PentaTrail

CTEM / ASM PLATFORM

Invisible assets become your greatest vulnerability

PentaTrail — The AI-native CTEM / ASM platform

What is PentaTrail

A CTEM / ASM platform that continuously discovers, assesses, and remediates your externally exposed domains, IPs, ports, and cloud assets. The "invisible assets" missing from your inventory are exactly where attackers strike first. Seeing your attack surface the way an attacker does, PentaTrail monitors it **daily**, shows what to fix first in priority order, and reports to the board in numbers.

0 days

Grace period, disclosure to mass 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

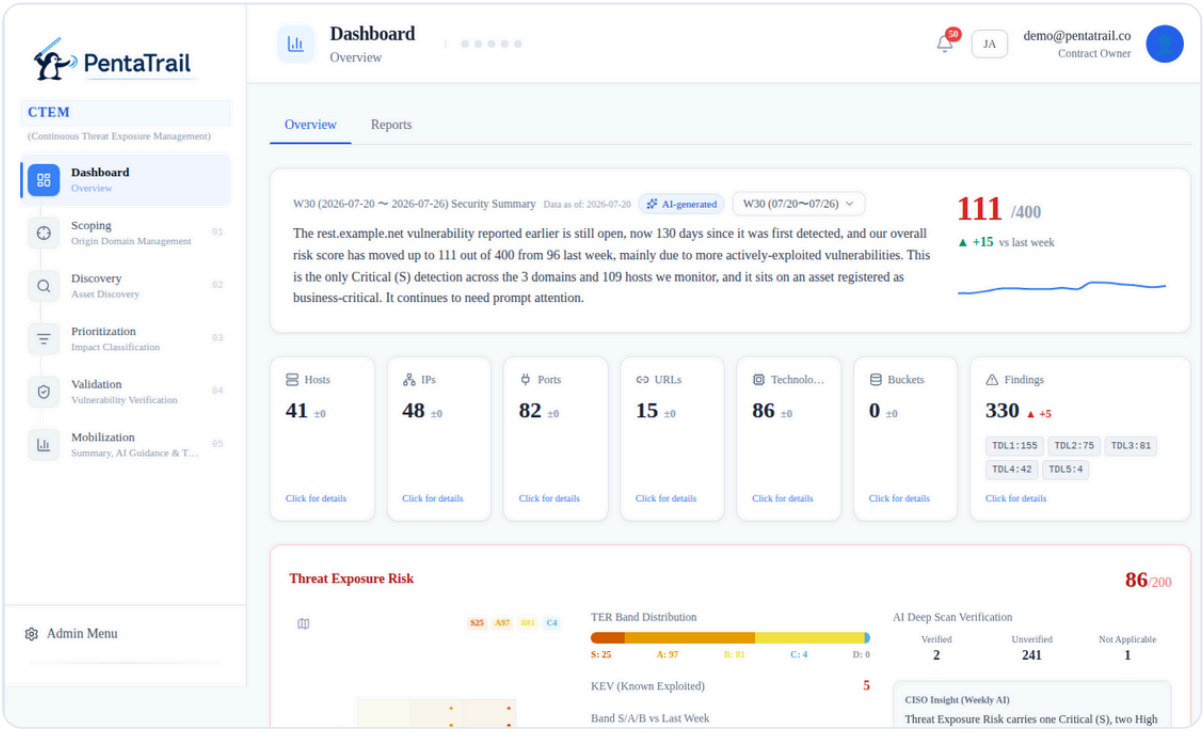

Figure 1 — Executive dashboard. Security score (vs. last period), severity distribution (S–D), risk matrix, KEV, and AI CISO insights on one screen. Answers "Are we secure? / Are we improving? / What's new?" in numbers.

USE CASES

Key use cases

Continuous external attack-surface monitoring

Automatically discover shadow IT and unmanaged subdomains, and track changes

Cloud exposure checks

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

M&A due diligence

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

Support for lean teams

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

Responding to supply-chain assessments (e.g. SCS)

Meet rising requirements such as METI's evaluation scheme with objective evidence of your external exposure

WHY PENTATRAIL

What sets PentaTrail apart

Difference	Why it matters
AI-native by design	Discovery is handled by deterministic techniques; AI focuses on validation, remediation guidance, and executive summaries. Even without a dedicated hire, you can run your attack surface with little manual effort.
Deterministic Discovery	DNS, CT Logs, WHOIS, reverse IP. No reliance on AI inference — only technically substantiated results are reported.
Daily scanning	Unlike monthly or annual assessments, we scan every day and detect changes by the next day. Weekly assessments can leave you blind for up to 7 days.
Non-destructive validation (AI deep scan)	AI auto-generates validation code and confirms non-destructively whether an attack actually succeeds — cutting false positives so you focus only on what's truly dangerous. Limited to ownership-verified domains; no operations that affect your systems.
Prioritization	We compute a Threat Discovery Level from CVSS, EPSS, and Evidence Grade, then multiply by Business Impact (BI) to derive Threat Exposure Risk. S–D bands show what to fix first.
MCP integration	Read and write your attack-surface data straight from AI tools you approve.

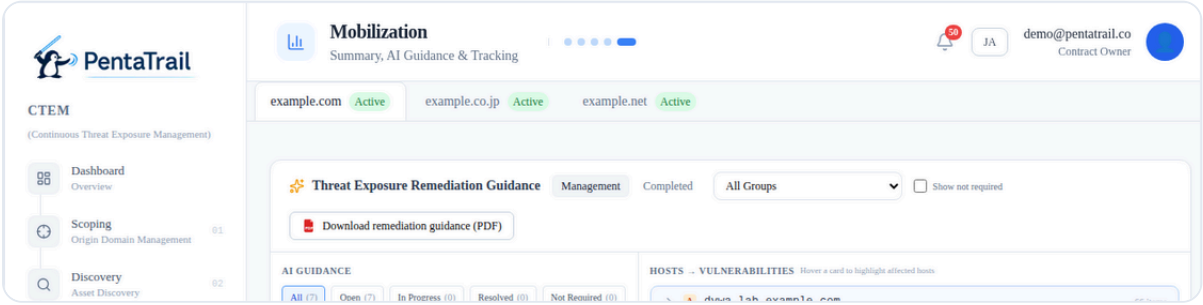

Figure 2 — AI remediation guidance. For each vulnerability, AI generates impact, remediation, and interim mitigation, and tracks status. One-click PDF export.

CTEM FRAMEWORK

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

Rather than a one-off assessment, we iterate through five stages continuously to shrink your attack surface. Coverage by plan is shown below.

1 **SCOPING**
Scoping
Define what to monitor

2 **DISCOVERY**
Discovery
Enumerate external assets

3 **PRIORITIZE**
Prioritize
Order by risk

4 **VALIDATION**
Validate
Confirm exploitability

5 **MOBILIZE**
Mobilize & report
Fix, then report

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)	✓	✓	✓	✓	✓

PRICING

Two simple plans

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

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

Start by checking your attack surface from the outside

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

① **Sign up**(5 min) → ② **Auto-discovery**(hours) → ③ **Review**(visualized on the spot)

pentatrail.co/ctem

14-day free trial

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.