Quick Start Guide

CROGL
AI for Enterprise Security

Prerequisites

Supported Operating Systems:

- **macOS:** Tahoe or later (Intel or Apple Silicon)
- **Linux**: Tested on Ubuntu 24.04, Ubuntu 22.04, Amazon Linux 2023, RHEL 9, and AlmaLinux 9; both x86_64 and arm64 are supported, including Graviton-class EC2 hosts. The installer adapts to the distribution it's running on, so other modern Linux versions generally work. If you run into an issue on a distribution not listed here, let us know.

Docker: Must be installed and your user must be a member of the docker group.

Hardware:

Resource	Testing (Min / Recommended)	Production (Min / Recommended)
CPU	8 cores / 16 cores	8 cores / 16 cores
RAM	8 GB / 16 GB	32 GB / 64 GB
Disk	5 GB / 12 GB	20 GB / 50 GB

Before You Begin

Have the following ready before starting installation:

- **LLM API Key**: An API key from Anthropic or OpenAI. From Anthropic, we recommend **claude-opus-4.5** or **claude-sonnet-4.5**, and from OpenAI, we recommencd **gpt-5.2**. If you're self-hosting a model instead, you'll need its endpoint URL.
- **Data source credentials:** API keys or credentials for at least one of the following. You can always add more connectors later.
  - A **querying system** — (SIEM, data lake, or log source such as Splunk, Elasticsearch, Sentinel, Databricks, or Cribl) lets Crogl search your logs and alerts during investigations, pull relevant events directly into the case, and run threat hunts across historical data.
  - A **case management system** (e.g. Jira, ServiceNow) — lets Crogl read and update cases, attach investigation findings as it works, and keep your ticketing system in sync without manual handoffs.
  - An **enrichment tool** (e.g. VirusTotal, CrowdStrike) — lets Crogl look up IPs, domains, and file hashes to add reputation, threat intel, and endpoint or identity context to every alert it triages.

1. Download Crogl

Download the installer for your platform from your download page.

2. Run the Installer

Open a terminal, navigate to the folder where you downloaded the installer, and run:

macOS

Shell

```
bash crogl-installer-macos.sh --start
```

Linux

Shell

```
bash crogl-installer-linux.sh --home "$HOME/crogl-test" --start
```

3. Trust the certificate (macOS only)

On macOS, Crogl needs to add a self-signed certificate to your system trust store. You'll be prompted twice: once in the terminal, once via a macOS system dialog.

Enter your Mac password at both prompts to proceed.

4. Create Your Credentials

The installer will prompt you to create a username and password. You'll need these to sign in to Crogl; Store them somewhere safe before continuing.

5. Save Your Credentials & Startup Key

When installation completes, the terminal will display a **startup key** (the encryption key your Crogl server uses to unlock its own secrets). You'll need it any time you restore, migrate, or recover this installation, and it cannot be regenerated. If you lose it, you must reinstall from scratch.

Save the startup key and the credentials from **step 4** somewhere secure before closing your terminal. A password manager is strongly recommended.

6. Open Crogl and Sign In

The installer will display the URL for your Crogl instance when it finishes. Open that URL in a browser. For macOS, fully quit and reopen your browser first to pick up the updated certificate trust.

Sign in with the credentials you created in **step 4**, then follow the setup steps to configure an LLM and connect Crogl to your environment.

7. What to Do Next

Once you've signed in, and configured Crogl to use your LLM and at least one Connector you are ready to use Crogl. You can use natural language to ask Crogl to triage or investigate alerts or use one of Crogl's skills to help you with your work. The pills (oval buttons below the chat) are short-cuts to use a skill:

- **Investigate alert:** Vendor-agnostic alert triage built around the MITRE ATT&CK framework. Works across EDR, network, identity, and cloud log sources to investigate and prioritize alerts, regardless of which tool generated them.
- **Threat hunt:** Investigate a threat advisory by URL, ID, or free-text description. Crogl researches the threat, generates a hunt plan tailored to your environment, and executes the hunt interactively with you.
- **Create a skill:** Guides you through creating a new skill or updating an existing one. Use it to extend Crogl with specialized knowledge about your team's workflows, or new tool integrations all in chat with no code required.
- **Incident report:** Assemble the findings, timeline, and remediation steps from an investigation into a structured report ready to share with stakeholders.

You can also ignore the pills entirely and just describe what you want to do and let Crogl decide which skill to use as needed.

What is a skill?

A **skill** is a reusable workflow you can ask Crogl to run. The four pills under the chat bar are all skills. Each one packages up the steps, the data sources, and the judgment needed to do a specific job, like triaging an alert or running a threat hunt. Click a pill (or call a skill by name) and Crogl follows that recipe end-to-end, so you don't have to spell it out every time.

The skills that ship with Crogl cover the common shape of SOC work, but every environment is different. Skills help Crogl understand your naming conventions, your tools, your escalation paths, your reporting format. That's where **Create a skill** comes in: it lets you turn any workflow into a reusable Crogl skill, just by describing it in plain language. No code, no query language.

Why building your own pays off:

- **Crogl adapts to your environment.** A custom skill captures the specific data sources, query patterns, and language your SOC actually uses. The more your skills reflect how your team really works, the better Crogl performs on the next investigation.
- **Repeatable work gets faster and more consistent.** Anything an analyst does more than twice (a particular hunt cadence, a vendor-specific triage flow, your weekly report) becomes a one-line invocation that produces the same output across analysts and shifts.

Building one is just a conversation. Run **Create a skill** and describe the workflow you want: what triggers it, what data it should pull, what decisions it should make, and what output you want. Crogl will draft the skill, run it with you, and save it once you're happy with the result. You can edit the skills you create or bring in by clicking the wand icon in the left-hand navigation bar.

Try this now. Pick something you do regularly and can describe in a few sentences (your standard alert triage template, your weekly hunt routine, or the report your manager asks for every Friday) and build it as your first skill.