CHECK POINT™

Attackers Already Know What's Important. Do You?

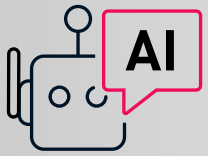
How security teams can move from exposure discovery to measurable risk reduction

Rishi Muchalla – Regional Director, Security Engineering | Western Canada and Evangelist, OCTO

November 2026

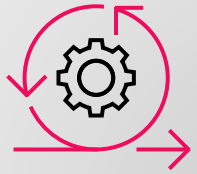
Attackers Now Move at Machine Speed

The same rules no longer apply. Defenders need tools that match the speed of the attacker.



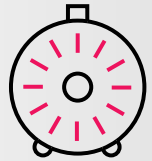
Automated at Scale

Agentic attackers test thousands of attack vectors in minutes — what used to take a human team weeks now runs continuously.



Dynamic and Adaptive

When one path is blocked, they pivot. They reason about your specific environment, chain observations, and keep going until they succeed.



Volume Overwhelms Triage

The pace of attacks now exceeds the pace of vulnerability triage, control correlation, and patching. The window between exposure and exploit has collapsed.

The time-to-being-hacked has collapsed. Detection and response cycles cannot keep up.

Where Do You Stand Today?

Exploitability
What percentage of your vulnerability backlog is actually exploitable?

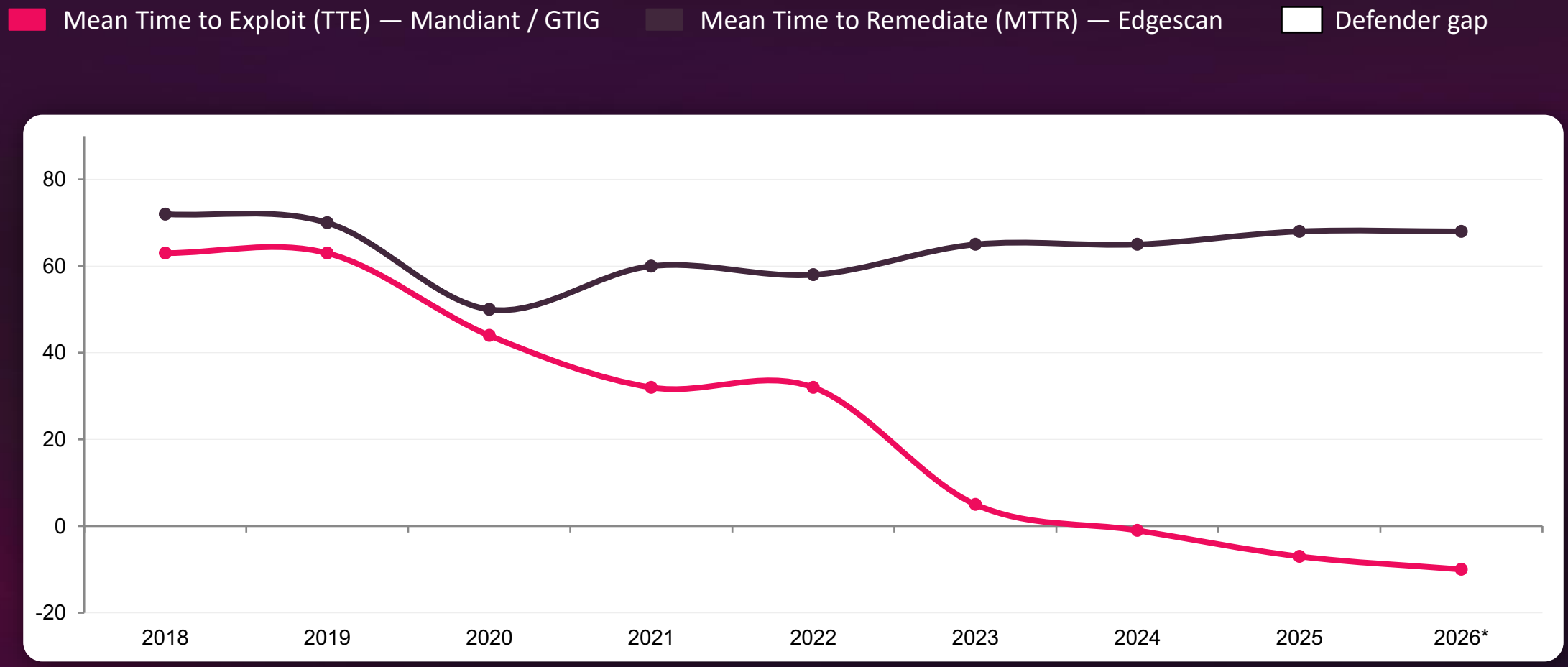
External Exposure
Which external exposure represents the highest business risk right now?

Control Effectiveness
Which of your current security controls are not protecting you as intended?

Time to Risk Reduction
If a critical exposure was discovered right now, how long would it take you to reduce the risk?

Effort Allocation
How much of your security effort is spent finding issues versus reducing them?

Mean Time to Exploit vs Mean Time to Remediate



Sources: Mandiant / Google GTIG M-Trends 2022–2026 · Edgescan Vulnerability Statistics Reports 2020–2025 · 2026* = partial year estimate · Negative TTE = exploitation precedes patch availability

Attackers Don’t See Your Security Tools

Vulnerabilities are only part of your exposure

External Surface

External facing assets
Services
Shadow infrastructure
Dark Web

Internal Exposure

Internal facing assets
Vulnerabilities
Misconfigurations
Identity and control gaps

Digital Risk

Leaked credentials, dark web activity, phishing and impersonation

Third Parties

Supplier relationships
Connected access paths

The Good News

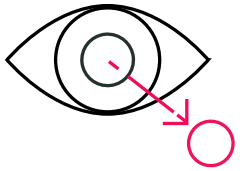
most organizations have the relevant controls in place



©2026 Check Point Software Technologies Ltd.

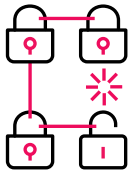
The Bad News

these controls are not continuously optimized to prevent current threats



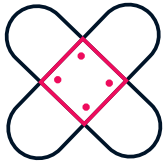
Intelligence Gap

What is being targeted, impersonated, and weaponized right now?



Prioritization Gap

Which vulnerabilities are truly exploitable, and which are noise?



Remediation Gap

Can teams reduce exposure safely and quickly through the controls they already own?

©2026 Check Point Software Technologies Ltd.

Context – Turning Signals Into Decisions



What attackers are doing?

Actors, campaigns, CVEs, IoCs, dark web, malicious infrastructure

What is exposed?

Assets, services, credentials, brands, identities and relationships

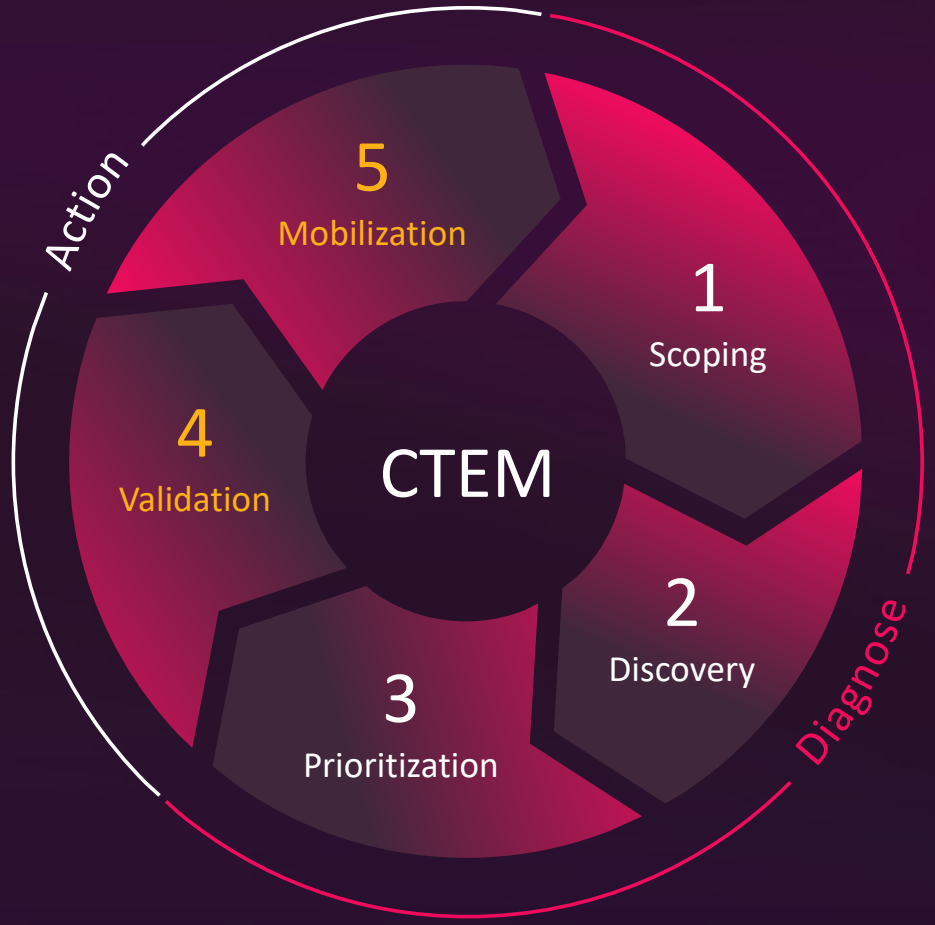
What is proven?

Evidence of exploitability and evaluation of existing control coverage

What does the business need?

Criticality, ownership, acceptable change and the safest response path

How CTEM Provides The Context



Diagnose continuously. Act continuously. Measure real life risk reduction.

Validation Changes the Quality of Every Downstream Decision

Threat Intelligence

Leaked credentials, exposed source code, CVE intelligence, dark web research, exploit research

Attack Surface Discovery

Domains, subdomains, certificates, technologies, open ports, services, web interfaces, exposed assets

AEV

Agentic Validation Engine

Reasons like an attacker

Tests at machine speed

Captures direct evidence

Validated Exposures

Evidence-backed findings security teams can act on:

- Extracted records, issued tokens, confirmed credentials
- Severity rated, with mitigation steps
- Unproven theories deleted, not shipped as noise

How Check Point operationalizes the CTEM cycle

Agentic Exposure Validation

Continuous Assessment & Prioritization

Threat Intelligence

Know what is exposed, leaked, impersonated or being targeted outside the perimeter

+ Strategic, targeted and tactical intelligence
+ Attack surface and digital risk
+ Brand, credential and third-part exposure

Exposure Prioritization

Connect external signals to asset inventory, vulnerabilities, business context and controls

+ Normalized asset and exposure view
+ Control and business context
+ Continuous assessment and prioritization

Safe Remediation

Close the loop by applying validated changes through existing tools and workflows

+ Virtual patching and control hardening
+ IoC enforcement and takedowns
+ Continuous impact validation

One continuous loop: see what attackers see, prioritize what truly matters, and remediate safely — proven by measurable risk reduction.

The CTEM Takeaway

See exposure.
Prove what matters.
Act with confidence.

Start with one business-critical segment: discover, validate, remediate — 30 days to a measured risk reduction.

