Carlos Sanchez

United States (Remote) · carl.sanchez010@gmail.com · sanchezonsecurity.com
linkedin.com/in/carlos-sanchez-b0926913b · github.com/SaltyCarl

SUMMARY

SOC operator and security tool builder. Five years in MSSP-scale security operations, with a parallel practice shipping production-quality security tools — analyst assistants, KQL investigation workbenches, home SIEM/SOAR — built around deterministic-by-design and AI-assisted SecOps workflows.

SELECTED PROJECTS

CARL — Contextual Alert Response Library · Python, FastAPI, single-file HTML

Deterministic SOC analyst assistant for CMMC-regulated environments. Eight dispatch engines, 500+ knowledge entries, no LLM inference; modeled for ~150K annual alert triage at 10-analyst MSSP scale. Replaces ad-hoc LLM workflows where data residency and reproducibility matter.

BASTION — KQL investigation workbench · Python, FastAPI, KQL, PowerShell

Multi-tab analyst console with a KQL Wizard (20 IOC-specific query templates), a PowerShell analyzer (Base64 decoder, 34 LOLBin signatures, layman explanations), and 100+ MITRE ATT&CK techniques mapped. Used for live SOC investigations.

HEARTH — Home SIEM/SOAR command center · OPNsense, Wazuh, Python, WireGuard

Hardened home network with multi-stage detection pipeline (18 hunt queries), segmented zero-trust topology (4 VLANs), and a custom orchestration layer forked from BASTION. Family devices on isolated VLANs via WireGuard.

ThreatWatch · Python, FastAPI, SQLite — Single-tenant MSSP threat-intel delivery: RSS poller, 3-layer dedup, weighted severity scoring, Slack digest + breaking-news; 240 tests.

Sentinel Workbook Generator · ARM/JSON, KQL, single-file HTML — Modular ARM template generator for Microsoft Sentinel: 34-panel catalog composes into named profiles (MSSP Monthly Report, Privileged Access Monitoring) that visualize incident KPIs and operational metrics. Production deployment surfaced 9 KQL runtime bugs that fed back into the tool.

EXPERIENCE

SOC Tier II Shift Lead — CyberSheath · Oct 2022 – Present

Promoted from Cyber Security Analyst I within an MSSP serving the Defense Industrial Base.

- Lead operations on shift across 200+ Tier 1 and Tier 2 customer tenants — alert queue balancing, SLA accountability, escalation point for T1 analysts during high-severity events
- Investigate and contain phishing, credential compromise, malware, and lateral-movement incidents in Microsoft Sentinel; execute account disablement, host isolation, and alert suppression as containment actions
- Build and tune SOAR workflows in Google SecOps for response automation; identify automation candidates from recurring alert patterns
- Mentor T1 analysts during live investigations; standardize SOPs, alert classification, and severity assignment across shifts

Information Security Analyst — Aptum · May 2021 – Oct 2022

- Conducted vulnerability assessments and tracked emerging and zero-day vulnerabilities; coordinated patch management
- Developed information security policy and procedural documentation
- Adopted security engineering best practices across the organization

Data Center Administrator — Aptum · Jun 2019 – May 2021

- Configured and deployed Juniper firewalls and switches across a managed-hosting data center; monitored network infrastructure underpinning customer workloads

CERTIFICATIONS

Active: CompTIA Security+ · CompTIA CySA+ · EC-Council CEH

Prior: AWS Certified Cloud Practitioner (expired 2025) · Microsoft SC-200 (expired) · Microsoft SC-900 (expired)

SKILLS

Microsoft Sentinel · Defender XDR · Google SecOps SIEM/SOAR · KQL · Python · PowerShell · FastAPI · Wazuh · OPNsense · Juniper · MITRE ATT&CK · Detection Engineering · Incident Response · SOAR Automation · AI-assisted SecOps (Claude Code) · Local model orchestration (Lemonade, Ollama)