Threat Hunting Is No Longer a Luxury

AI-driven attack discovery systems like Mythos make it easier to identify weaknesses and attack paths across an environment.

Detection alone cannot fully cover all possible attack paths and behaviors. It is designed to react to known patterns and signals, so some activity will always go undetected.

As a result, security teams need to go beyond reacting to alerts and incorporate proactive validation, using threat hunting to continuously test for what may be happening outside of detection.

THE Daylight Service

Daylight provides threat hunting as a managed service.
Security experts define what to look for. A coordinated swarm of AI agents executes the investigations across your environment.
This allows threat hunting to run at scale, without being limited by analyst time.

Hypothesis-based Hunts

Hypotheses are defined to proactively test for activity not covered by detection across your environment.
Each hypothesis is executed across historical data.

IOC-based Hunts

When threat intelligence surfaces specific indicators like IPs, domains, file hashes, Daylight hunts them across your environment.

New intel becomes an active hunt in seconds.

THE Daylight Difference

01 Hunts cover the **last 90 days** of telemetry, with extra context pulled via API.

02 An **AI swarm** runs multiple threat analyses across your environment in parallel.

03 Every hunt goes from hypothesis to findings in **under 5 minutes**.

04 Every hunt is fully auditable: what ran, what was analyzed, what was found.

HOW IT WORKS

From hypothesis to outcome in minutes

1. **Hypothesis Definition**
   A Daylight expert defines a hypothesis (e.g. service-account misuse, lateral movement) and selects analyses from a maintained catalog.
2. **Deterministic Data Extraction**
   Each analysis starts with a predefined query across up to 90 days of telemetry. All analyses run in parallel.
3. **Iterative Investigation**
   Specialized agents form a coordinated swarm—each iteration refines the dataset, eliminating benign activity until only unexplained behavior remains.
4. **Controlled Orchestration**
   A central system tracks every query, decision, and output—enforces execution bounds and provides full traceability.
5. **Outcome Determination**
   Either all activity is explained (hypothesis disproven), or unexplained activity is escalated and converted into new detections.

Three approaches. One clear leader.

	daylight	Traditional Hunting	Automated Tools
End-to-end execution (no analyst-driven workflow)	●	○	◑
Hypothesis-driven discovery of unknowns	●	◑	○
Adaptive investigation (not template-bound)	●	◑	○
Scales beyond human capacity (parallel hunts)	●	○	◑
Controlled, explainable, and auditable	●	◑	○
Continuous, not episodic	●	○	◑

THE DAYLIGHT SOLUTION

Expert Brain. Agentic Muscle.

Security experts define the methodology. A coordinated swarm of AI agents executes investigations in parallel, in minutes.

daylight

Visit **daylight.ai** or email **info@daylight.ai**