primesight

Security Through Agentic Intelligence

WHAT IS THE PROBLEM?

- Security teams drown in vulnerability reports from diverse client deployments.
- Strict compliance timelines force hasty analysis and costly remediation errors.
- Most vulnerabilities remain unresolved and gradually expand the attack surface of organizations.

VULNERABILITY MANAGEMENT
A CRISIS OF SCALE

Enterprise security teams are overwhelmed by an unprecedented volume of vulnerabilities that far exceeds remediation capacity.

40,000+

NEWLY IDENTIFIED CVES JUST IN 2024

Cyber threats multiply daily, overwhelming traditional manual processes for risk assessment and response coordination.

Source: cve.org

65 DAYS

AVERAGE MEAN TIME TO REMEDIATE A VULNERABILITY

Operational constraints and limited headcount extend exposure periods far beyond acceptable risk thresholds.

Source: allaboutgrc

45.4%

UNRESOLVED WITHIN A 12-MONTH PERIOD

Unaddressed vulnerabilities pile up faster than remediation efforts, exponentially increasing organizational attack surface.

Source: Edgescan 2025 vulnerability report

THE SOLUTION

An AI-first platform vertically integrated into your security team’s workflow with 3 modules:

- Continuous Threat Modelling;
- Passive Environment Monitoring;
- Dynamic Discovery & Exploitation.

CONTINUOUS THREAT MODELLING

Live, continuously updating threat model that integrates with the other models in order to:

- Constantly discover business-critical assets and attack pathways, assess impact and exploitation complexity;
- Summarize findings, generate reports and offer guidance;
- Create or update the risk profile of your business.

PASSIVE ENVIRONMENT MONITORING;

AI-first aggregator with a dedicated vulnerability management platform that vertically integrates in your workflow to:

- Extract product-specific information from collaborative workspaces (such as Confluence);
- Collect and update issues from ticketing platforms (such as Jira) for vulnerability deduplication;
- Autonomously inspect code from container registries to statically validate vulnerabilities and update risk.

DYNAMIC DISCOVERY & EXPLOITATION

A two-step process meant to:

- Actively discover additional attack surface and expand entry points;
- Autonomously validate vulnerabilities and updating threat intelligence using agentic penetration testing;
- Create bespoke, detailed reports and offer guidance and protective measures.

WHAT POWERS IT ALL? OUR CORTEX

A unified, continuously updating, client-specific intelligence context that persistently aids agents to focus on targeted, business-critical risks.

Cortex seamlessly integrates with all modules in order to keep your threat model up to date, as well as syncing your collaborative workspaces and ticketing platforms.

PRODUCT INTEGRATIONS

We offer a great variety of integrations in order to target every customer, from SMEs to complex enterprise environments with strict requirements.

MARKET VALIDATION

>$730 billion

software market size in 2024

11.3% CAGR

forecasted for 2025-2030

>61% on-premise

software deployment share in 2024

>$183.9 billion

information security spending in 2024

>40,000

CVEs identified in 2024

~64 working days

average remediation time for a new vulnerability

sources: grand view research, gartner, cyberpress, allaboutgrc

MARKET TARGETS

>$183.9 billion

information security spending in 2024

→

40 early adopters

in the first year of business

→

$1m ARR

with sustainable momentum

BUILT BY DOMAIN EXPERTS

Enterprise security veterans with AI deployment and startup scaling experience, bringing both technical depth and execution capability.

CEO

Robert Dobre

Founding Engineer @ **SF Standard**

Security Research Engineer @ **CertiK**

CTO

Mihai Cioata

Security Engineering Manager @ **UiPath**

CTO @ **3DLook, IOS**

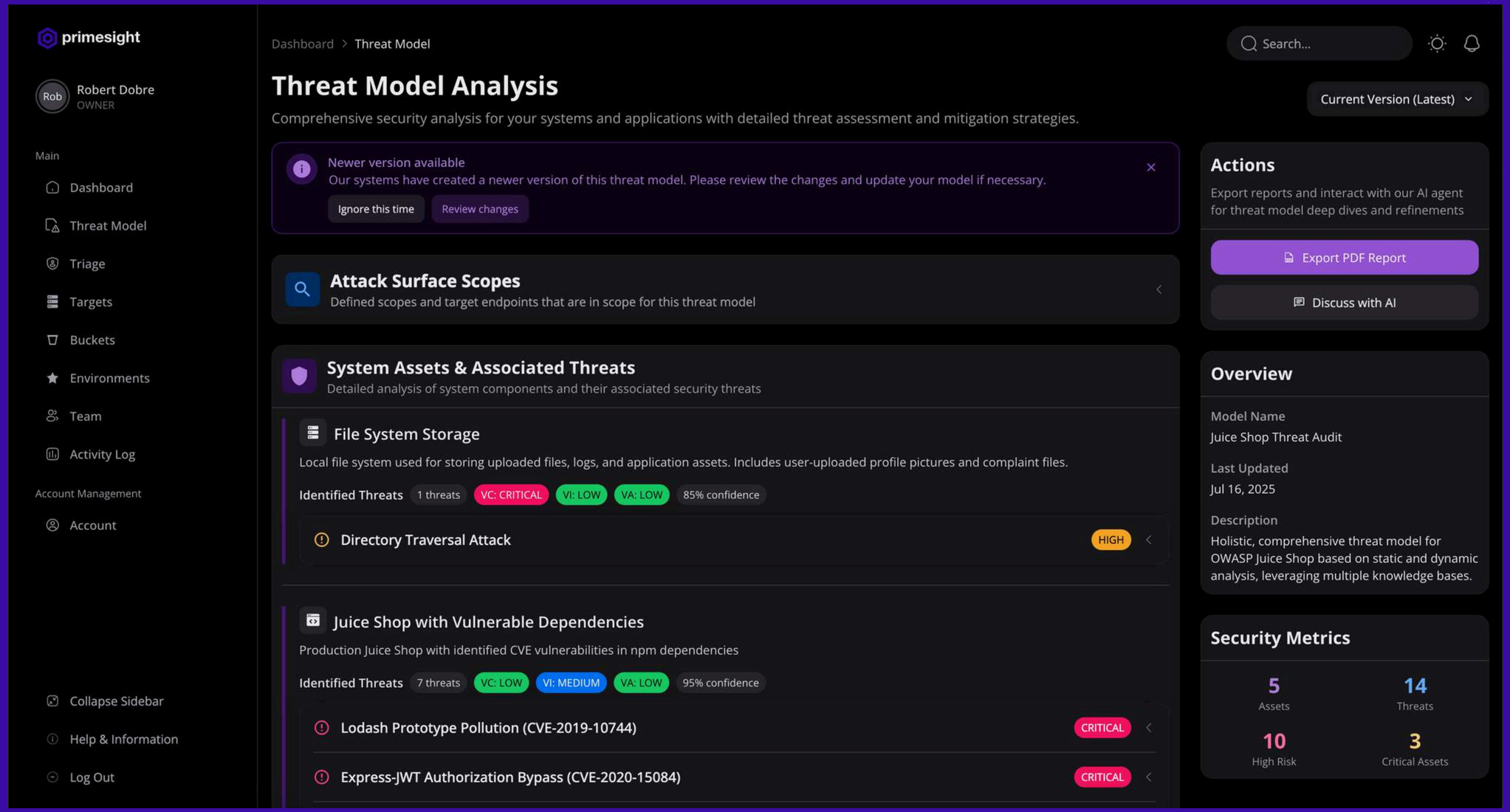
Head of AI

Tiberiu Baron

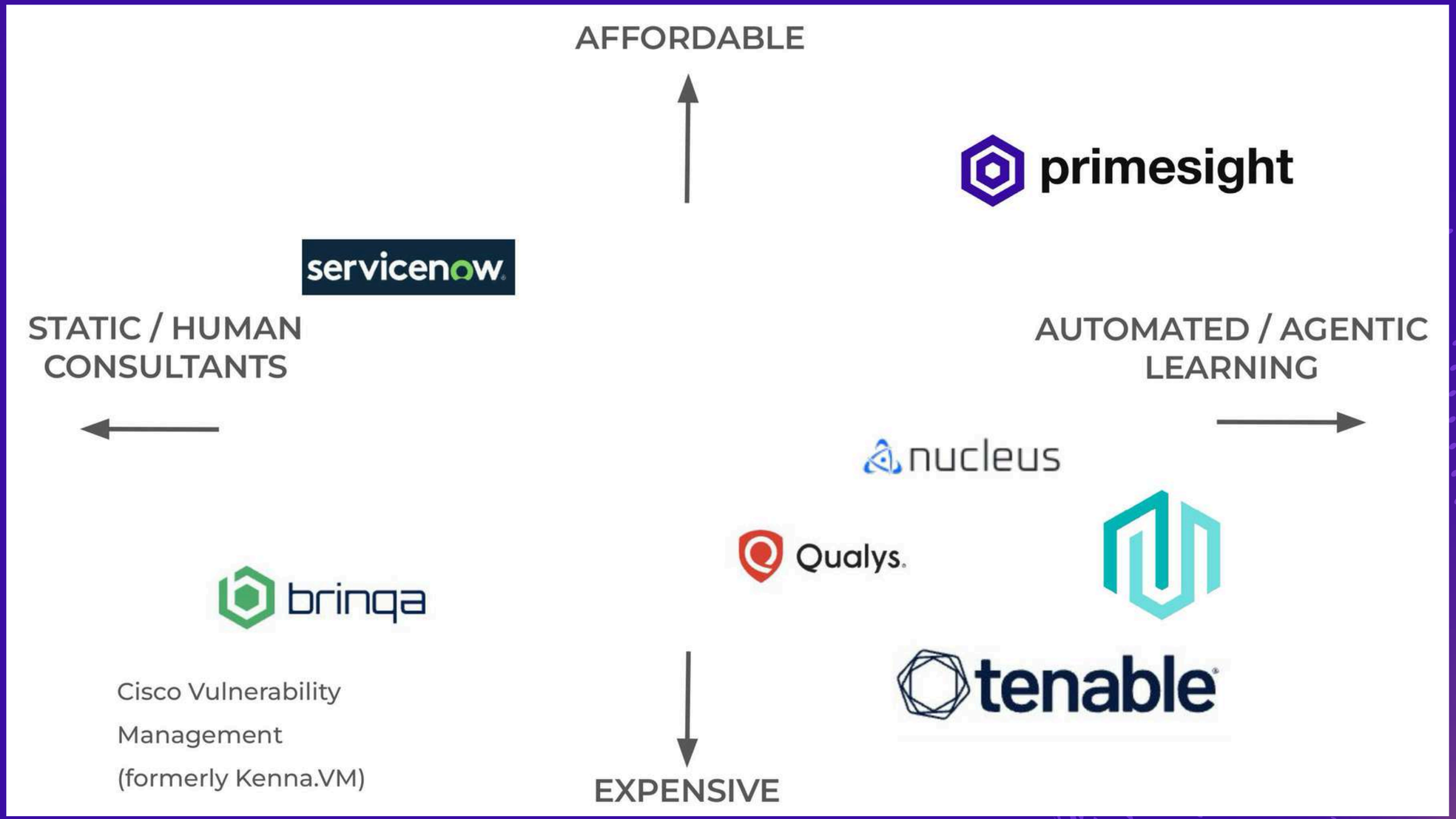
Senior Security Engineer @ **UiPath**

Tech Lead @ **IOS**

LET’S SEE THE MAGIC



HOW DO WE COMPARE?



BUSINESS MODEL - PASSIVE ENVIRONMENT MONITORING

- $2000/mo base to $5000/mo enterprise (20% off/yr -> $19,200/yr to $48,000/yr);
- Annual expansion through additional product modules;
- Bespoke features and analytics for top customers;
- 86% gross margins with AI infrastructure costs declining yearly (o3 -> $2/$8 per 1m tokens).

BUSINESS MODEL - DYNAMIC DISCOVERY & EXPLOITATION

- On-demand, usage-based pricing:
  - medium sized target ~$2,500 / run;
  - rolling cost for detected changes.
- Trained on testing any type of attack surface: applications, infrastructure, servers, mobile, etc.
- Information is directly connected to our Cortex.

BUSINESS MODEL - CONTINUOUS THREAT MODEL

- Usage-based pricing for attack surfaces of any size - starting from $1,500/mo to $4,500/mo.
- Vertically integrated with popular tools for recording of risks.
- Aimed towards the business team, keeping recommendations actionable and easy to understand.

COMPETITIVE ADVANTAGES

- Bespoke automated agentic assessment integrated in your workflow;
- Instant meaningful feedback integrated with your ticketing platform;
- Long-term product memory that improves;
- Zero learning curve;
- Founding team with proven enterprise security expertise;
- Cloud-based or on-premise, per-tenant deployment for strict compliance;
- Flexible, predetermined or usage-based pricing that makes sense.

PRODUCT ROADMAP

- Fully automated triage with code analysis (GitHub/Gitlab);
- Complex vulnerability validation using automated scans;
- Rich integrations with popular SME solutions;
- Auditor - Client - Vendor secure messaging platform;
- Industry tailored compliance modules;
- Human-in-the-loop engineers for understaffed teams.