

# Security Operations for the Modern Age

Security teams face a dynamic and increasingly complex cybersecurity landscape. This situation has spawned a host of one-size-fits-all security solutions—and vendors trying to be all things to all users. Teams find themselves forced to stitch together a fragmented collection of inflexible solutions, resulting in tool sprawl, security gaps, integration challenges, inefficiency, and high costs.

The cybersecurity industry doesn't need yet another tool or solution. It needs an entirely new paradigm—a transformation comparable to what the IT public cloud did for IT. The **LimaCharlie SecOps Cloud Platform (SCP)** is this new approach for our industry.

The SCP delivers the core components needed to secure and monitor any organization, similar to how IT cloud providers deliver foundational IT capabilities. The SecOps Cloud Platform represents a truly modern approach to security operations. It is the future of cybersecurity.



If I was to build a new cybersecurity company, I'd build it on top of LimaCharlie.

—Philip Martin, CSO, Coinbase

## SCP Capabilities and Features

The SecOps Cloud Platform is an environment where many security capabilities and integrations can exist, not as a collection of random tools, but as a series of cybersecurity solutions designed to interoperate in an un-opinionated way. For this reason, the SCP offers unparalleled value to security teams and the organizations they defend:



### On-demand and API-first

- ◆ Gain full control over and visibility into your security stack with a platform that offers all capabilities as cloud-native cybersecurity primitives through an open API.
- ◆ Access cybersecurity capabilities on-demand without having to worry about contract negotiations, mandatory sales meetings, or vendor gatekeeping.



### Multi-tenancy

- ◆ Manage multiple organizations consistently and seamlessly from a single platform.
- ◆ Implement advanced role-based access across organizations for fine-grained control.
- ◆ Spin up new pre-configured tenants in seconds.
- ◆ Roll out changes to hundreds of organizations at once using infrastructure as code.



### Detection and response

- ◆ Leverage a powerful and customizable EDR to respond to events on endpoints at wire speed (within 100ms).
- ◆ Improve your detections by writing highly customized detection logic or subscribing to open-source and curated rule sets like SOC Prime, Soteria, Sigma, and YARA.



### Automation

- ◆ Define and execute automated actions on endpoints, accelerating incident response and reducing manual effort.
- ◆ Enable proactive threat hunting and mitigation.



### Unified data format

- ◆ All telemetry data normalized to an open JSON format, giving you increased control over your data and a single plane of visibility.



## Telemetry ingestion and retention

- ◆ Ingest logs and file types from any source—allowing you to centralize your telemetry data and run everything through our advanced Detection, Automation and Response Engine.
- ◆ One-year free telemetry storage offers immediate cost savings and a simple way to reduce the amount of data sent to SIEMs and costly data lakes.
- ◆ Use our powerful and intuitive query capability to explore telemetry data from within the SCP



## Data forwarding

- ◆ Send telemetry data to any destination you like to reduce costs and improve observability.
- ◆ Transform, enrich, and anonymize data in-flight for granular control over your telemetry outputs.



## Ecosystem of capabilities and integrations

- ◆ Take advantage of a rich ecosystem of 100+ capabilities and integrations—including numerous open-source tools and services.



## Flexible, transparent pricing

- ◆ On-demand, pay-as-you-go pricing model reduces costs and keeps spending predictable.
- ◆ No contracts, capacity planning, or price modeling to give you greater flexibility and freedom.
- ◆ Pure usage-based billing options that offer a cost-effective way to pre-deploy sensors to endpoints if needed.

# SCP Use Cases

The SecOps Cloud Platform offers myriad use cases for enterprises, MSSPs, and cybersecurity solutions builders—and because the SCP follows the model of the IT public cloud, teams and organizations can leverage its capabilities progressively:



### Replace expensive data lakes and reduce SIEM spending

The SCP's ingestion, retention, and forwarding capabilities make it ideal as a pass-through to optimize data routing—reducing the amount of data sent to high-cost SIEM tools and replacing expensive data lakes with the platform's free storage feature.



### Use the SCP as an observability pipeline

Normalized telemetry data means the SCP can be used to gain visibility across your entire organization under a single plane—no matter what the source of the telemetry.



### Enhance or replace existing EDR tools

The SCP's powerful Detection, Automation, and Response Engine is built for speed and customization, and offers the widest platform support industry-wide with feature parity across operating systems. Write custom detections, speed MTTD and MTTR, automate responses and security workflows, and move toward replacing your current EDR solution altogether.



### Build scalable security operations

The SCP's multi-tenant architecture, on-demand capabilities, and fine-grained role-based access control allow service providers and organizations to manage security operations at scale. The SCP's infrastructure-as-code approach lets you provision new tenants in seconds and roll out changes to thousands of endpoints with a click.

## LIMACHARLIE SCP IS SUITABLE FOR

### Enterprise

Simplify your stack, reduce costs, and free your team from the task of integrating and managing fragmented tools.

### MSSP

Simplify and standardize the management of your clients.

### Builders

Create customized products and services quickly using the SCP's robust, well-documented capabilities and open API.

## ABOUT LIMACHARLIE

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