CHECK POINT™

EXPOSURE MANAGEMENT

Von Risiken zu echter Resilienz

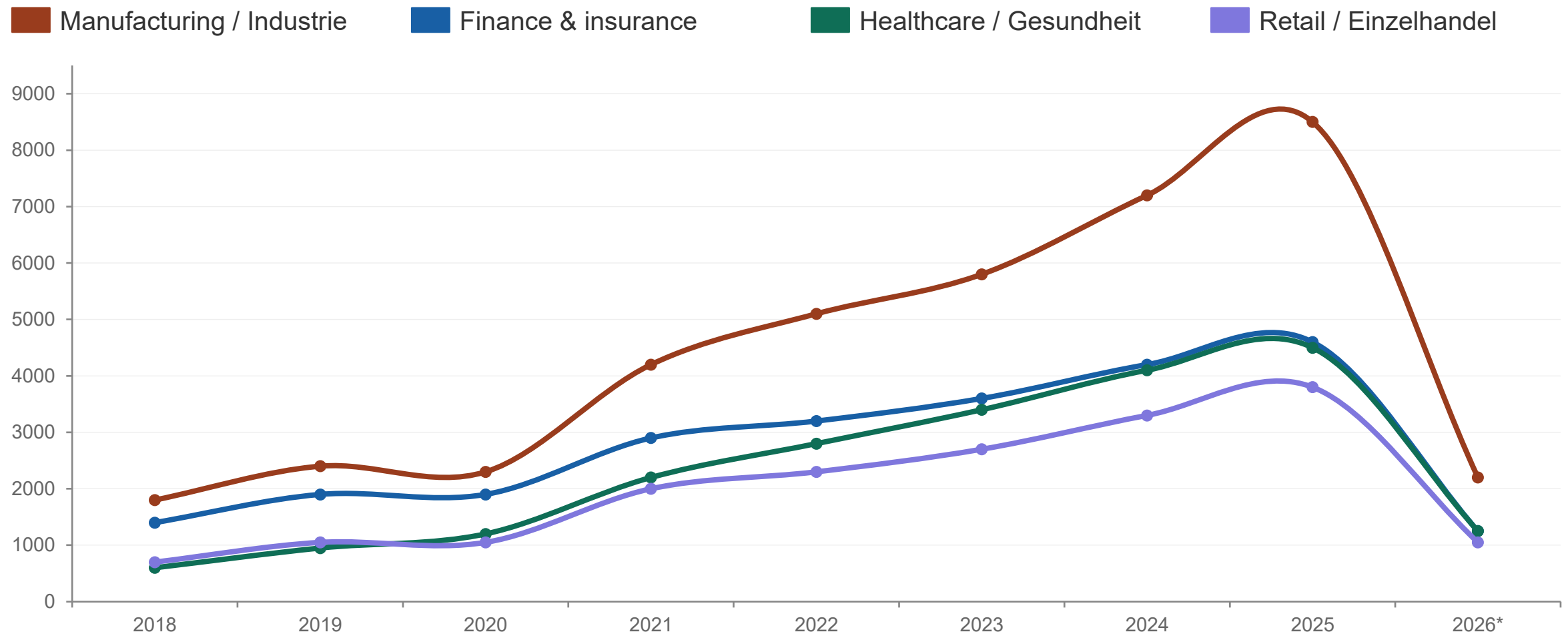
Bernd Knippers & Michael Stichel

Juni 2026

Beobachtungen

Germany - Cyber Breaches by Sector (2018-2026)

Estimated reported incidents · BSI Lagebericht · Bitkom Wirtschaftsschutz · BKA Cybercrime Situationsbericht · 2026 = Q1 only



Manufacturing 2024: ~7,200 (est. incidents)

Finance 2024: ~4,200 (est. incidents)

Healthcare growth 2020–24: +241% (fastest-growing rate)

All-sector 2021 spike: +53% (BSI / Bitkom YoY)

Sources: BSI Lageberichte (2019–2025) · Bitkom Wirtschaftsschutz surveys · BKA Cybercrime Situationsberichte · ENISA Threat Landscape · KonBriefing.com | Estimates derived from sector proportion data applied to BKA total case counts. Germany has no direct ICO-equivalent public dataset.

Cybersicherheit · Gesundheitswesen · Deutschland

Cyberangriffe im deutschen Gesundheitswesen 2026

Betroffene Einrichtungen · Datenabflüsse · Regulatorische Konsequenzen

100.000+
Betroffene Patienten

5+
Kliniken & Dienstleister

4–10 Mio €
Ø Schaden pro Angriff

Chronologie der Vorfälle

Januar – Mai 2026

7. Jan.

Kreisklinik Roth (Bayern)

Externer IT-Einbruch · Notaufnahme kurz geschlossen · LKA ermittelt

22. Feb.

BDH-Klinik Greifswald (M-V)

Ransomware · Komplettausfall Kommunikationsnetz · Datenleck bestätigt

26. März

Patienten-Erpressung (Folge BDH)

Kriminelle nutzen Gesundheitsdaten für gezielte Erpressungs-E-Mails an ehemalige Patienten

14. Apr.

Unimed Abrechnungsservice

Datendiebstahl · 100.000+ Patienten · 6 Uniklinika betroffen

21. Mai

Öffentliche Warnung der Unikliniken

BW-Kliniken informieren: Freiburg, Ulm, Heidelberg, Tübingen

Fallstudie: Unimed Abrechnungsservice

Größter Healthcare-Cybervorfall Deutschland 2026 · April – Mai 2026

ANGRIFF & ABLAUF

Datum	14. April 2026
Ziel	Privatärztliche Verrechnungsstelle (Wadern/Saarland)
Methode	Double Extortion – Verschlüsselung verhindert
Datenabfluss	Ja – Abrechnungs- & Gesundheitsdaten
BSI informiert	16. April 2026
Öffentlichkeit	**22. Mai 2026 (5 Wochen später)**

BETROFFENE KLINIKEN

Uniklinikum Freiburg	**~54.000 Fälle**
Uniklinikum Ulm	**Bestätigt**
Uniklinikum Heidelberg	**Bestätigt**
Uniklinikum Tübingen	**Bestätigt**
UKE Hamburg	**>5.000 Fälle**
Uniklinikum Mainz	**Bestätigt**
Uniklinikum Saarland	**~1.200 Fälle**

GESAMT: Über 100.000 betroffene Datensätze Bundesweit · BSI & Landesdatenschutzbehörden ermitteln

Strukturelles Versagen

Warum deutsche Kliniken so verwundbar sind

70%

nennen fehlende Finanzmittel als Haupthindernis

82%

europäischer Kliniken sehen Cyberrisiko als hoch oder extrem

10%

haben realistische Cyber-Notfallübungen durchgeführt

59%

trauen sich 24h ohne elektronische Patientenakte zu

€

Budget-Engpass

70% der Kliniken fehlen Mittel für angemessene IT-Sicherheit

Fachkräftemangel

1/3 der Kliniken hat offene IT-Sicherheitsstellen, die nicht besetzt werden können

Supply-Chain-Risiko

Angriffe auf Dienstleister (Unimed) treffen Kliniken ohne direkten Einbruch

NIS2-Lücke

Nur 11.000 von 29.500 betroffenen Unternehmen bei BSI registriert (März 2026)

PROJEKT GLASSWING · PROGNOSE

Das Zeitfenster schließt sich.

KI-gestützte Bedrohungen entwickeln sich schneller als Verteidiger reagieren können.

STAND: JUNI 2026

SCHLÜSSELZAHLEN · APRIL – JUNI 2026

10.000+

kritische Schwachstellen gefunden (1 Monat)

<1%

davon bisher gepatcht – Patch-Pipeline ist der Engpass

6–12 Mo.

bis Angreifer gleichwertige KI-Modelle haben

89%

mehr KI-gestützte Angriffe 2026 (CrowdStrike)

Powered by Claude Mythos Preview (nicht öffentlich verfügbar)

In 6–12 Monaten haben Angreifer dieselben Fähigkeiten.

Anthropic warnt: Andere Anbieter werden Mythos-ähnliche Modelle entwickeln – wahrscheinlich ohne gleichwertige Sicherheitsvorkehrungen.

JETZT

Der Engpass verschiebt sich

KI findet Schwachstellen schneller als Teams sie patchen können. Weniger als 1% der 10.000+ Befunde sind bisher geschlossen. Disclosure, Verifizierung und Deployment sind der neue Flaschenhals.

6–12 MONATE

Demokratisierung der Angriffswerkzeuge

Billige, schnelle KI-Modelle mit Angriffsfähigkeiten werden verfügbar – möglicherweise ohne Safeguards. KI-gestützte Angriffe stiegen bereits um 89%. Frequenz und Unvorhersehbarkeit steigen weiter.

AB ENDE 2026

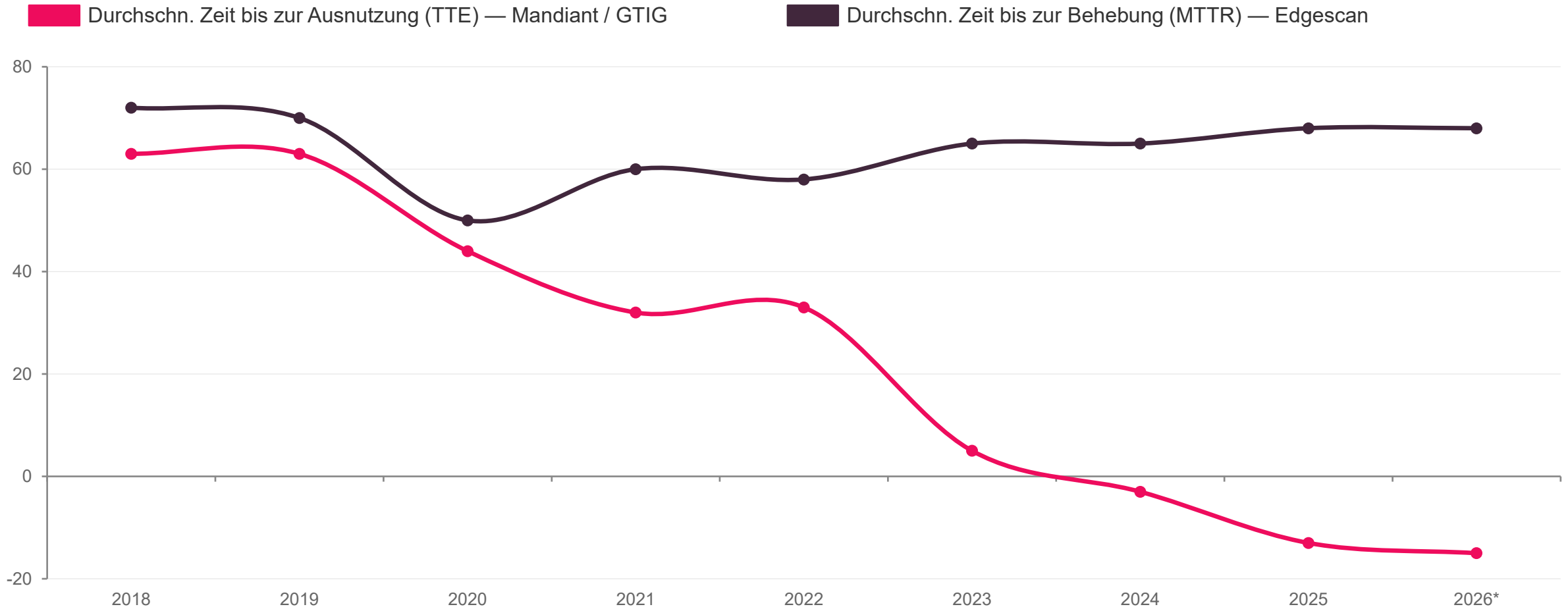
Irreversible Schutzlücke

Unternehmen ohne KI-native Verteidigung bauen eine Lücke auf, die sie nicht mehr schließen können. Ein schwerer Angriff auf kritische Infrastruktur könnte über 100 Mio. Menschen treffen.

Quelle: Anthropic Project Glasswing Update, CyberScoop, Dataconomy – Juni 2026

Durchschnittliche Zeit bis zur Ausnutzung vs. Zeit bis zur Behebung

Tage ab Bekanntgabe der Schwachstelle – 2018 bis 2026 · Negativer TTE = Ausnutzung bevor ein Patch existiert



Quellen: Mandiant / Google GTIG M-Trends 2022–2026 · Edgescan Vulnerability Statistics Reports 2020–2025 · 2026* = Schätzung für Teiljahr · Negativer TTE = Ausnutzung vor Verfügbarkeit des Patches

Pollfrage #1

The Modern CISO Challenge

In the Era of Agentic Attackers

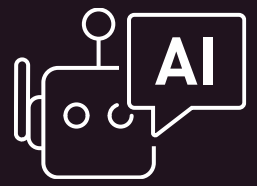
01

The CVE Flood

29,000+

CVEs published annually — impossible to patch them all

- Zero-day exploits are weaponized before any patch exists
- Agentic AI compresses Mean Time To Exploit (MTTE) from weeks to hours
- Mean Time To Remediate (MTTR) remains 60+ days — Mythos widens this gap to a critical breach window



02

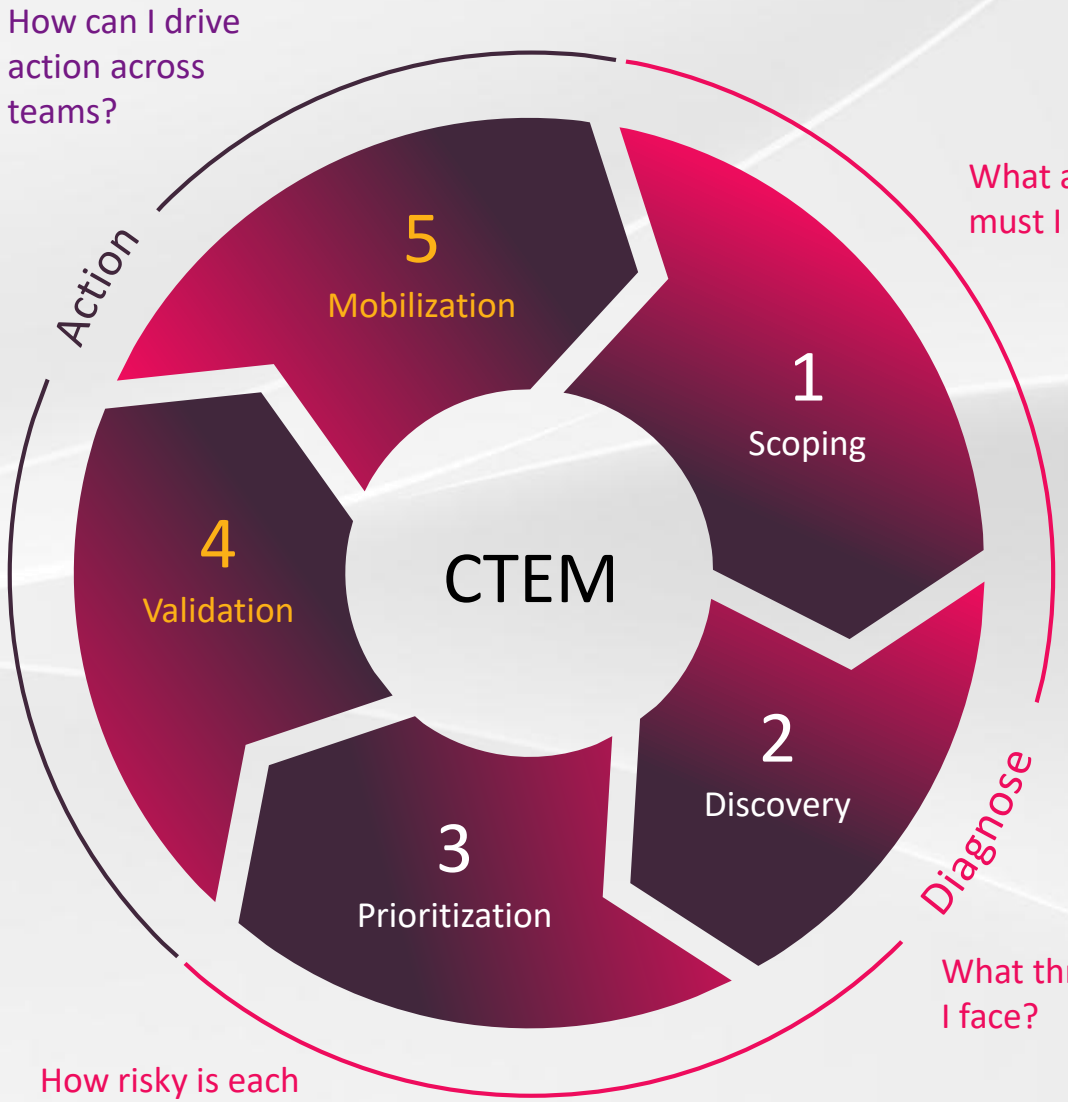
The Agentic Attacker Era

AI-Native

- Security stacks built for human-speed threats are inadequate against agentic attackers
- AI attackers auto-discover and chain exploits at machine speed
- Traditional perimeter defenses cannot model autonomous threat behavior

Continuous Threat Exposure Management (CTEM) Framework

An holistic framework created by Gartner to address exposure across complex, multi-team environments



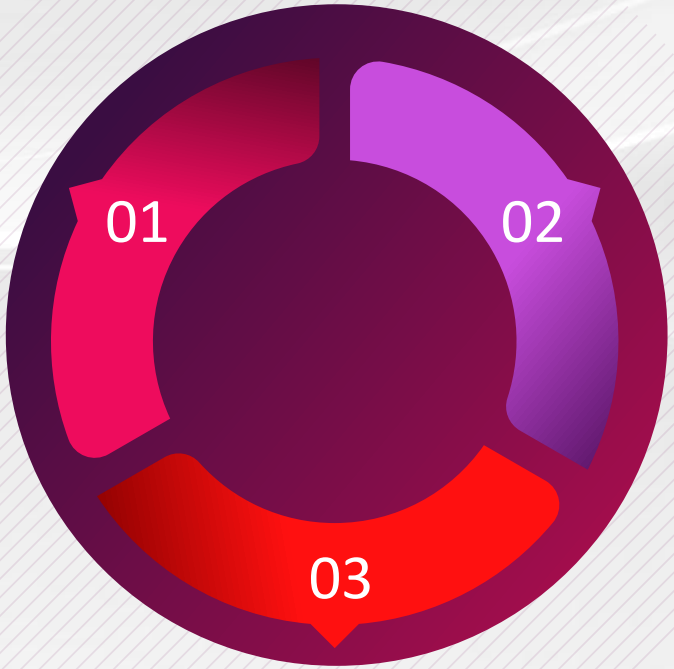
EXPOSURE
MANAGEMENT

Exposure Management:

Intelligence-led, Remediation-driven

A Unified Capability Across the Full CTEM Cycle with 3 Main Elements

THREAT INTELLIGENCE



EXPOSURE PRIORITIZATION

SAFE REMEDIATION

Exposure Management:

Intelligence-Led. Remediation-Driven.

Continuous Assessment & Prioritization

1 Threat Intelligence

Intelligence That Shows What's Being Weaponized

+ Attacker Tools and Infrastructure
+ Campaign and Dark Web Intel
+ Brand Impersonation Signals

2 Exposure Prioritization

Prioritization That Reflects Real Risk

+ Misconfigurations of internal & external assets
+ Deduplications and False Positives
+ Unpatched vulnerabilities across network, OS-level, apps

3 Safe Remediation

Remediation You Can Enforce With Confidence

+ Security Controls
+ Attacker Infrastructure
+ 3rd party, ITSM and collab. tools

1

Threat Intelligence

Check Point Telemetry Is A Structural Advantage

100K+

Check Point Firewalls deployed worldwide. Every blocked connection, C2 attempt, and scanning IP

200M+

Emails scanned daily. Phishing infrastructure, malicious senders, weaponized domains and attachments.

3,700,000,000
Websites and files inspected

146,000,000
Full content emails

86,000,000
File emulations

20,000,000
Potential IoT devices

1,700,000
Malicious indicators

1,800,000
Newly installed mobile apps

3,700,000
Online web forms

IPs
Domains
URLs
File Hashes

THREATCLOUD AI

1 2 3

Pollfrage #2

1

Threat Intelligence

2

Exposure Prioritization

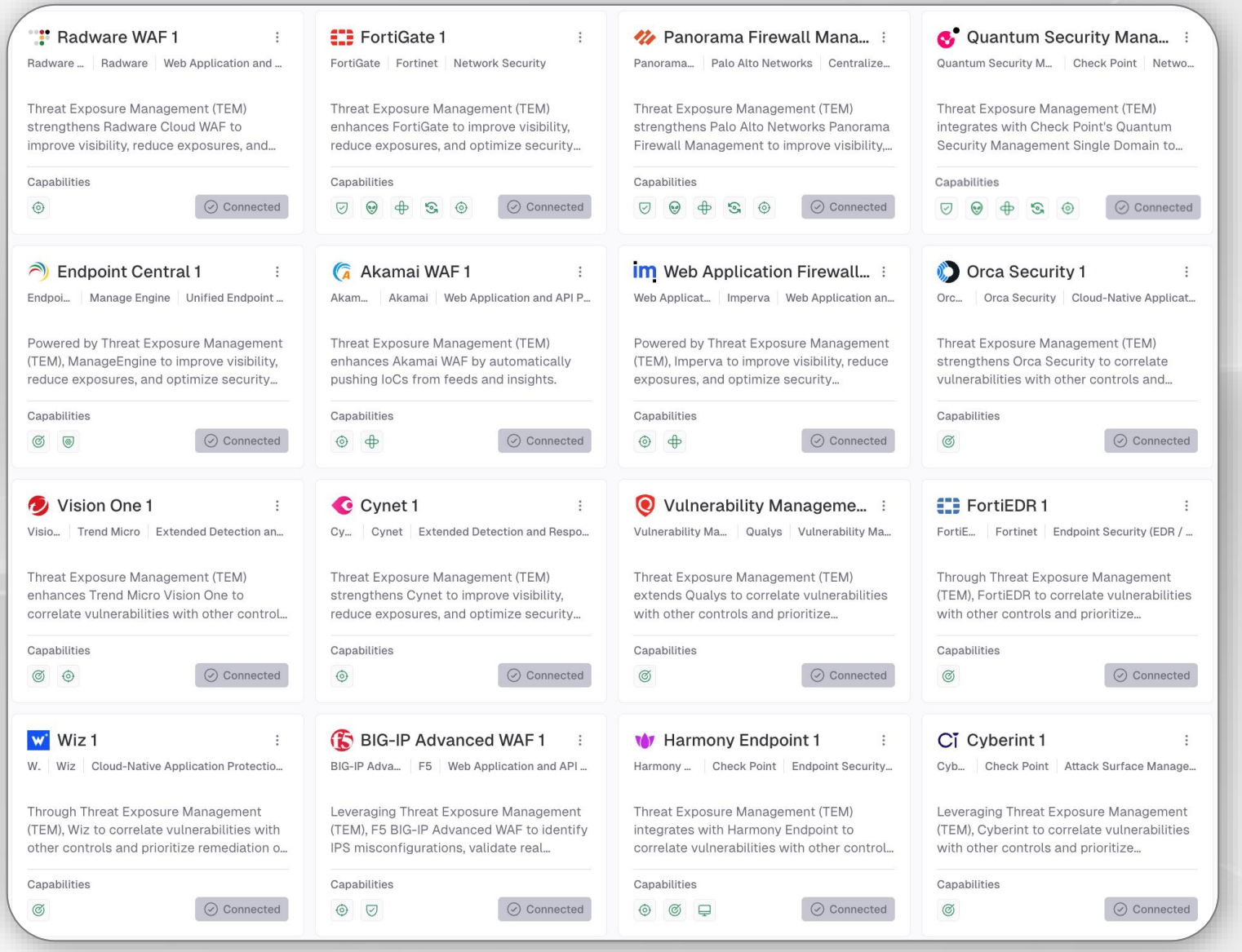
3

Connect All Company Systems

OVER 150 INTEGRATIONS

Coverage across
IT & security vendors:
Network, Endpoint, Cloud, Email, Identity,
OS and more…

- Bi-Directional API integration
- No agents needed

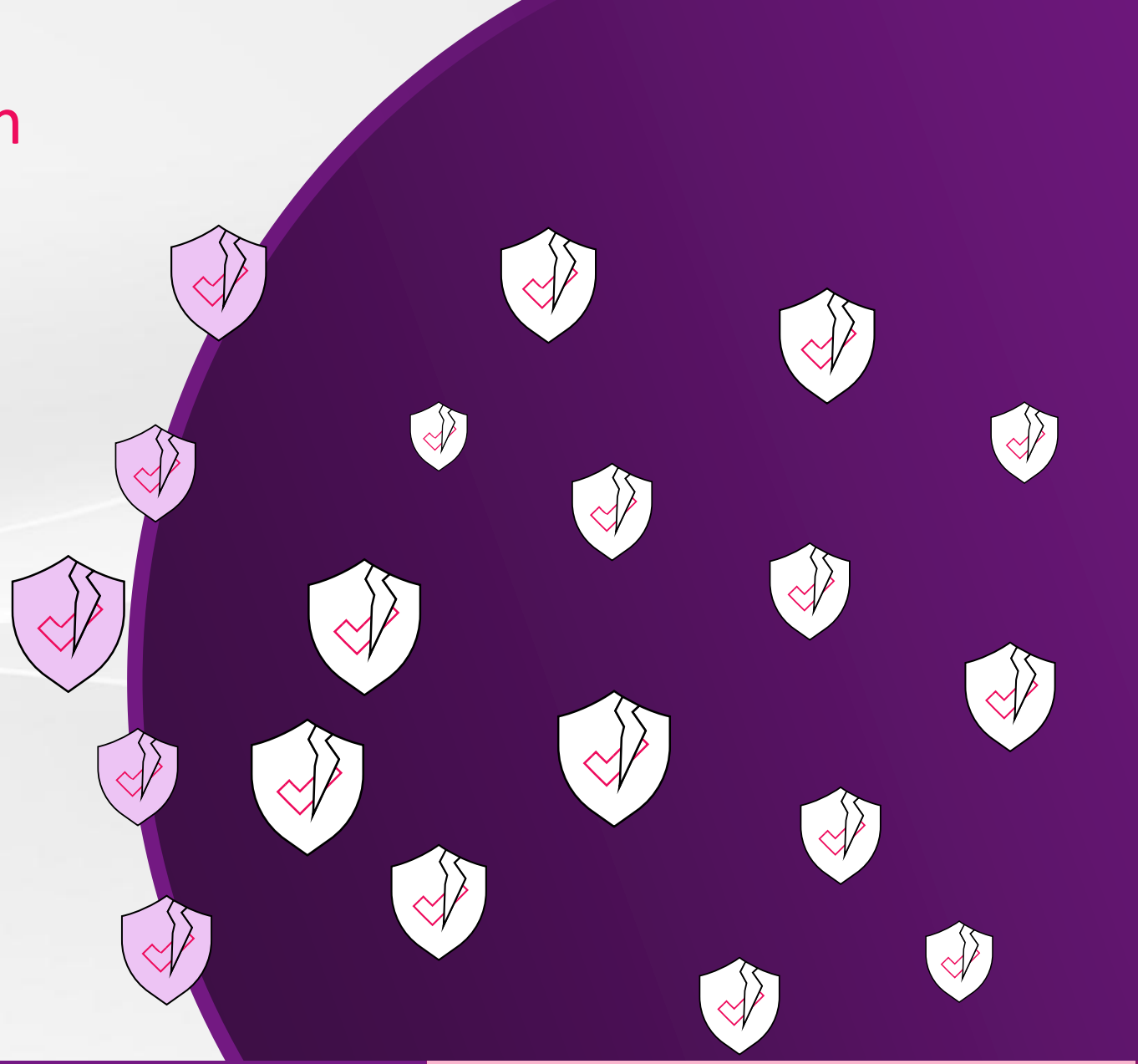


Vulnerability & Misconfiguration
Discovery

1) External ASM

2) Connect to existing vulnerability Scanners

Discover Internal network & endpoint vulnerabilities



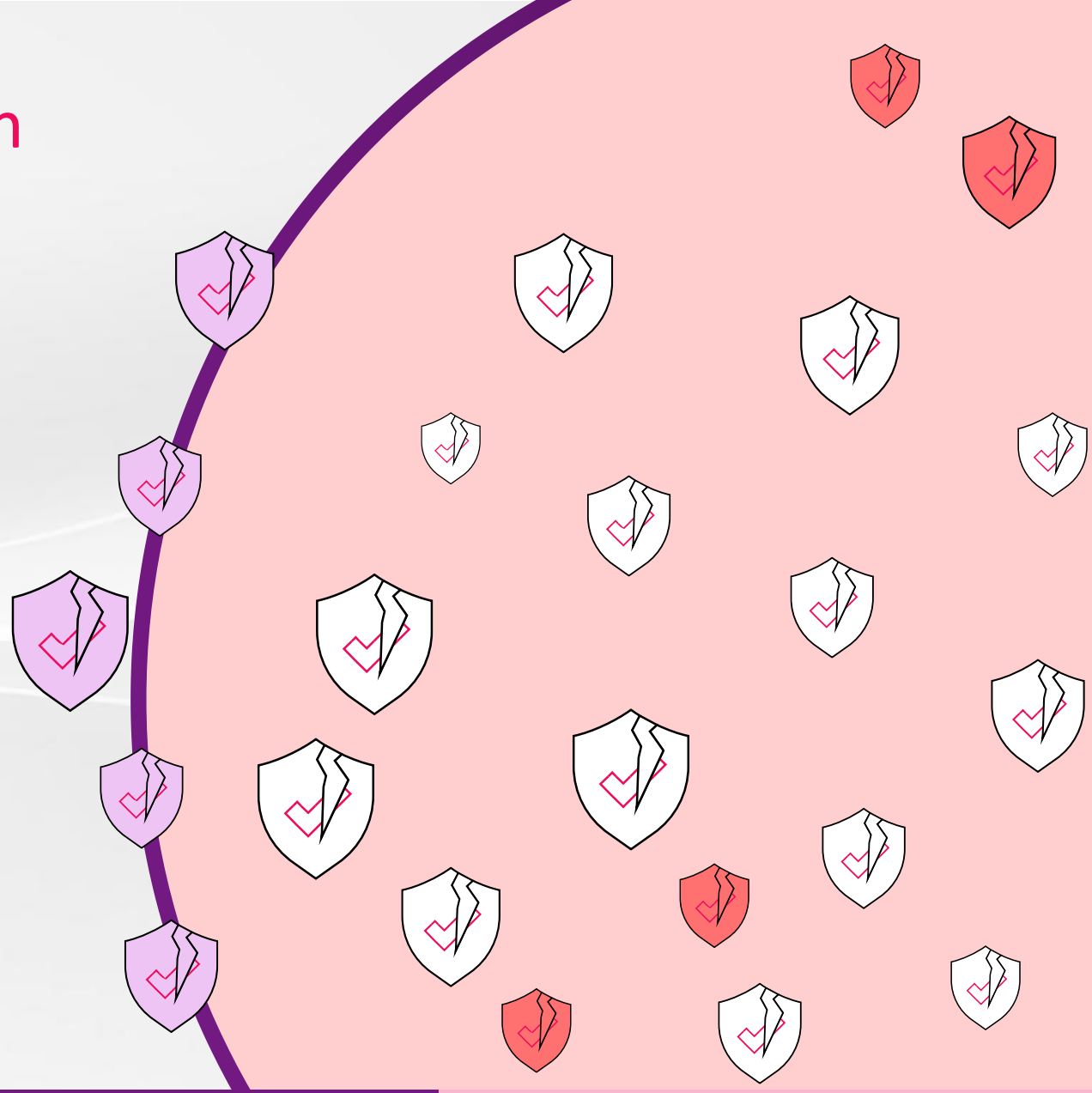
Vulnerability & Misconfiguration
Discovery

1) External ASM

2) Connect to existing vulnerability Scanners

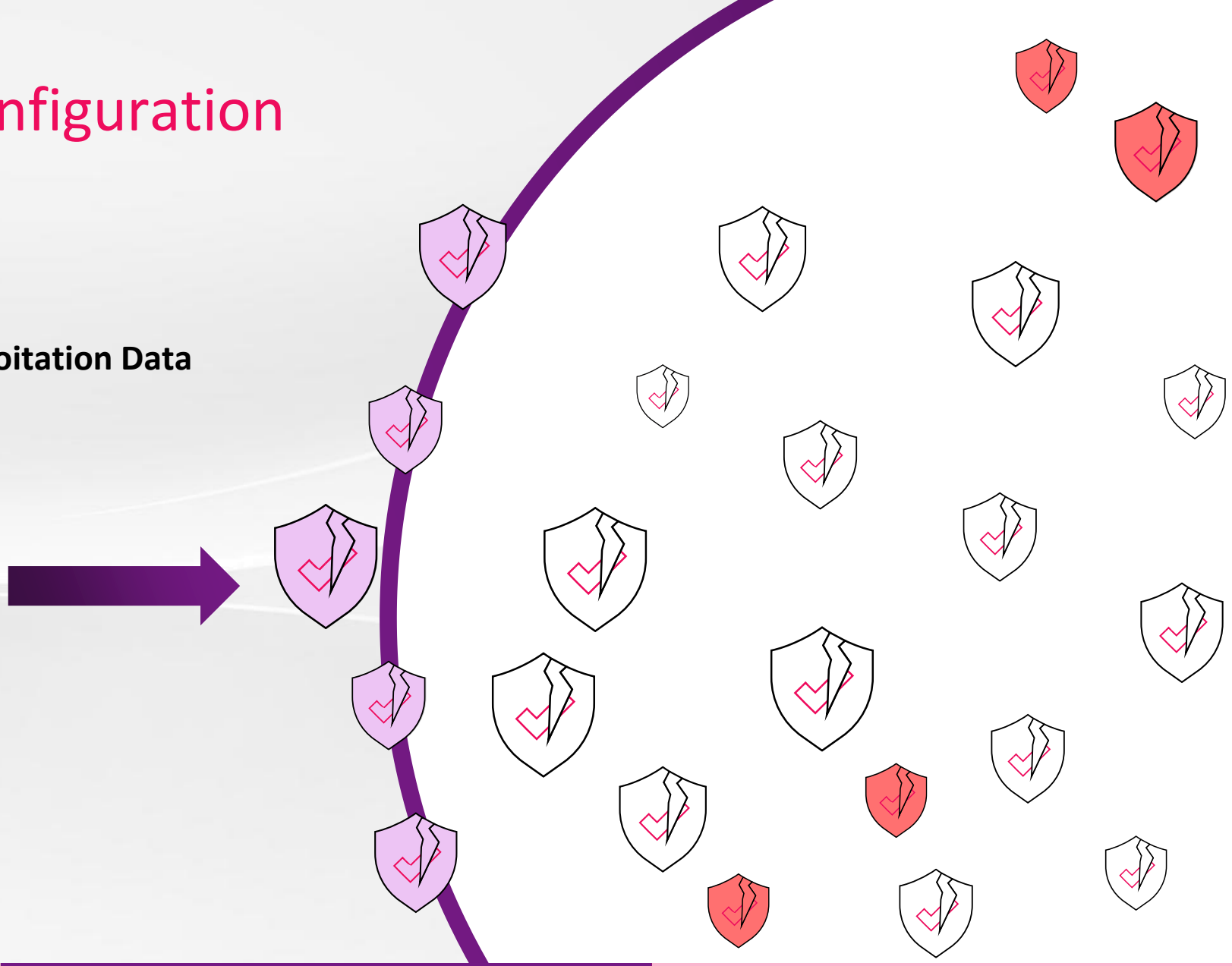
3) CAASM Based Discovery

- Discover assets not covered by scanners
- Extract CVEs based on software inventory
- Find agent coverage gaps (EDR, MDM) or misconfigurations
- Identify assets with non authorized software
- Discover out of policy users (no MFA)



Vulnerability & Misconfiguration
Prioritization

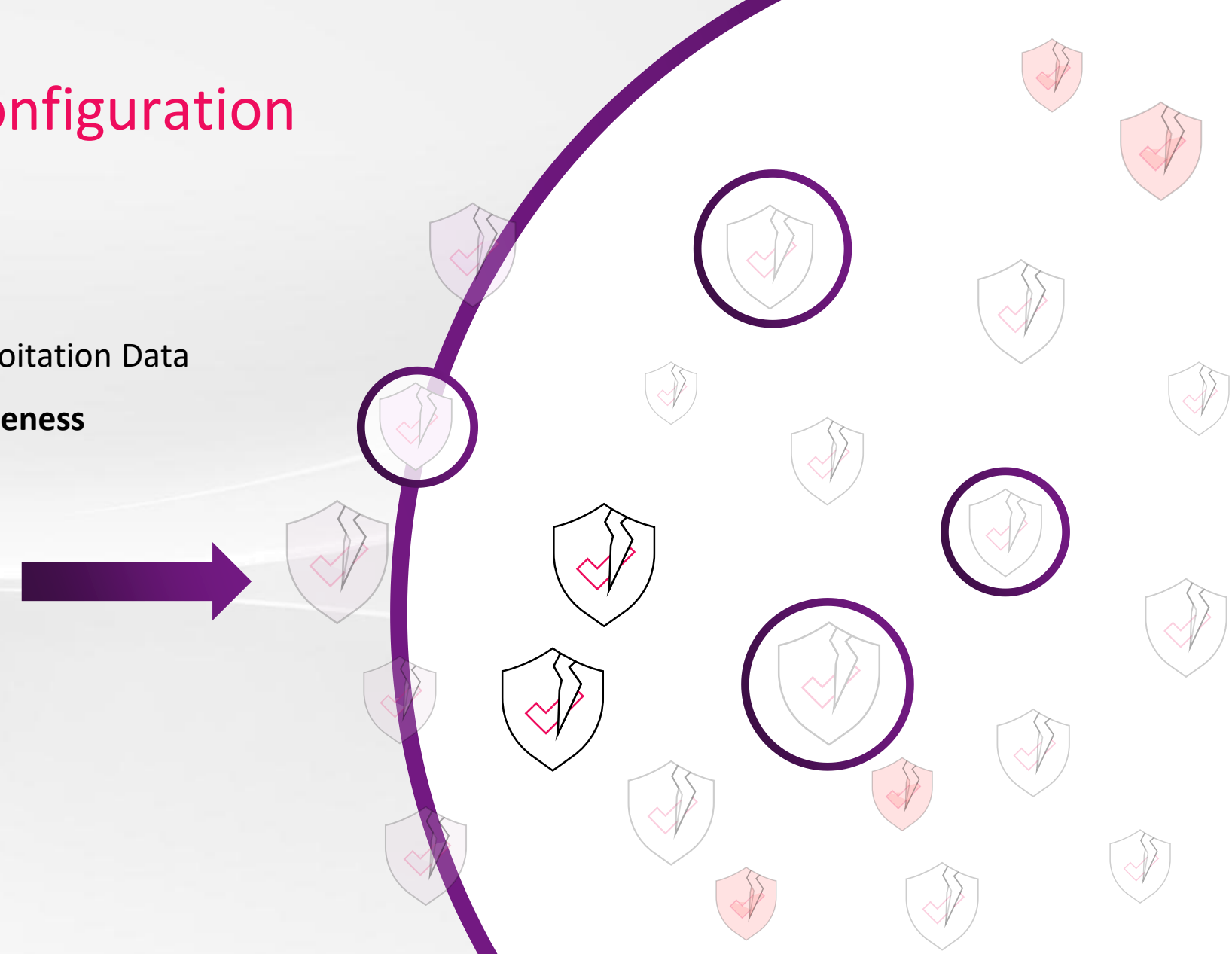
1) Augment Intelligence & CVE Exploitation Data



Vulnerability & Misconfiguration
Prioritization

1) Augment Intelligence & CVE Exploitation Data

2) Existing Security Control Effectiveness

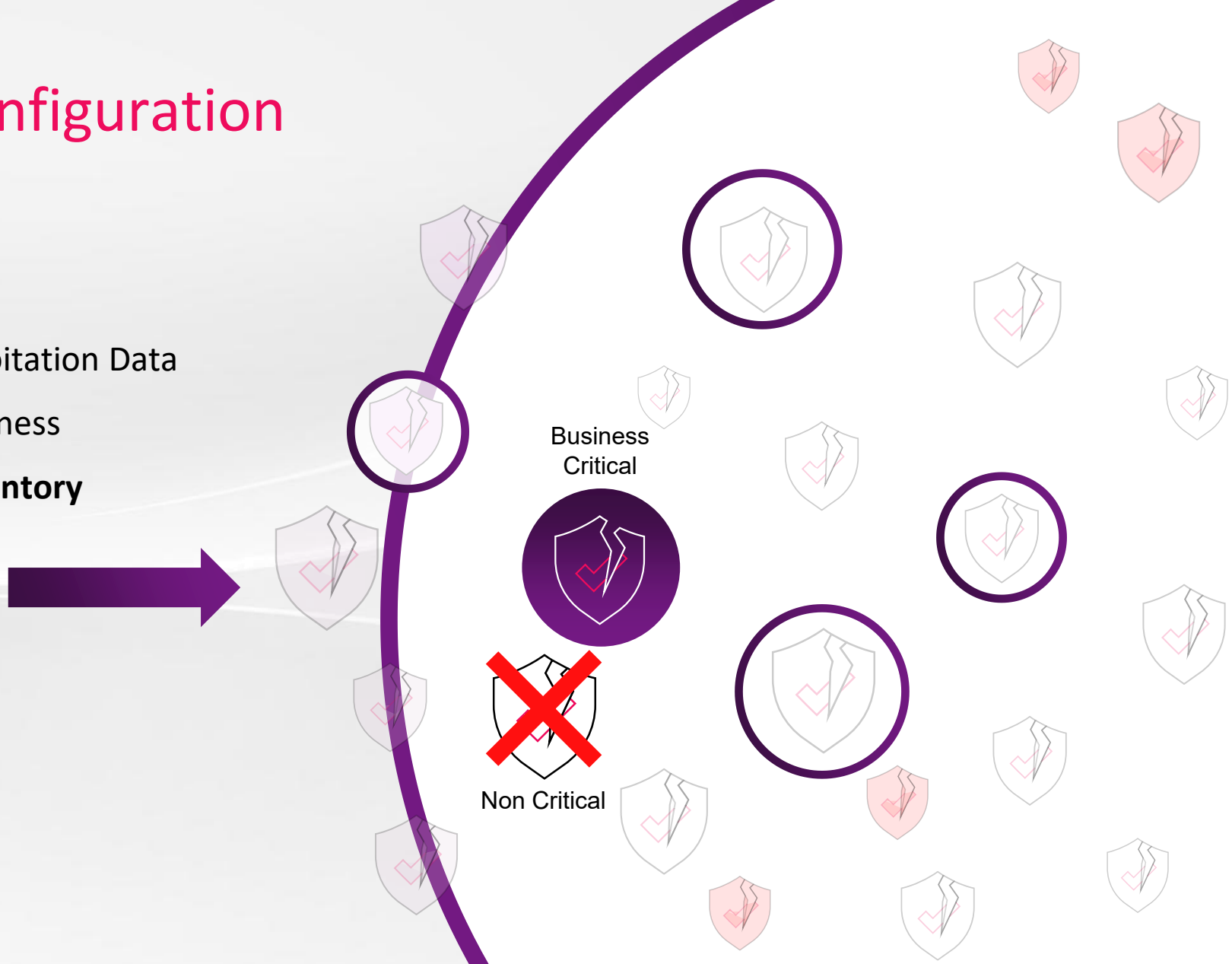


Vulnerability & Misconfiguration
Prioritization

1) Augment Intelligence & CVE Exploitation Data

2) Existing Security Control Effectiveness

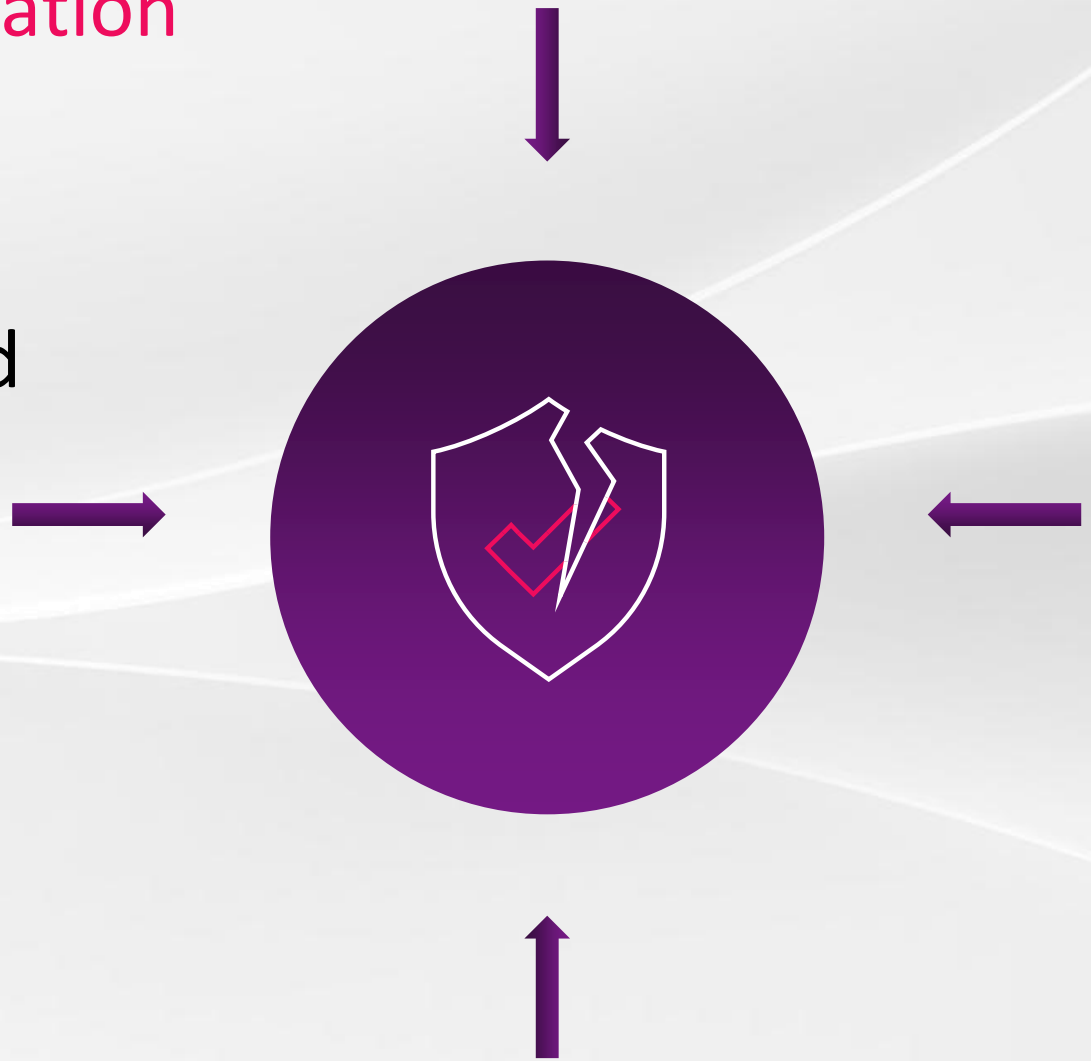
3) Business Context from Asset Inventory



Vulnerability & Misconfiguration

Prioritization

Prioritized & Contextualized
Remediation plan



1 2 3

Exposure Prioritization

- Prioritization of Vulnerabilities & Misconfigurations of Internal & External Assets
- Correlating against Existing Security Controls across Network, Endpoint & Application

1

Threat Intelligence

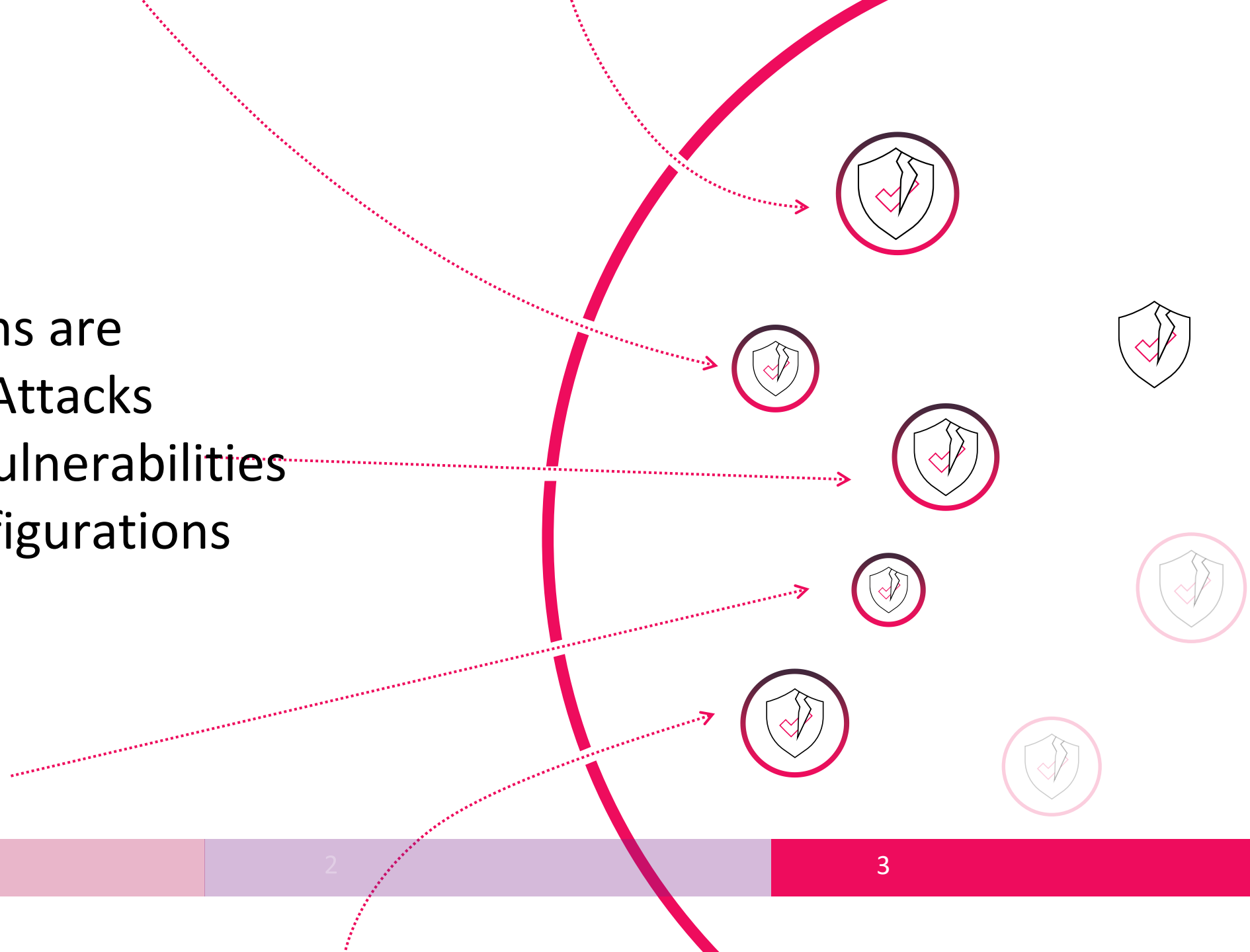
2

Exposure Prioritization

3

Safe Remediation

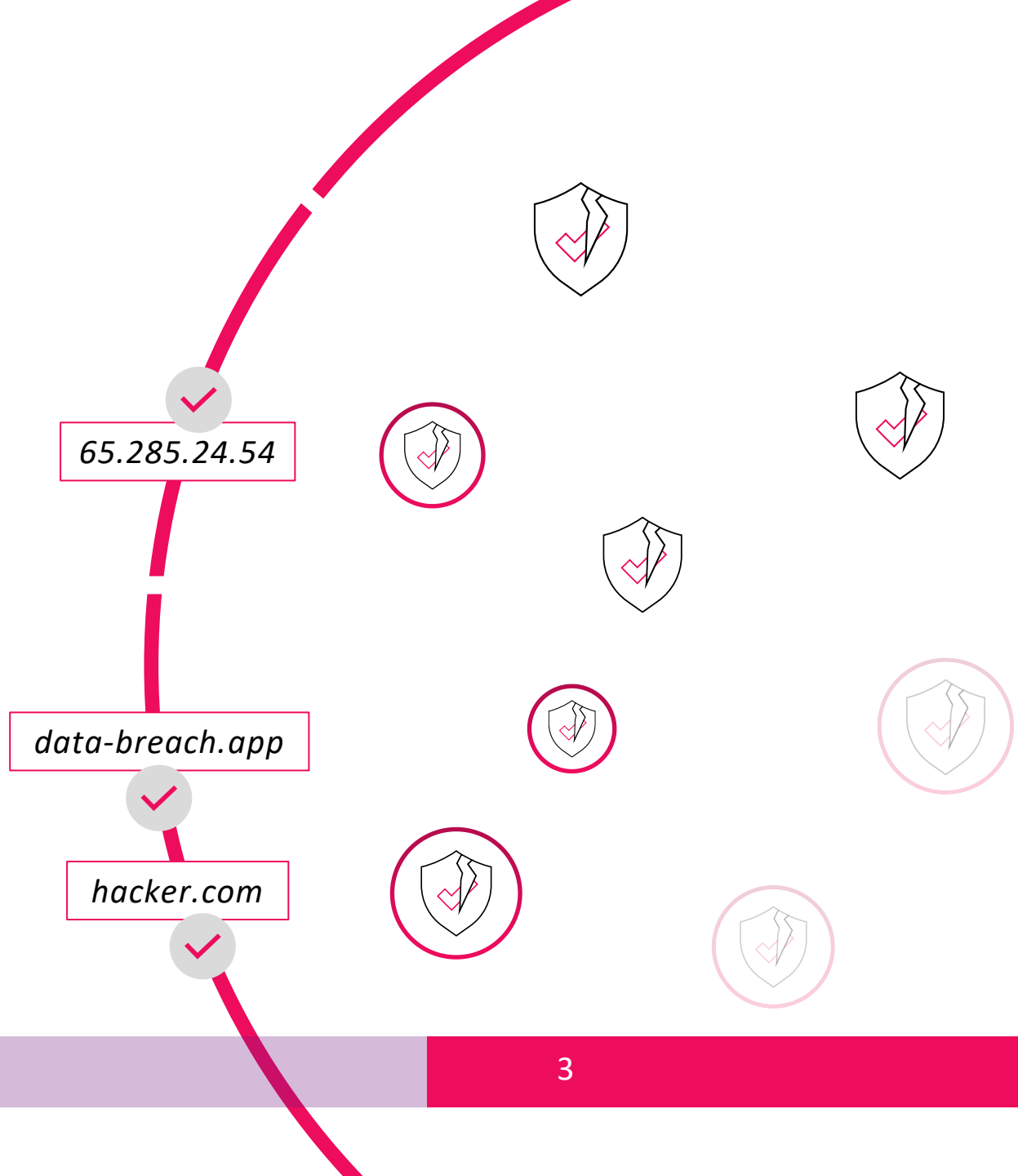
Organizations are Exposed to Attacks Exploiting Vulnerabilities and Misconfigurations



Safe Remediation

Man-in-the-Loop

1) Utilizing Intelligence By Feeding IoCs for Prevention & Blocking

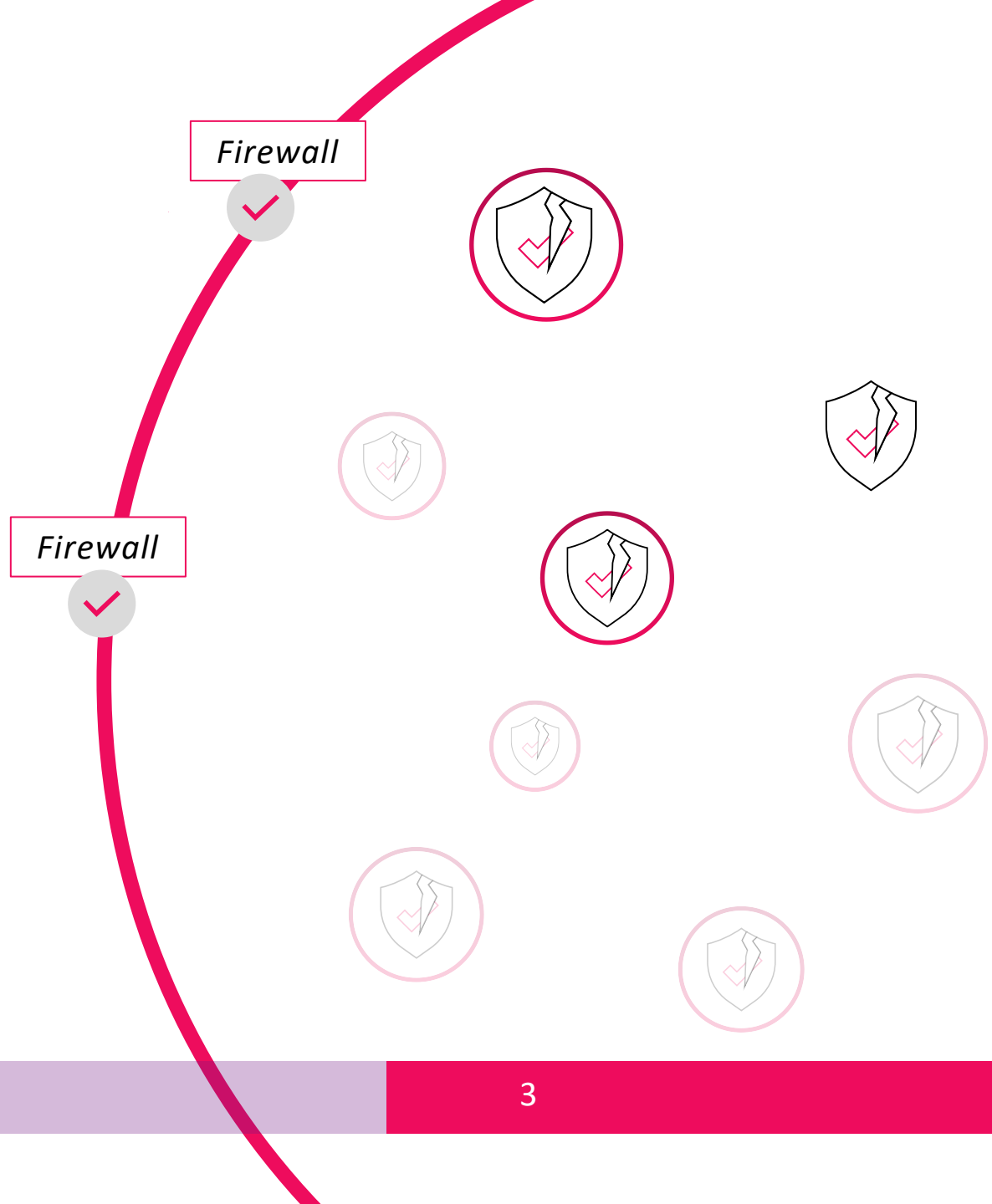


Safe Remediation

Man-in-the-Loop

1) Utilizing Intelligence By Feeding IoCs for Prevention & Blocking

2) Virtual Patching: Applying Security Control Updates



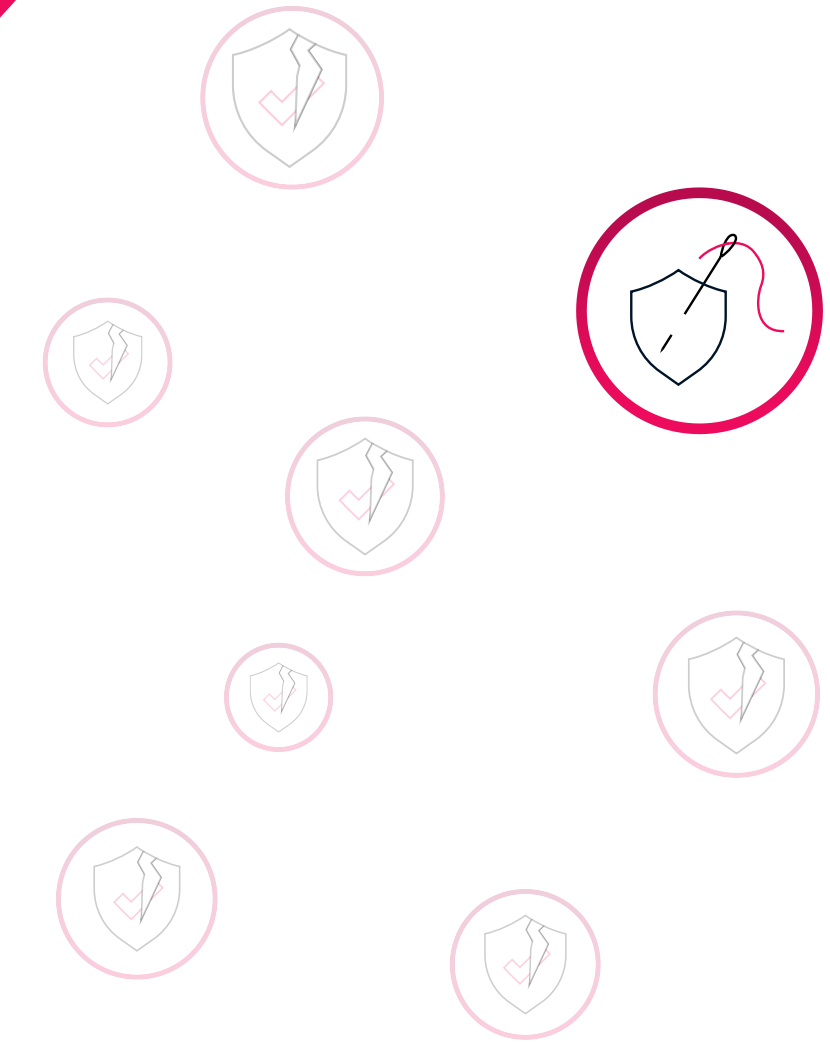
Safe Remediation

Man-in-the-Loop

1) Utilizing Intelligence By Feeding IoCs for Prevention & Blocking

2) Virtual Patching: Applying Security Control Updates

3) Patching: Hardening Endpoints & OS



Safe Remediation

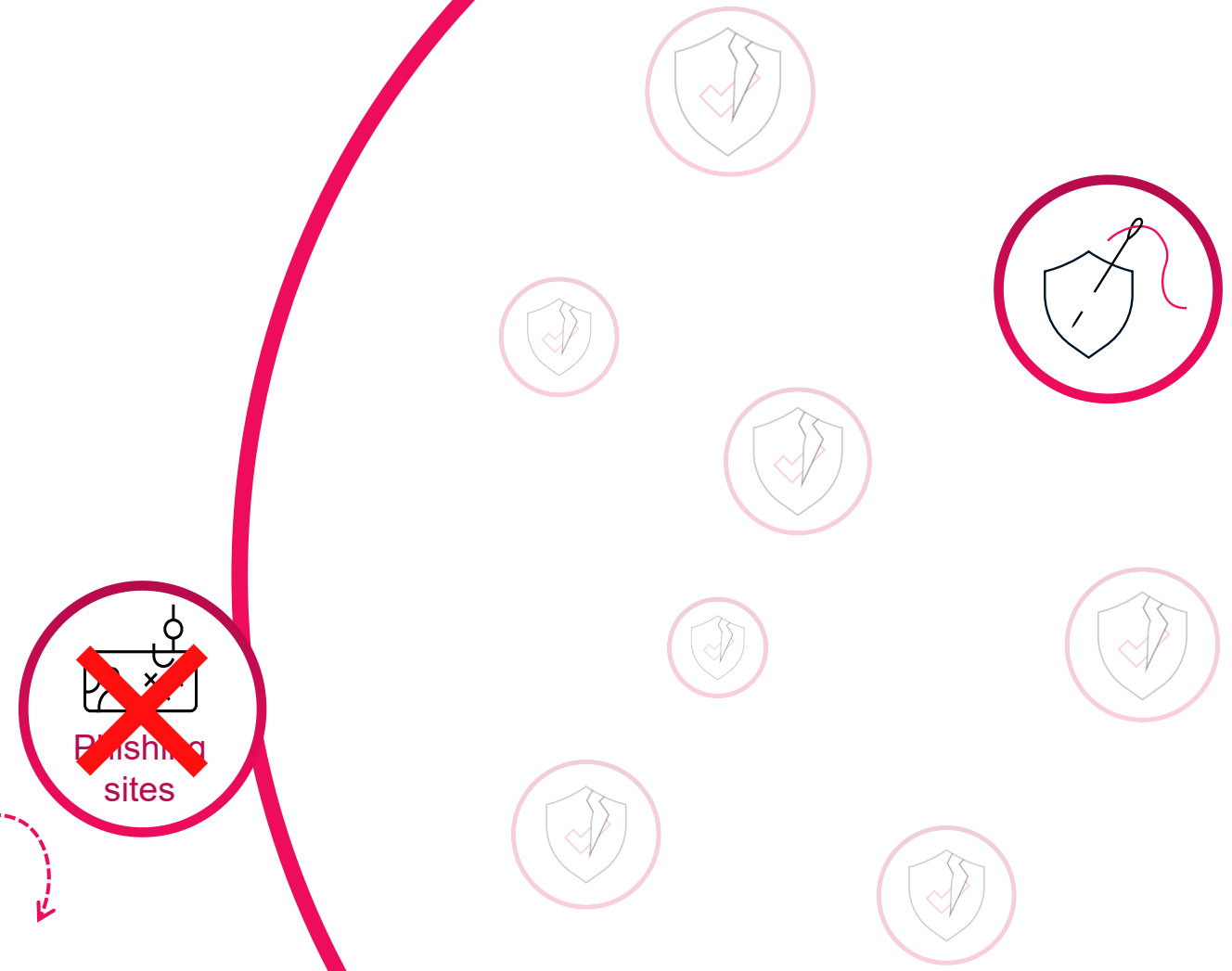
Man-in-the-Loop

1) Utilizing Intelligence By Feeding IoCs for Prevention & Blocking

2) Virtual Patching: Applying Security Control Updates

3) Patching: Hardening Endpoints & OS

4) Taking Down Phishing Sites

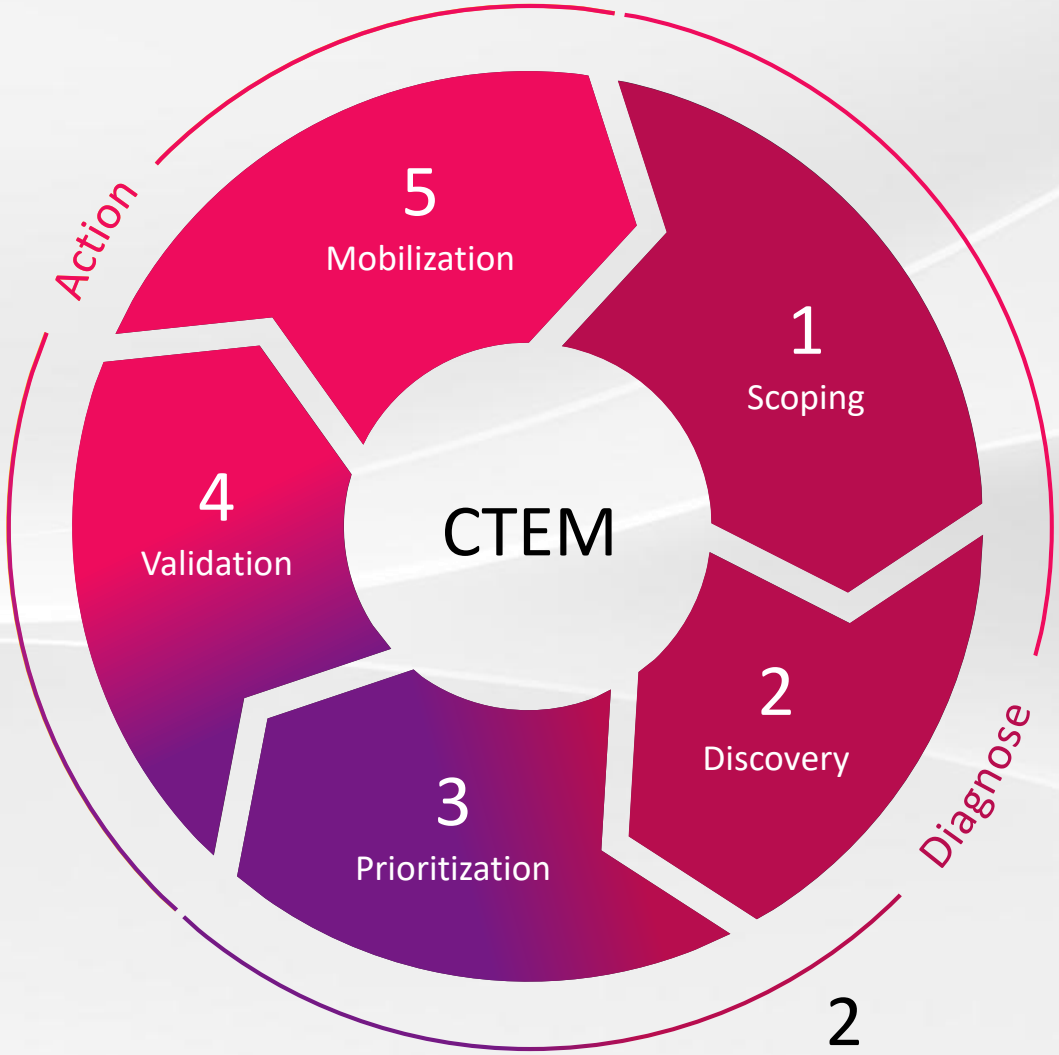


- Utilizing Security Controls to Patch
- Disseminating & maximizing Intelligence
- Disrupting Attacker infrastructure

Safe Remediation

Exposure Management

Creating Teams' Trust and Confidence



1

Threat Intelligence

2

Exposure Prioritization

3

Safe Remediation

Pollfrage #3

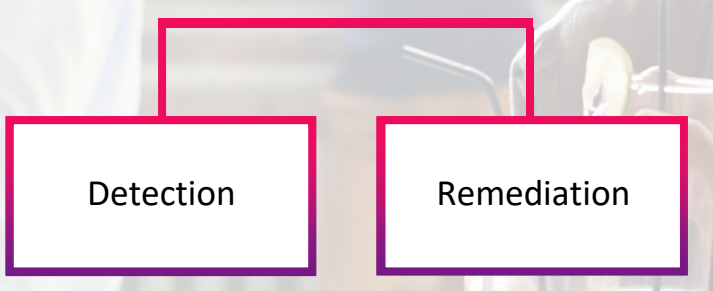
In the AI Era – It is all about the time to remediate

Organizations are trying to prioritize and pray to meet the SLA within days to weeks

In the AI Era – It is all about the time to remediate

With Check Point Exposure Management:

Intelligence based, contextualized **prioritization** with active **safe remediation -** shortening SLA to hours



CHECK POINT

EXPOSURE MANAGEMENT

Thank You