



INTERRO AI

// AUTOMATION ENGINEERING SHOWCASE

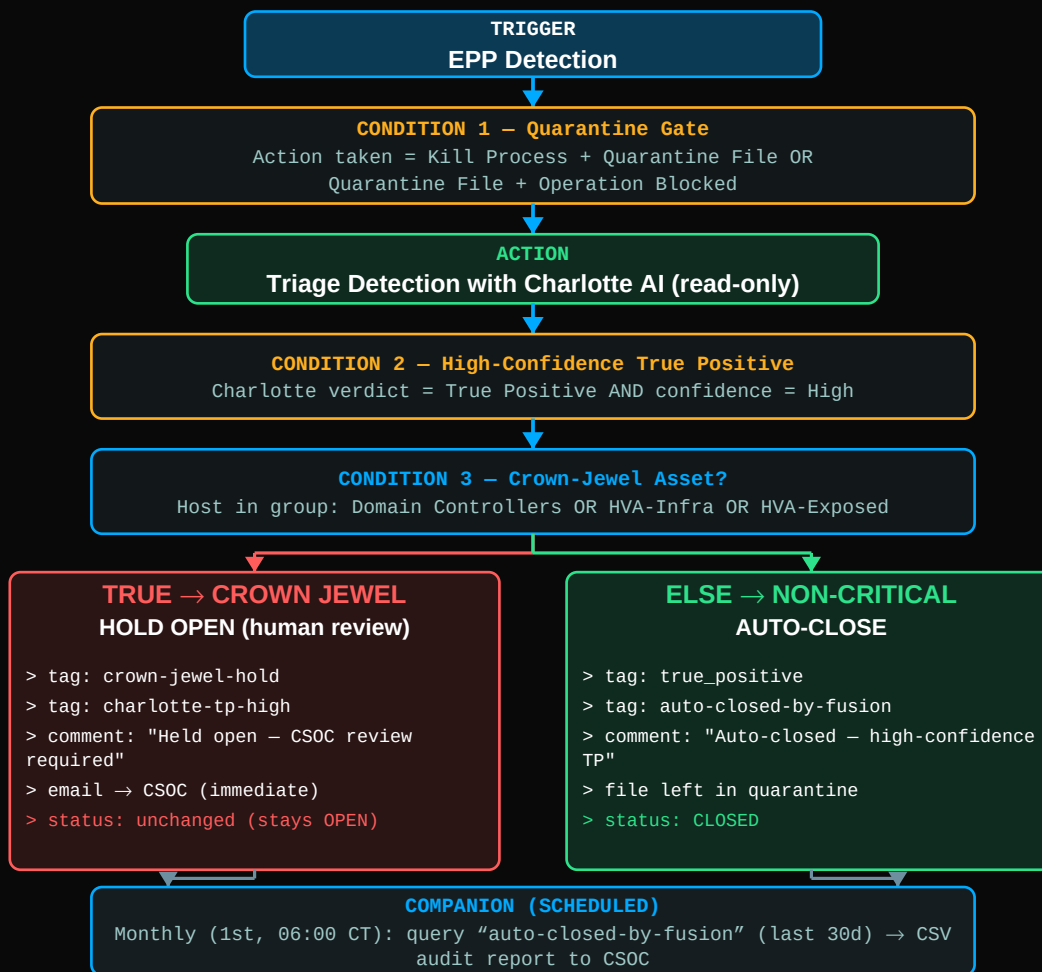
// CROWDSTRIKE FUSION SOAR × CHARLOTTE AI

Crown-Jewel-Aware Auto-Close

An automated triage workflow that lets Charlotte AI close the alerts it's confident about — and automatically holds the ones that touch your most critical systems for a human to review.

The Workflow

EPP DETECTION → TRIAGE → CROWN-JEWEL CHECK → CLOSE OR HOLD



Why It Matters

Most auto-close automation is a blunt instrument: it either closes everything a model is confident about, or it closes nothing and analysts drown in the queue anyway. This workflow does neither.

Charlotte AI enriches; it doesn't decide alone. The AI's verdict is one gate among three — it only ever triggers an action alongside a hard technical condition (quarantine confirmed) and an asset-criticality check. No single signal can close or suppress an alert on its own.

Crown jewels always get a human. Domain Controllers and other high-value infrastructure are hard-coded to bypass auto-close entirely, regardless of how confident Charlotte is. The alert stays open, tagged, and emailed to CSOC immediately.

Everything closed automatically is still auditable. Auto-closed detections are tagged distinctly and swept into a monthly CSV report sent straight to CSOC — so “automated” never means “unaccountable.”

Built to reduce fatigue, not risk. The goal isn't fewer alerts on a dashboard. It's fewer low-value alerts competing for analyst attention with the ones that actually touch critical infrastructure.

// This is one workflow from a broader Fusion SOAR automation library built for critical-infrastructure Falcon environments.