Refraction Point Inc.
340 S Lemon Ave #5258
Walnut, CA 91789
United States

MSSP Starter Kit

limacharlie.io

Welcome to the LimaCharlie.io MSSP Starter Kit. In this document you will find information on starting your evaluation and deployment of customers on LimaCharlie.io as well as MSSP best practices and training/material available.

Our focus on MSSPs means that if you find yourself looking for advice, training or information, we have resources available to you.

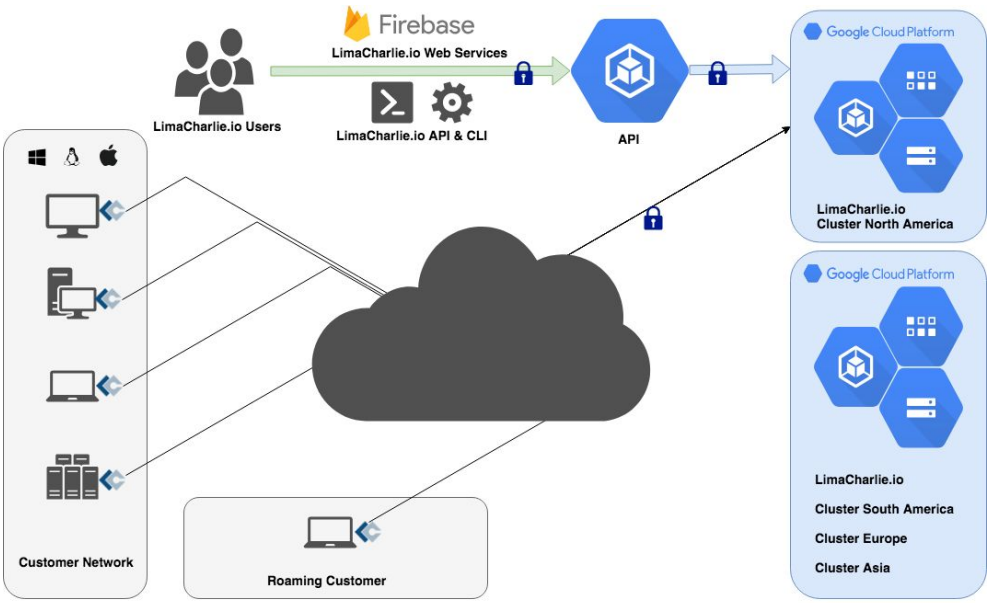
The terms “agent” and “sensor” are used interchangeably.

For more information on this document or other MSSP related topics, you can reach us at: mssp@limacharlie.io

TABLE OF CONTENT

Architecture

LimaCharlie.io is a multi-tenant architecture built on top of Amazon Web Services.



Security is of the utmost importance, which translates into multiple levels of security.

Every cluster is built across multiple availability zones to maintain high-availability.

Clusters are available in multiple regions to deal with any legal requirements. All access to these clusters is transparent, allowing MSSPs to provision new customers wherever they see fit.

Connectivity between agents and the clusters is done point-to-point and is secured using pinned SSL certificates.

This enables extremely easy deployments and seamless transition of assets between offices and networks.

Each cluster has its own transport keys and each organization has its own command keys. All keys are encrypted in storage and runtime access to the envelope keys is limited to server containers. All sensitive output configurations are encrypted per organization.

Agents support Windows XP and up, MacOS and Linux distributions.

Setting Up an MSSP

Concepts

As an MSSP, you will have multiple customers on-boarded into LimaCharlie.io. We aim to make this multi-tenancy as easy as possible.

The first concept to understand is the concept of Organization. Each of the following types of objects are managed per-organization:

- **Agents** belong to a specific organization.
- **Installation Keys** are keys used to enroll an agent within the organization.
- **Outputs** are forwarding rules for parts of the data generated by an organization's agents.
- **D&R rules** are automation rules used both to manage agents as well as to perform automated Detection & Response and are managed by organization.
- **API Keys** are secret keys you use to interact with our API and are limited to the scope of an organization.
- **Quotas** are simply the maximum number of agents that may be online at one time for an organization. There is no minimum and it can be adjusted at any time.

Billing / quota is also managed at the organization level. This means that in most cases, you will want to use one organization for one customer. This makes billing, onboarding, management and termination much easier.

Users are simply accounts on LimaCharlie.io and are identified using an email address. A user can be granted access to multiple organizations and an organization can have multiple users associated with it. Users having access to an organization are also able to transitively grant access to other users. Obviously everything is logged, auditable and the logs can be transmitted to an archival facility in order to be tamper-proof.

More advanced facilities to manage MSSP membership and user association are going to be available in the near future.

Organizations can be created at will and always include a free tier (2 sensors). This makes it easy to streamline a small proof-of-concept

with a new customer and simply grow it as needed when they begin wider rollouts.

All accounts have an initial limit on the number of organizations they may create. If you need more simply get in touch with us and we will increase your limit.

Onboarding Checklist

This checklist is meant as a discussion on topics that are relevant prior to onboarding a new customer.

Organization

Transferring agents between organizations is a complex affair, but scaling up and down as well as granting access to an organization is easy. This means the first step to onboarding a new customer, even if only for a trial, should be to create an organization.

Organizations are free and begin with a two agent free tier, so don't hesitate. If you hit the maximum number of organizations, get in touch with us and we'll increase your limit.

Installation Keys

The Installation Keys (IK) are used to enroll new agents. One IK can be reused as many times as you want, it remains valid until you delete it, after which time agents already enrolled will keep their access, but new agents will not be able to enroll with it.

This makes it easy to revoke keys and maintain a tighter control over installer agents.

The main reason to have multiple IKs is to associate tags with agents. Each IK has a list of tags to attach to agents enrolling using it. For an MSSP this provides an easy first pass at categorizing agents.

For example, you may create an IK with tag "server", and another with "desktop". Then it's a matter of asking your customer to use the relevant IK for the relevant assets.

Tags can also be added/removed either programmatically or interactively after enrollment.

Outputs

The Outputs is the component forwarding the data to your infrastructure. The data is composed of three main “streams”: event, detect and audit.

The audit stream tends to be the easiest, where do you want to store a copy of the audit messages. It’s not technically required, but we recommend to at least send it to a write-only location like an AWS S3 bucket.

Next is the detection stream. Usually this is fairly high priority data and therefore you will want it to go a live system rather than an archiving one. It is common to send it to the SIEM or a product like Splunk.

If some of the detections can be more verbose, you can also customize outputs so that only certain detection types go to a cold storage and others to a live system.

Finally, the event stream is by far the most verbose. It contains the raw events coming from the agents. Most cost-conscious MSSPs will, as a general rule, send all the events to cold storage. A popular method is to use an AWS S3 bucket with a retention period set (like 3 months), and to upload data to it with compression enabled.

The event data is very verbose so that it can be easily used operationally, but it also compresses extremely well (~90%). So for cold storage, enabling compression is a good idea.

Another common setup is to tag sensitive agents as “vip” and configure an Output to send the event stream from these agents to a live system like Splunk so that it is always readily available.

Automation

The first few organizations you onboard will likely be done manually. But you will quickly want to store your “infrastructure as code”.

Using the sync tool part of the Python API, you can backup an organization's configuration as YAML files and organize them so that you re-use base configurations across all your customers.

The tool will allow you to export to YAML and apply the YAML back up to the cloud. This results in a more efficient onboarding process and a better repeatable process.

For a more complete discussion, see the related blog post: https://www.limacharlie.io/blog/2018/7/5/organizing-detection-response-rules

Training

LimaCharlie.io offers several types of training for different purposes.

MSSP Onboarding Training

Duration: 1 day

When an MSSP first begins to use LimaCharlie.io, this training provides help in evaluating the various types of architectures, data flows and integrations possible.

This training is highly customized to the specific needs of the customer.

Common topics include:

- SIEM Integration
- Agent Deployment Strategies
- Detection & Response rules development and maintenance
- Use cases and demonstrations to customers
- LC data interpretation and interaction

Basic Operator Certification

Duration: 1 day

The Basic Operator Certification (BOC) uses a curriculum targeted to operators that will be dealing with LimaCharlie operations day-in day-out. This certification is officially recognized by LimaCharlie.

Curriculum covers:

- LC data interpretation
- LC agent interaction
- Detection & Response rules creation, testing and tweaking
- Threat feed integration

LC Certified Trainer Program

Duration: 2 days

The Certified Trainer Program (CTP) covers in-depth topics relating to all aspects of deployment and operation of LimaCharlie. This

certification is officially recognized by LimaCharlie and trainers are listed and recommended through LimaCharlie websites.

Curriculum covers:

- Agent deployment and connectivity troubleshooting
- Advanced agent capabilities and customization
- Creation of advanced data flows and integrations
- Advanced API usage
- Advanced Detection & Response rules development
- Best practices for MSSPs at the organization level

Custom Requests

We also offer customized training. Whether it is a specific topic, or you would like training in your own language, contact us and we will refer you to LC Certified Trainers that can meet your demand.

training@limacharlie.io

Documentation

LimaCharlie.io offers public documentation at http://doc.limacharlie.io.

Of particular interest if this is your first time using LimaCharlie.io is the Quick Start section which includes information that should get you up and running in no time.

Additional, documentation and source for bindings in other languages:

- **Python**: https://github.com/refractionpoint/python-limacharlie/
- **JavaScript**: https://github.com/refractionPOINT/limacharlie-js

The underlying REST API Swagger documentation:
https://api.limacharlie.io/static/swagger/

White Labelling

LimaCharlie.io strives to make it easy for customers to white-label capabilities created on top of it. Part of this effort is to ensure the systems built by us are based on the same APIs (REST, Python and JS) our customers have.

The main starting point towards white-labelling LimaCharlie.io is in the Digger system (digger.limacharlie.io). This system is a standalone React webapp that serves as a simple web-based portal to navigate LC data as well as interrogate LC agents.

It is entirely built onto the public API and we make the source available to MSSPs as it provides a great starting point to creating a customized set of tools to your customers.

For other questions regarding white-labelling, drop us a line at:

mssp@limacharlie.io

Demo Scenarios

The MSSP Starter Kit will include a list of demonstrations of various features and capabilities of LimaCharlie in a format easy to reproduce. These will be available in the near future.