Blue Team Defense + Red Team Offense = Purple Team SOC

PURPLE SOC

AI Purple Team Security Operations Center

AIR-GAP COMPATIBLE | ZERO CLOUD DEPENDENCY

// OVERVIEW

What Purple SOC Does

A traditional SOC requires analysts watching screens 24 hours a day, manually triaging alerts. AI Purple SOC replaces analyst fatigue with agents that run continuously, never miss an alert, and correlate events across your entire environment simultaneously — combining Blue Team defense and Red Team offense in a single locally-hosted platform with no licensing costs.

<90s	9	$0	100%
ALERT TO REMEDIATION	AI AGENTS	LICENSING COSTS	LOCAL DEPLOYMENT

// BLUE TEAM

Defensive Agents (24/7 Passive)

LOGWATCHER
Ingests logs from all systems via Filebeat/Syslog. Detects failed logins, privilege escalations, unusual process spawns, and file changes in real time.

THREATDETECTOR
Classifies anomalies against 10,000+ local Sigma rules — the same detection rules used by enterprise SOCs worldwide. No cloud lookup required.

NETWORKSENTINEL
Monitors network flows using Zeek/Suricata. Flags lateral movement, unexpected outbound connections, and port scanning between systems.

INCIDENTRESPONDER
Builds full incident timeline, scores severity, drafts response playbook. Holds for human approval before taking any action.

// RED TEAM

Offensive Agents (Scheduled)

CYBERSCOUT
Runs scheduled nmap scans against all systems to find open ports and running service versions. Returns structured data to VulnAnalyst.

VULNANALYST
Cross-references discovered services against offline NVD/CVE database. Assigns CVSS risk scores and identifies actively exploited vulnerabilities.

EXPLOITVERIFIER
Human-gated. Uses Metasploit in check-mode to verify if a CVE is actually exploitable — not just theoretically present — before reporting.

REMEDIATOR
Generates specific bash or Ansible patch scripts for confirmed vulnerabilities. Activated only after human approves ExploitVerifier findings.

// PURPLE LAYER

SOCDirector — Master Orchestrator

SOCDirector is the master orchestrator running on the LLM hub. It routes tasks between Blue and Red agents, correlates findings from both sides, and connects the dots automatically. Example: Red Team finds Apache CVE-2021-41773 (CVSS 9.8) on a host. Three days later, Blue Team sees path traversal in the logs on that same host. SOCDirector links these two events and escalates immediately — because it knows from the Red Team that this host is vulnerable to exactly this attack pattern. Total time from first failed login to remediation option presented: under 90 seconds.

HUMAN-IN-THE-LOOP: Critical actions require explicit operator approval via the dashboard before execution.