Elastic Security 9.6 adds AI agents for SOC alert triage



Elastic Security 9.6 introduces AlertZero, AI agents that triage alerts and hunt threats, plus Linux ransomware protection and 143 detection rules for AI platforms. AlertZero is in technical preview.

- AlertZero groups AI Workers into four Watches: triage, threat hunting, detection engineering and forensics; the technical preview has six Workers.
- Three autonomy levels (Manual, Assisted, Supervised) control whether analyst approval is needed before an action runs.
- Elastic Defend extends behavior-based ransomware protection to Linux and adds custom YARA scanning of process memory.
- 143 SIEM rules cover hijacked coding agents, malicious MCP servers, leaked credentials in prompts, jailbreaks and stolen API keys.

> - Self-managed and cloud-hosted availability is expected in early December.

Elastic has announced Elastic Security 9.6, with AlertZero as its main addition: a set of AI agents that work in the background on alert triage, threat hunting and detection rule tuning.

How AlertZero works

Agents are called Workers and are organized into four teams: triage, threat hunting, detection engineering and forensics. The technical preview includes six Workers. Each runs on a schedule or reacts to events such as new alerts, then proposes an action, for example closing a false positive or isolating a host, with supporting evidence.

Teams choose among three autonomy levels. In Manual mode every action needs analyst approval. In Assisted mode Workers can investigate rules and coverage gaps on their own, but changes still need approval. In Supervised mode selected actions run without prior approval and analysts review them afterward. Approved actions run with the analyst's privileges and are recorded as that analyst's decisions. Customers also choose the model tier, including open-weight and self-hosted options.

Other changes in 9.6

Elastic Defend brings behavior-based ransomware protection to Linux hosts and allows custom YARA signatures to scan process memory. The release adds 143 SIEM detection rules for AI-related threats, mapped to MITRE ATLAS and MITRE ATT&CK, and improved entity resolution across endpoint, identity and cloud data. Automatic Migration now supports chat-based editing of rules translated from Splunk, QRadar and Microsoft Sentinel.

Availability

AlertZero is in technical preview in Elastic Cloud Serverless. Elastic expects 9.6, including the new Elastic Defend features, in Elastic Cloud Hosted and Self-Managed deployments in early December. Teams considering it should treat the autonomy setting as a governance decision rather than a default.

What to do now

1. If you use Elastic, review the 9.6 release notes and plan testing once it reaches your deployment model in early December.
2. Start any AlertZero pilot in Manual mode and define which actions, if any, may later move to Supervised mode.
3. Confirm that analyst approvals of agent-proposed actions are logged and fit your SOC accountability and audit requirements.
4. Check where model processing occurs and whether self-hosted models are needed before sending alert

data to an AI service.

5. Review the new AI-threat detection rules against your own use of coding agents and MCP servers.