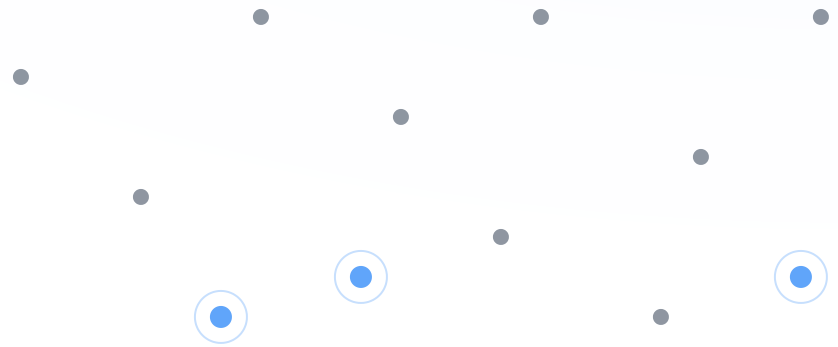
PentaTrail

Invisible assets become your greatest vulnerability

The AI-native CTEM / ASM platform

Externally exposed domains, IPs, ports, and cloud buckets. The assets missing from your inventory are exactly where attackers strike first. PentaTrail continuously monitors your attack surface the way an attacker sees it.



WHY NOW

The time you can leave exposure unaddressed has hit zero

The gap between a vulnerability's disclosure and its mass exploitation is vanishing. An annual assessment can no longer keep up.

0 days

Grace period, disclosure to exploitation

Median time from disclosure to mass exploitation for edge-device KEVs (known-exploited vulns) / Verizon DBIR 2025

84%

Intrusions via internet-facing devices

Ransomware entry via VPNs, remote desktop and other internet-facing devices / Japan NPA, H1 2025

73%

Caused by unmanaged assets

Security leaders who suffered an incident caused by unknown or unmanaged assets / Trend Micro · CSO Online 2025

METI's "Security Measures Evaluation Program for Supply-Chain Strengthening (SCS)" is slated to launch by the end of FY2026. Partners increasingly ask for objective evidence of your posture.

BLIND SPOTS

Three blind spots organizations face today

External assets you can't see

Cloud migration, M&A, per-department subdomains. An IT asset inventory alone can't capture your full external exposure. What attackers can see, you can't.

Security operations that hinge on individuals

Interpreting scan results, judging priority, reporting to executives — all resting on one person. When people change, quality and risk judgment change too.

Risk you can't explain

When asked "Are we safe?", can you answer with numbers rather than gut feel? You need to explain risk with quantitative evidence.

→ **PentaTrail closes these three blind spots.** From automatically enumerating external assets, to ordering them by risk, to reporting to the board in numbers — end to end.

CTEM FRAMEWORK

Don't stop at finding — run all five CTEM stages continuously

CTEM (Continuous Threat Exposure Management) is a framework for continuously discovering, assessing, and remediating externally visible weaknesses. Rather than a one-off assessment, you keep cycling through five stages to shrink your attack surface.

1 SCOPING

Scoping

Define the domains to monitor

2 DISCOVERY

Discovery

Deterministically enumerate assets

3 PRIORITIZE

Prioritize

Reorder by risk

4 VALIDATION

Validate

Confirm real exploitability

5 MOBILIZE

Mobilize & report

Fix it and show the board

Iterate continuously — your attack surface changes daily

Coverage by plan	① Scoping	② Discovery	③ Prioritize	④ Validate	⑤ Mobilize
ASM (find · targetability)	✓	✓	Risk scoring	—	View AI guidance
CTEM (validate · fix · report)	✓	✓	✓	✓	✓

DISCOVERY

Enumerate your "invisible assets" with technical evidence, not guesswork

The assets missing from your inventory are exactly where attackers strike first. From public sources, PentaTrail deterministically discovers only technically substantiated assets — with no reliance on AI inference.

From deterministic signals Public sources

- DNS
- CT Logs (certificates)
- WHOIS
- Reverse IP

Without relying on AI inference, we use only **technically substantiated signals**. We never "invent" assets from guesswork.

→

Discover "invisible assets" beyond the inventory

- Domains & subdomains
- IP addresses
- Open ports
- Tech stack
- Cloud assets & buckets
- Public URLs

Down to shadow IT and unmanaged subdomains. **We scan daily** and detect new assets and newly opened ports by the next day.

PRIORITIZATION

Don't rank by CVSS alone

Hundreds of vulnerabilities can surface each week — you can't fix them all. PentaTrail ranks in two stages. First, from severity (CVSS), exploit probability (EPSS), and detection-evidence quality (Evidence Grade), it computes a **Threat Discovery Level**. Multiplying that by Business Impact (BI) yields **Threat Exposure Risk**, showing you what to fix first.

TDL **Threat Discovery Level**
Severity (CVSS) × exploit probability (EPSS) × detection-evidence quality (Evidence Grade), adjusted by exploitation history (KEV), expressed as a technical threat level of 1–5.

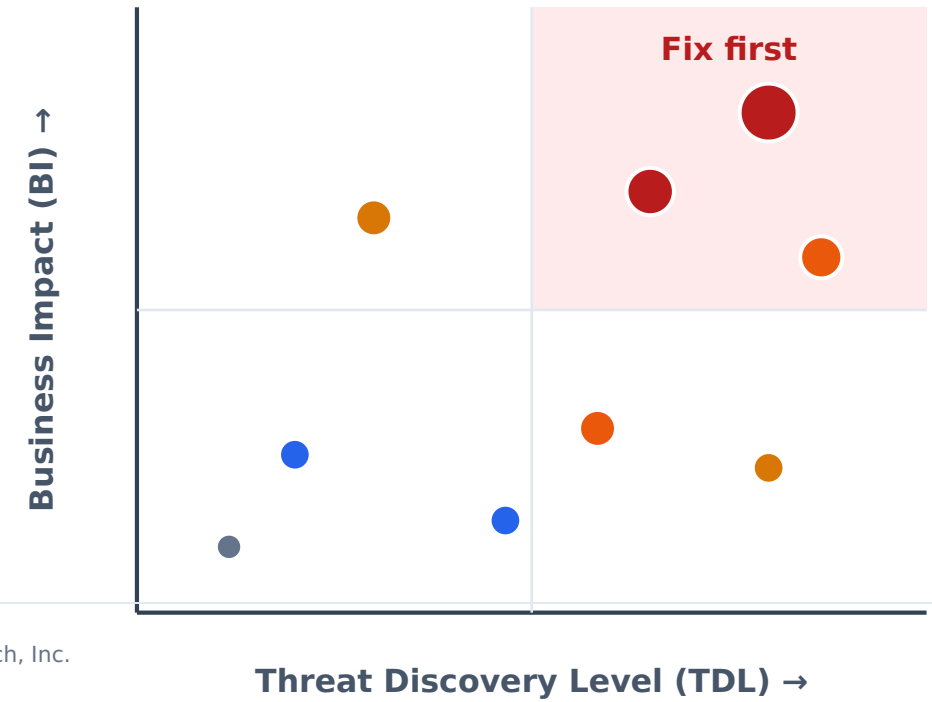
Evidence **Evidence Grade**
A = verified / B = directly tested / C = CPE match / D = suspected backport. Risk is raised or lowered by the certainty of the detection evidence, not by guesswork.

Business impact **BI score**
Weights each asset by purpose, data type, and availability. The same vulnerability weighs differently on a payment system than on a test environment.

Threat Discovery Level × Business Impact = Threat Exposure Risk → five bands, S–D:

S	A	B	C	D
Critical	High	Medium	Low	Info

Threat Exposure Risk = Threat Discovery Level (TDL) × Business Impact (BI)



VALIDATION

Don't stop at "found" — AI proves whether it can actually be exploited

A theoretical CVSS score alone won't tell you what's actually dangerous. For each candidate, AI Deep Scan auto-generates validation code and tests non-destructively to confirm whether an attack actually succeeds.

AI auto-generates validation code

For each CVE, AI generates proof-of-exploit code and tests the target host safely.

Non-destructive validation

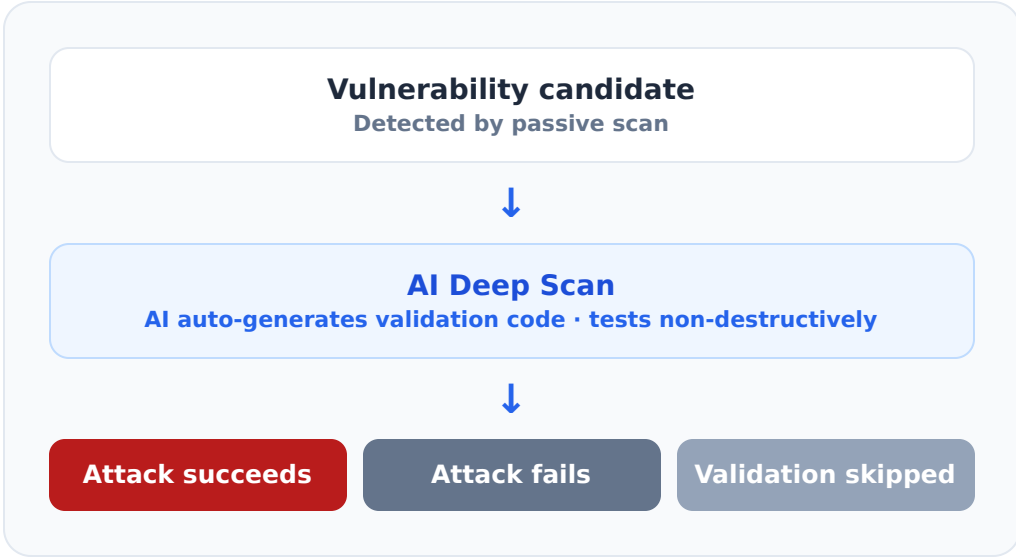
Limited to domains you've proven you own via DNS verification. No operations that affect your systems.

Confirm attack "success / failure"

Judged by whether an attack actually succeeds, not by theory — giving your risk ratings real backing.

Fewer false positives

Focus your limited remediation resources only on what's truly dangerous.



MOBILIZATION

Don't stop at finding — AI even shows you how to fix it

Don't leave found vulnerabilities sitting. AI generates remediation for each one, tracks response status, and exports to PDF. Even a small team can see fixes through.

AI generates remediation

For each vulnerability, auto-generates impact, remediation, and interim mitigation. You know what to fix and in what order.

Operations that don't hinge on individuals

Consistent-quality guidance every time, regardless of staff skill or turnover.

Distribute straight to PDF

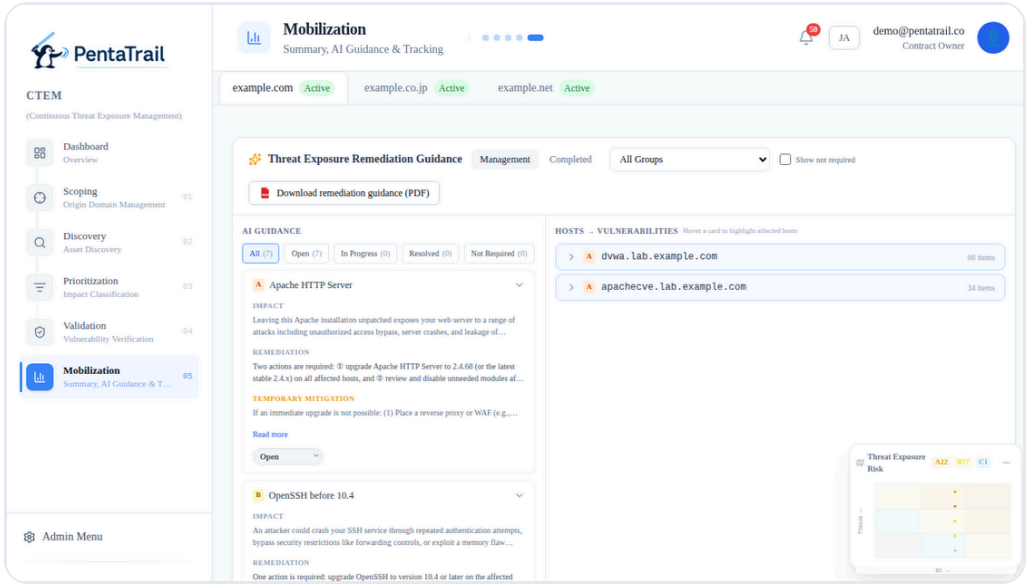
Share with both frontline teams and executives in one click.

Track response status

Manage Open → In Progress → Resolved in a ledger to prevent anything slipping through.

Integrate via MCP

Read and write your attack-surface data straight from AI tools you approve.



Actual AI remediation guidance — generates impact, remediation, and interim mitigation per vulnerability and tracks status. One-click PDF export.

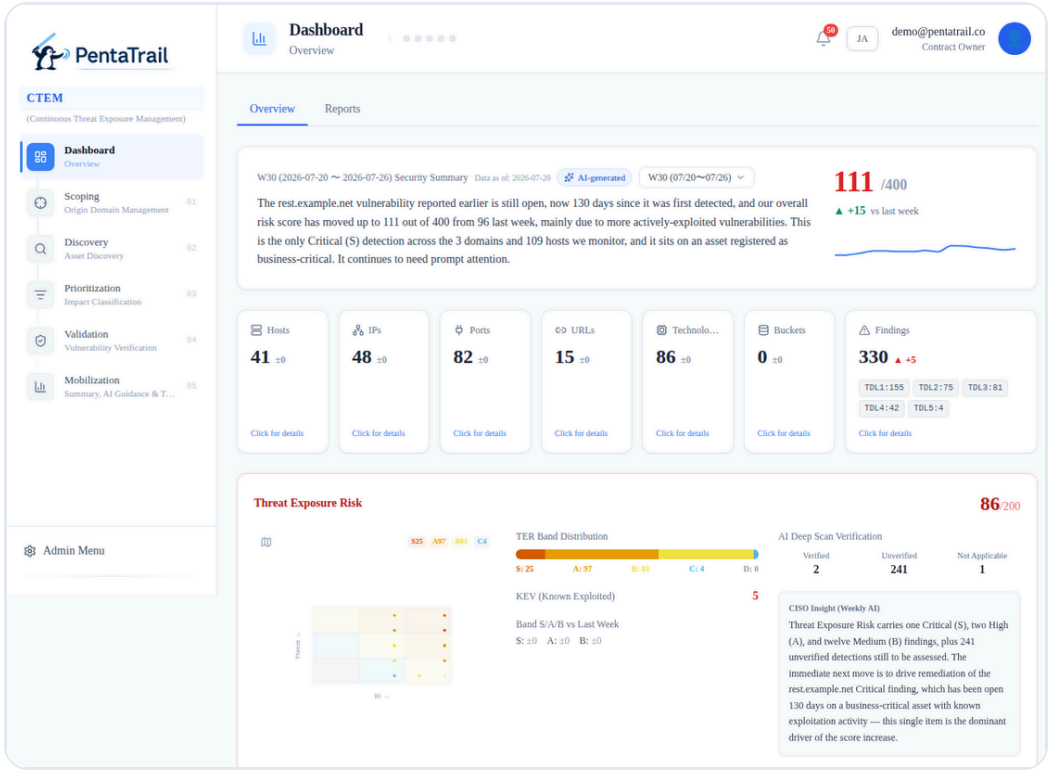
EXECUTIVE REPORTING

Answer the board's three questions with numbers

What the board asks its security lead comes down to three questions. PentaTrail answers all three from a single dashboard.

1. **Are we secure?**
   Show your current posture with a security score (out of 400) and severity distribution
2. **Are we improving?**
   Track your progress with the score trend (vs. last period)
3. **What's new?**
   Catch recent changes with change detection (new assets, opened ports)

> It even shows threat distribution by business impact, so you can explain security ROI quantitatively.



Actual executive dashboard — security score, Threat Exposure Risk, severity distribution (S–D), and AI CISO insights on one screen.

USE CASES

Manage your attack surface in every scenario

From continuous external attack-surface monitoring to M&A due diligence and supply-chain assessments. Even a small team can keep it running.

Continuous external attack-surface monitoring

Automatically discover shadow IT and unmanaged subdomains, and track changes

Cloud exposure checks

Detect public buckets and unintended public resources across AWS/GCP/Azure

M&A due diligence

Present a target's external assets to leadership in a single score report

Support for lean security teams

Run continuous attack-surface management even as a one-person IT team

Responding to supply-chain security assessments

Meet rising requirements such as the SCS program with objective evidence of your external exposure

→ All of this,**in a single subscription.** 3 domains and 5 users included (unlimited subdomains), with no extra fees.

PRICING

Two simple plans — choose by what's included

	ASM $290 /mo Find, monitor, and order by risk	CTEM $490 /mo Validate, remediate, and show the board
Automated external asset discovery Discovery	✓	✓
Daily scanning & change detection Monitoring	✓	✓
Risk scoring (KEV / EPSS / BI) Prioritization	✓	✓
View AI remediation guidance Mobilization	✓	✓
Vulnerability validation Validation	—	✓
Remediation task operation & tracking Mobilization	—	✓
Executive reports (score & trends) Reporting	—	✓
MCP integration	✓	✓
Both: 3 domains & 5 users included (unlimited subdomains)	✓	✓

All prices are per month (USD). The larger your attack surface, the lower the cost per asset.

COMPANY

Company

Company	Pentacon Research, Inc. (株式会社ペンタコン研究所)
CEO	Kazuya Hiradate
Founded	February 2026
Capital	10 million JPY
Head office	2-17-6 Nihonbashi-Kayabacho, Chuo-ku, Tokyo, Japan
Business	1. Planning, development & delivery of information-security SaaS 2. Research, analysis & consulting in information security 3. R&D in information systems, cloud, and AI technologies

CEO

Kazuya Hiradate 平舘 一哉

After joining Nomura Research Institute, spent 20+ years in cybersecurity at NRI SecureTechnologies, serving as General Manager in the managed security services business and the corporate security management division. That business-development and governance expertise is built into PentaTrail's AI-driven engineering.

MISSION

The power to see invisible risk, for every organization.

Combining radical efficiency from AI-driven development with hands-on corporate-security experience, we deliver security you can sustain.

VISION

Toward a society where security blends in like air.

We aim for a world where everyone enjoys a safe cyberspace without thinking about security.

GET STARTED

Start by checking your attack surface from the outside

Sign up in as little as 5 minutes; see your first attack surface within hours.

Sign up 5 min → **Discovery** hours → **Review** visualized on the spot

Try it free | **pentatrail.co/ctem**

Scan with your phone

14 days, free. The AI-native CTEM / ASM platform