

## THE LIMACHARLIE SECOPS CLOUD PLATFORM

# Helping MSSPs Improve Security Operations and Gain Competitive Advantage

The LimaCharlie SecOps Cloud Platform (SCP) is a unified platform for modern cybersecurity operations. Unlike other vendors in our industry, the SCP delivers core cybersecurity capabilities and infrastructure on-demand, pay-per-use, and API-first.

For the cybersecurity industry, this is a paradigm shift for cybersecurity comparable to how the IT public cloud revolutionized IT. For managed security services providers (MSSPs), the SCP represents a new way to improve security operations and compete more effectively.



**Our ability to onboard customers quickly and confidently has dramatically increased, because our ability to scale is no longer limited by our ability to maintain our security infrastructure.**

—Andrew Cook, CTO, Recon InfoSec

## How MSSPs Benefit from the SCP

The SCP gives MSSPs full control over how they build and scale their businesses. Here are the core benefits for service providers:



### Flexibility

- ◆ All capabilities are delivered on-demand and API first as in an IT public cloud model.
- ◆ Choose only the capabilities you want. Never pay for something you don't need. Scale up or down as needed.
- ◆ Build custom solutions that suit your SecOps workflows rather than changing or limiting your workflows to fit a vendor's solution.
- ◆ Access new capabilities and enroll new client organizations with ease—and without contract negotiations, sales meetings, and vendor gatekeeping.



### Easy management

- ◆ Leverage multi-tenant architecture and advanced role-based access control to manage multiple organizations in a single platform.
- ◆ Subdivide client environments as needed in a fine-grained way.
- ◆ Spin up pre-configured tenants in seconds to streamline onboarding of new customers.
- ◆ Roll out changes to multiple clients at scale using infrastructure as code.



### Simplicity

- ◆ Import logs, file types, and other telemetry data from any source—including other EDRs and third-party tools.
- ◆ Normalize all telemetry data to a common JSON format for a single pane of visibility.



### Advanced detection, automation, and response

- ◆ Improve response times and operational efficiency with the SCP's powerful Detection, Automation, and Response Engine.
- ◆ Respond to events on endpoints at wire speed (<100ms) using the SCP's powerful, lightweight agent.
- ◆ Use automation to eliminate time-consuming manual tasks and define and automate response actions based on telemetry data.
- ◆ Unify detection and response with an EDR that has the widest platform support industry-wide and feature parity across operating systems.
- ◆ Write highly customized detection logic or subscribe to open-source and curated rule sets like SOC Prime, Soteria, Sigma, and YARA.



## Cost control

- ◆ The SCP's public cloud-like pricing model provides transparent, predictable pricing (always).
- ◆ Pay only for what you use. No contracts, capacity planning, or price modeling—and no surprises.
- ◆ Choose the billing format that works best for you—whether you want a single invoice for all of your customer organizations or billing separated out by client.



## Free storage

- ◆ All telemetry data brought into the SCP includes one year of retention.
- ◆ Meet compliance needs without needing to send every byte of data to a high-cost storage solution.
- ◆ All telemetry is stored in a rich, queryable format to allow you to perform retroactive threat hunts.



## Capabilities on demand

- ◆ The SCP offers a rich ecosystem of capabilities and integrations (100+ and growing).
- ◆ Add new capabilities for your customers without having to take on a new vendor.
- ◆ Reduce tool sprawl and eliminate one-off vendors in your stack by replacing these solutions with SCP alternatives.
- ◆ Leverage open-source tools that have SCP integrations, such as Velociraptor, Atomic Red Team, Canarytokens, YARA, Sigma, Zeek, and more.



**We truly feel like LimaCharlie is an extension of our own team. The tech is great—but the relationship is easily the best part.**

—Glenn Starkman, CEO, Soteria

## ABOUT THE MSSP PARTNER PROGRAM

The LimaCharlie *MSSP Partner Program* helps service providers take advantage of joint marketing opportunities, customer referrals, and our experienced team of business and technical advisors.

To learn more and become a partner, visit [limacharlie.io/mssp-partners](https://limacharlie.io/mssp-partners)

## ABOUT LIMACHARLIE

LimaCharlie is creating a new paradigm for security operations teams and enterprises through the SecOps Cloud Platform. To learn more, book a demo, or try the SCP for free, visit [limacharlie.io](https://limacharlie.io)

# SCP Use Cases for MSSPs

Here are some of the ways our MSSP partners are already leveraging the SCP to improve security operations, save money, and compete more effectively:



### Solve narrow problems for customers

If a client asks for a capability or service you don't offer, you can deliver using the SCP's on-demand, pay-per-use capabilities. The SCP lets you say "yes" to customers without having to purchase new tools or build bespoke solutions from the ground up.



### Improve SLAs with usage-based billing

The SCP offers pure usage-based billing options, allowing MSSPs to pre-deploy EDR sensors to client environments in "sleeping mode" at a very low cost and activate them only when needed. This enables incident responders to offer extremely competitive SLAs—in some cases as fast as 20 minutes.



### Create efficient, scalable workflows through automation

The SCP is designed to enable an engineering-centric approach to security operations. Create scalable, automated security workflows that eliminate manual tasks, increase operational leverage, save time and money, and free your teams to pursue higher-value tasks.



### Build a brand with our custom branded offering

LimaCharlie can be used as an OEM provider, white-labeled, and using your own custom sub-domain. Take full control over your pricing and convey the value you provide to your customers by listing the SCP as your underlying infrastructure.