

INTERRO AI — In Simple Terms

WHAT IT IS

INTERRO AI is a subscription platform giving security teams an expert AI security analyst on demand. Ask it questions or hand it tasks in plain English, and it performs the skilled SOC work — across whatever SIEM or tools you already run (Chronicle, Sentinel, Splunk, Cortex XSIAM, CrowdStrike, and more). It's tool-agnostic, so teams aren't locked into one vendor's query language.

WHAT IT ACTUALLY DOES

- Writes detection rules in the right language for your platform (YARA-L, KQL, SPL, XQL, Sigma).
- Enriches indicators — IPs, hashes, domains, CVEs — from threat-intel sources in one step.
- Builds playbooks, threat reports, and incident write-ups, exported to PDF or Word.
- Maps findings to MITRE ATT&CK and NIST D3FEND, so results stay framework-grounded.
- Assesses vulnerability and threat posture, and suggests remediations.

THE PROBLEMS IT SOLVES

AREA	PROBLEM TODAY	HOW INTERRO HELPS
Time drain	Writing a detection rule, report, or enrichment by hand takes hours.	Done in minutes, correctly formatted for your platform.
Workload & alert fatigue	Small teams are buried in repetitive triage and lookups.	Offloads repetitive analysis so analysts focus on real decisions.
Skills gap	Not everyone knows every query language or framework.	Junior analysts get senior-level, cross-platform depth instantly.
Inconsistency	Output quality varies by who's on shift.	Standardized, framework-mapped results every time.
Cost of scaling	Hiring more analysts or consultants is expensive.	A subscription that lets a lean team punch far above its size.

IN ONE SENTENCE

INTERRO AI turns hours of specialized SOC work — rule-writing, enrichment, reporting, investigation — into minutes, in plain English, across any security stack. It saves analyst time, cuts workload, closes the skills gap, and scales expertise without scaling headcount.