# JULIAN VARGAS

Coachella, California · +1 (760) 906-4231 · julivnexe@gmail.com
julivn.dev · github.com/julivnexe · linkedin.com/in/julivnexe

*Open to remote DevOps, SRE, and Platform Engineering roles · Pacific Time*

## SUMMARY

Self-taught systems engineer focused on production-shaped Linux infrastructure, IaC, and observability. Build modular Terraform, containerized observability stacks, and CLIs that own the full lifecycle of a small cloud footprint. Bilingual EN/ES, US/Mexican dual citizen.

## SKILLS

**Infrastructure & IaC:** Terraform, Ansible, cloud-init, Cloudflare, Vultr, S3-compatible object storage (Cloudflare R2), Let's Encrypt

**Runtime & Security:** Linux, systemd, Docker, Docker Compose, UFW, fail2ban, sshd hardening, Caddy

**Observability & Tooling:** Prometheus, Grafana, Python, Bash, Click, POSIX shell, Git, GitHub Actions (CI/CD)

## PROJECTS

### terraform-homelab — Solo, 2026

*github.com/julivnexe/terraform-homelab · Live: julivn.dev*

- End-to-end IaC: modular Terraform (ssh, compute, dns) provisions a hardened Ubuntu VPS on Vultr; Cloudflare-managed DNS; HTTPS via Caddy + Let's Encrypt; remote state on Cloudflare R2 (S3-compatible).
- Cloud-init bootstrap: non-root user, sshd hardening drop-in, UFW, fail2ban, unattended-upgrades. Site redeploys via null_resource keyed on archive checksum — content edits never rebuild the VM.

### monitoring-platform — Solo, 2025–present

*github.com/julivnexe/monitoring-platform*

- Containerized observability stack (Prometheus + Grafana + node-exporter + custom Python exporter) in Docker Compose, running 24/7.
- Exporter runs in host network mode (NET_ADMIN) reading iptables counters and ss -uan socket state for real-time DDoS detection. Two alert channels: Discord webhooks for events, Prometheus for trends.

### Halo-CE-Command-Center — Solo, 2026

*github.com/julivnexe/Halo-CE-Command-Center*

- Self-hosted DDoS defense + Discord notifier for Halo CE servers, with a pluggable adapter pattern (CSV file as the integration boundary, schema versioned) so other UDP/TCP game servers can plug in.
- Auto-banner: on PPS spikes, runs a brief tcpdump, groups source IPs by /24, adds attacker subnets to ipset (24h TTL). Reputation feeds (~4,600 CIDRs from FireHOL + Spamhaus) pre-block known-bad IPs.

### infra-automator — Solo, 2026

*github.com/julivnexe/infra-automator*

- Click-based Python CLI (infra up | harden | deploy | status | destroy) wrapping Terraform, Ansible, and Docker Compose across Vultr and DigitalOcean.
- Secrets via TF_VAR_* env vars at apply time, never written to disk. CI on every push: lint, type-check, unit tests, Terraform fmt/validate per provider.

### halo-vps-ansible — Solo, 2026

*github.com/julivnexe/halo-vps-ansible*

- Idempotent Ansible playbook (5 roles: user, sshd hardening, firewall, docker, monitoring) reverse-engineered from the live production VPS.
- Running against the live host produces zero changes — playbook is a true codification of running state, not aspirational config. Repeatable rebuilds from a fresh Ubuntu image.

## EXPERIENCE

### Independent Systems Engineer — 2024 – Present

*Self-directed, Remote*

- Designed, built, and operate production-shaped Linux infrastructure end-to-end: provisioning (Terraform), configuration (Ansible, cloud-init), runtime (Docker Compose), and observability (Prometheus / Grafana).
- Found and closed a publicly-exposed Grafana on my own production VPS during a documentation pass — rebound the container to localhost, removed the public firewall rule, switched to SSH-tunnel access for admin work.
- Reverse-engineered the live VPS hardening into an idempotent Ansible playbook — playbook matches running state with no drift, runnable against a fresh VPS for repeatable rebuilds.

## EDUCATION

Self-taught — focused on Linux systems administration, infrastructure-as-code, and observability since 2024.