A New Model of MDR

Not a traditional MDR. Not an AI SOC tool.

AI agents run investigations at scale. Security experts provide the context, judgment, and ownership needed to resolve alerts—eliminating backlogs quickly.

THE Daylight Service

Daylight MDR combines an AI-native platform with security experts in a unified architecture for the full SOC cycle. The platform integrates deeply across endpoint, cloud, identity, and SaaS, collecting business context to reach definitive verdicts, not escalations. Security experts from IR and threat hunting backgrounds resolve ambiguous cases, customize detections, build knowledge that improves future investigations, and lead response during confirmed incidents.

Three approaches. One clear leader.

	daylight	Traditional MDR	AI SOC Tools
Full investigation on every alert	●	○	◐
Cross-system context per investigation	●	○	◐
Custom detection	●	◐	○
24/7 security expert coverage	●	◐	○
Full transparency into decisions	●	○	◐
Alert backlog eliminated at source	●	○	○
Custom response	●	◐	○

THE Daylight Difference

AI-Native, Not AI-Augmented

Built from day one as an AI-native platform, not a legacy MDR with AI bolted on. A fundamentally different architecture.

Glass Box Transparency

Every investigation shows what data was consulted, what logic was applied, and why the verdict was reached. See the work, not just the outcome.

Integration in Days, Not Months

120+ integrations, built in days. Every integration is bi-directional, we don't just detect threats, we close them at the source.

Senior Experts Only

10+ years in IR and threat hunting. No junior analysts. No after-hours quality variance. Experts continuously improve context and detections.

Three built-in coverage extensions

Extending MDR into surfaces most providers leave unmonitored.

01 AI Security Detection & response for AI-native threats

Daylight builds detection coverage on top of Claude Enterprise activity logs, Otel runtime telemetry and the Compliance API, and integrates with AI security tools including Noma Security, Zenity, and more.

- Detects unauthorized MCPs, prompt injection attempts, credential exfiltration via agents, and risky AI usage patterns.
- Every AI-native alert investigated in full enterprise context.
- Investigate alerts triggered by AI security tools.

02 Phishing Investigation & Response

Every alert investigated to a verdict. Daylight integrates with your email security platform and investigates every alert end to end, including user-reported phishing - at a scale analyst-driven MDRs can't match. High alert volumes are handled at the scale that analyst-driven MDRs cannot sustain without triaging cases away.

- Full investigation for every alert, including user-reported issues, not just high-severity cases.
- Agentic investigation removes the volume constraint that forces traditional MDRs to skip cases.
- Response coordinated across email, identity, endpoint, and SaaS context.

03 DLP Investigation & Response

Thorough investigation where most MDRs Stop. Daylight integrates with your DLP platform and conducts full investigations, not alert routing. DLP events are low volume but complex; most MDR providers decline to investigate them due to the analyst time and expertise required.

- Full investigation of complex data loss events, not surface-level triage.
- Determines intent: accidental exposure, policy violation, or deliberate exfiltration.
- Response-ready findings with affected data scope, timeline, and containment recommendations.

THE DAYLIGHT SOLUTION

Expert Brain. Agentic Muscle.

AI agents handle the full detection-to-response cycle. Security experts step in where human judgment matters most.

daylight

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