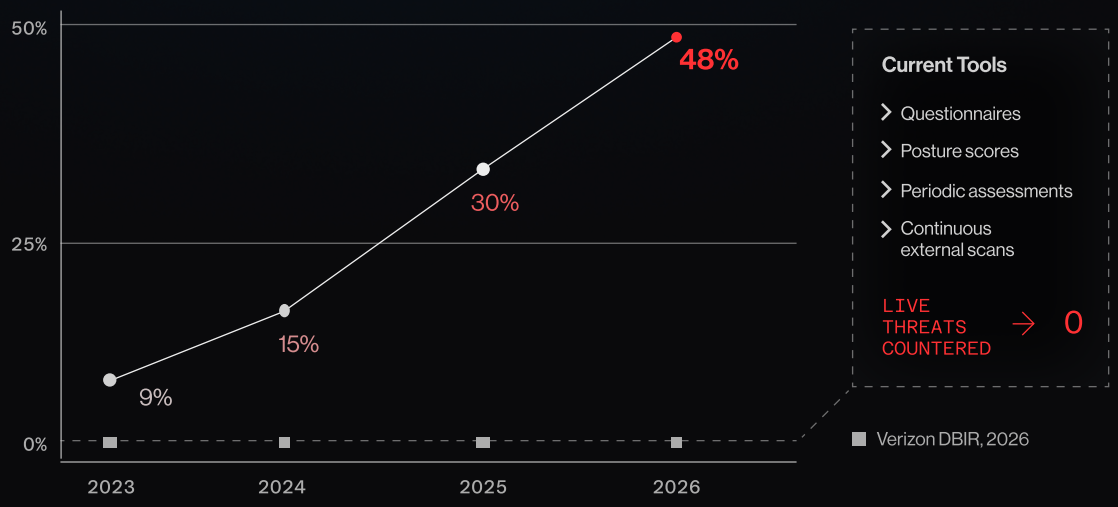
Counter Threat Operations for your entire Ecosystem

iCOUNTER delivers managed detection and response across your extended ecosystem, identifying active threats to third parties, subsidiaries, and portfolio companies and driving remediation before they impact your business.

Ecosystem breaches are on the rise, up 60% year over year

48%

of all breaches now involve a Third Party



The Counter Threat Operating System™

CTOS™delivers live threat detection and response for your entire ecosystem and third parties.

COLLECT

Owned global collection edge across thousands of sources

UNDERSTAND

AI correlation and contextual analysis of raw signals

DETERMINE

What matters to your environment and your ecosystem

ACT

Drive risk remediation and counter threats

LEARN

Outcomes retrain the system back to the collection edge

COLLECTION SOURCES

- Dark web
- Code Repos
- Social Media
- Paste Sites
- Threat Feeds
- OSINT
- Ransomware Sites
- Cybercrime Forums
- Credential Markets
- Threat Actor Chatter

Inputs mapped to at-risk third parties, prioritized for criticality

OUTCOMES

- Alert / Intel fatigue reduced
- Time to remediation compressed
- Allocation of resources more efficient

Who CTOS is made for

CISOs

Real-time view of which third parties are under attack across the ecosystem, and board-ready evidence of what was done about it.

Threat Intel Teams

Active attacks surfaced as they happen, already correlated to your ecosystem, so nobody hand-correlates generalized intel.

SOC Leaders

We triage and remediate with third parties directly, so only validated threats ever reach your queue.

Third-Party Risk Teams

Runs on your own tiers and risk framework, and scales to new vendors without adding headcount.

DEPLOYMENT COST	0
OPERATIONAL COST	0
ADDITIONAL HEADCOUNT	0

> Current solutions cannot detect and mitigate attacks live on the wire. The future of cyber defense requires **a single operating system to identify, validate and counter active threats**

iCOUNTER fills critical gaps in your TPRM Program

Security Ratings	Scores that don't reflect active threats.	STATIC VULNERABILITIES
Questionnaires	Annual self-attestation that goes stale on day one.	POINT-IN-TIME
GRC Platforms	Workflow and documentation, not live defense.	ADMINISTRATIVE
Threat Intelligence	Feeds that inform analysts but don't drive action.	INFORMATIONAL
SOC Tools	Triage after compromise — not before.	REACTIVE
iCOUNTER CTOS	**Live external intelligence to ecosystem remediation**	LIVE & ADAPTIVE

Getting Started with iCOUNTER

See immediate value by simply providing a list of your priority ecosystem partners

- Frictionless onboarding
- Immediate time to value
- No additional resources/ headcount required
- No sensitive data-sharing required
- Channel-friendly / Marketplace availability
- Identify third parties with a simple CSV