

Gathering Is Not Triage. Open Every Case Ready to Decide.

First-line analysts spend the opening minutes of every case collecting context across the ticketing system, the SIEM, the EDR, directories, and threat intelligence before they can judge anything. Legion gathers first, from the systems you already run, and writes the recommended next steps into the ticket. Your analysts make the call, and the right action follows.

Why does every case begin with a hunt across tools?

Ticketing holds the case and its history	SIEM holds the logs	EDR holds the detections	Directories hold who and what was involved	Threat intelligence holds the reputation of what was seen
--	-------------------------------	------------------------------------	--	---

Five sources each hold part of the case, and no single system holds the whole truth, so the analyst assembles it by hand as the SLA clock runs. Legion reads all five the moment a ticket is created and writes the evidence and the recommended next steps into the ticket.

TODAY — STATUS QUO

Every case is assembled by hand

01 Ticket lands Queue assigned	02 Open the tabs Tool by tool	03 Check history Search by hand	04 Judge severity Experience only	05 Write it up From a blank note	06 Escalate Tier 2 reworks	CASE REBUILT
--	---	---	---	--	--	-------------------------------

WITH LEGION INTELLIGENCE

Nothing is executed without an analyst's decision

01 Ticket lands Legion starts	02 Evidence pulled All sources, once	03 History found Past cases linked	04 Severity set SLA clock flagged	05 Recommendation Written to ticket	06 Analyst decides Resolve, escalate	CLEAN HANDOFF
---	--	--	---	---	--	--------------------------------

IN THE PACK

Triage Recommendation · evidence summary and recommended next steps, in the ticket

Duplicate Ticket Grouping · related reports under one parent case

Severity and Escalation · signals, SLA deadlines, escalation package

Historical Context Enrichment · prior tickets and outcomes as work notes

URL and IOC Analysis · reputation and OSINT results in the ticket

Response Actions Status Report · completed, skipped, and open remediation steps

ANALYSTS KEEP DECISION AUTHORITY

Legion gathers, validates, and recommends. Your analysts decide and act. No autonomous defensive actions. CUI and restricted data stay compartmentalized under attribute-based access control.

No rip-and-replace. Legion works across the ticketing, SIEM, EDR, directory, and threat-intelligence systems you already run, at machine speed, in a single view. ServiceNow, Splunk, and CrowdStrike Falcon are connected today. Your data stays in your environment, and models never train on it.



Start With Your Busiest Queue

We'll run an approved sample of your tickets through the Pack and show the summaries, groupings, and escalation packages, with your analysts deciding.

[LEGIONINTEL.COM](https://legionintel.com)

TRUSTED WHERE THE DATA CAN'T LEAVE

Running on-prem at a U.S. Department of Energy national laboratory, inside the lab's own access controls.

