

Investigate at the speed adversaries move



AI for Adversary Risk Intelligence
(AI for AI)

RECOGNIZED BY



ABOUT US

Protos Labs: Built by Cyber Operators, Powered by AI

Who We Are

Protos Labs is a Singapore-based **Cyber AI company** founded by **ex-Booz Allen cyber operators**.

- 1 **Focused on Adversary Risk Intelligence**
Focused on analyzing bad guys and their risk to an enterprise.
- 2 **Battle-Tested with DIAs**
Co-built and deployed with Defense & Homeland Security agencies since 2024.
- 3 **Global AI & Cyber Recognition**
Nvidia Inception, Microsoft AI Accelerate, CSA Cybercall 2 x Winner
- 4 **Multi-Market Presence**
Active business in SG, US, and TH markets.

The Founders



Joel Lee

Co-founder & CEO
Ex-Booz Allen (Cyber Intelligence)



Simeon Tan

Co-founder & CTO
Ex-Booz Allen (OT Security)

The US Team



Sam Goh
Field CISO &
GM of USA
(Based in New York)

Ex-CISO, Siam Commercial Bank
DataX (Data & AI CoE)

The Advisors

Winston Chir

Ex-CISO, advisor to Alphabet
(Based in San Francisco)

Tzachi Karako

CISO for Data & AI,
Standard Chartered Bank
(Based in Singapore)

OUR ACHIEVEMENTS

Trusted by Investors, Clients & Partners Worldwide

\$ INVESTORS

We are backed by top-tier institutional investors across APAC and USA.

👥 CLIENTS & PARTNERS

Proven with **Defense & Homeland Security agencies** and **government**, now expanding into commercial enterprises.

🏆 RECOGNITIONS

NVIDIA Inception
Global AI programme (2026)

Microsoft
AI Accelerate programme (2026)

CSA CyberCall — 2× Winner
Cyber & Sovereign AI

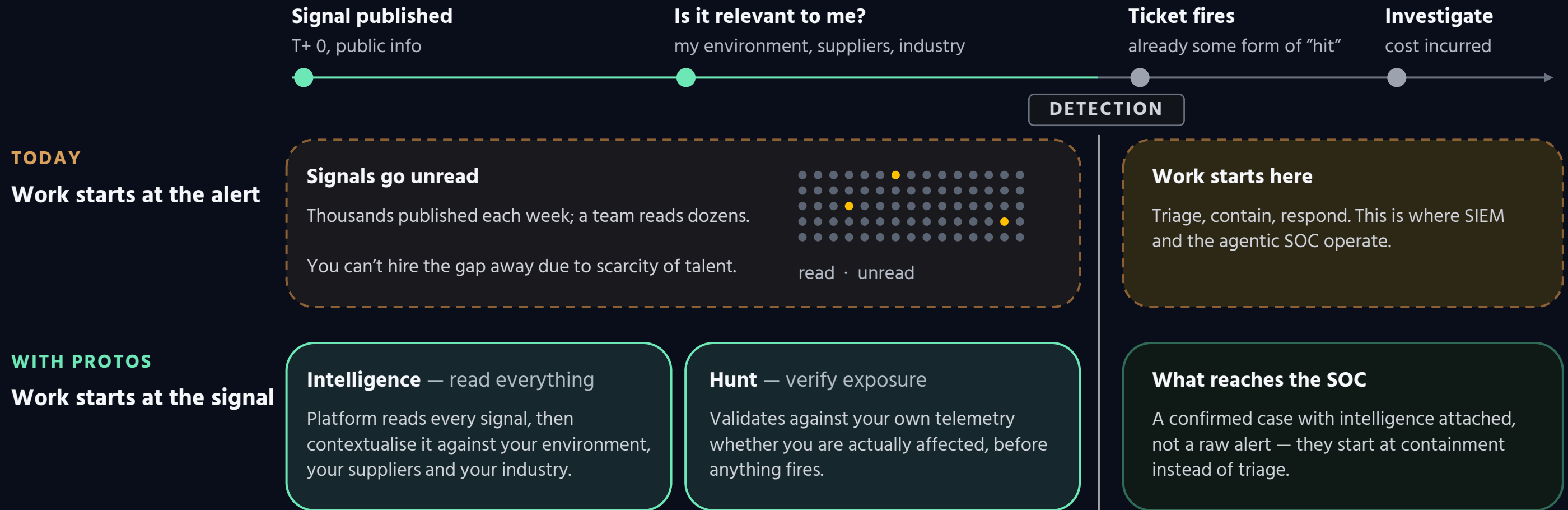
Top 20 Startups in Singapore
Recognized by Tech in Asia

Lloyd's of London Lab
First Singapore company admitted

NCSA
People's Choice Award

THE PROBLEM

Proactive cyber defence should start at the signal, not the ticket



An agentic SOC starts at the ticket. **We start at the signal.**

Protos AI – Adversary Risk Intelligence Platform

Protos AI starts upstream with early warning signals, so your SOC acts on verified intelligence before the ticket fires.



USE CASES

What do people use our platform for?

CORE TODAY



Pre-Attack Vuln. Mgmt

Act on brewing exploits before a CVE drops, and map exposure within minutes after

Deep-dive: [slide 8](#) →



Software Supply Chain Risk

Assess every vendor's cyber exposure and monitor them for active targeting



Influence Operations

Expose the operators and networks behind a hostile narrative before it shapes opinion

Deep-dive: [slide 10](#) →



Cyber Threat Investigations

Turn IOCs and new threat reports into actor-linked leads across your logs



Autonomous Threat Hunting

Turn adversary intel into hunt plans and sweep your telemetry for compromise

EXPANDING



Financial Crime Investigations

Enrich transactions with fraud patterns and dark web intelligence, and screen entities against sanctions, ownership structures and adverse media

Our Differentiators

Forged at the frontier

D&I → commercial

Built on the hardest national-security problems, then brought to commercial enterprises. It's a capability that rivals can't buy and customers can't build for themselves.

Patent filed in Singapore; US filing in progress.

Optimised for cost efficiency & accuracy

The right method for each task

We use agents only where necessary. Established AI/ML methods handle the deterministic steps, such as entity extraction, and agents are kept for work that needs judgement. This helps to reduce cost and enhance data collection accuracy.

Model-agnostic by design

Never locked in

Models change constantly, and ours isn't tied to any single one. That keeps our focus on domain tradecraft, enterprise integration and scale, not on which model tops this week's benchmark.

Data we collect ourselves

Proprietary data collection

We run our own first-party data collection using our tech + tradecraft, something rivals can't replicate.

High-level methodology can be shared under NDA.

Tailored to customer's workflow

Sticky by design

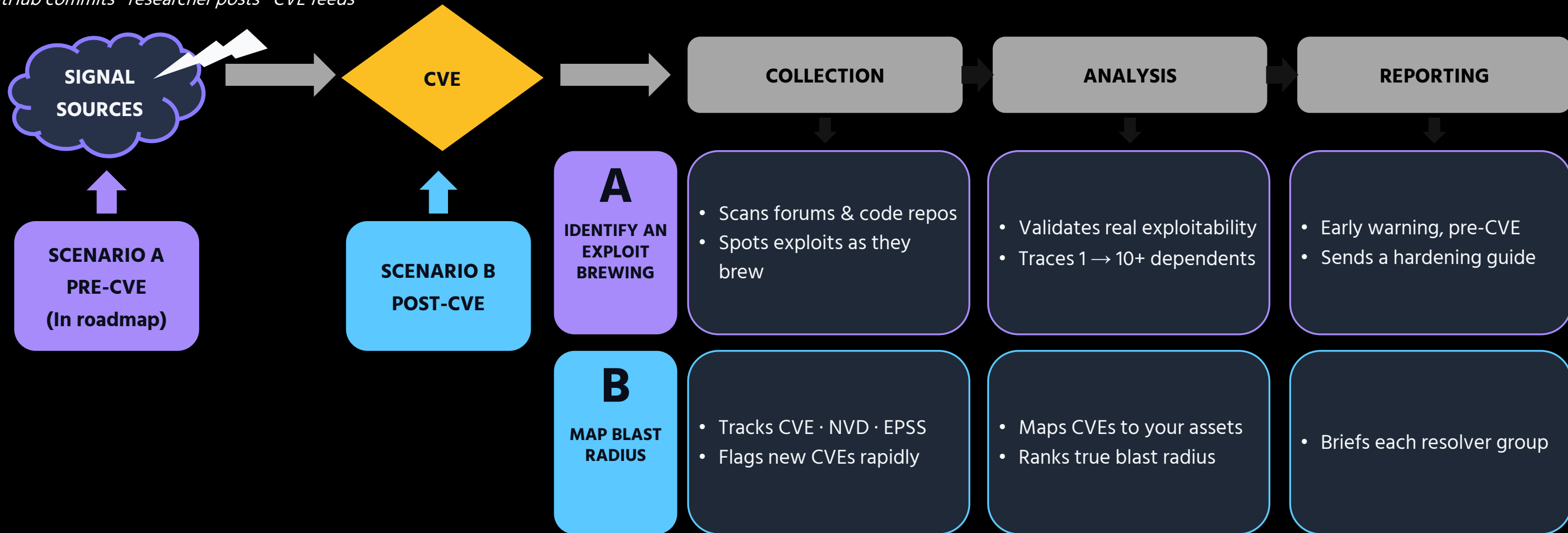
Our software is designed to codify how each customer works, specifically data sources, investigation workflows and analytical methods. That knowledge compounds and is what makes us hard to replace.

SAMPLE USE CASE

Use Case #1 – Pre-Attack Vulnerability Management

TODAY	Teams act only after a CVE is published	CVEs need manual contextualization to customer environment.	"A vuln exists somewhere"
WITH PROTOS	Track upstream signals before a CVE exists (e.g. Github commits)	Contextualization is automatic. Exposure pinpointed within minutes	" This one reaches you ", and how

Github commits · researcher posts · CVE feeds

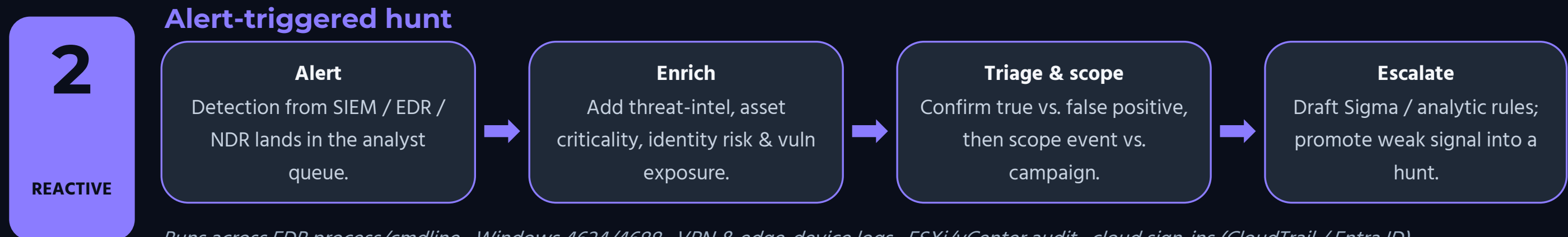


Use Case #2 – Autonomous Threat Hunting

Two triggers for threat hunting — proactive and alert-initiated.



e.g. UNC3886 / CAULDRON PANDA — ESXi/vCenter & Fortinet 0-days (CVE-2023-34048, -2022-41328); valid-account + LOTL persistence.

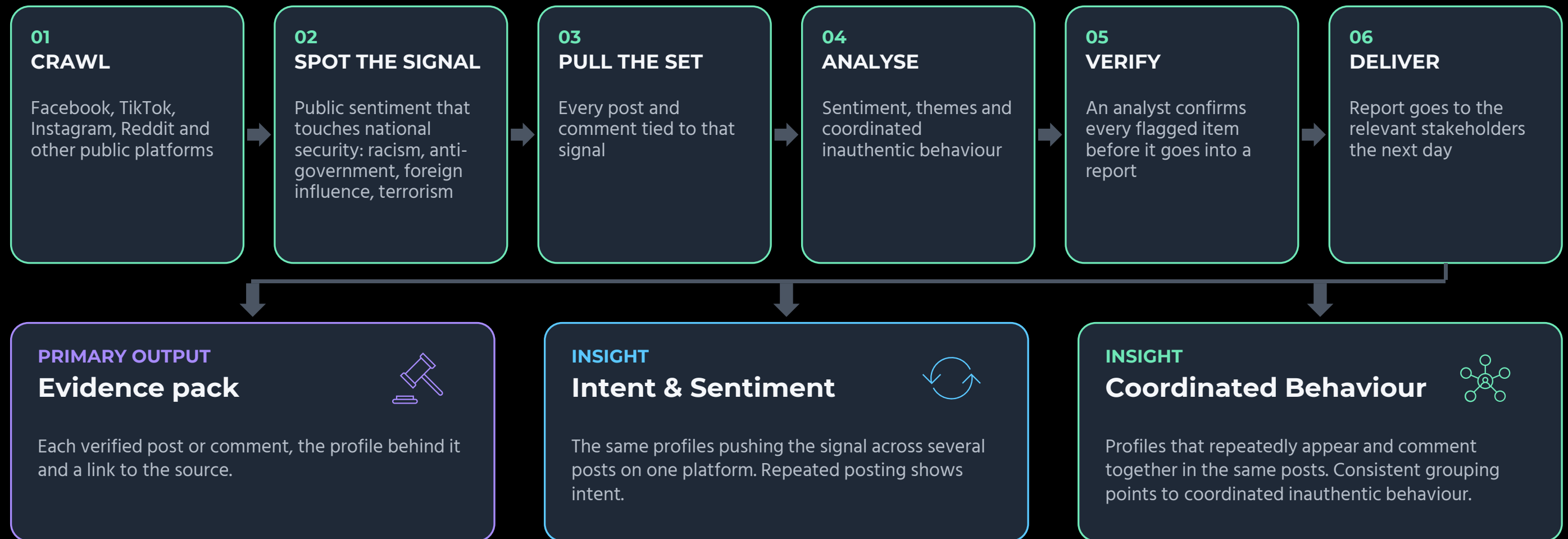


Runs across EDR process/cmdline · Windows 4624/4688 · VPN & edge-device logs · ESXi/vCenter audit · cloud sign-ins (CloudTrail / Entra ID)

SAMPLE USE CASE

Use Case #3 - Influence Operations

TODAY	Only search-indexed links readable	Images and video go unread	Profile updates have to be manually read by a human	Reports take days to compile
WITH PROTOS	Every post and comment can be pulled, even non indexed ones	OCR and transcripts used to read images and video	Watchlists flag new posts as they are published	Report delivered the next day



CASE STUDY

Retrospective Threat Hunt: 1M Log Rows, Found 1 Anomalous Event in 2 hours

The Challenge

A **sectoral lead** providing core network infrastructure to education and research institutes in Singapore — data-rich, lean on dedicated security staff, and answerable for sensitive research data — needed to know whether any threat had **slipped through undetected** over a 30-day window. Without AI, that meant a retrospective hunt across **~1M rows of network logs**.

- A full month of telemetry — **~1M log rows**, far too many to review manually.
- **Manual hunting too slow** as in-house team lacked the tradecraft; also, the need to correlate with external intelligence feeds added tooling complexity

The Solution & Outcome

With **Protos AI** running an **autonomous retrospective threat hunt**, ~1M rows of logs were analysed and enriched with cyber-threat intelligence for every event:

- **Speed** — the full hunt completed in **~2 hours, versus 16+ hours** of manual analyst work
- **Signal found** — amid the noise, **1 anomalous finding** surfaced, later confirmed by one of the member organisation's CISO to coincide with a real incident
- **Now routine** — threat hunting is now fast and cheap enough to **run as BAU**, not a one-off specialist activity

CASE STUDY

Threat-Intelligence Analysis: A 4-Hour Manual Cycle, Done in **15 Minutes**

The Challenge

A **cyber threat intelligence team** producing threat intelligence at volume for multiple critical-infrastructure sectors — a small analyst pool working across a sprawl of separate feeds and enrichment tools. Without AI, every investigation meant **manually stitching data across disconnected tools**, and each analysis cycle took **~4 hours or more** — capping how many threats the team could cover in a day as an outfit dependent on government funding.

- IOC enrichment — domains, IPs and hashes looked up across **separate, disconnected tools**
- Context buried in **unstructured reports**, advisories and PDFs
- **~4 hours or more** per cycle, capping daily throughput

The Solution & Outcome

With **Protos AI** acting as an **autonomous enrichment and correlation engine**, it queries open-web, structured feeds, dark web feeds and enrichment tools in parallel, parses the unstructured reports, and clusters IOCs, victimology and TTPs into one analysed view:

- **Speed** — each enrichment cycle cut from **~4 hours to ~15 minutes** (a ~16x speed-up)
- **Throughput** — the same team runs far more investigations per day, with **no added headcount to keep costs low**.
- **Focus** — analysts move from repetitive low-value work to recommendations and in-person briefings

CASE STUDY

Financial-Crime Investigations: Automating Case Evidence Review & Offence Mapping

The Challenge

A government law-enforcement agency with statutory investigative powers, running document-heavy financial-crime cases where every finding must hold up as court evidence. Without AI, investigators **manually analysed large volumes of case files in different structured and unstructured formats** — slow, hard to keep consistent, and reliant on tacit knowledge to map offences to the right statutes.

- Manual collation of **high document volumes** slowed every case
- Consistency hard to hold across investigators and case types
- Every finding needed **clear, auditable links** back to source evidence
- Mapping offences to statutes relied on investigators' **tacit knowledge**

The Solution & Outcome

With **Protos AI**, tailored to the team's analysis workflow and report templates, every data retrieved is analysed as supporting evidence, with **full traceability**:

- **Speed** — document analysis cut from **days to hours**, freeing investigators from reading and processing to focus on judgement
- **Accuracy & rigour** — **94.7% accuracy** across ~180 submitted documents, with offences mapped to the relevant statutory offices
- **Scale** — a **tailored, repeatable workflow** lets the team clear more cases consistently, without adding investigators

CASE STUDY

All-Source Intelligence Fusion: Cyber, OSINT & Dark-Web in One Workflow

The Challenge

A **national-security organisation** with an all-source intelligence remit spanning cyber, social-media and geopolitical collection, turning raw feeds into decision-ready reporting under time pressure. Without AI, multi-source collection arrived in **incompatible, siloed pipelines**, leaving analysts with **no unified way to make sense of it**.

- Requirements span cyber, social-media and geopolitical domains
- Data arrives in **multi-format sources** in large scale
- **No unified sensemaking** — pattern-finding stayed largely manual and slow

The Solution & Outcome

With Protos AI, purpose-built for multi-source investigation, cross-domain collection is normalised and correlated in a **single analytic environment** — enriching and profiling indicators across OSINT, social, deep- and dark-web sources:

- **Unified picture** — open, social and deep/dark-web inputs **correlated in one workflow**
- **Speed** — indicators enriched and profiled **at machine speed, not through manual querying of tools**
- **Tailored output** — strategic, operational and tactical products from **one pipeline to support senior-level decision-making**

Ready to See Protos AI in Your Environment

Protos AI has been in mission-critical environments since 2024 and is now available to commercial enterprises as well.

The fastest way to evaluate it for your team is a 4-week paid Proof-of-Concept (POC) on a live use case in an environment that mimics yours.

Sam Goh

Field CISO & Sales Lead for USA

sam_goh@protoslabs.io

Swee En Tan

Account Executive & Sales Lead for Singapore

swee_en_tan@protoslabs.io

