Katrina Natura

katalystque.com• echo@katalystque.com • Los Angeles, CA • github.com/katalyst-que• linkedin.com/katrina-natura

TECHNICAL SKILLS

Programming Languages	JavaScript, Python, PowerShell, SQL
Operating Systems	Windows, Windows Server 2019/2022, Linux (Kali, Ubuntu, Mint), macOS
Security Tools	Azure Sentinel, SIEM, Splunk, OpenSCAP, Wireshark, Nmap, T-Pot, Metasploit, Burp Suite, Nessus

EDUCATION

Bachelor of Science in Cybersecurity and Information Assurance, Western Governors University | Salt Lake City, UT Feb. 2026

- Relevant Coursework: Incident Response & Forensics, Risk & Vulnerability Management, SQL Database Security, Network Defense, NIST & PCI-DSS Compliance

Cybersecurity Bootcamp Graduate, University of Oregon| Eugene, CA April 2020

- Relevant Coursework: Secure Cloud Network Architecture, Forensics and Network Intrusion, Security Software Design

CERTIFICATIONS

CompTIA CySA+, PenTest+, Security+, Network+, Project+, A+ | ISC2 SSCP | ITIL 4 Foundation | LPI Linux Essentials | ISC2 Member

WORK EXPERIENCE

Founder | Cybersecurity & IT Integration Consultant, KatalystQue | Los Angeles, CA May 2024 – Present

- Conduct PCI-DSS gap analysis for retail clients, migrating unsecured transaction flows to encrypted POS systems and implementing network segmentation for scope reduction
- Design governance policies for Physician's Preferred Hospice and Frieden Hospice Care, achieving a "Zero Deficiency" rating during state audits within HIPAA compliance standards by enforcing strict IAM and data encryption standards
- Architect secure workflows integrating AI automation and localized backup strategies to ensure business continuity and data integrity for distributed teams

Cybersecurity Instructor, SoLa Impact| Los Angeles, CA Sept. 2024 – Present

- Create & Instruct CompTIA Security+ & Network+ curriculum to diverse cohorts, translating complex GRC, cryptography, network defense, threat intelligence, and incident response through hands-on labs and real-world attack simulations

Lead Software Validation Engineer / Client Platform Validation, Intel Corporation| Hillsboro, OR Oct. 2022 – Oct. 2024

- Led validation and compliance testing lifecycle for 500+ enterprise bare-metal systems, performing BIOS/UEFI hardening, firmware management, virtualization setup, asset provisioning, and DPMO assessment reporting within complex technical environments.
- Re-architected validation lab network topology and resolved critical packet loops through root cause analysis, strengthening system stability, configuration governance, and operational resilience across distributed engineering teams
- Served as escalation engineer diagnosing complex hardware/software failures using low-level debugging tools; coordinated global teams to validate remediation, maintain continuous testing operations, and ensure secure system functionality

Senior Technical Support, Zwift | Eugene, OR Oct. 2020 – Sep. 2022

- Delivered real-time incident response and operational support during global live broadcasts, maintaining application stability and secure system performance in high-pressure, deadline-driven environments
- Conducted cross-platform log analysis and forensic troubleshooting to identify root causes of network, device, and application failures across Windows, macOS, Android, and iOS ecosystems
- Identified recurring technical risks through ticket trend analysis, authored engineering bug reports for remediation, and supported GDPR/COPPA-aligned data handling and operational compliance processes

ACADEMIC PROJECTS

Cloud Threat Intelligence & Deception System (Azure/T-Pot)

- Deployed honeypot-based threat detection lab capturing 478K+ malicious interactions and implementing CIS-aligned hardening and egress filtering controls validated through OpenSCAP

Automated Identity Governance System (PowerShell/AD)

- Developed least-privilege ABAC/JIT access engine enforcing separation of duties and automated privilege revocation in simulated enterprise environment

Cloud Infrastructure Monitoring Baseline (ELK/Ansible)

- Automated deployment of highly available cloud infrastructure with centralized logging and anomaly detection baseline using ELK stack