのユーザーとシステムに制限し、機密ファイルと共有資源へのアクセスに最小権限の原則を適用してください。

修正シミュレーション



#5	6.0	スクリプトファイルに平文認証情報が保存されている可能性

是正優先度　深刻度

是正／推奨事項

認証情報は暗号化されたファイルまたは文書に保存し、いかなるファイルにも平文パスワードを保存しないことを推奨します。

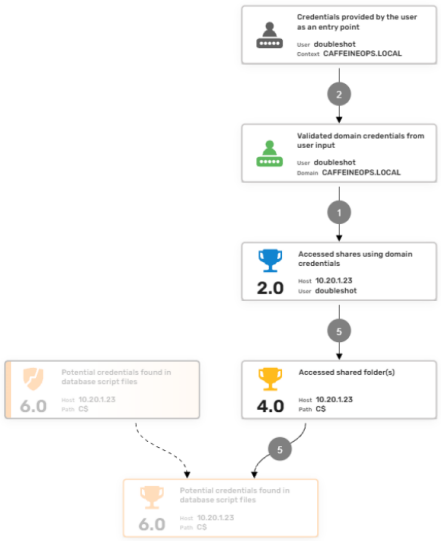
#6	6.0	データベーススクリプトファイルに平文認証情報が保存されている可能性

是正優先度　深刻度

是正／推奨事項

ファイル内に平文の認証情報を保存しないでください。

修正シミュレーション



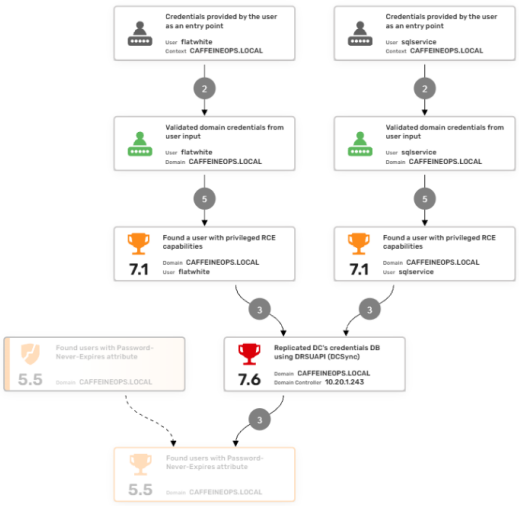
#7	5.5	ユーザーアカウントに「パスワードを無期限にする」属性が設定

是正優先度　深刻度

是正／推奨事項

「パスワードを無期限にする」属性は通常、サービスアカウントとして使用するユーザーアカウントに設定します。多くのセキュリティポリシーでは一定期間内のパスワード変更を求めるため、その他のユーザーには設定しないでください。多くの組織では少なくとも 90 日ごとの変更が必要です。

修正シミュレーション



#8	2.3	ホスト上で閉じたポートを検出
是正優先度	深刻度	

是正／推奨事項

閉じたポートがファイアウォール越しに到達可能な場合、悪用される可能性があります。悪性ソフトウェアが閉じたポートを介して C2 チャネルを確立することを防ぐため、ファイアウォールで閉じたポートを遮断することを推奨します。

#9	2.5	許可されるパスワード有効期間が長すぎる
是正優先度	深刻度	

是正／推奨事項

定期的なパスワード変更を強制し、変更間隔が 42 日を超えないようにしてください。

#10	1.0	Security Account Manager Remote Protocol（SAMRPC）が有効
是正優先度	深刻度	

是正／推奨事項

このリスクを軽減するには、最新のセキュリティ更新を適用し、ポリシー「ネットワークアクセス：SAM へのリモート呼び出しを許可するクライアントを制限する」を構成します。Windows 2003 メンバーサーバーおよび XP コンピューターでは、「ネットワークアクセス：匿名の SID／名前変換を許可する」を選択し、ポリシーが無効であることを確認してください。詳細：https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls および https://www.itprotoday.com/windows-78/securing-administrator-account 。任意の追加対策として、SMB サーバーコンポーネントを無効化するか SMB 通信を遮断し、SMB 経由の照会を防止できます。詳細：https://support.microsoft.com/en-in/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

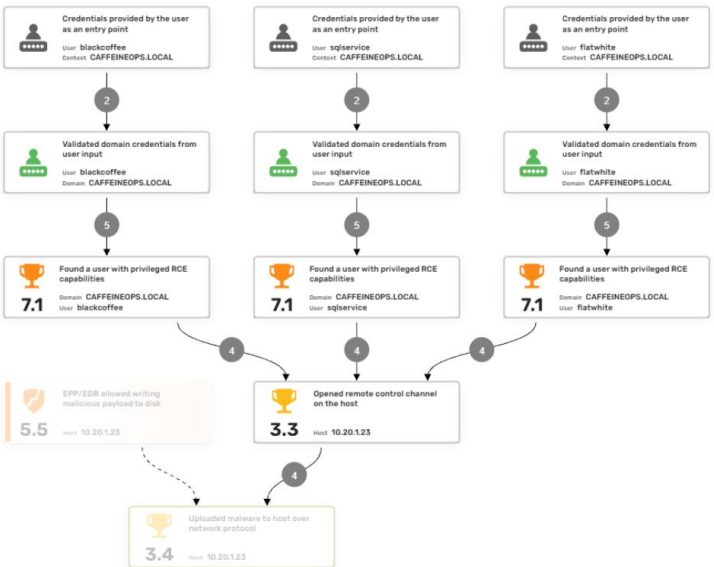
#11	5.5	EPP/EDR が悪意あるペイロードのディスク書込みを許可
是正優先度	深刻度	

是正／推奨事項

次のいずれかの是正対応を検討してください:

1. エンドポイントに EDR ソリューションを導入する
2. 導入済み EDR ソリューションの防御レベルを引き上げる。

修正シミュレーション



#12	1.0	SMB メッセージ署名が無効

是正優先度	深刻度

是正／推奨事項

SMB 署名の有効化は OS のレジストリ値を編集することで行えます。ただし、グループポリシーは異なる設定が可能でローカル変更を上書きする場合があるため、値を直接変更するのではなく、グループポリシーで設定することを強く推奨します。SMB 署名には 2 つではなく 3 つの設定があります: - Enabled: 攻撃者が端末に署名なし通信への切り替えを要求できるため、悪性活動を防止できません。 - Disabled - Required: 推奨設定です。OS に署名付きメッセージのみを使用させます。SMB 署名が Enabled の場合、端末は署名付き SMB メッセージで通信できますが、署名なし通信も許可します。SMB 署名が Enabled に設定されている場合、端末は署名付き通信を優先しますが、要求に応じて署名なし通信へフォールバックします。

#13	8.8	AV が悪意あるペイロードをブロックしなかった

是正優先度	深刻度

是正／推奨事項

AV/EDR ポリシーを強化し、ネットワーク内の不審な振る舞いを監視してください。

8　レッドチーム分析と攻撃者視点

レッドチームの観点から、本評価は、CAFFEINEOPS.LOCAL 環境への有効なアクセスを得た攻撃者が、初期認証を越えてリモート実行、認証情報アクセス、ラテラルムーブメント、および侵害後の活動へ進み得ることを示しています。対象は EC2AMAZ-ROBUSTA（10.20.1.23）、EC2-LIBERICA（10.20.1.125）、ドメインコントローラーEC2AMAZ-ARABICA-DC（10.20.1.243）の 3 ホストです。Pentera は WMI（43 件）、WinRM（11 件）、PsExec（5 件）を使用し、59 件のリモート実行に成功しました。実行には flatwhite、sqlservice、blackcoffee、doubleshot の各アカウントが使用され、さらにこれらのアカウントで 107 件の SMB アップロー

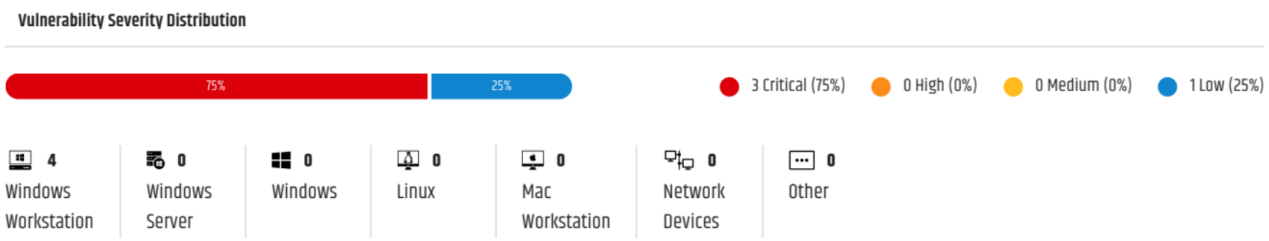
ド・実行が成功しました。これは「ドメインユーザーが 2 台を超えるホストでリモートコード実行権限を持つ」という Pentera の所見と一致し、侵害されたドメイン認証情報によってシステム間のアクセス拡大が可能になることを示します。3 ホストすべてで認証情報アクセスも実証されました。Pentera は SAM ダンプを 21 件実行し、内訳は EC2AMAZ-ARABICA-DC が 10 件、EC2-LIBERICA が 6 件、EC2AMAZ-ROBUSTA が 5 件です。さらに MSBuild によるメモリ内認証情報抽出が 52 件成功し、EC2AMAZ-ROBUSTA と EC2-LIBERICA が各 20 件、EC2AMAZ-ARABICA-DC が 12 件でした。脆弱性結果では、guest アカウントの空パスワード、および EC2AMAZ-ROBUSTA 上のスクリプト／データベーススクリプトに平文認証情報が存在する可能性も確認されました。

エンドポイント保護も重大な懸念です。Pentera は、暗号資産マイニングのペイロードを AV/EDR がブロックしなかった 3 ホストと、悪意あるペイロードをディスクへ書き込め、AV にもブロックされなかった同じ 3 ホストを特定しました。アクションログではさらに、ホストへのマルウェアアップロード 153 件、SMB 経由のアップロード 141 件、暗号資産マイニングペイロード実行 10 件、ランサムウェアエミュレーション 10 件の成功が記録されています。これらは、評価で実施した代表的な侵害後活動をエンドポイント制御が一貫して阻止できなかったことを示します。最後に、Pentera は 6 件のファイル持ち出しに成功しました。内訳は EC2AMAZ-ARABICA-DC から 3 件、EC2AMAZ-ROBUSTA から 2 件、EC2-LIBERICA から 1 件です。実証されたリモート実行および認証情報アクセス能力と合わせると、十分なアクセスを確立した攻撃者は、システム間を移動するだけでなく、データへアクセスして転送できる可能性があります。レッドチームの観点では、より深い手動検証の主な対象は、認証情報の再利用と権限昇格、3 ホスト間のラテラルムーブメント、EC2AMAZ-ARABICA-DC で取得可能なアクセス範囲、および実証されたエンドポイント保護の弱点により Pentera で実施した手法を超えて攻撃者が活動を継続できるかどうかです。

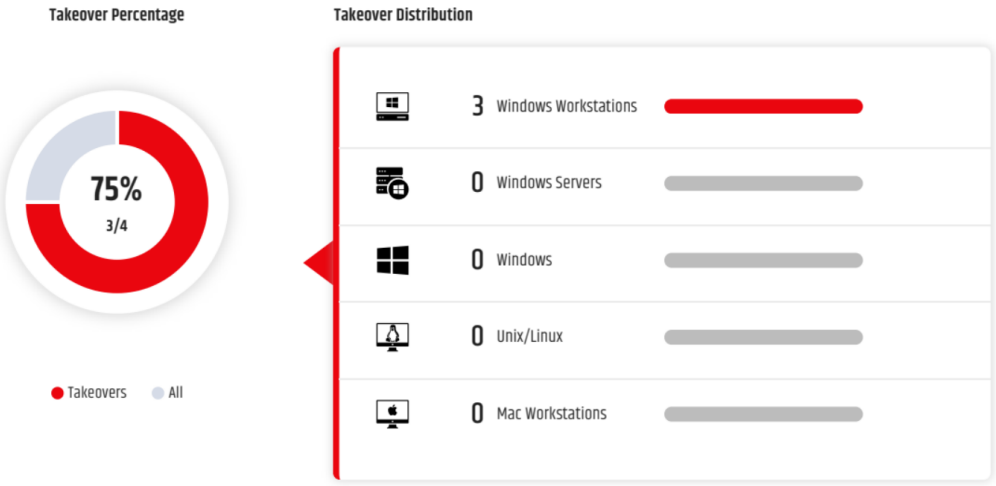
9 付録

検出されたデバイス

ホスト



ホスト侵害



ユーザー

Username	Account Type	Host / Domain Name	Privileged	Compromised By	Cleartext Password Obtained	Obtained Cleartext Password By	Critical	Validated
administrator	Domain User Account	CAFFEINEOPS.LOCAL	No	Post exploitation	No	Cracking	No	Yes
krbtgt	Domain User Account	CAFFEINEOPS.LOCAL	No	Post exploitation	No	Cracking	No	No
EC2AMAZ-ROBUSTA$	Computer Account	CAFFEINEOPS.LOCAL	No	Post exploitation	No		No	Yes
EC2-LIBERICA$	Computer Account	CAFFEINEOPS.LOCAL	No	Post exploitation	No		No	Yes
EC2AMAZ-ARABICA$	Computer Account	CAFFEINEOPS.LOCAL	No	Post exploitation	No		No	Yes
LATTE$	Computer Account	CAFFEINEOPS.LOCAL	No	Post exploitation	No		No	Yes
EC2-EXCELSA-DC$	Computer Account	CAFFEINEOPS.LOCAL	No	Post exploitation	No		No	Yes
guest	Domain User Account	CAFFEINEOPS.LOCAL	No	Post exploitation	No	Cracking	No	No

レジリエンス・スコアカード

Critical Assets
Congratulations! Pentera wasn't able to compromise any critical assets in your network

Credentials and Account Takeover
Gained access to 1 accounts: 1 Domain user(s)
Critical

Sniffing
No credentials were sniffed, either Pentera and the network under test are in different broadcast domains or there is no user network activity

Password Strength
Cracked 1 out of 3 passwords: 1 easy
Medium

Lateral Movement
Performed lateral movement to 3 Windows Workstation(s)

Accessible Data
Gained access to 174711 File(s), 3 Hosts (with complete access) and Found 3 files with potential credentials
Critical

Host Takeover
Pentera was able to 'take over'[1] 3 out of 4 hosts (75%): 3 Windows Workstation(s)
Critical

AV/EDR Bypass
Bypassed AV/EDR and opened remote command sessions on 3 host(s) using 3 file-based payload exploits and using 3 file-less payload exploits
Microsoft Defender ATP
High

AV バイパス

6 Antivirus/EDR Bypass Events

Bypassed 2 AV/EDR vendors and opened remote command session on 3 hosts

Bypass Events Distribution Per Vendor

File based exploits　Fileless exploits

6 Windows Defender　Microsoft Defender ATP　3　3