MARIO SANCHEZ

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

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). 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, and deep expertise across PAN-OS, Prisma Access, Prisma Cloud, and NGFW platforms.

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 & Monitoring: Docker, Kubernetes (familiar), Podman, Proxmox VE, Linux (Debian/Ubuntu), LXC Containers, Graylog/OpenSearch (SIEM), Prometheus/Grafana, Wazuh XDR, CIS Benchmarks

CERTIFICATIONS

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

EXPERIENCE

Extended Expertise Consultant (Professional Services)
December 2020 – Present

Palo Alto Networks • Santa Clara, CA (Embedded at Cummins Inc.)

- Serve as subject matter expert and embedded senior technical consultant for Cummins' global Prisma Access deployment spanning 100,000+ users across 34+ regions on AWS and Azure, 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.
- 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.
- 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.
- 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.
- Identified and remediated 4,000 disabled rules, 1,100+ unused services, and 600+ unused address objects in Panorama, building reusable documentation and cleanup methodologies.

Customer Success Engineer, Network Security (Prisma Access)
August 2019 – December 2020

Palo Alto Networks • Santa Clara, CA

- 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.
- Delivered operational presentations and quarterly business reviews to executive stakeholders.

Technical Support Engineer (Prisma Access)
July 2017 – August 2019

Palo Alto Networks • Santa Clara, CA

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

PROJECTS

AI-Integrated Security Infrastructure Lab
2023 – Present

50+ service security research environment across a 4-node Proxmox cluster with PA-440 NGFW (PAN-OS 11.2) and defense-in-depth across 6 VLANs. Local LLM inference, AI agent pipelines, OWASP Top 10 LLM threat testing. Terraform + Ansible IaC, Docker orchestration, Semaphore CI/CD, Graylog SIEM, Wazuh XDR, Prometheus/Grafana observability.

Prisma Access DNS Automation Engine
2025

Python automation for DNS config management across 18 global Prisma Access regions, managing 150 internal domains. Reduced deployment from 25–35 hours to under 1 minute (99.9% reduction), eliminating 2,700+ manual entries.

SCM Address Group Converter
2025

Enterprise Python tool using SCM SDK to convert static address groups to dynamic tag-based groups at scale. OAuth 2.0 auth, batch processing (200–400 objects/min), backup/rollback, exponential backoff retry logic.

github.com/mareox/panw-script_group-addr-static-to-dynamic

EDUCATION

Mission College • Santa Clara, CA • Network Administration (Information Technology)