

Paul Altamirano

Rockville, MD | 240-543-5908 | paul.j.altamirano@gmail.com | Secret Clearance | pa-systems-portfolio.pages.dev

PROFESSIONAL SUMMARY

Cybersecurity professional with experience spanning network administration, threat intelligence, security operations, and cloud security monitoring. Skilled in threat hunting, detection engineering, and incident response support using Microsoft Sentinel, Defender for Endpoint, Cisco Umbrella, and Recorded Future. Proven ability to build operational processes, develop detection logic, support government cybersecurity initiatives, and translate threat intelligence into actionable security outcomes. Recognized for rapidly advancing from systems administration into security-focused responsibilities while supporting mission-critical environments.

TECHNICAL SKILLS

Cloud & SaaS: Microsoft Azure, Microsoft 365, Entra ID, AWS

Security: Microsoft Sentinel, Defender for Endpoint, Defender for Cloud Apps, Recorded Future, Cisco Umbrella, Qualys, Threat Hunting, Threat Intelligence, Incident Response

Networking: DNS, DHCP, VPNs, Network Monitoring, TCP/IP, Network Topology Analysis

Systems: Windows Server, Active Directory, Endpoint Administration

Automation & Data: Power BI, Azure DevOps, KQL

PROFESSIONAL EXPERIENCE

CoHo Consulting | Bureau of International Narcotics and Law Enforcement Affairs | Washington, DC

Network Administrator | Threat Intelligence & Security Operations | *July 2025 – Present*

- Help establish the organization's threat intelligence capability by developing Recorded Future alerting, refining detection criteria, validating threat relevance, and integrating intelligence into daily security operations.
- Serve as a trusted technical resource for government leadership, providing threat intelligence analysis, cybersecurity recommendations, and operational support for domestic and international mission environments.
- Conduct proactive DNS-based threat hunting using Cisco Umbrella telemetry to identify malicious activity, investigate anomalies, and validate organizational exposure.
- Develop, tune, and investigate an average of 25–30 threat intelligence alerts each week using Recorded Future and Cisco Umbrella, assessing organizational relevance, validating indicators of compromise (IOCs), and distinguishing actionable threats from false positives.
- Design, test, and optimize Microsoft Sentinel analytic rules by refining detection logic and thresholds to improve Azure cloud visibility while reducing false positives.
- Leverage Microsoft Sentinel, Defender for Endpoint, and Defender for Cloud Apps to support threat detection, investigation, and incident response activities.
- Partner with the ISSO to evaluate security controls, identify configuration and visibility gaps, and recommend security improvements across international non-enterprise environments.
- Assess cybersecurity risks affecting international training sites and develop practical recommendations to improve network visibility, endpoint security, access control, and incident readiness.
- Contribute to the development of the organization's Incident Response Plan, including escalation, detection, and remediation procedures.
- Review network architecture and topology to identify visibility gaps, improve monitoring capabilities, and strengthen defensive posture.
- Present threat intelligence findings and remediation recommendations to cybersecurity leadership, enabling risk-based prioritization of identified threats.

ZenPoint Solutions | Bureau of International Narcotics and Law Enforcement Affairs | Washington, DC

Systems Administrator | *April 2025 – July 2025*

- Served as the primary liaison between infrastructure and cybersecurity teams, supporting network operations, vulnerability management, and security initiatives.
- Developed vulnerability remediation plans, RACI matrices, and operational checklists to standardize remediation efforts across technical teams.
- Assisted with the migration from Microsoft Defender for Cloud Apps (MDCA) to Cloudflare, improving cloud visibility and security monitoring capabilities.
- Developed Power BI dashboards to provide leadership visibility into network performance, vulnerabilities, and operational metrics.
- Partnered with cybersecurity personnel to support vulnerability remediation initiatives and track progress through Azure DevOps.

- Analyzed network topology and infrastructure configurations to identify optimization opportunities and reduce operational risk.
- Developed technical documentation and mentored incoming personnel to ensure operational continuity during organizational transition.
- Develop security reporting and dashboards to communicate threat trends, vulnerabilities, and operational metrics to stakeholders.

CERTIFICATIONS

CompTIA Security+ | CompTIA | 2023

CompTIA Network+ | CompTIA | 2023

AWS Certified Cloud Practitioner | Amazon Web Services | 2025

Microsoft Certified: Azure Fundamentals | Microsoft

EDUCATION

Bachelor of Science, Cybersecurity | University of Maryland Global Campus | 2023