LIMA CHARLIE

AGENTIC SECOPS WORKSPACE

Security infrastructure for human and AI operators

Security vendors sell you products. LimaCharlie provides infrastructure. Our security hyperscaler is built for modern operations where human analysts and agentic AI work side by side.

Every capability (detection, response, automation, multi-tenancy, telemetry) is delivered as an API-accessible primitive that both your team and AI agents use the same way. Our Agentic SecOps Workspace (ASW) ensures every AI action is visible, governed, auditable, and reversible.

Unlike advisory or chatbot-driven "AI SOCs," LimaCharlie treats AI as an accountable security operator that can investigate, decide, and act directly within real environments.

ASW Features and Capabilities

The Agentic SecOps Workspace is an API-native environment where security capabilities and resources integrate seamlessly. Tools, services, and AI operate as equals, designed to interoperate without vendor-imposed constraints or gatekeeping.

API-first, on-demand

All ASW capabilities are delivered as cloud-native security primitives through an open API. Teams gain full control and visibility over their security stack without contracts, mandatory sales cycles, or capacity planning.

Detection and response

High-performance EDR enables endpoint response in under 100ms. Teams can author highly customized detections, subscribe to open and curated rule sets (including Sigma, YARA, SOC Prime, and Soteria), and allow agentic AI to investigate and act within predefined workflows.

Multi-tenancy

Manage multiple organizations consistently from a single platform. Granular role-based access, rapid tenant provisioning, and infrastructure-as-code deployments make it easy to scale operations across hundreds of environments.

Automation and agentic workflows

Define and execute automated actions on endpoints to reduce manual effort and accelerate response. Orchestrate complex investigations, threat hunting, and remediation using rules, workflows, or natural language prompts with agentic tools like Claude Code.

Unified data format

All telemetry is normalized into an open JSON schema, providing a single plane of visibility and greater control over how security data is queried, transformed, and reused.

Telemetry ingestion and retention

Ingest logs and files from any source and process them through detection, automation, and response pipelines. One year of free telemetry retention reduces SIEM and data lake costs while enabling powerful queries and AI-driven exploration.

Ecosystem and integrations

Access a rich ecosystem of 100+ built-in capabilities and integrations, including open-source tools like Atomic Red Team and Velociraptor. Bring your own LLM and deploy agentic AI on your terms, without platform lock-in.

Flexible, transparent pricing

Pure usage-based pricing eliminates contracts, capacity planning, and opaque cost models. Pre-deploy sensors cost-effectively and avoid the overhead of advisory-only AI SOC services by running AI directly on shared infrastructure.

Data forwarding and control

Route telemetry to any destination. Transform, enrich, or anonymize data in-flight to reduce costs, improve observability, and retain full control over data outputs.

> **If I were building a new cybersecurity company, I'd build it on top of LimaCharlie.**
>
> —Philip Martin, CSO, Coinbase

ASW Use Cases

The Agentic SecOps Workspace supports enterprises, MSSPs, and security builders with an API-first, cloud-scalable foundation for automated and AI-driven operations.

1. Investigate and respond with AI agents

Unlike advisory AI SOC tools, ASW enables AI agents to conduct full investigations, query telemetry, execute response actions, and remediate threats within governed workflows.

2. Reduce SIEM and data lake costs

Use ASW as an observability pipeline to filter, enrich, and route telemetry. Minimize data sent to high-cost SIEMs and replace expensive data lakes with one year of free rolling storage.

3. Enhance or replace legacy EDR

Deploy consistent detection, automation, and response across operating systems. Teams and AI agents can author detections, automate workflows, reduce MTTD and MTTR, and decrease reliance on traditional EDR platforms.

4. Scale security operations

Native multi-tenancy, granular access controls, and on-demand infrastructure allow teams to provision environments in seconds and deploy changes across thousands of endpoints with a single command or AI prompt.

Who is ASW for?

MSSPs

Standardize operations across clients with built-in multi-tenancy and scalable agentic workflows.

Enterprise

Simplify your security stack, reduce costs, and deploy auditable AI.

Builders

Ship faster using open APIs, well-documented primitives, and bring-your-own-LLM flexibility.

About LimaCharlie

LimaCharlie is the only security operations platform where AI operates, not just advises. Book a demo or try ASW for free at **limacharlie.io**