

アクティブ サイバー経営管理ダッシュボード (Active Cyber Readiness Dashboard)

断片化したセキュリティシグナルを測定可能な運用規律へと転換

KELAGROUP]

KELA

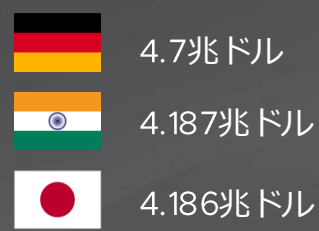
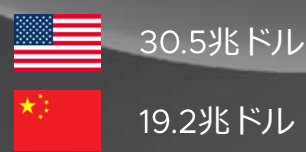


SLING

ビジネスプロセスに組み込まれたサイバー空間の脅威

サイバー攻撃の年間被害額

2025年のGDPランキング(IMF)
Source: <https://eleminist.com/article/4294>



2025年
サイバー犯罪被害額推定*1

**10.5兆ドル
(約1,650兆円)**

2026年
サイバー犯罪被害額推定*2
11~12兆ドル (1,870兆円)

ランサムウェアによる年間被害額予測*3

2025年

570億ドル (約9兆円)

2031年までに

2,750億ドル (約43兆円)



初期攻撃ベクトル	侵害あたりの被害額
サードパーティ・サプライチェーン侵害	491万ドル (約7.4億円)
認証情報の侵害	467万ドル (約7億円)
脆弱性の悪用	424万ドル (約6.4億円)



狙われたのか、偶然ヒットしたのか

※ 10~30%は個別に狙われる攻撃で対象は、政府系組織、重要インフラ、WWでの大企業など

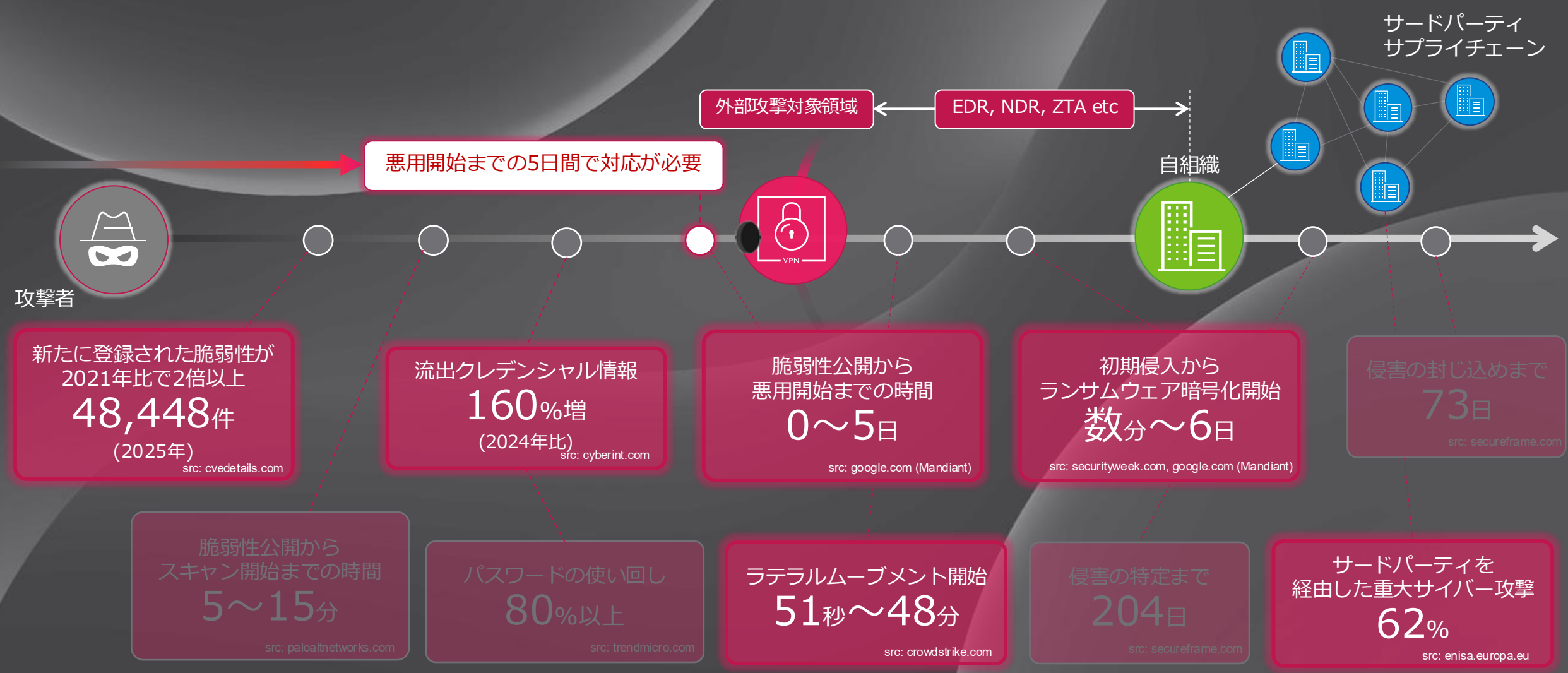
企業の場合は、**全体の**

70~90%

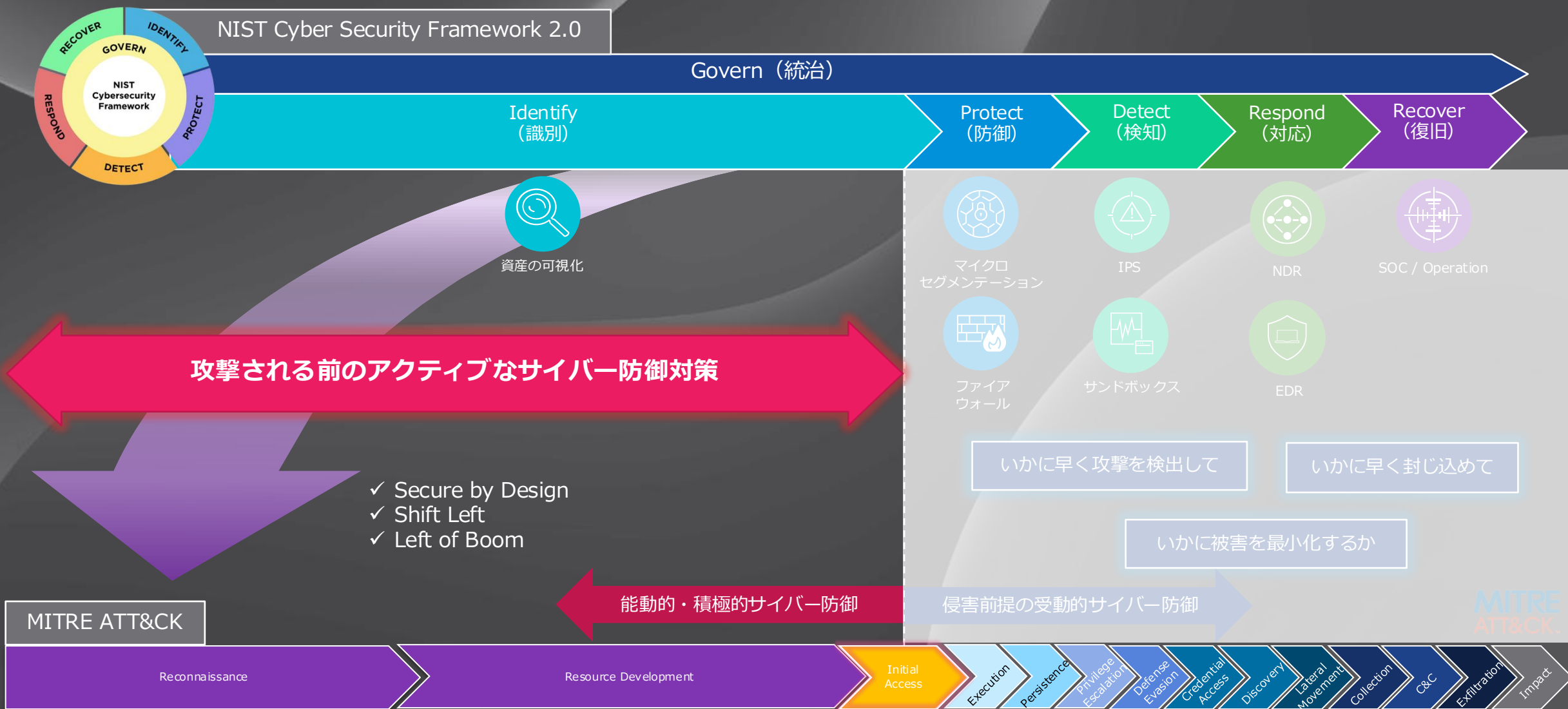
が偶然の結果

*1: Source: <https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime> *2: Source: <https://www.proxyrack.com/blog/global-cybercrime-report-2025/>
*3: Source: <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/> *4: Source: <https://www.ibm.com/jp-ja/reports/data-breach>

侵害前提の受動的サイバー防御の限界



KELAグループの積極的サイバー防御の考え方



KELAグループの積極的サイバー防御の考え方

攻撃開始前に攻撃されない状態にして維持継続

莫大な数の攻撃機会
48,448件
(2025年)

漏洩・窃取された
クレデンシャル情報
160%増

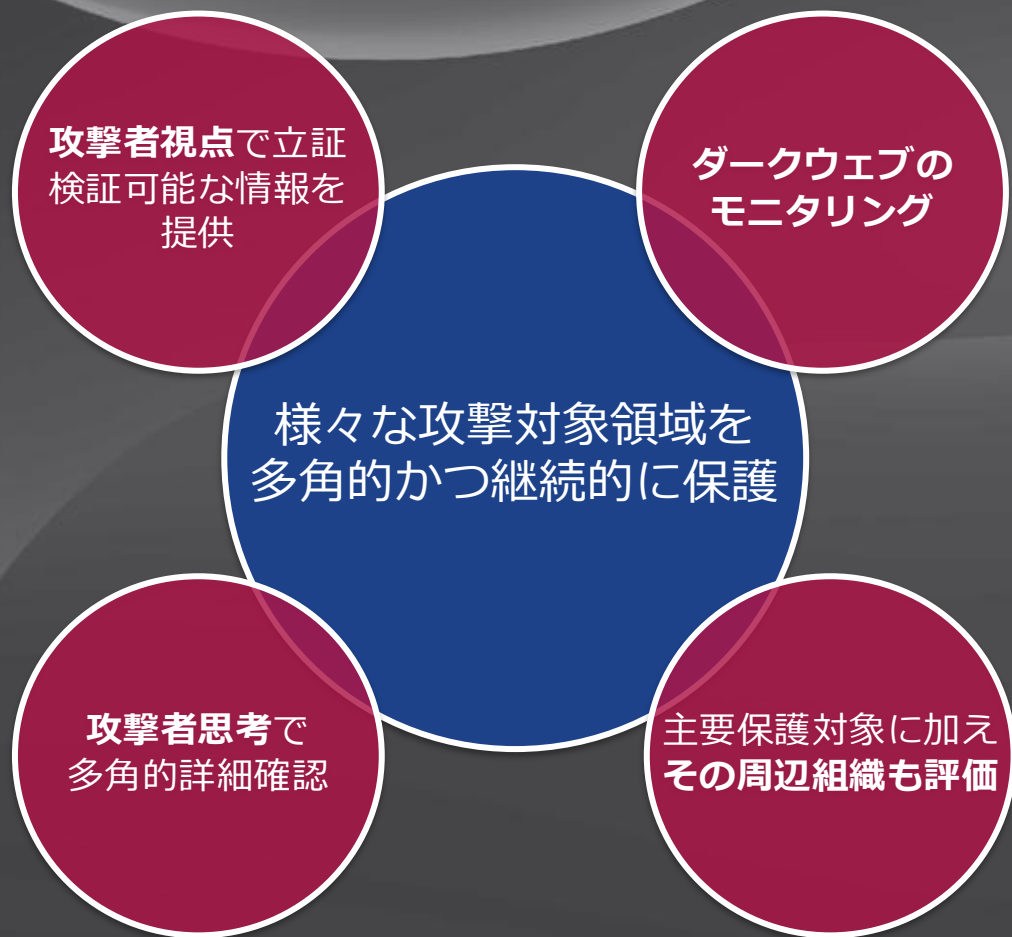
依存した侵害前提の
受動的サイバー防御では
時間的に保護が困難

攻撃機会
+
漏洩クレデンシャル
の併用

サードパーティを
経由した
重大サイバー攻撃
62%

KELAグループの積極的サイバー防御の考え方

攻撃開始前に攻撃されない状態にして維持継続



KELA

流出したアカウント情報をダークウェブをモニター・検出して
乗っ取りなどの悪用を防ぐ



ULTRARED
Continuous Threat Exposure Management

レッドチームによる攻撃者視点と攻撃者思考で、外部からお客様環
境を深層解析し、実践でのトリアージに利用可能な結果を提示



SLING

サードパーティはセキュリティ対策が弱く、主要保護対象との間は、
ビジネスプロセスのための甘い設定のため盲目的に信頼せずに常に
評価する

積極的サイバー防御態勢の必要性



理論的適合性の欠如

- それぞれ異なる攻撃対象領域の解析
- 目的が異なるアラートとその関連性
- 製品オリエンテッドな結果の集合体
- OSINTとアクティブの結果
- サイロ化



サイバー対応態勢の計測と態勢

- 継続的に測定可能な準備態勢
- 実証可能な積極的対応能力
- 継続的な監視と進捗管理
- 定量的な評価軸の確立
- サイロ化からの脱却

サイロ化された積極的サイバー防御機能の結果を、体系的な準備態勢として統合し経営管理に活用

積極的サイバー防御態勢の必要性

KELA



ULTRARED
Continuous Threat Exposure Management

SLING

理論的適合性の欠如

“Active Cyber Readiness” に対応した

- それぞれ異なる攻撃対象領域の解析
- 目的が異なるアラートとその関連性

“Active Cyber Readiness Dashboard” の提供

- OSINTとアクティブの結果
- サイロ化

KELAGROUP

アクティブサイバー経営管理ダッシュボード

サイバー対応態勢の計測と態勢

継続的に測定可能な準備態勢

- 実証可能な積極的対応能力

継続的な監視と進捗管理

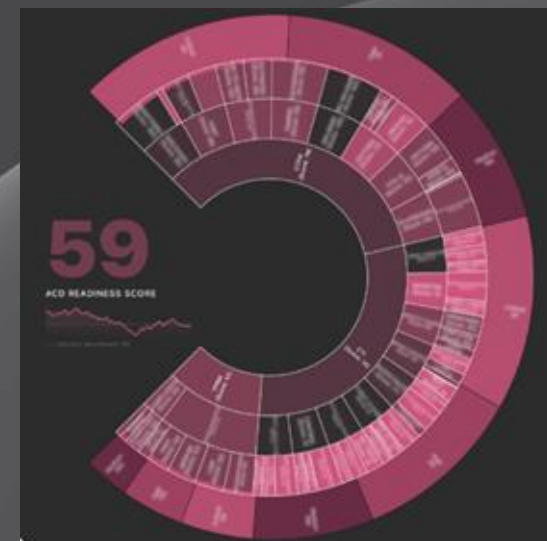
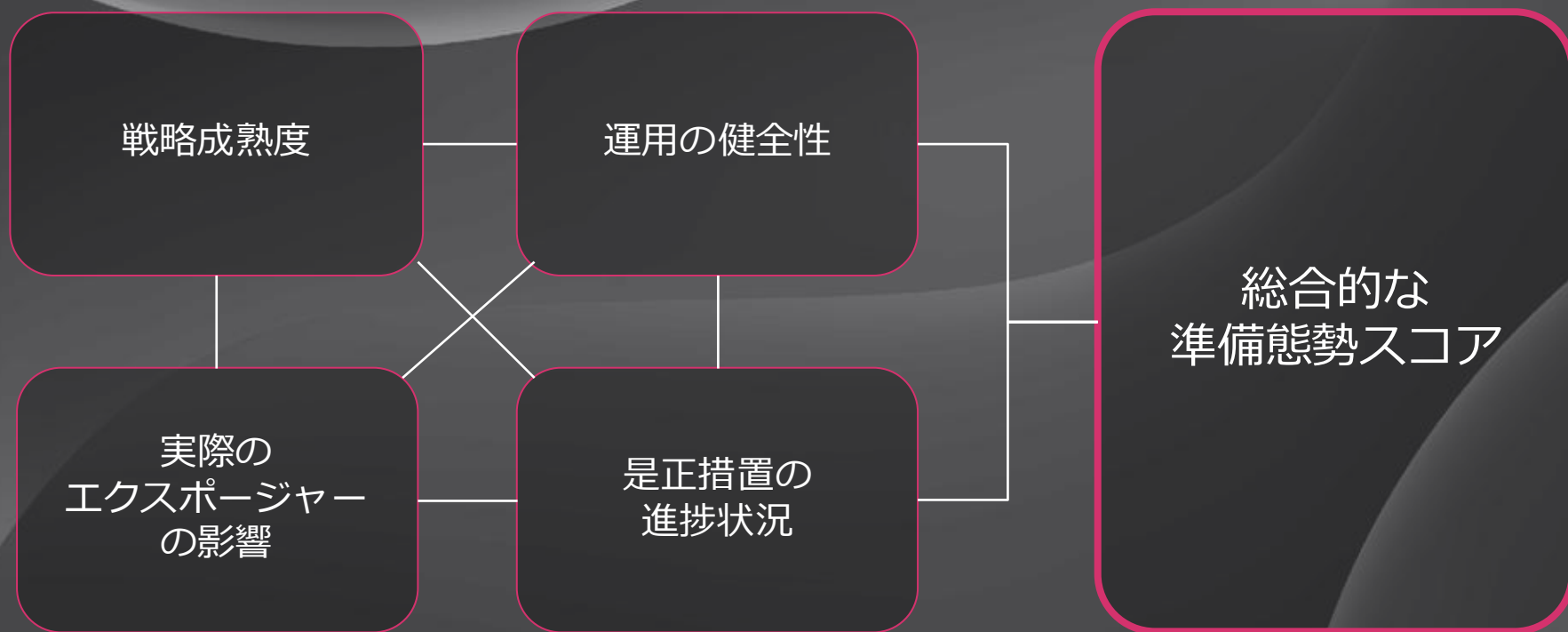
- 定量的な評価軸の確立
- サイロ化からの脱却

サイロ化された積極的サイバー防御機能の結果を、体系的な準備態勢として統合し経営管理に活用

アクティブ サイバー経営管理ダッシュボード

Active Cyber Readiness Dashboard

定量的な積極的サイバー防御準備態勢を経営層に提供



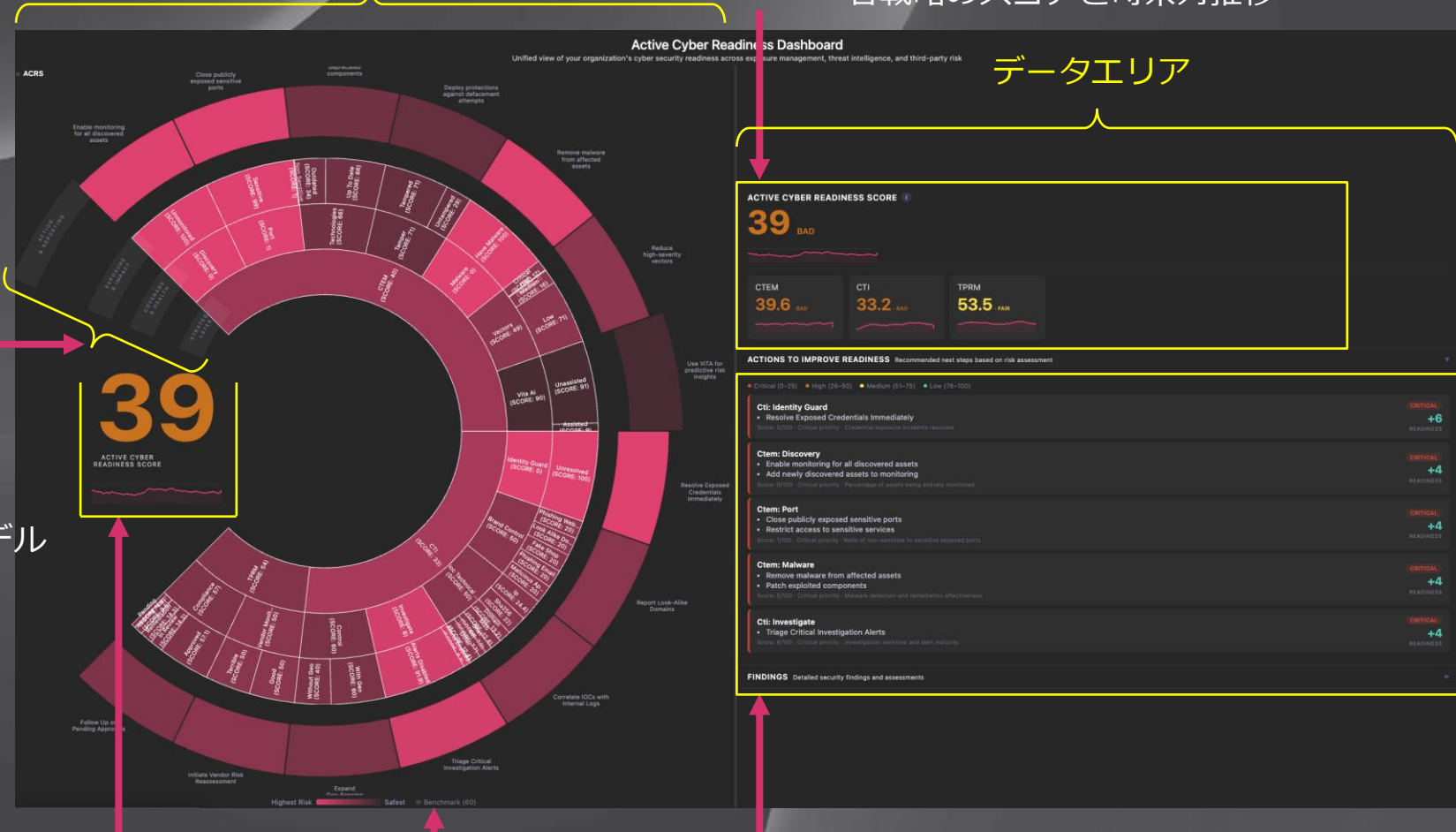
時間の経過に伴って追跡可能（トレンド分析） | 所属業界のベンチマークとの比較 | 事業部門横断で測定可能

アクティブ サイバー経営管理ダッシュボード概要

チャートエリア

- 準備態勢スコアと時系列推移の根拠
- ✓ 各戦略のスコアと時系列推移

- 4層対応エンジン
- ✓ 戦略
- ✓ カバレッジ
- ✓ エクスポーチャー
- ✓ アクション
- を階層接続するドリルダウンモデル



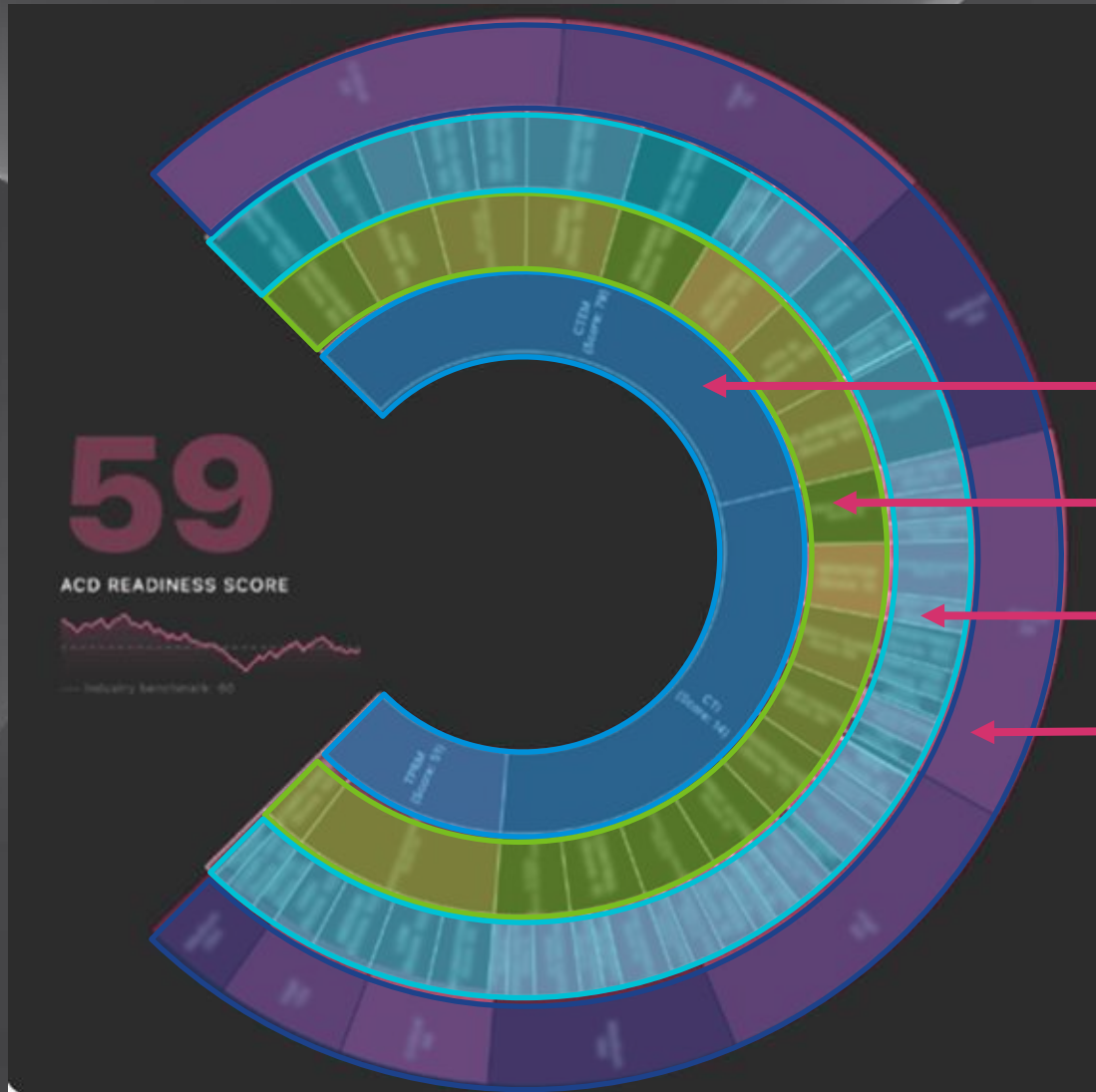
データエリア

- 積極的サイバー防御の準備態勢スコア
- ✓ 全ての領域の総合評価

- 所属業界の平均スコア

- 優先付けされた修復が必要な対応
- ✓ 潜在的な準備態勢スコアへの影響とリスク低減に基づく
- ✓ 定量的な優先度に記述された実行可能な対策

階層化されたドリルダウンモデル



レイヤー1: 戦略 (CTEM, CTI, TPRM)

レイヤー2: カバレッジとその健全性

レイヤー3: エクスపోージャーとインパクト

レイヤー4: アクション

戦略をアクションへとマッピング

レイヤ1: 戦略

組織として積極的サイバー防御の準備態勢としての基盤整備状況の把握

CTI

サイバー脅威インテリジェンス

受動的脅威インテリジェンスと
サイバー攻撃者側を監視

Cyber Threat Intelligence

CTEM

継続的脅威エクスポージャー管理

攻撃者視点と攻撃者思考で、外部から
お客様環境のエクスポージャーを
深層解析

Continuous Threat Exposure Management

TPRM

サードパーティリスク管理

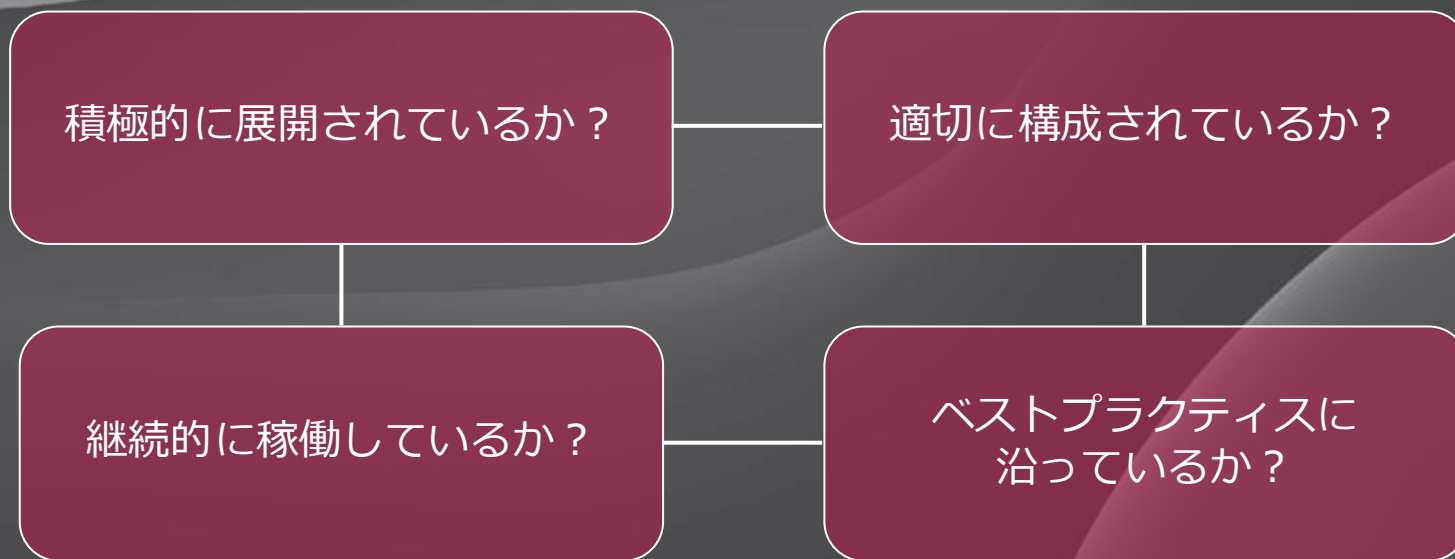
サードパーティ及びサプライチェーン
のリスク評価

Third Party Risk Management

各戦略には、加重されたモジュールのパフォーマンスに基づいて基準スコアが割り当てられ、
これが本規格の中核を形成

レイヤ2: カバレッジとその健全性

組織として、積極的サイバー防御メカニズムの正常稼働確認



スコアリングロジックは、検知機能の利用状況、資産カバレッジ、情報収集の深度、ベンダーコンプライアンスなどを測定

レイヤ3: エクスపోージャーとインパクト

組織の積極的サイバー防御の準備態勢を低下させている要因追求

重大なベクトル？

インテリジェンス
アラート？

サーボパーティの
調査結果

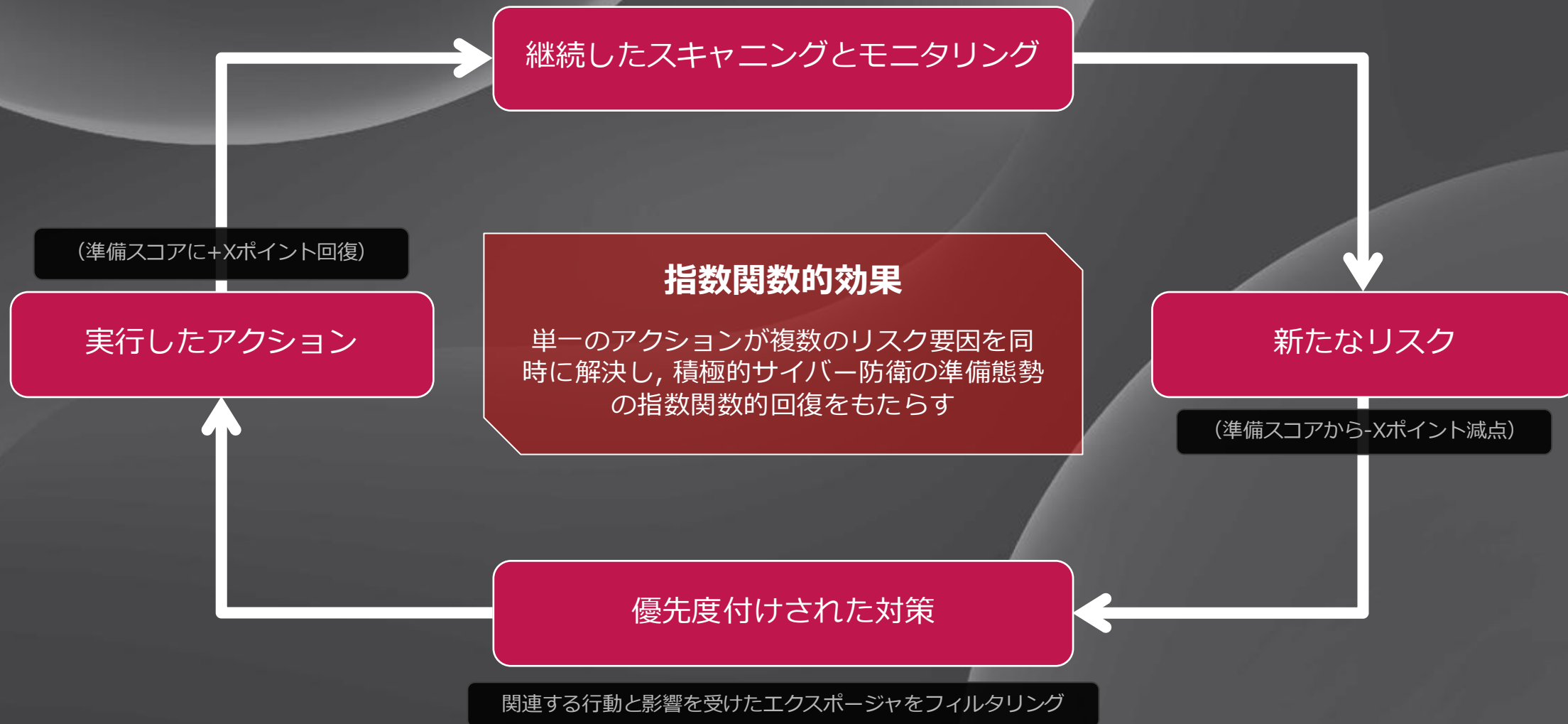
準拠していない
ベンダー？

設定ミス？

監視対象外の資産

エクスపోージャー評価は、実際のリスク影響と規制上の関連性を反映し、
中核となる戦略ベースラインからスコアを減点

レイヤ4: アクション



アクティブサイバー経営管理フレームワーク

積極的サイバー防御態勢は、攻撃対象領域に存在するエクスポージャの各カテゴリを統合
継続的測定から定量的結果を導き出し、優先付けされた脅威の具体的是正へと誘う

	従来のセキュリティプロセス	アクティブサイバー経営管理フレームワーク
データ	孤立したサービスの乱立による、 攻撃機会や脆弱性とアラート	以下を統合 <ul style="list-style-type: none">✓ 継続的脅威エクスポージャー管理✓ サイバー脅威インテリジェンス✓ サードパーティ管理
性質	事後対応型のインシデント追跡	積極的かつ測定・評価可能な対応
影響	抽象的で断片的なリスク指標	脅威となるエクスポージャーを戦略的準備態勢 スコアに直接連動
成果	優先順位付けされていないタスクの無限 リスト.	スコアリング済みで優先付けされた具体的な是 正措置の道筋

まとめ

サイロ化からの脱却

積極的サイバー防御技術を
統合し, 継続的な運用を確認

継続的な可視性

積極的に監視し継続的脅威と
改善の可視化を実現

経営層向け報告

複雑な技術テレメトリを,
先制的な能力を示す
経営層向けの指標に変換

アクティブ サイバー経営管理ダッシュボード (Active Cyber Readiness Dashboard)

デモンストレーション

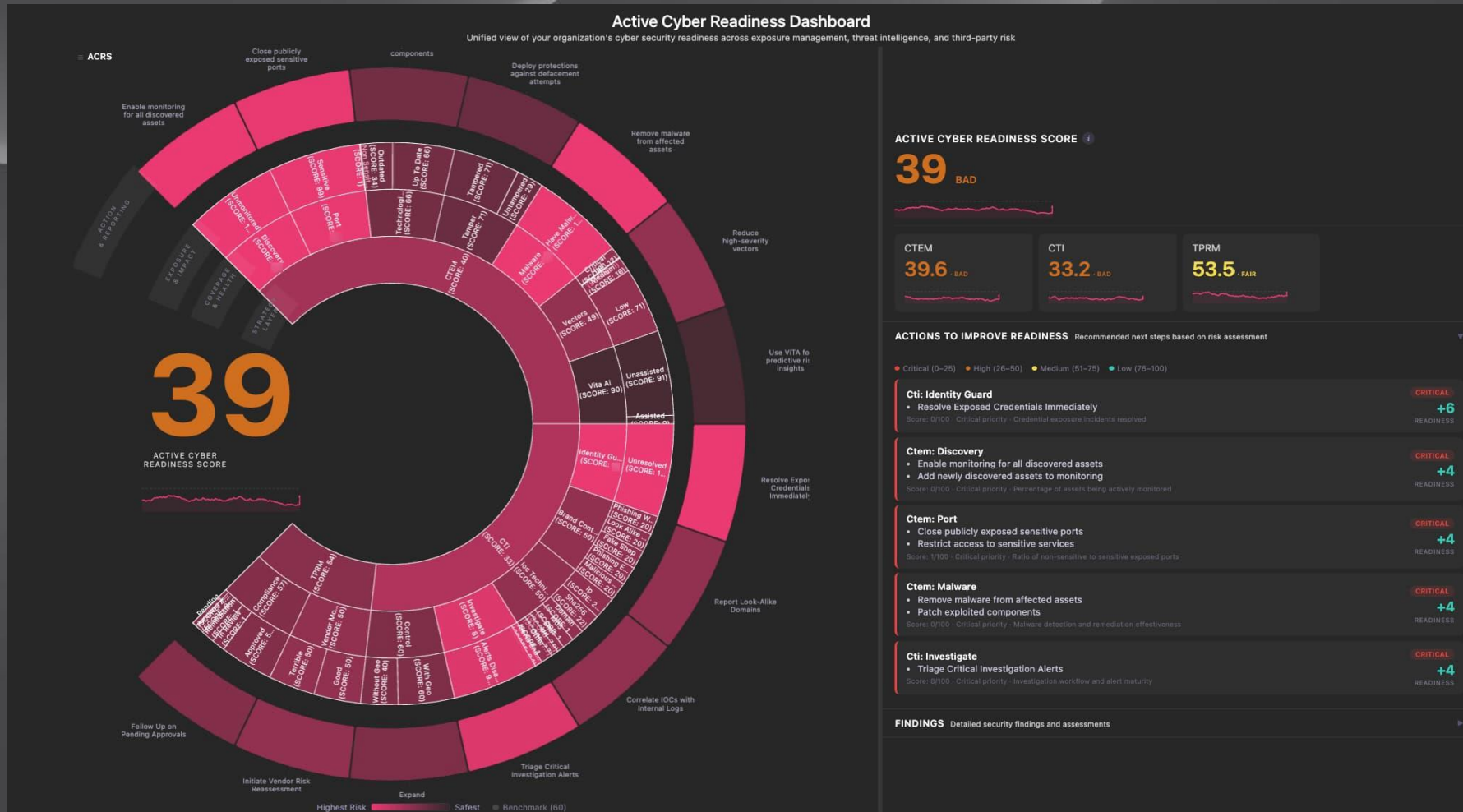
KELAGROUP

KELA

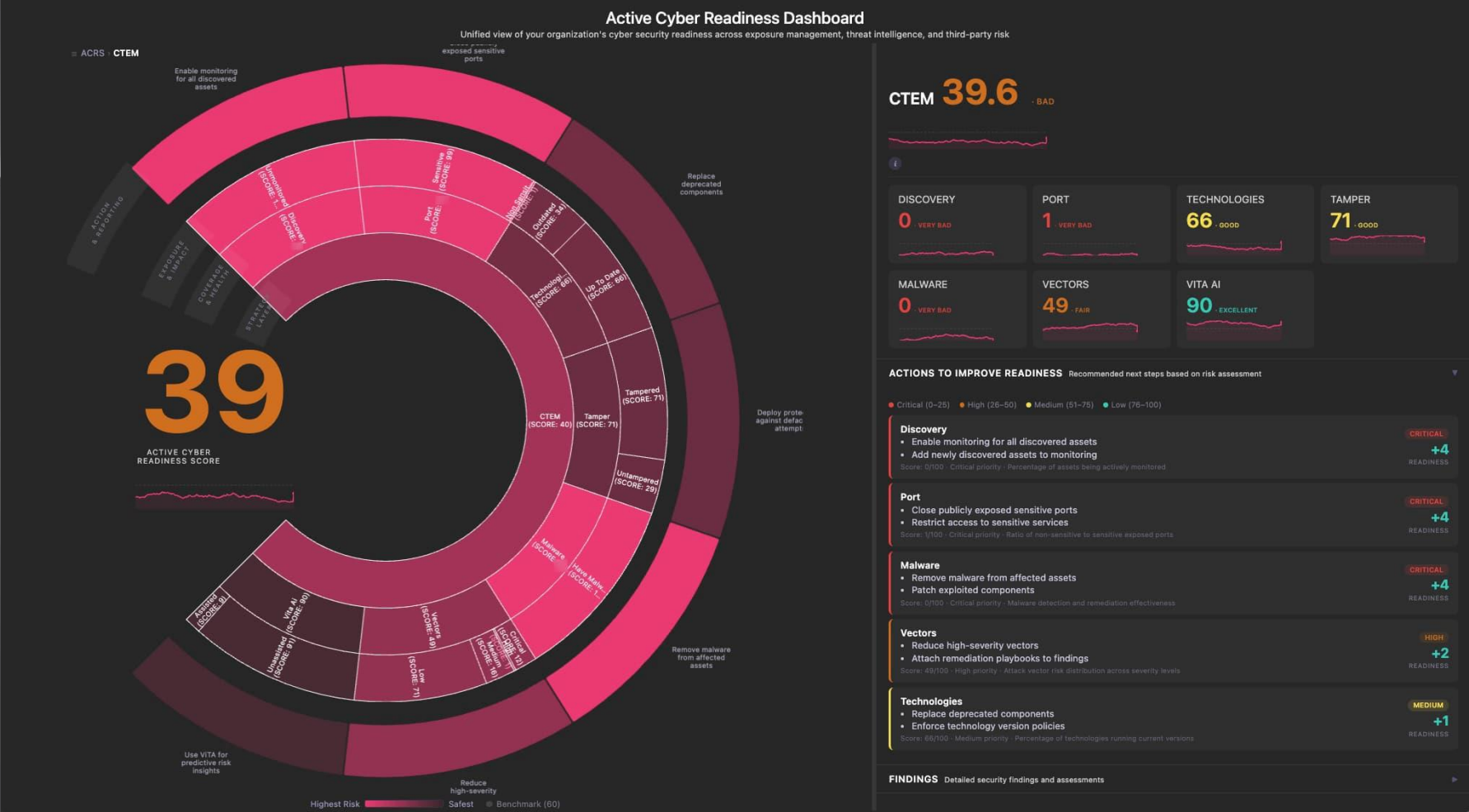


SLING

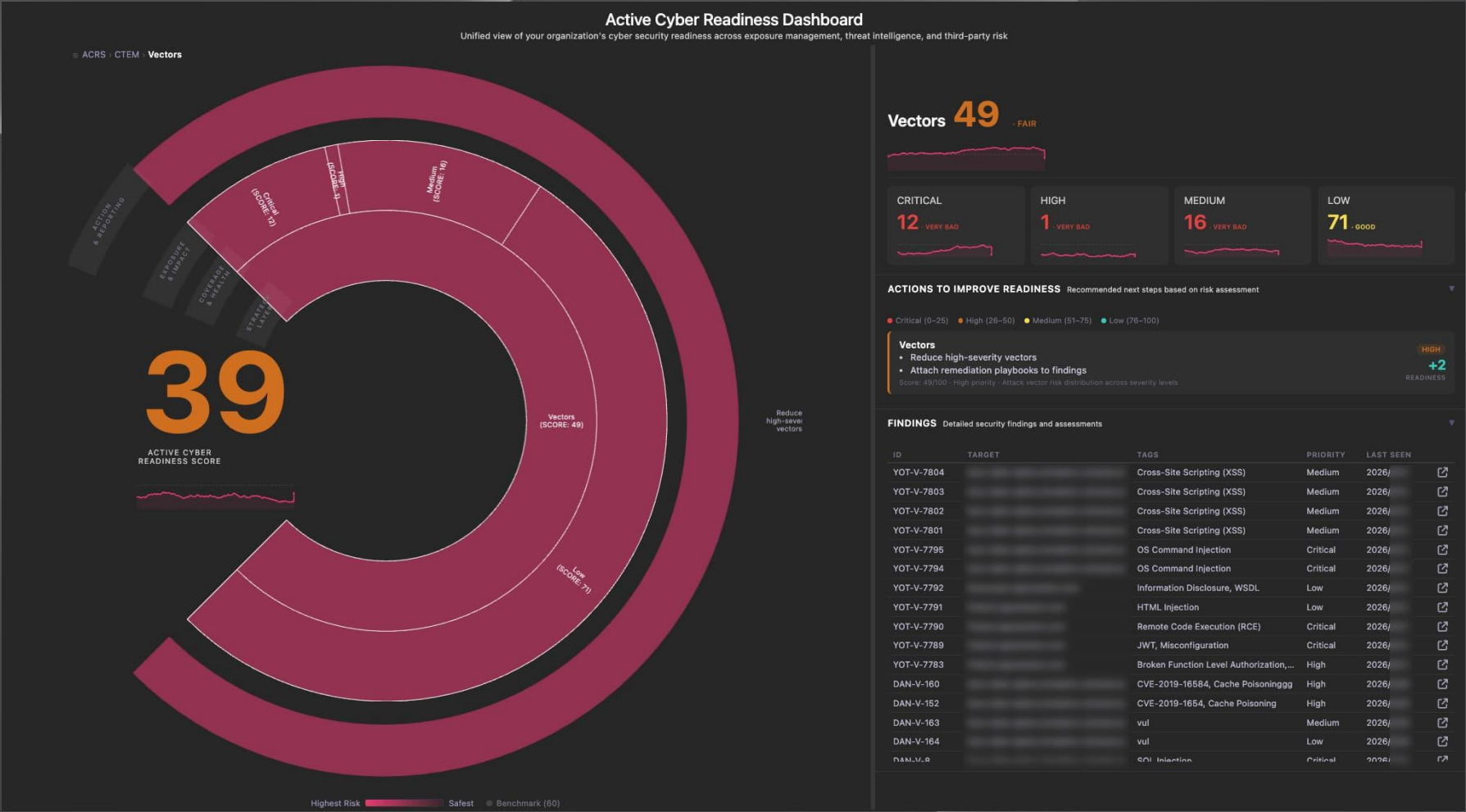
Active Cyber Readiness Dashboard - Portal



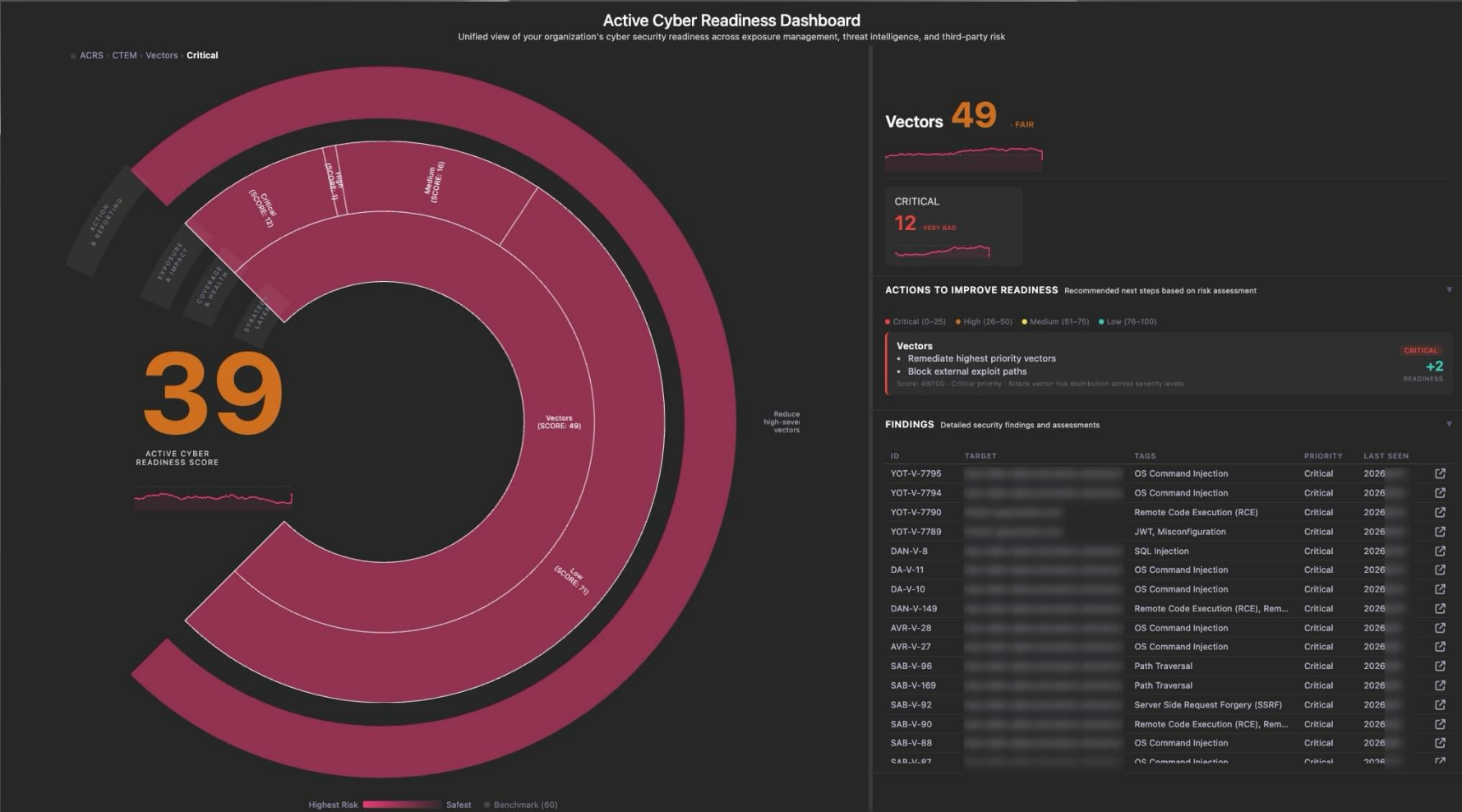
Active Cyber Readiness Dashboard - CTEM



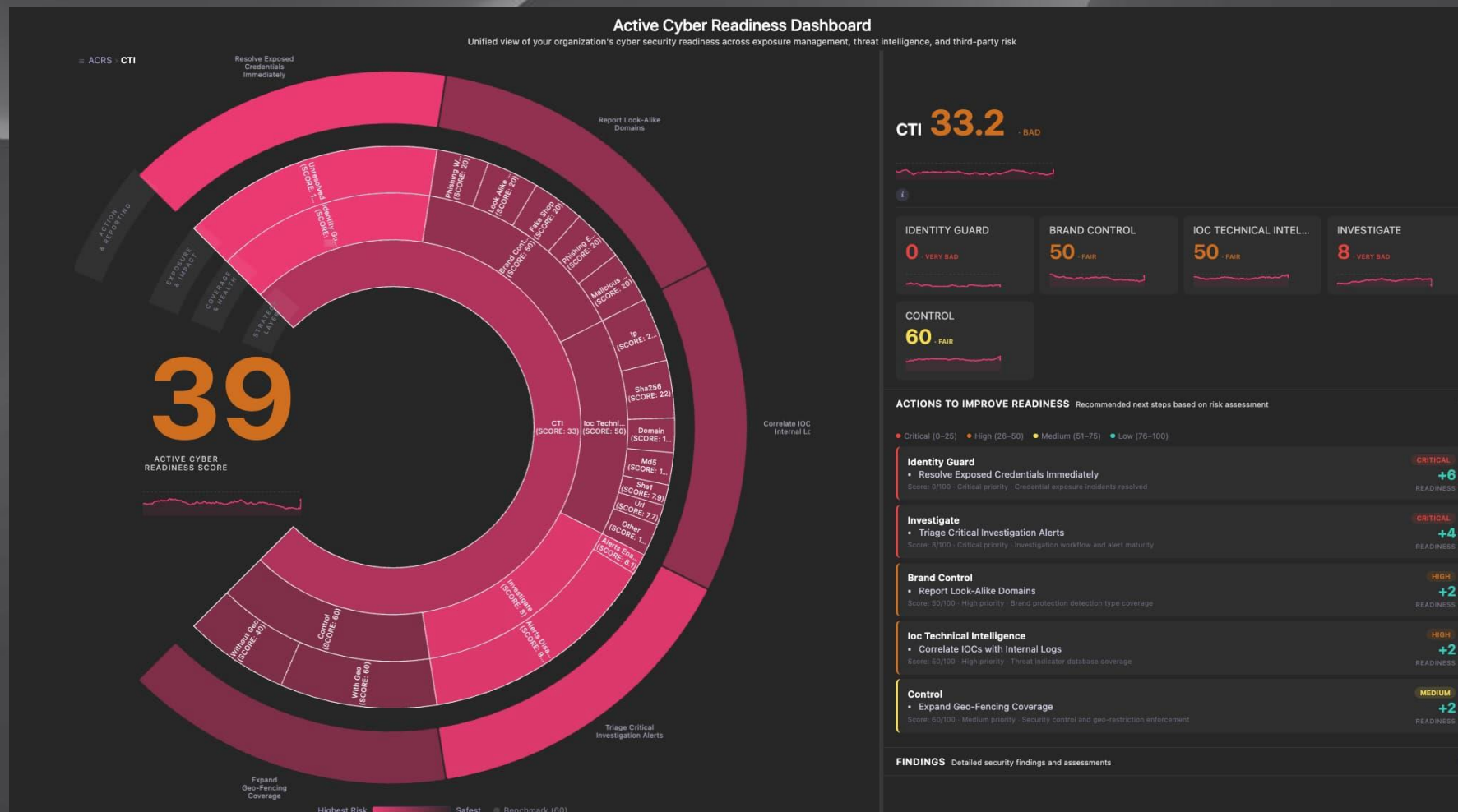
Active Cyber Readiness Dashboard – CTEM Vectors



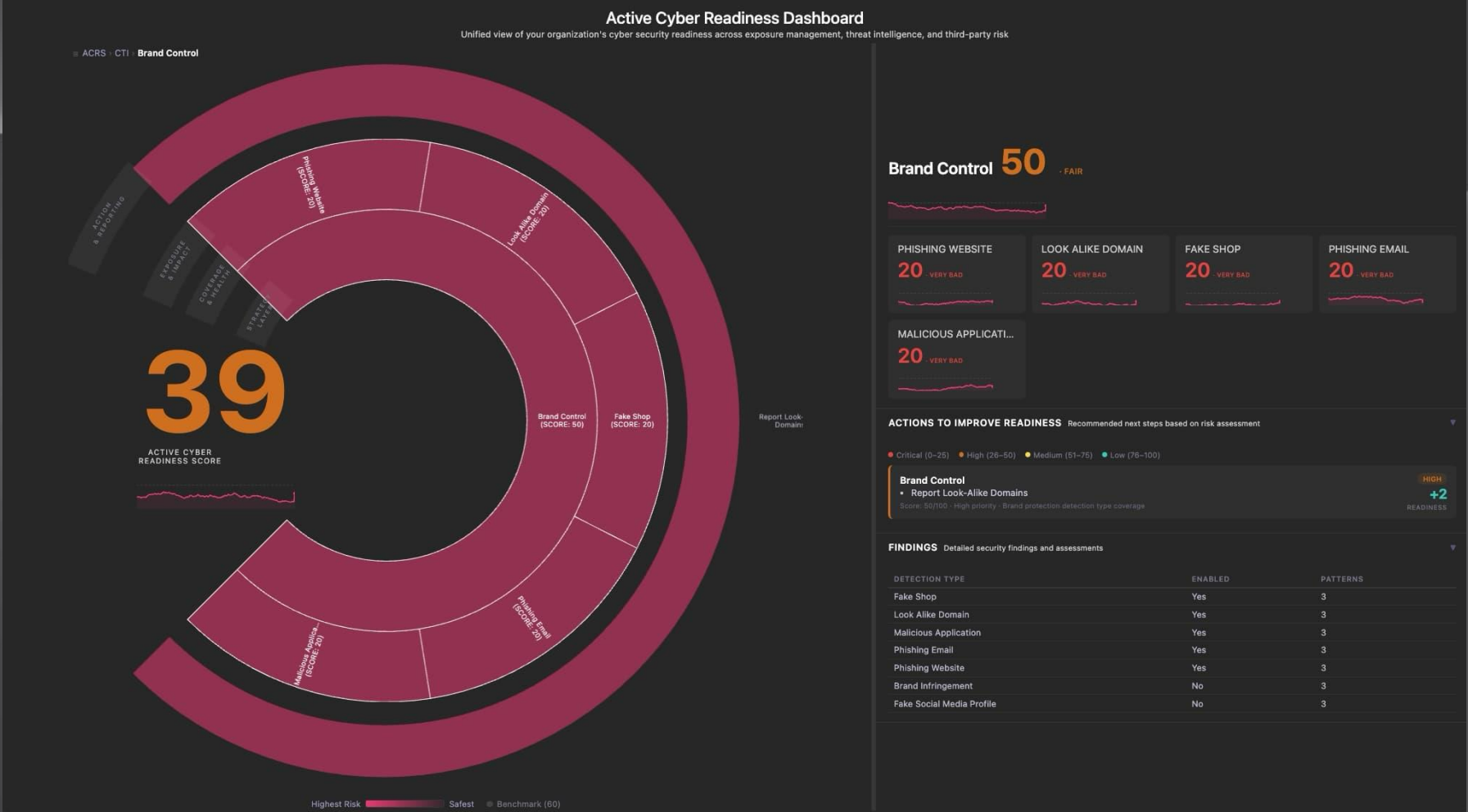
Active Cyber Readiness Dashboard – CTEM Critical Vectors



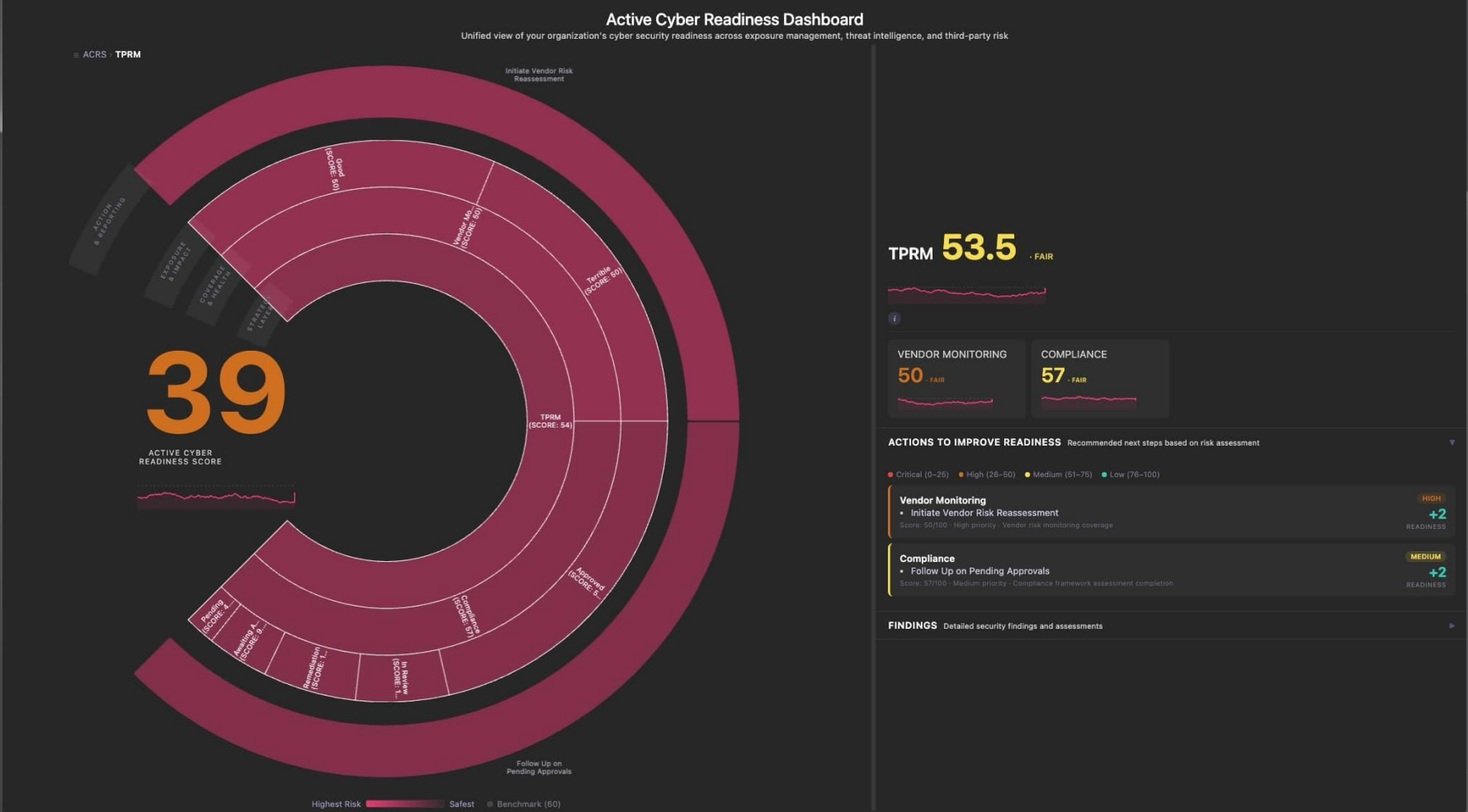
Active Cyber Readiness Dashboard – CTI



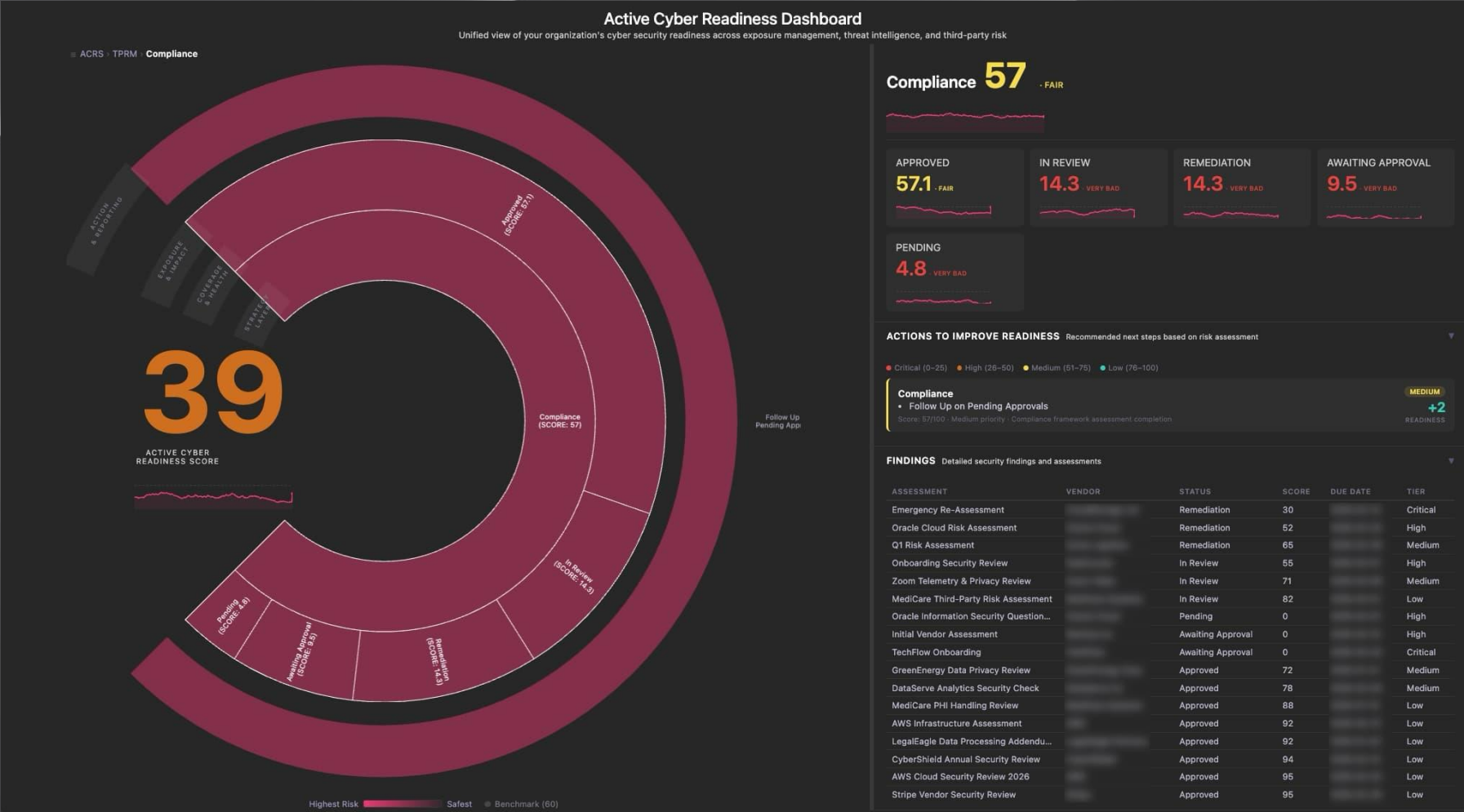
Active Cyber Readiness Dashboard – CTI Brand Control



Active Cyber Readiness Dashboard - TPRM



Active Cyber Readiness Dashboard – TPRM Compliance



アクティブ サイバー経営管理ダッシュボード (Active Cyber Readiness Dashboard)

Thank you.

KELAGROUP

KELA



SLING