corelight

Solution brief

Investigator Agentic Triage

Drive future-ready defense by automating the investigation lifecycle with agentic triage

Corelight Investigator Agentic Triage is built on a modern GenAI agent architecture designed specifically for real-world security operations. Integrating Agentic Triage into your SOC workflows allows teams to automate the predictable, repeatable parts of investigations. Security teams can conduct entity-centric investigations grounded in expert-authored playbooks to ensure every investigation follows consistent, defensible triage logic.

The challenge

Security operations teams are operating under a convergence of pressures, making traditional SOC approaches unsustainable. Adversaries are leveraging GenAI to increase the speed and volume of threats, while SOC teams struggle with limited time, staff, and alert fatigue. To detect and respond to these threats today, teams need AI automation, but existing solutions introduce critical limitations:

AI-accelerated attacks
Adversaries are actively experimenting with GenAI to automate reconnaissance, scale phishing campaigns, and accelerate attack execution. Security teams must respond faster and more consistently to keep pace.

Alert overload and analyst burnout
It has become increasingly difficult for SOC analysts to keep up with the volume of alerts, facing screen fatigue and excessive false positives. Scaling manual, alert-by-alert triage is unrealistic.

The "black box" trust problem
Many security vendors rebrand legacy machine learning systems as "AI," providing minimal transparency. Proprietary AI systems conceal their reasoning and evidence, eroding analyst trust, introducing risks such as AI hallucination, and making audits more difficult.

Complex automation workflows
Traditional SOAR initiatives frequently fail due to their complexity, heavy engineering requirements, ongoing maintenance burden, and poor alignment with real-world analyst workflows.

The solution

Corelight delivers Agentic Triage built on a modern GenAI agent architecture that executes structured, defensible playbooks created by Corelight's network experts. Unlike proprietary AI systems or complex SOAR tools, Agentic Triage strategically embeds into the investigative workflow to automate routine work while preserving human judgment and oversight.

Accelerate incident response: Entity-centric investigations

- Consolidate hundreds of individual alerts into single, entity-centric investigations to reduce alert fatigue
- Receive high-fidelity, evidence-backed triage outcomes driven by structured, expert-designed security playbooks
- Reduce mean time to recover (MTTR) from hours to minutes for critical entities

Trusted AI for enterprise SOCs: "Trust but verify"

- Gain an instant understanding of alerts with transparent AI-powered step-by-step reasoning that explains exactly how a verdict was reached
- Ensure safe AI adoption with clear privacy handling; no customer data is ever used to train or fine-tune models
- Pivot to pre-correlated, raw forensic-quality data without leaving the page to validate every AI decision

Accelerate SOC efficiency: Consolidate for results

- Automate the predictable, repetitive parts of investigation work, allowing analysts to focus on high-value decision-making
- Streamline workflows with single-screen triage; one click takes analysts from an entity-centric summary to pre-correlated context and interactive visual timelines
- Receive clear confidence assessments (high/medium/low) for each triage outcome, helping teams prioritize response efforts
- Increase analyst productivity, enabling teams to handle up to three times as many cases

The solution in action

Agentic Triage shifts the focus from a massive queue of individual alerts to a short, prioritized list of the highest-risk entities, so analysts can start their day looking at actual, pre-triaged threats. The system has automatically consolidated the alerts into a single, entity-centric case for a compromised Windows workstation, executing an expert playbook that identifies malware downloads and C2 beaconing. The analyst is provided with a transparent summary of the blast radius and the exact playbook logic used to reach the verdict, enabling them to confidently validate the evidence and initiate an enterprise-wide response in minutes rather than hours.