

Mario Sanchez

Bay Area, CA | 510-371-3756 | mareox@gmail.com | linkedin.com/in/mareox

Senior Security Consultant and subject matter expert with 8+ years of customer-facing experience at Palo Alto Networks spanning Technical Support, Customer Success, Solutions Architecture, and Professional Services. Currently embedded as the dedicated technical advisor for one of PANW's largest global SASE engagements (100,000+ users, 34+ regions across AWS, Azure, and GCP environments). Pioneer in applying Large Language Model tools to security operations with documented productivity gains adopted at the team level. Hands-on Python and Terraform automation, AI/ML security research including OWASP Top 10 for LLMs (prompt injection, data leakage, model poisoning), and deep expertise across PAN-OS, Prisma Access, Prisma Cloud, and NGFW platforms. Seeking to leverage consulting experience and AI-enhanced engineering skills to deliver AI Model Scanning and AI Red Teaming engagements at enterprise scale.

PROJECTS

AI-Integrated Security Infrastructure Lab

2023 - Present

Architect and operate a 50+ service security research environment across a 4-node Proxmox cluster with 50+ VMs/containers, PA-440 NGFW (PAN-OS 11.2), and defense-in-depth security across 6 VLANs. Deploy local Large Language Model inference (Ollama/PyTorch) and AI agent pipelines for security research, including testing OWASP Top 10 LLM threats (prompt injection, data leakage, model poisoning) and AI model scanning workflows. Implement Terraform and Ansible-driven infrastructure-as-code with Docker, Kubernetes-compatible container orchestration, and Semaphore CI/CD. Manage centralized SIEM (Graylog + OpenSearch), XDR (Wazuh with CIS compliance), Prometheus/Grafana observability, and MLOps-style automation pipelines.

Prisma Access DNS Automation Engine

2025

Designed and deployed Python automation for DNS configuration management across 18 global Prisma Access regions, managing 150 internal domains simultaneously. Reduced deployment time from 25-35 hours to under 1 minute (99.9% reduction), eliminating 2,700+ individual manual entries and potential human error.

SCM Address Group Converter — [GitHub](#)

2025

Built enterprise Python tool using Strata Cloud Manager SDK to convert static address groups to dynamic tag-based groups at scale. Features OAuth 2.0 authentication, intelligent batch processing (200-400 objects/min), comprehensive backup/rollback, and exponential backoff retry logic.

EXPERIENCE

Extended Expertise Consultant (Professional Services)

Palo Alto Networks | Santa Clara, CA (Embedded at Fortune 500 Clients)

December 2020 — Present

- Subject matter expert and embedded senior technical engineer leading global Prisma Access deployments for Fortune 500 organizations — 100,000+ users across 34+ regions worldwide, acting as single technical bridge between customer leadership, PANW engineering, TAC, and partner teams.
- Developed Python automation tools using PAN-OS SDK and Strata Cloud Manager API that reduced DNS configuration management from 25-35 hours to under 1 minute across 18 global regions, eliminating 2,700+ manual entries with 100% accuracy.
- Pioneered AI-enhanced engineering workflows using Large Language Model tools (Claude, Gemini) for configuration review, technical analysis, and automated reporting — saving 5-10 hours/week with practices requested by management for company-wide adoption. Evaluated data leakage risks and implemented guardrails for secure AI tool usage in enterprise context.
- Led GlobalProtect client rollout expansion from 2,000 to 52,000+ users with 2,500 users/day peak deployment, resolving critical cross-platform authentication and captive portal issues through hands-on field testing and structured troubleshooting methodologies.
- Engineered strategic China tenant architecture pivot, migrating mobile users to global tenant via Hong Kong/Singapore — proactively identified BGP timer misconfigurations and DNS session issues before they caused outages for thousands of users.
- Delivered technical workshops, presentations, and strategic recommendations to executive stakeholders through weekly business updates and quarterly business reviews, aligning security posture with enterprise digital transformation objectives.
- Built enterprise Python and Terraform-ready automation tools including SCM SDK address group converter with OAuth 2.0 authentication, batch processing at 200-400 objects/minute, and reusable delivery templates for global scaling.
- Identified and remediated 4,000 disabled rules, 1,100+ unused services, and 600+ unused address objects in Panorama, building reusable documentation and cleanup methodologies adopted across engagements.

- Collaborated with Product and Engineering teams channeling field insights into product development, including early adoption and feedback for SCM cloning tool and Prisma Access proxy features.

Customer Success Engineer, Network Security (Prisma Access)

Palo Alto Networks | Santa Clara, CA

August 2019 — December 2020

- Drove 40% Prisma Access adoption across 20 enterprise clients through solutions architecture, cloud security assessments on AWS and Azure environments, and deployment of cloud-native SASE solutions.
- Led migration of 10,000+ L4/L7 proxy rules to Palo Alto NGFW explicit proxy and security policies, reducing policy conflicts by 60% and boosting network performance by 20%.
- Designed Zero Trust architectures including secure web gateways, network segmentation, and advanced packet inspection for multinational enterprise networks across public cloud platforms.
- Delivered operational presentations and quarterly business reviews to executive stakeholders, aligning security strategies with enterprise digital transformation objectives.

Technical Support Engineer (Prisma Access)

Palo Alto Networks | Santa Clara, CA

July 2017 — August 2019

- Provided customer-facing technical support for cloud-based NGFW firewalls, Panorama, and early Prisma Access platform, troubleshooting routing, VPN, and security issues across enterprise deployments.
- Hardened authentication implementations with SAML, SSO, and MFA integrations (Okta, Azure AD) for enterprise customers on AWS, Azure, and GCP cloud platforms.
- Collaborated with engineering teams on complex technical escalations, contributing field insights that informed product development and improvement cycles.

TECHNICAL SKILLS

Security & Cloud Platforms: Prisma Access (SASE/SSE), Prisma Cloud, PAN-OS NGFW, Panorama, GlobalProtect, ZTNA 2.0, Strata Cloud Manager, Zero Trust Architecture, AWS, Azure, GCP, SSL/TLS Decryption, Network Segmentation

AI/ML Security & Automation: Large Language Models (LLM Security), OWASP Top 10 for LLMs, Prompt Injection / Data Leakage / Model Poisoning, AI Model Scanning, AI Red Teaming, LLM Inference (Ollama/PyTorch), MLOps Pipelines, AI Agent Security

Programming & IaC: Python (PAN-OS SDK, SCM SDK, Pydantic, OAuth 2.0), Terraform, REST API Automation, Infrastructure-as-Code (Ansible, Docker Compose), CI/CD (Semaphore)

Infrastructure & Containers: Docker, Kubernetes (familiar), Podman, Proxmox VE, Linux (Debian/Ubuntu), LXC Containers, Cloudflare Tunnel/Access

Monitoring & SecOps: Graylog/OpenSearch (SIEM), Prometheus/Grafana, Wazuh XDR, CIS Benchmarks, SNMP/Syslog

EDUCATION

AA Network Administration — Mission College, Santa Clara, CA

CERTIFICATIONS

PCNSE - Palo Alto Networks Certified Network Security Engineer	2024
PCNSE - Palo Alto Networks Certified Network Security Engineer	2019
CCNA CyberOps	2018
CCNA Security	2017
CCNA Routing & Switching	2016