



EBOOK

The TPRM Team's Guide to Threat Intelligence

How real-time internet data fills the gap your questionnaires can't see

A third-party breach rarely begins with a vendor failing an audit. The origin is likely quieter than that, with an exposed server, a forgotten subdomain, or a set of credentials surfacing on a dark web forum weeks before anyone opens a risk ticket. By the time the incident reaches your queue, the vulnerability that started it was already long visible to anyone scanning the open internet.

This is the structural problem at the heart of traditional third-party risk management (TPRM). Most TPRM programs run on questionnaires, point-in-time assessments, and compliance checklists. They're retrospective by design, using instruments that capture a vendor's posture on the day it was documented and assuming it will hold until the next review cycle. But the threat landscape doesn't pause between assessments. Vendors stand up new infrastructure, acquire other companies, and accumulate unpatched vulnerabilities continuously. Attackers operate on the same continuous clock, probing for exposure daily.

Thankfully, the fix doesn't mean abandoning practices that work. It requires adding a layer that many TPRM programs have historically lacked: continuous, internet-scale threat intelligence. This guide describes what that layer is, where it belongs, and how it can help TPRM and SOC teams work together more effectively than ever.



The TPRM gaps that cost you

The disconnect between what TPRM teams know and the actual reality of their vendor ecosystem isn't a team failure; it's a structural limitation of legacy assessment models. It's built into the very tools the discipline has relied on for years.



The questionnaire paradox

Questionnaires are the backbone of most vendor risk programs, but they share a single structural weakness: vendors self-report, and TPRM teams largely accept those answers at face value. Even a diligent vendor can only report what it knows about its own environment. Unfortunately, few organizations have complete visibility into their own attack surface. A questionnaire is a snapshot taken on a single day. Attackers make their living exploiting the drift that accumulates after the shutter closes.



The audit cycle problem

Most programs assess vendors annually or semi-annually. That cadence leaves more than 300 days a year when a vendor's posture goes unmonitored. A great deal can change during that window. New cloud services launched without IT approval. Subdomains left pointing to decommissioned infrastructure. Software vulnerabilities left unpatched for months. None of that shows up on a schedule that only checks once or twice a year.



The perimeter's dissolution

Third parties no longer have clean, well-defined network boundaries. That means you don't either. SaaS sprawl, shadow IT, and ongoing M&A activity are expanding vendor attack surfaces faster than any questionnaire can track. Consider a case in which a vendor acquires a smaller company that happens to operate a legacy server with a known CVE. That exposure is now part of your extended attack surface. But if your questionnaire never asked about acquisitions, you'd have no way to know.

KEY TAKEAWAY

TPRM's blind spot isn't a process failure. It's a data gap. Questionnaires collect intent, but threat intelligence captures reality.

Threat intelligence: A TPRM translation

For many TPRM practitioners, “threat intelligence” sounds like a SOC concern. They assume it refers to raw scan data and feeds that belong to the security operations team. That framing doesn’t tell the full story. For TPRM, threat intelligence is about having a continuous, objective signal on a vendor’s risk posture that doesn’t depend on the vendor reporting it.

It also helps to be clear about what threat intelligence is not. It’s not surveillance, a replacement for the vendor relationships you’ve built, or something that only matters after a breach. If you already use security ratings, you’re already closer to the answer than you realize. Those ratings are the output, and threat intelligence is the underlying fuel that makes them accurate, current, and comprehensive.

A handful of specific data types matter most for developing continuous intelligence about vendor risk:

- **Internet scan data** tells you what services and ports a vendor is exposing on its IP space right now, like an automated “knock on every door” across the internet.
- **DNS and subdomain intelligence** maps a vendor’s full internet-facing footprint, including forgotten assets and shadow IT, to reveal domains that shouldn’t exist.
- **WHOIS and IP registration data** surfaces who owns which IP ranges and domains to attribute infrastructure to specific vendors and help spot unauthorized changes.
- **Certificate transparency logs** record every TLS certificate publicly issued for a domain, with a sudden spike in new subdomains possibly signaling rapid, risky infrastructure growth or typosquatting attacks.
- **Passive DNS and historical records** map infrastructure changes over time, allowing you to trace past IP and domain associations to identify the residue of previous attacks.
- **Darknet and credential intelligence** surfaces leaked credentials from third-party breaches that could provide attackers with a foothold into your vendor.

KEY TAKEAWAY

Threat intelligence is what the internet sees when it looks at your vendor ecosystem. An honest, transparent perspective that vendors have no power to alter.

Threat intelligence in action

Defining threat intelligence is one thing. Seeing what it surfaces is another. Questionnaires are structurally unequipped to identify the risks below. The right external visibility, however, can bring them clearly into view.

Attack surfaces your vendors don't know they have

Most vendors have exposures they're genuinely unaware of which show up plainly in internet scan data, including:

- Administrative interfaces like RDP, SSH, and VNC left exposed on vendor IPs
- Unencrypted services such as FTP, Telnet, and SMB broadcasting sensitive information in the clear
- Misconfigured cloud storage buckets tied to the vendor's infrastructure
- Expired or self-signed TLS certificates that signal poor security hygiene
- Open mail relays or broken DMARC/SPF records that leave the door open to phishing

None of these require insider access to detect. They're visible to anyone looking from the outside, including attackers.

The "fourth-party" problem: Supply chain exposure

Your vendors have vendors, and those vendors have vendors. Each link extends your real attack surface and almost none of it is captured by a questionnaire. Threat intelligence, however, can map this nth-party exposure through shared IP ranges, shared hosting environments, and certificate relationships. Consider a case where two of your critical vendors quietly rely on the same managed hosting provider with a known vulnerability. Threat intelligence surfaces the shared dependency and the risk it creates. A questionnaire wouldn't.

Real-world threat patterns TPRM should track

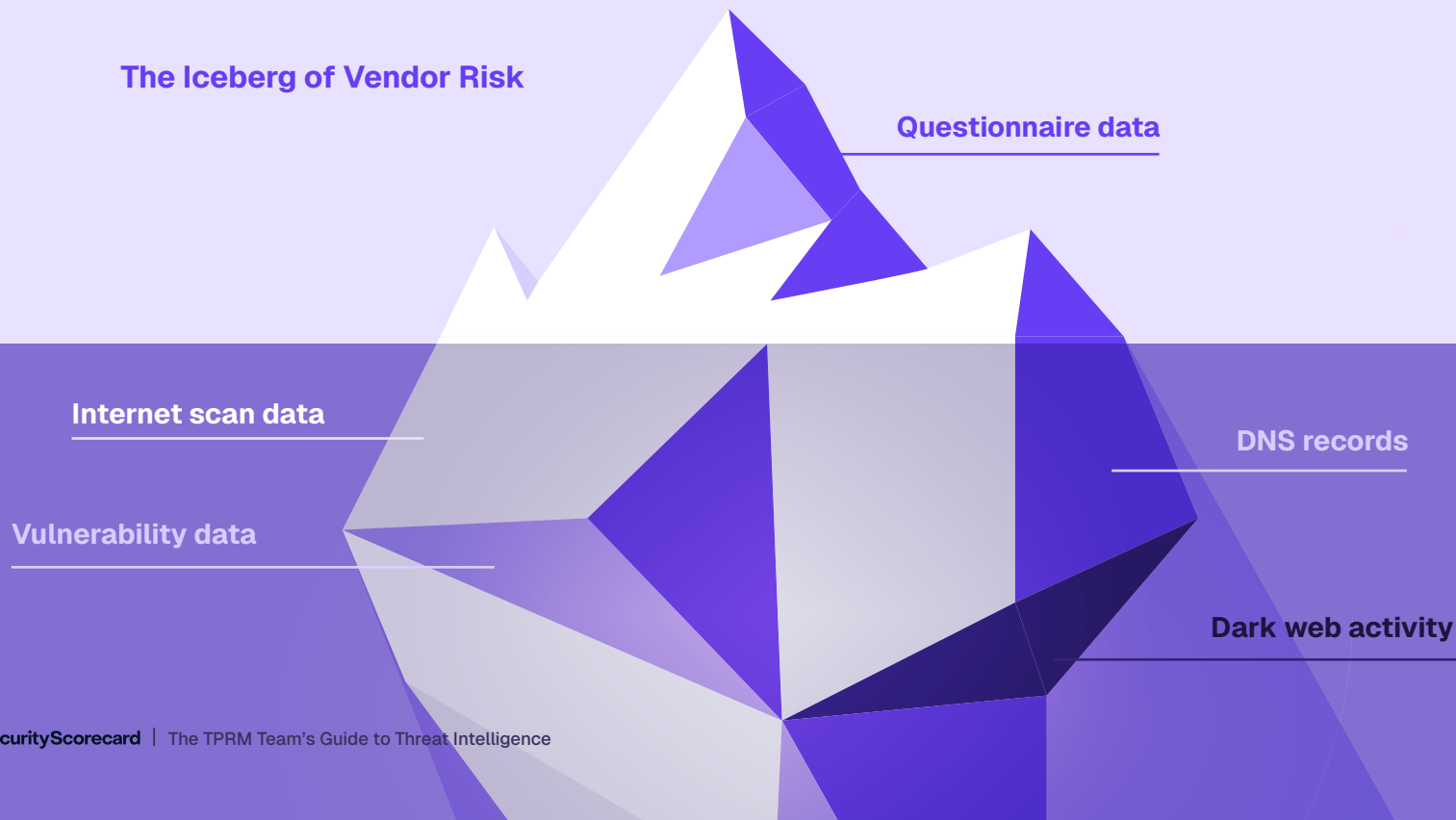
Visibility matters because it lets you ask better questions. When ransomware groups target a specific industry, which of their tactics should inform how you monitor vendors in that sector? When you review threat feeds, are any of your vendors' IP ranges showing up in them? And when a new CVE drops, how quickly can you tell how many of your vendors are running the affected software?

Threat intelligence doesn't answer these questions automatically, but it gives you the raw visibility to start asking them with more precision.

KEY TAKEAWAY

Threat intelligence is a continuous risk signal, not just raw data. The internet already has a detailed picture of your vendor's attack surface. Do you?

The Iceberg of Vendor Risk



How SOC and TPRM teams can finally work together

Most organizations already have the pieces needed to close the vendor risk gap. They're just held by two teams that rarely connect them.

SOC teams have access to rich threat intelligence, but their mandate is internal threat detection. For example, they may flag a suspicious IP without knowing it belongs to one of your most critical vendors. TPRM teams have the opposite problem: they understand vendor relationships and business context deeply, but lack threat intelligence tooling. They may complete a clean quarterly review without knowing the vendor was hit by ransomware the week before.

That gap is where risk lives. A critical vendor could be actively targeted and neither team would connect the dots. No one failed, but there's no shared workflow, vocabulary, or alerting to join what each side knows.

The two functions are far more complementary than competitive:



SOC TEAM STRENGTHS

- Threat intelligence feeds
- Malware and TTPs knowledge
- Real-time alerting capabilities
- Technical depth on CVEs/IOCs



TPRM TEAM STRENGTHS

- Vendor inventory and criticality data
- Risk scoring and business context
- Contractual leverage and remediation workflows
- Regulatory and compliance expertise



Here are five workflow examples where their collaboration pays off:

- 1. Vulnerability disclosure response.** When a critical CVE drops, SOC identifies the affected software stacks, and TPRM maps them to the vendor inventory and prioritizes outreach. Response time drops from weeks to hours.
- 2. Vendor incident triage.** SOC is often first to spot signs of vendor compromise while TPRM holds the playbook to engage the vendor, invoke contract clauses, and document the incident.
- 3. Continuous monitoring integration.** SOC's threat intelligence platform feeds real-time signals into TPRM's vendor risk register. So, scores update automatically, and alerts fire the moment a vendor's posture changes.
- 4. M&A and onboarding due diligence.** Before onboarding, TPRM requests an internet-facing asset scan from SOC to catch surprises before contracts are signed.
- 5. Regulatory reporting.** Frameworks like DORA, NIST CSF, and ISO 27001 increasingly expect continuous monitoring. SOC's threat intelligence supplies the evidence TPRM needs to demonstrate it.

KEY TAKEAWAY

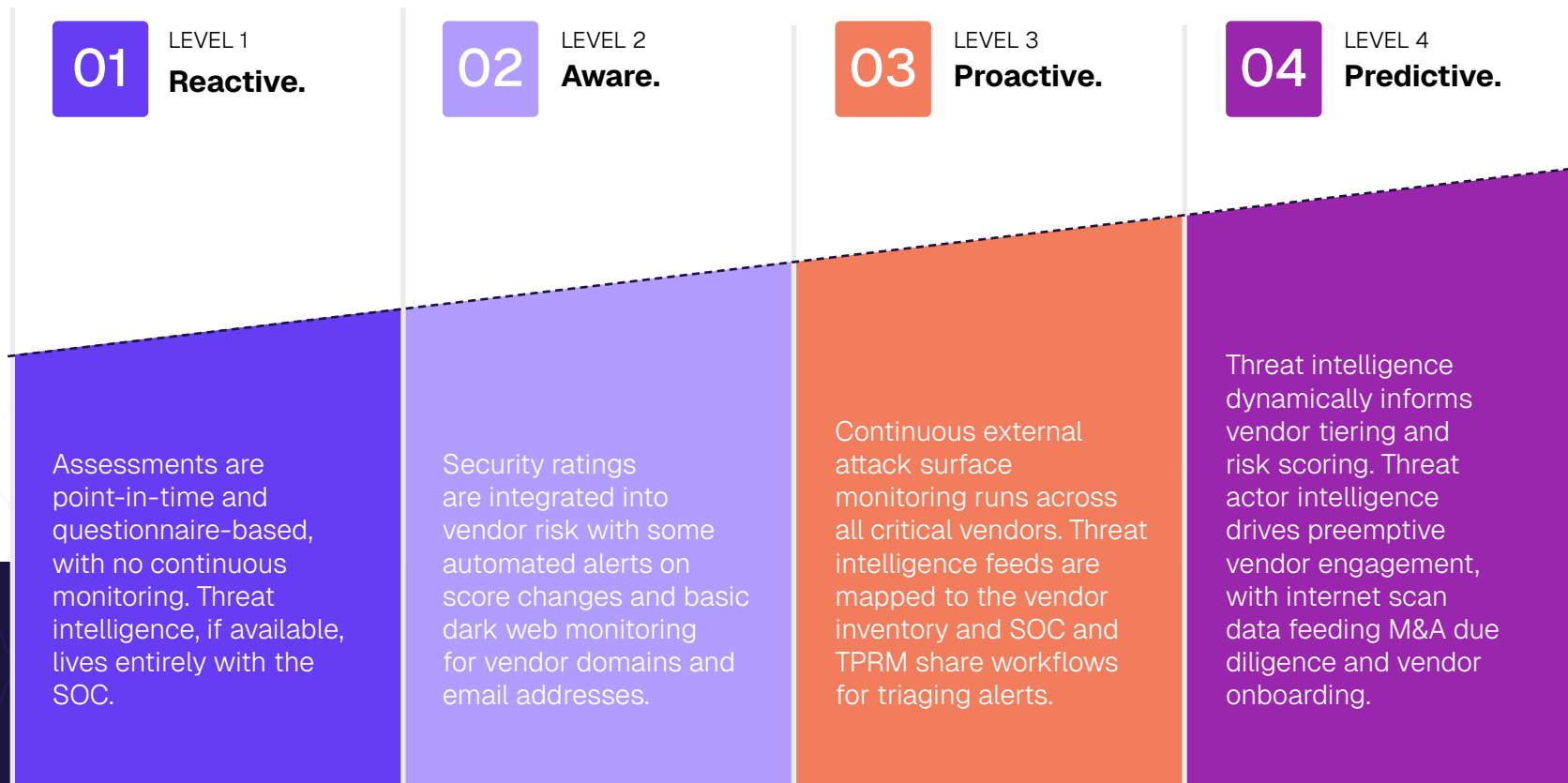
*SOC has the intelligence.
TPRM has the context.
Together, they can build a proactive
vendor risk program neither team
could develop alone.*

Practical first steps to build the bridge

- 01** Establish a shared vendor inventory both teams can access and annotate.
- 02** Create a joint escalation path for vendor-related threat intelligence alerts.
- 03** Run a quarterly threat intelligence briefing where SOC shares intelligence relevant to TPRM.
- 04** Agree on a severity framework that defines when a threat intelligence signal should trigger a vendor re-assessment.
- 05** Address the “shared language problem” with a translation layer between key SOC and TPRM metrics.

From reactive to proactive: Building a threat-informed TPRM program

Operationalizing threat intelligence isn't a switch that you flip. Where you start depends on where your program sits today. It helps to see the progression as a maturity curve:



With a few strategic moves, TPRM teams can achieve quick wins that pay off immediately:

- Run an internet-facing asset scan on your 10 most critical vendors and see what surfaces.
- Build a complete list of the domains and IP ranges your top vendors own, which is something most teams don't have.
- Integrate a security ratings feed if you aren't already receiving continuous signals on posture changes.
- Request a joint threat briefing with your SOC team to ask what's currently targeting your industry's supply chain.
- Map threat-informed TPRM practices to specific regulatory requirements in DORA Article 28, NIST SP 800-161, ISO/IEC 27036, and SEC cybersecurity disclosure rules.

Then, you can track progress with metrics that best reflect speed and coverage rather than just activity:

- Mean time to detect (MTTD) for vendor-related threats.
- Percentage of critical vendors under continuous external monitoring.
- Number of proactive vendor engagements triggered by threat intelligence versus reactive ones.
- Reduction in time-to-remediate after identifying a vendor risk.

KEY TAKEAWAY

Moving up the maturity curve doesn't mean ripping out what you have. You just need to add the right intelligence layer on top of the processes that already work.

Why internet-scale intelligence changes everything

A single, continuously refreshed, internet-scale dataset shows exactly what every internet-connected organization is exposing right now and how that exposure changes over time. With continuous, global internet scan coverage, a TPRM program can do things that point-in-time assessment simply can't. It can instantly identify newly exposed services on any vendor's IP space. Correlate certificate transparency logs with vendor domains to catch shadow IT and acquisitions as they happen. Identify shared infrastructure between vendors that quietly creates concentration risk. And most importantly, it can deliver real-time alerts when a vendor's posture degrades before they disclose it. Sometimes, before they even know.

The practical payoff is a shift in how teams spend their time: less of it chasing questionnaire follow-ups, and more on substantive risk-reduction conversations with vendors.

KEY TAKEAWAY

Organizations that lead on TPRM over the next five years will be the ones making faster, more confident decisions because they have the best data.

Once-impossible questions can also now be answered:

"Did any of our vendors deploy new internet-facing services this week?"

"Which vendors are still running software affected by this CVE?"

"Are any Tier 1 vendors sharing infrastructure with each other or known bad actors?"

"What does our vendor's attack surface look like from an attacker's perspective?"

The future of TPRM is already here

The third-party threat landscape has outpaced the methods traditional TPRM was built on. Questionnaires and annual audits still have a role, but on their own they describe a vendor as it was, not as it is. That lag is exactly where modern breaches take hold.

Threat intelligence is no longer just a SOC-exclusive tool, but table stakes for any mature TPRM program. Collaboration between SOC and TPRM is an organizational imperative in a world of continuous supply chain threats. Programs that pull ahead will not succeed by abandoning what already works. Instead, they'll combine the relationship depth of traditional TPRM with continuous, internet-scale intelligence to show what's actually happening across their vendor ecosystem.

The data exists. The question is whether or not you're using it.

Are you ready to see what threat intelligence reveals about your vendor ecosystem?

Request a TITAN Secure demo today.

You can also explore SecurityScorecard's continuous monitoring capabilities with a free Vendor Risk Assessment.

