PENTERA

CTEMってなに？ ASM・BASも包括する最新フレームワーク

Pentera Securities Ltd.
カントリー・マネージャー
ミッチェル ディバート

2024年5月16日

PENTERA

世界中で信頼されています

2018年
販売開始

350
従業員数

$1.5億
出資受け入れ額

awz Blackstone INSIGHT PARTNERS K1 evo/ution EQUITY PARTNERS

50
か国・地域

1000
お客様数

TOYOTA NHS GAP Blackstone Casey's teva Telefónica
SEPHORA JANSEN City of Vienna FP FRANCISCO PARTNERS Azul Bell Virgin
BlackRock Deloitte. CHIPOTLE MEXICAN GRILL NORTHERN TRUST CITY NATIONAL BANK AN RBC COMPANY ADDSECURE APRIA HEALTHCARE

PENTERA

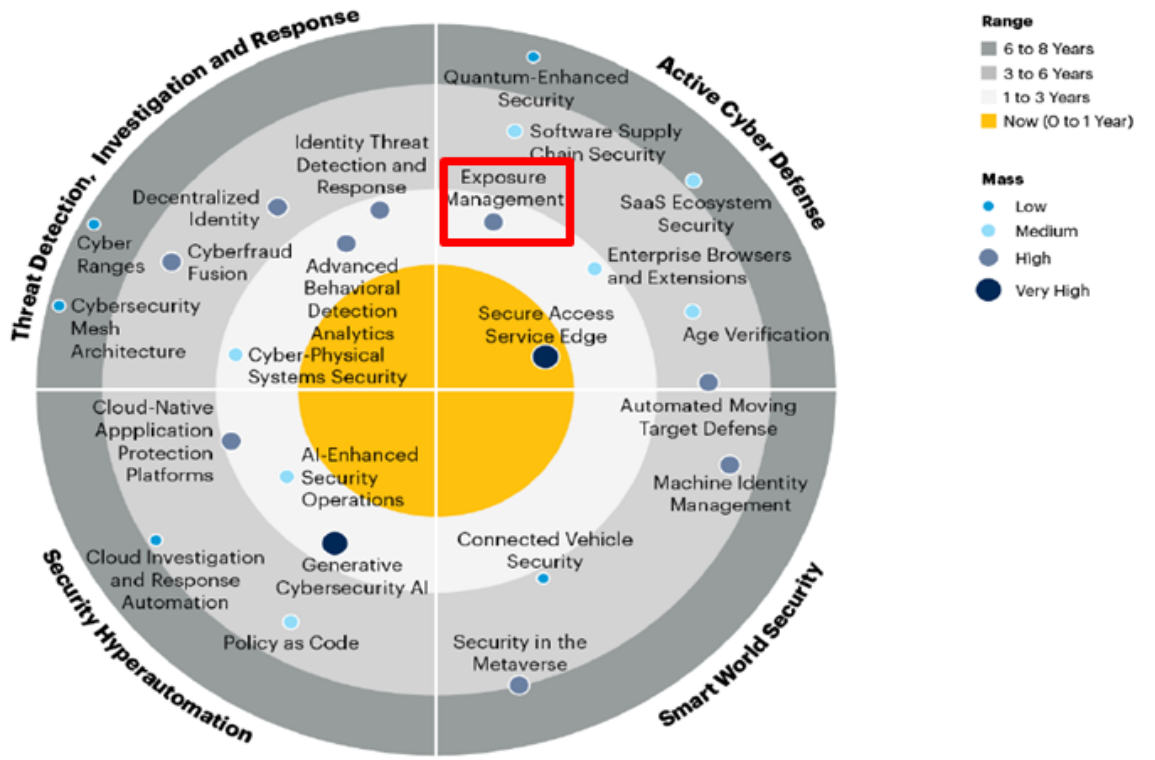
CTEMとは？

PENTERA

Gartner

新興テクノロジーインパクトレーダー: 2023年セキュリティ

Figure 1: Impact Radar for Security



Published 6 October 2023 - ID G00785546

"自動化された侵入テストは3-4年後には脆弱性スキャナーを持つのと同じくらい広く利用されていると思われます。

(最高情報責任者 セキュリティ責任者（CISO）の立場として継続的な検証を実現して、最高の人材を維持し、レッドチームによる侵入テストをより頻繁に実行したいならば Penteraのようなプラットフォームが必要です"

PENTERA

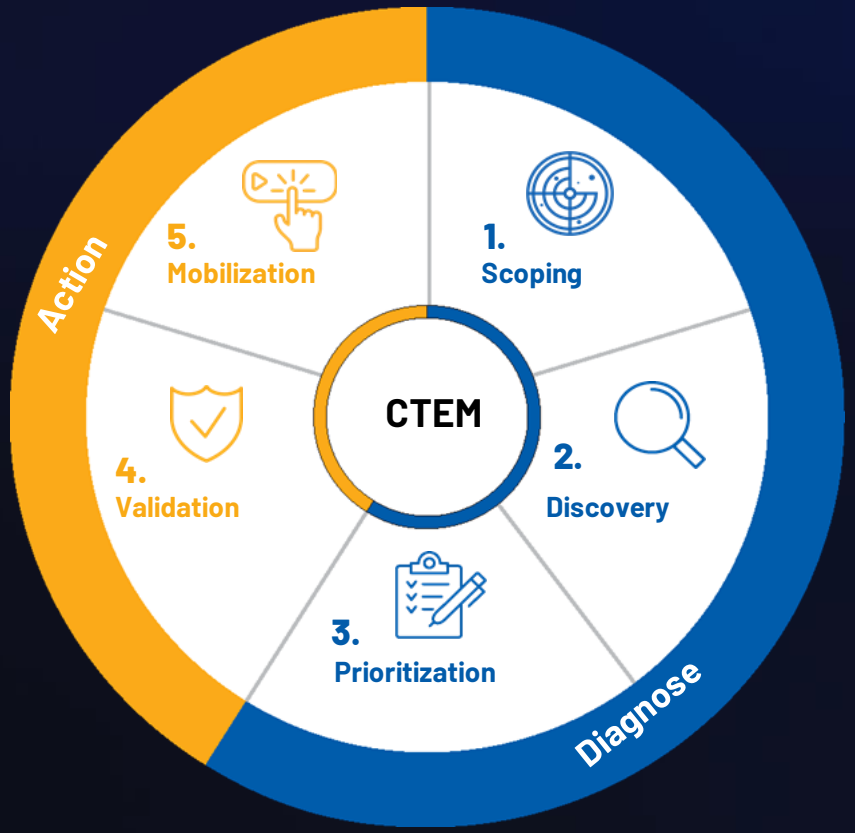
エクスポージャーマネージメントの

サンプルベンダーに選出されております。

PENTERA

Gartner

Continuous Threat Exposure Management (CTEM)



1. Scoping / スコープ設定
2. Discovery / 発見
3. Prioritization/ 優先順位付け
4. Validation / 検証
5. Mobilization / 動員

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

PENTERA

(E)ASMと(CT)EMとの違い

Exposure Management の構成要素 Gartner

（エクスポージャーマネジメント）

攻撃表面	脆弱性	検証
内部	優先順位付け	対象を定めた
外部	分類	包括的
デジタルリスク	認知	コンプライアンスに基づく

※検証とは本物の攻撃手法を使って、脆弱性を発見することです。

出典：「ASM (Attack Surface Management）導入ガイダンス」
（2023年5月、経済産業省商務情報政策局サイバーセキュリティ課）

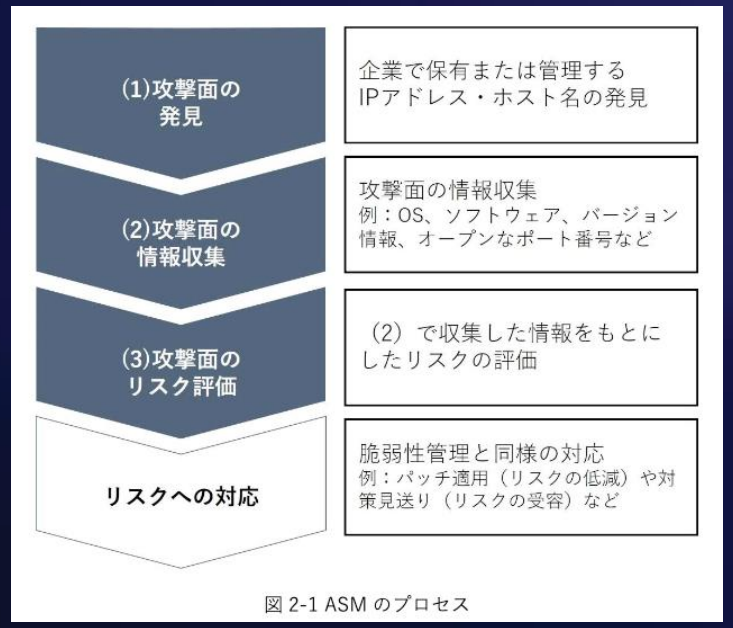


図 2-1 ASM のプロセス

攻撃表面管理（ASM）の構成要素

攻撃表面管理（ASM）

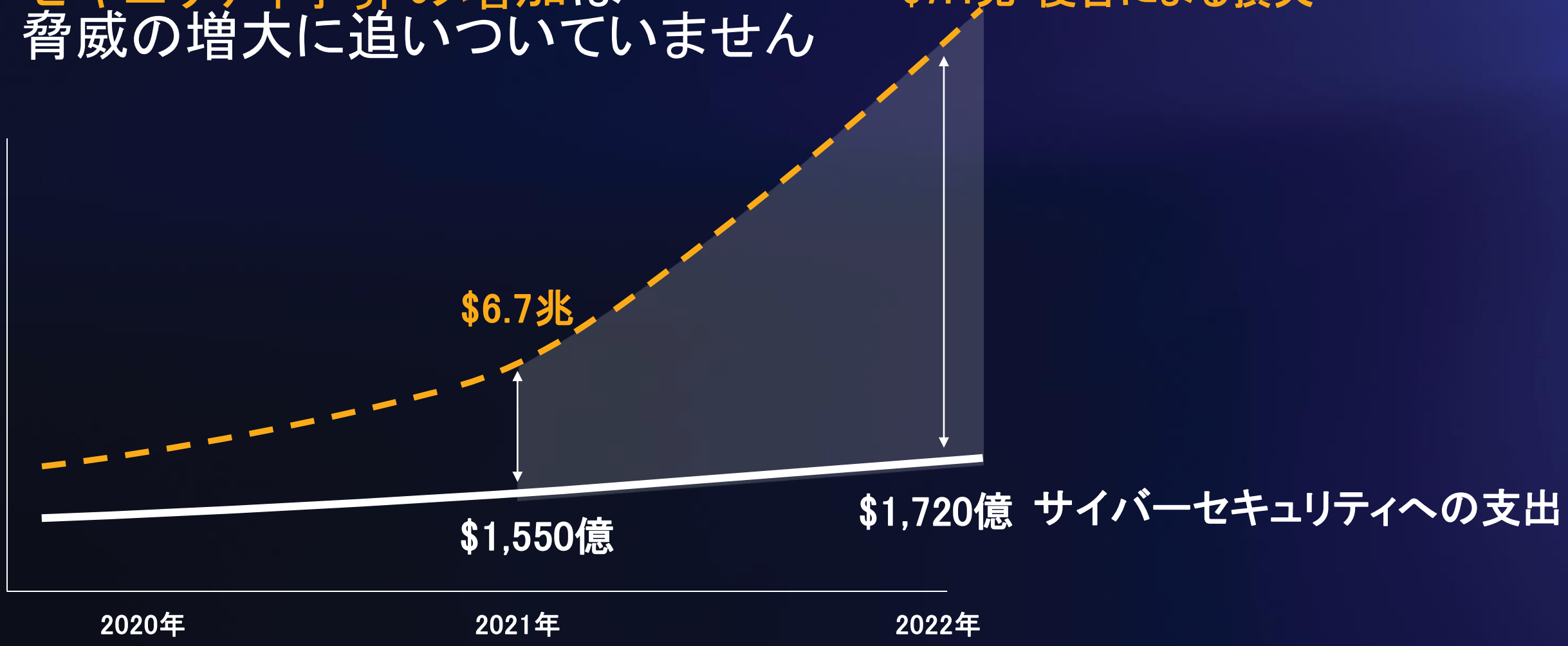
攻撃表面	脆弱性	
外部		
	認知	

PENTERA

企業の置かれている現状

PENTERA

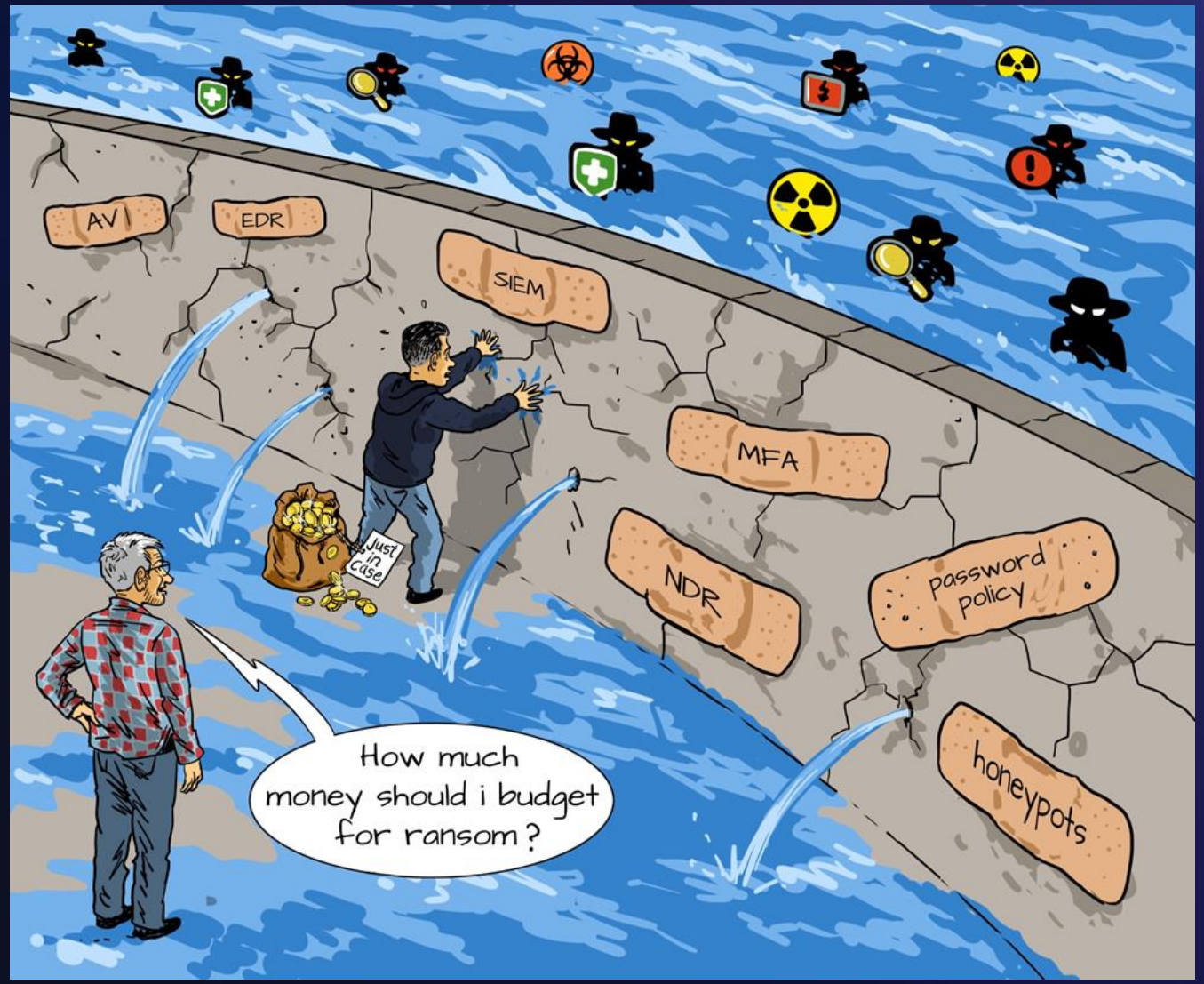
セキュリティ予算の増加は脅威の増大に追いついていません



出典: Gartner (2022年10月) Gartner | Cybersecurityventures

PENTERA

なぜ攻撃が減らないのか？



PENTERA

対

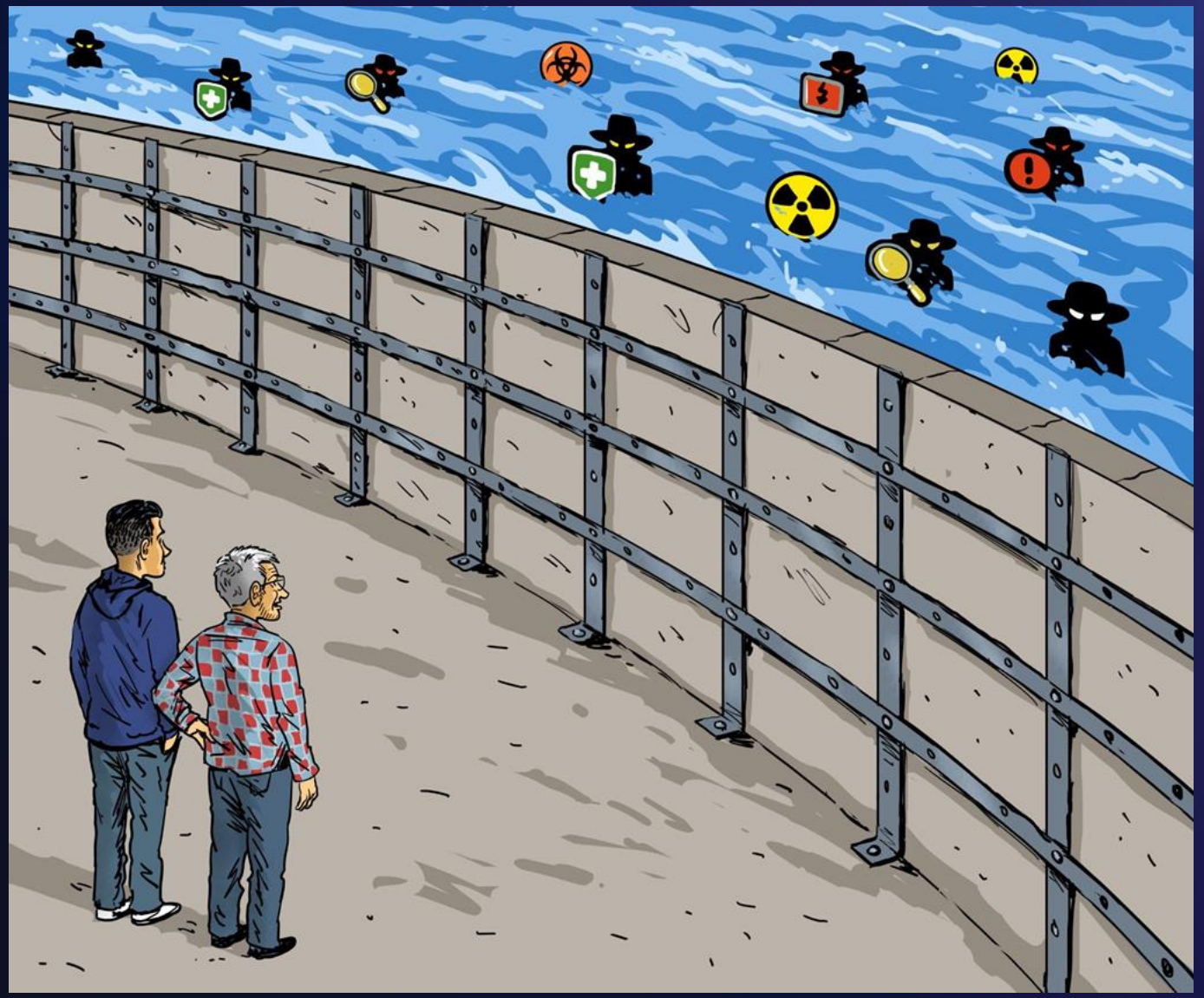
防御側
点で考える

攻撃者側
グラフで捉える

出典: John Lambert氏, Microsoft

PENTERA

自動化されたセキュリティ検証の活用



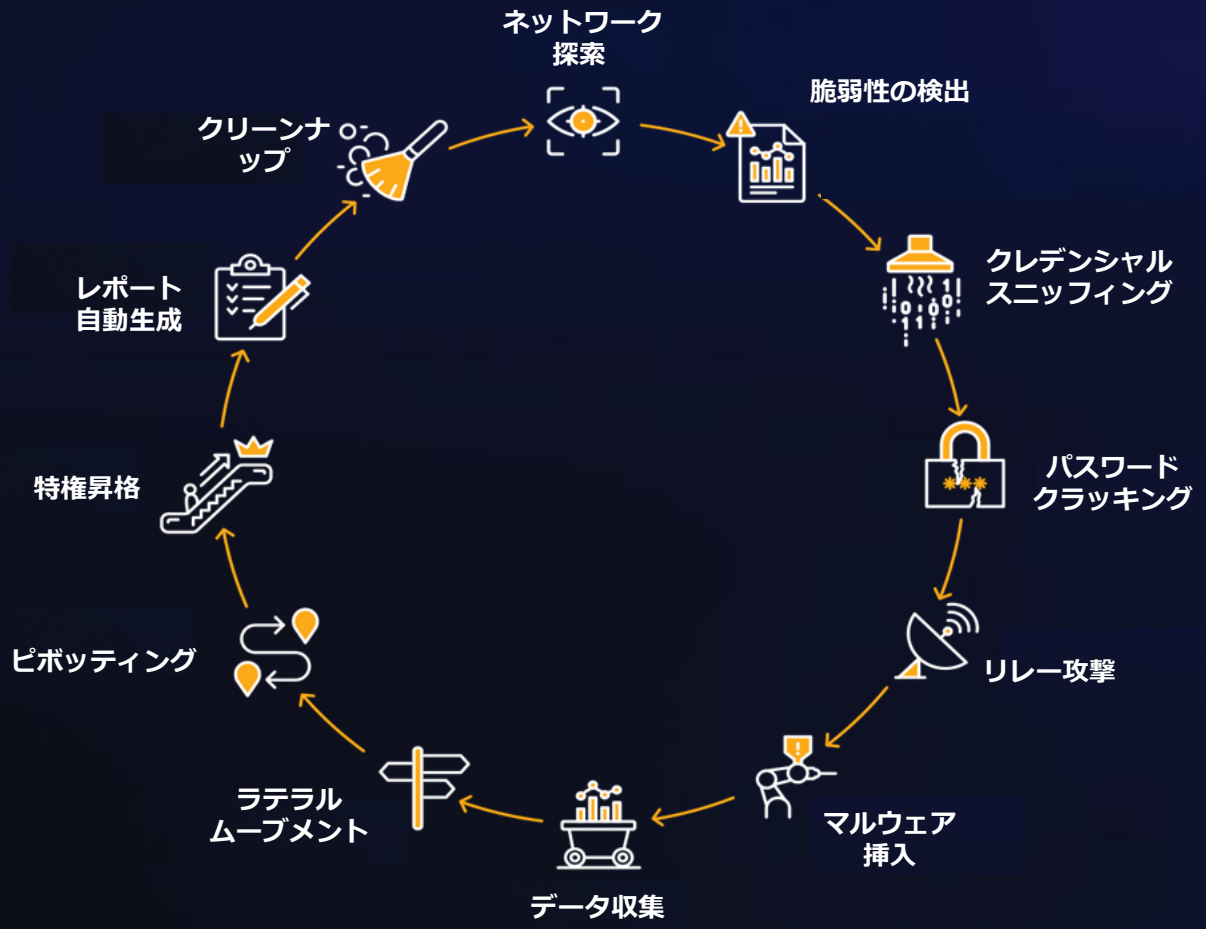
PENTERA

PenteraによるCTEM運用の効率化の実現

PENTERA

Peteraが考える検証とは？

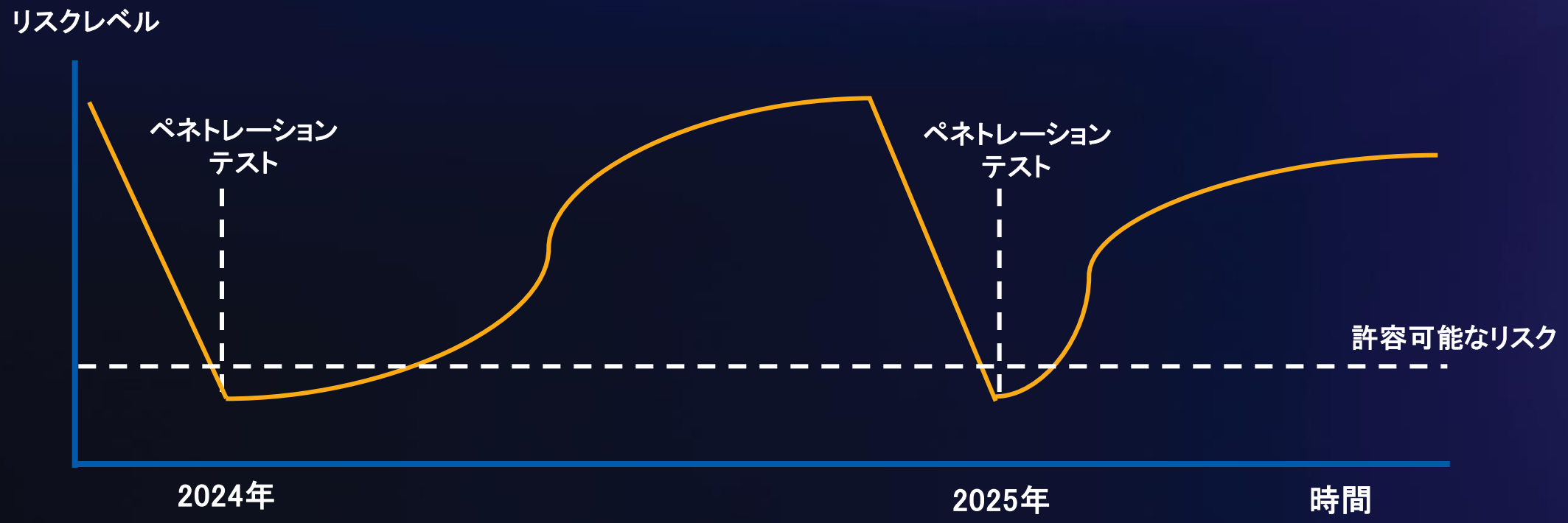
ASV（Automated Security Validation）



- 自動化
- 実際の攻撃をもとにしたテスト
- 安全
- 継続性
- エージェント不要
- 対応策のご案内

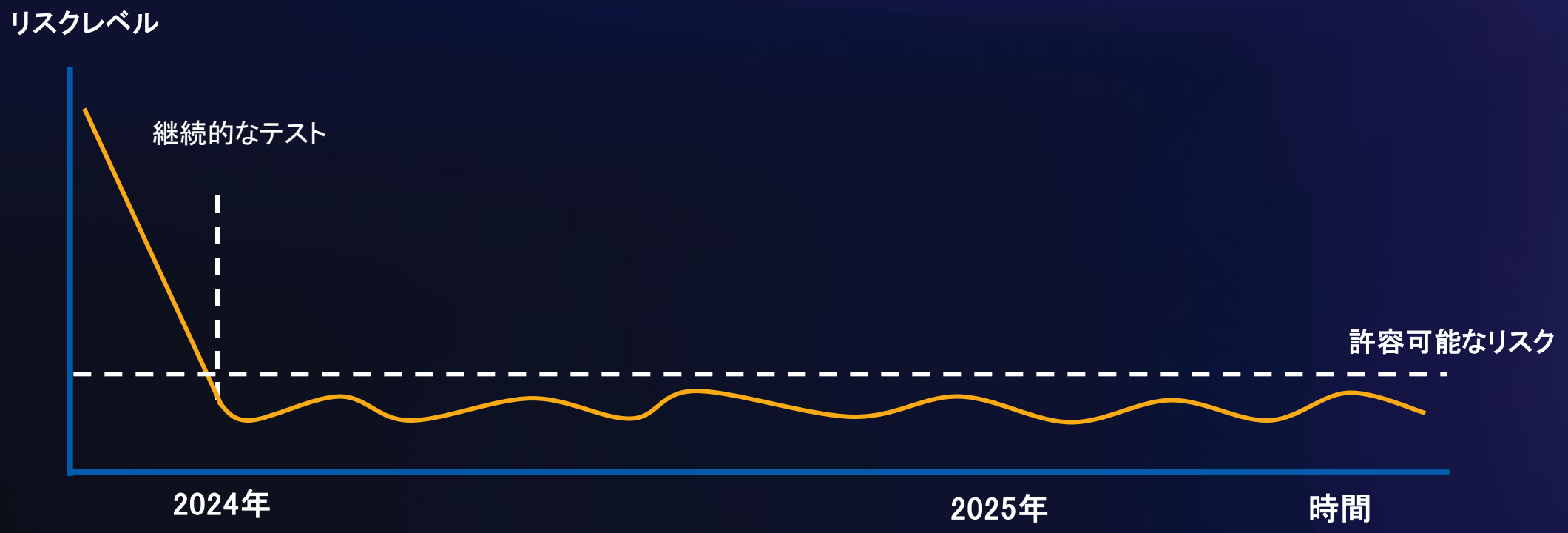
PENTERA

従来のセキュリティ検証
年に一度、ITの5%～10%を実際にテスト



PENTERA

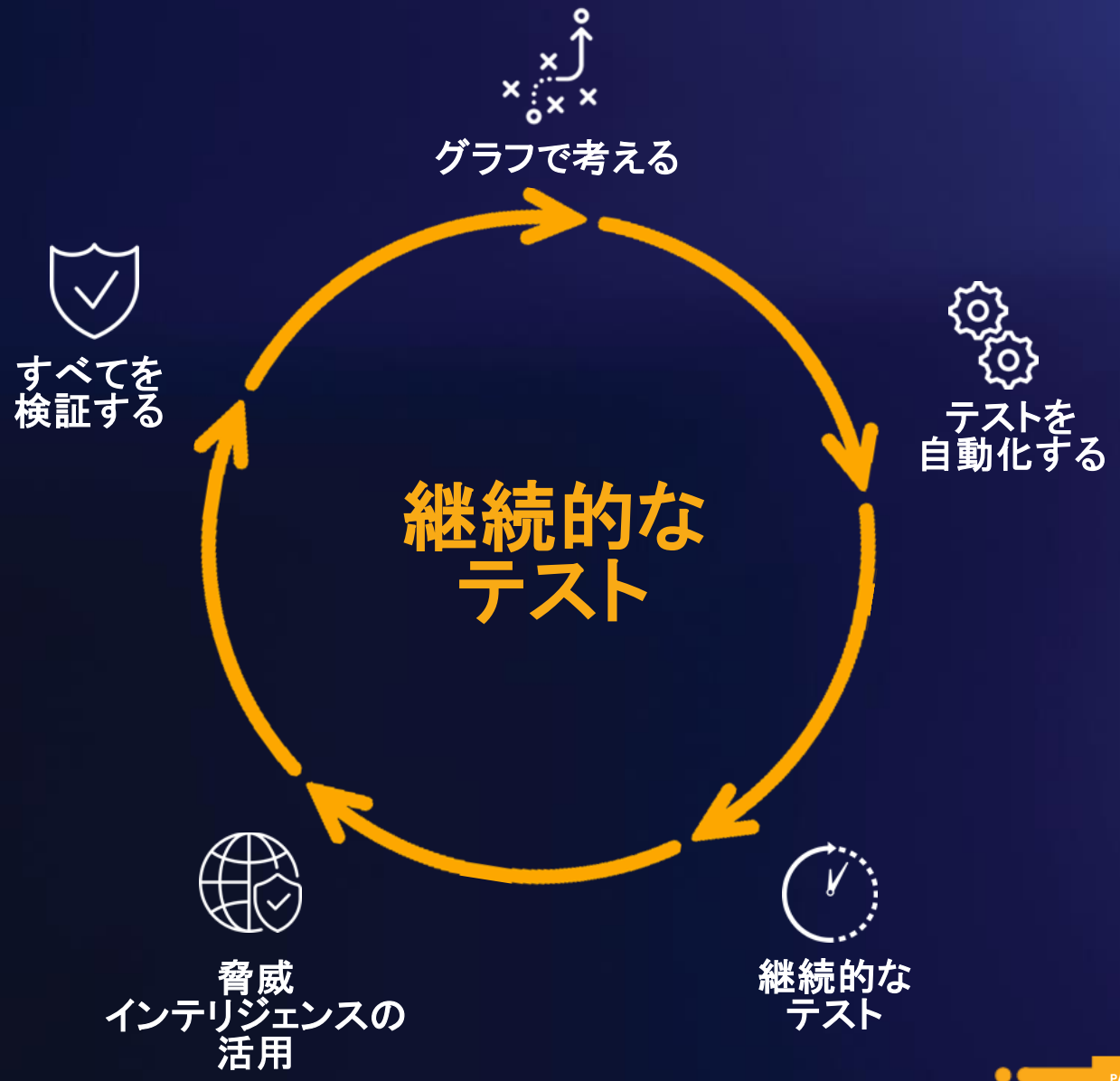
継続的なセキュリティ検証



PENTERA

まとめ:

CTEMの中核となる検証＝Petera



PENTERA

CTEMでは、セキュリティ検証能力が一番のキーポイントになります。

PENTERA

Thank You.

Penteraの活用事例

海外銀行事例

City National Bank
設立：1954年
総資産：14兆円*

継続的な診断を行うことにより、
正確にセキュリティ運用状況を
把握することができている。

Pentera**を用いることにより、**
網羅的にセキュリティ状況を把握、
改善策の立案ができている。

Penteraを用いることにより網羅的なセキュリティ状況の把握、
セキュリティ耐性の継続的な改善に繋がっている。

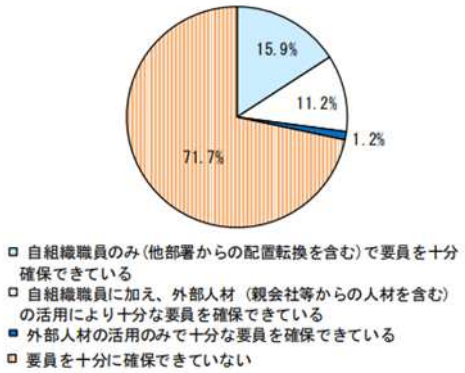
- $93.72B （2024年1月31日）

引用：https://pentera.io/resources/case-studies/page/3/、

ユースケース 1

リスク評価が可能な人材の不足

図表 8　新たなデジタル技術導入により生じ得るサイバーセキュリティに関するリスク評価が可能な人材の確保状況



脅威の重大性評価ができる人材の不足

Penteraの特徴

攻撃範囲をステップで可視化

成功した攻撃の重大度スコアづけ

脅威の重大性評価が可能に

出典：「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2022年度）」（日本銀行金融機構局、金融庁総合政策局）（https://www.fsa.go.jp/news/r4/cyber/honbun.pdf）

ユースケース 2

リスク診断の工数、コスト

1. 委託先検討
2. 診断前すり合わせ
3. 診断前内部調整
4. 診断実施
5. 診断後のレポート待ち

多くの工数
高い委託費

Penteraの特徴

エージェントレス
診断対象の調整負荷小

少ない設定項目で
診断を即時開始

工数、委託費のトータルコストを削減

CTEMハンズオンのご案内

6月6日開催！CTEMを試せる！！

CTEMハンズオンを開催！

Gartner　Exposure managementのカテゴリのサンプルベンダー
Penteraを使って、CTEMのアプローチを簡単に実現する方法を体験できます。

PENTERA

実施内容

- 導入：Penteraコンセプトのご説明
- 実践1：Coreライセンスを使った内部環境への診断
- 実践2：Ransomware＋パスワード耐性診断
- クロージング：QA

※定員：最大4組（1組5人まで）

申し込みはこちらから

会場　東京エレクトロンデバイス　新宿サポートセンター
〒160-0023　東京都新宿区西新宿4-33-4　住友不動産西新宿ビル 4号館 1F

東京エレクトロン デバイス