LEISHKA PAGAN

Los Angeles, CA | (714) 797-5715 | Leishka.pagan1@gmail.com
linkedin.com/in/leishka-pagan | github.com/leishka-pagan

PROFESSIONAL SUMMARY

Security & Cloud Infrastructure Engineer with **9+ years** operating in high-availability enterprise environments, supporting **5,400+ users** and serving as the final escalation point for identity and infrastructure failures. Designed and deployed **AI-driven security systems** on Azure, including multi-agent vulnerability intelligence platforms and production applications with code-enforced safety layers. **Cross-layer investigator** across network traffic, host-based artifacts, and memory forensics, combining enterprise-scale identity governance with hands-on detection engineering and DFIR. Placed **3rd internationally** in the Microsoft AI Innovation Challenge (March 2026), an invitation-only competition.

PROFESSIONAL EXPERIENCE

Cybersecurity Research & AI Security Engineering | Independent Practice *2023 – 2026*

AI Security Systems

- Built **Sentinel**, a custom AI-powered vulnerability intelligence platform using a **multi-agent architecture** (Claude orchestrator, Queen + Alpha reasoning) with a formal finding state machine, **OWASP ASVS/WSTG** and **MITRE ATT&CK** mapping, and a hard-scoped safety layer enforcing **zero destructive actions**. Produced evidence-backed JSON and Markdown reports with confirmed, refuted, and inconclusive classifications.
- Served as **Primary Engineer** on **ClearStep**, an AI-powered decision-support application deployed across 10 Azure services, using a **three-layer safety pipeline** (Azure AI Content Safety, Azure OpenAI signal classification, Anthropic Claude reasoning). Built a Python validation layer enforcing prompt-injection mitigation and deterministic schema output. **Placed 3rd internationally** in the Microsoft AI Innovation Challenge (March 2026).
- Engineered **AXIOM**, an evidence-driven cybersecurity reasoning engine with a five-agent architecture and human-gated trust promotion. Implemented append-only evidence storage and a deterministic confidence scoring model across execution evidence, source quality, consensus, environment match, recency, and stability. Enforced structural boundaries **preventing shadow reasoning**. 134 tests executed.

Security Operations & Detection Engineering

- Authored custom Snort IDS rules from live packet analysis, isolating malicious **RDP traffic** from baseline behavior and validating detection accuracy with a **low false positive rate**.
- Built Splunk detection workflows using custom SPL queries, correlating logs across sources and reducing **3,000+ events** to **targeted IOCs**, with all confirmed findings mapped to MITRE ATT&CK techniques.
- Conducted Windows event log threat hunting using Hayabusa, authored Sigma rules for cross-platform detection standardization, and performed **memory forensics** with **Volatility** to **recover credentials** from volatile memory.
- Designed segmented **multi-VLAN lab environments** using Windows Server, pfSense, and Kali Linux to replicate enterprise conditions; performed **network traffic analysis** (Wireshark, tcpdump) and validated IDS/IPS detections using **Suricata and Zeek**.

Incident Response & Investigations

- Completed externally graded IR investigations through IronCircle TDX Arena, earning TDX Arena IR Expert and CyberAdvantage certifications. Investigations included memory forensics for **credential recovery**, **SIEM pivot analysis** from exposed **POP3** services, and **malware identification** in cases where AV failed detection.
- Performed static malware analysis and reverse engineering on live samples, authoring YARA detection rules validated against multi-engine analysis.

Infrastructure & Operations Support (Senior Office Specialist) | Metro Net Fire Authority *Mar 2024 – Mar 2025*

Anaheim, CA

- Supported uptime of dispatch communications equipment in a controlled-access **24/7 facility** where downtime directly impacts **911** response, working alongside engineering on hardware troubleshooting and change management.
- Performed secure extraction of dispatch logs, call recordings, and radio communications in response to **subpoenas**, **warrants**, and records requests, ensuring evidentiary integrity and audit readiness within **CJIS**-aligned workflows.
- **Re-engineered the QA reporting workflow**, building a VBA automation pipeline executing **240+ discrete actions** per cycle and reducing manual processing time by **75-80%**.
- **Extended automation end-to-end**: data extraction from individual review workbooks, dictionary-based team assignment across 20+ dispatchers, auto-generated pivot analysis with conditional formatting, and Outlook-integrated PDF distribution.
- Maintained data integrity within the Computer-Aided Dispatch (CAD) system, updating address records, coordinates, and response codes directly impacting routing accuracy and system reliability.

Career Break *2020 – 2023*

Full-time caregiver during COVID-19. Returned to technical practice via independent study and lab work in 2023.

Systems Administrator, Enterprise Infrastructure & Identity | Spectrum *Jan 2014 – Feb 2020*

Los Angeles, CA | Formerly Time Warner Cable; retained through acquisition by Charter Communications (2016)

- Advanced from sole administrator supporting **100+ dispatch agents** to co-owning **identity and access governance** for **250–300 users** across multiple facilities; one of two senior administrators on a 4-person team.
- Administered **identity and access lifecycle** for **5,400+ field technicians** across enterprise platforms (ARRIS, CSG, SageQuest, Kronos, Avaya, Microsoft 365), enforcing RBAC and least-privilege access in **SSO**-enabled environments.
- Served as the **final escalation point** for enterprise infrastructure, authentication, and workflow failures across regional dispatch operations, handling **20-40+ escalations daily** with volume spiking post-maintenance; resolved issues no other tier could and coordinated directly with ARRIS senior engineering to accelerate resolution.
- Established **real-time monitoring** of call queue performance and handling thresholds across multiple truckyards; documented anomalies led to internal reviews and process corrections, improving compliance with handling policy.
- Administered **Active Directory** identity lifecycle including user provisioning, **GPO** management, access governance enforcement, and authentication troubleshooting; executed proactive monitoring and remediation initiatives that reduced user-reported incidents by **~15%**.
- Conducted monthly **access audits** and event-driven reviews triggered by **onboarding** and **offboarding**, validating permissions across multiple enterprise systems with separate authentication environments to ensure no misconfigured or residual access remained.
- Led infrastructure upgrades, **patch lifecycle management**, disaster recovery planning, and overnight maintenance windows; drove enterprise technology transitions including migration to iPad-based field workflows.
- Developed operational **SOPs**, escalation playbooks, and visual job aids adopted across administrator and technician teams; led technical training across dispatch teams and supervisors, reducing recurring support requests and improving onboarding consistency.

Dispatcher II, Operations Coordination | Time Warner Cable *Feb 2012 – Jan 2014*

- Promoted from Dispatcher I to Dispatcher II within 6 months; informally elevated to senior responsibilities within the first year.
- Selected as sole pilot tester for the company's auto-routing system prior to enterprise rollout; validated functionality, identified issues, and provided feedback that led to company-wide approval and deployment.

TECHNICAL SKILLS

- **Cloud & Identity: Azure** (App Service, **Entra ID**, Key Vault, Managed Identities, PIM, Conditional Access, **AI Content Safety**, **Prompt Shields**, AI Language, AI Speech, **OpenAI**, Blob Storage, Cosmos DB, Application Insights), Microsoft Foundry, AWS IAM, **Active Directory**, Microsoft 365, **RBAC**, **MFA**, **SSO**, Identity Governance, RADIUS/TACACS+, 802.1X, GPO, DefaultAzureCredential
- **AI Security & LLM Engineering: Prompt injection mitigation** (XML delimiting), **multi-layer safety pipelines**, content safety / guardrails, structured output validation, multi-agent architecture, **Anthropic Claude API**, **Azure OpenAI**, **OWASP ASVS/WSTG**, **MITRE ATT&CK** mapping
- **Detection & SIEM: Splunk** (custom SPL authoring), **Sigma rules**, **Snort** (custom rule authoring from packet analysis), Suricata, Zeek, Hayabusa, Chainsaw, DeepBlueCLI, **IDS/IPS detection engineering**, detection rule tuning
- **DFIR & Forensics: Volatility3**, Autopsy, KAPE, Velociraptor, **memory forensics**, timeline analysis, **IOC extraction**, cryptographic hash verification, evidence integrity, UTF-16 / Base64 payload analysis
- **Malware Analysis & RE:** Ghidra, x64dbg, PeStudio, **YARA**, ClamAV, **VirusTotal** multi-engine analysis, static analysis
- **Network & Infrastructure:** LAN/WAN, **VLAN segmentation**, pfSense, firewall policy, network segmentation, patch management, **system hardening**, Wireshark, tcpdump, **Nmap**, Samba/SMB, POP3/SMTP, RDP, DNS, TCP/IP analysis, VPN (IPSec), **Zero Trust**
- **Development: Python** (Flask, Pydantic), **PowerShell**, Bash, JavaScript, HTML/CSS, SQL (SQLite), **Excel VBA**, REST API design, **CI/CD** (GitHub Actions), Git, Gunicorn, Docker
- **Vulnerability Assessment:** Burp Suite, Metasploit, OSINT, Nmap, **authorized VDP research** (Bugcrowd)

CERTIFICATIONS & EDUCATION

- **CompTIA Security+** (SY0-701), Active 2026-2029
- **Cybersecurity Professional Certificate**, California State University, Long Beach (ThriveDX), coursework across DFIR, threat hunting, network security, Microsoft security administration, and ethical hacking; **150+ hands-on labs completed**
- **TDX Arena IR Expert & CyberAdvantage Certifications**, IronCircle, externally graded incident response cases
- **Microsoft Azure Security Engineer (AZ-500)**, In Progress
- WiCyS Member; **Authorized VDP Researcher** (via Bugcrowd)
- Women in Cloud Member; **Microsoft AI Innovation Challenge**, Placed **3rd internationally** (March 2026)