

# JOHN MARK LOREJO

Technical Engineer

Taytay, Rizal, Philippines | +63 951 146 1981 | jmlorejo013@gmail.com

---

## PROFESSIONAL SUMMARY

Enterprise-scale Network Operations Center (NOC) engineer with 8+ years of IT experience specializing in infrastructure management, observability, incident management, and operational excellence. Expert in real-time infrastructure monitoring, P1/P2/P3 incident triage with SLA compliance, and event correlation for alert noise reduction (30-50% achieved). Proven track record managing 220M+ user-facing systems across multi-region AWS environments. Strong foundation in hands-on hardware security systems and data center operations. Skilled in AIOps automation, business service-level monitoring, and resilience/availability initiatives.

## PROFESSIONAL EXPERIENCE

### NOC Engineer | Trust Wallet

May 2025 - Present

- Operated enterprise-scale Network Operations Center (NOC) managing 12+ microservices with 10+ components each across multi-region AWS infrastructure serving 220M+ users
- Implemented real-time observability and monitoring infrastructure using Grafana, LogicMonitor, and Auvik; maintained business-critical dashboards tracking service health, error rates, and availability KPIs
- Achieved 30-50% alert noise reduction through in-depth investigation, collaboration and event correlation, alert tuning, and false-positive validation; collaborated with cross-functional resolver teams on anomaly detection and root cause analysis
- Executed P1/P2/P3 incident triage and escalation with SLA compliance: P1 (immediate response, 30-min MTTR), P2 (immediate response, 2-6 hrs MTTR), P3 (30-min MTTR, 4-24 hrs MTTR)
- Led post-incident reviews and postmortems; drove resilience and availability initiatives with MTTR/MTTD optimization reporting to senior management on weekly basis
- Focusing business service-level monitoring (BSM) for mission-critical crypto transaction workflows including on/off ramps, staking, swaps, transfers, deposits, and withdrawals with full telemetry visibility
- Automated critical event detection via AI-powered Crypto Events Bot—fetching and delivering real-time intelligence on hardforks, network upgrades, and security threats to organization-wide messaging platform

### System Engineer (NOC) | IT By Design

Feb 2024 - May 2025

- Monitored and optimized network and system performance using Auvik, Meraki, NinjaOne, and ConnectWise Automate
- Troubleshoot LAN, WAN, VPN, and firewall issues using Ping, Traceroute, and network logs

- Managed Windows Servers (2008-2022) and Azure cloud services to resolve performance and security issues
- Administered ITSM tools like ServiceNow, ConnectWise, AutoTask, and Kaseya for incident management
- Coordinated with ISPs, firewall vendors (Fortinet, Palo Alto, Cisco ASA, Microsoft), and network teams for issue resolution

## **IT Helpdesk Technician / Command Centre Operations | ProbeCx**

Jun 2022 - Feb 2024

- Provided first-line technical support and incident triage via integrated ticketing system (ServiceNow) with full alert forwarding and ITSM workflow automation
- Diagnosed and remediated infrastructure issues across servers, endpoints, and network services; escalated to resolver teams with comprehensive runbooks and contextual incident data
- Executed Standard Operating Procedures (SOPs) including RTOs, escalation policies, and incident response workflows for time-sensitive production incidents
- Managed Active Directory (AD), Azure AD, and Okta for identity and access management; resolved authentication and authorization issues affecting enterprise systems
- Performed health checks on Microsoft 365 ecosystem (Outlook, Teams, OneDrive) and VPN connectivity to ensure business continuity

## **Hardware Security Systems Technician | MainHardware Inc.**

Jun 2016 - Feb 2020

- Installed, configured, and maintained enterprise-grade hardware security devices including CCTV systems, access control systems, magnetic door locks, and turnstile gates across multiple client locations
- Designed and implemented data center infrastructure for security device configuration and centralized monitoring; managed all connectivity, power distribution, and environmental controls
- Collaborated with cross-functional teams to plan physical security rollouts and integrate hardware systems with existing IT infrastructure and facilities management
- Performed preventive maintenance, troubleshooting, and repair of security hardware systems; maintained detailed asset inventory and system documentation for compliance
- Achieved 99%+ uptime on monitored security systems through proactive monitoring and rapid incident response protocols; provided technical support and training to end-users on system operation and security best practices

## **TECHNICAL SKILLS**

### **Observability & Monitoring**

Grafana, LogicMonitor, Auvik, APM, Real-time dashboards, Service health monitoring, Business service-level monitoring (BSM), Event analytics

### **Incident & Event Management**

P1/P2/P3 triage & escalation, SLA management, MTTD/MTTR optimization, Incident correlation, Alert tuning & validation, False-positive reduction (30-50%), Event grouping & aggregation

### **AIOps & Automation**

Event correlation rules, Alert noise reduction, AI-powered automation, Crypto Events Bot development, Critical event detection, Intelligent alert filtering

### **Infrastructure & Cloud**

Server monitoring, Endpoint monitoring, Network operations, AWS multi-region deployments, Application Performance Monitoring (APM), Infrastructure-as-code concepts, Data center operations, Physical security systems

### **Identity & Access Management**

Active Directory (AD), Azure AD, Okta, MFA (Duo, Okta, MS Authenticator), Access control, User provisioning & deprovisioning

### **ITSM & Ticketing Integration**

Shortcut, ConnectWise, Freshdesk, ServiceNow, Alert forwarding to ticketing systems, Runbook creation & execution, SOP documentation, Escalation matrices, Postmortem leadership

## **KEY ACHIEVEMENTS & IMPACT**

### **Enterprise-Scale Operations**

- Operated NOC managing 12+ services × 10+ components in multi-region AWS serving 220M+ users
- Maintained 99%+ uptime through proactive monitoring and incident response excellence across all infrastructure tiers
- Weekly KPI reporting on uptime, availability, and operational metrics to leadership

### **Incident Resolution Excellence**

- Contribute and partake on multi-team incident response involving security threats from bad actors exploiting endpoints via VMs/bots
- Implemented real-time IPv4/IPv6/device ID tracking and blocking using security tools
- Established postmortem culture driving continuous process improvement across teams
- Achieved consistent P1 response & 30-min resolution targets in mission-critical environment

### **Alert Noise Reduction & Observability**

- Achieved 30-50% alert noise reduction through intelligent event correlation and tuning strategies
- Designed and optimized monitoring dashboards for business-critical services with full telemetry visibility

### **Automation & AIOps**

- Designed Crypto Events Bot leveraging AI for critical event detection (hardforks, upgrades, network changes)
- Zero-cost automation by integrating existing observability tools with custom logic
- Automated critical event detection and alerting for real-time threat intelligence

### **Infrastructure & Systems Management**

- Managed enterprise-grade hardware security systems (CCTV, access control, physical security) with 99%+ uptime
- Designed and maintained data center infrastructure supporting 100+ security devices with centralized monitoring
- Trained technical and non-technical users on system operation, troubleshooting, and security best practices

## TOOLS & TECHNOLOGIES

### Observability & Monitoring

Grafana (dashboards, alerting, APM) • LogicMonitor (infrastructure monitoring) • Auvik (network operations) • Real-time telemetry & event analytics

### Ticketing & ITSM

Shortcut • Freshdesk • ConnectWise • ServiceNow (incident management) • Notion (runbooks & SOP documentation)

### Cloud & Infrastructure

AWS (multi-region deployments) • Windows Server & Azure AD • Okta & MFA systems • Security tooling (IPv4/IPv6 blocking) • Data center infrastructure and management

### Security & Hardware Systems

CCTV systems and IP camera networks • Access control systems and physical security integration • Hardware security device configuration and troubleshooting • Network connectivity and system configuration for security devices

## CERTIFICATIONS

- Google Cybersecurity Professional Certificate
- Google IT Support Professional Certificate
- ISC2: Certified in Cyber Security
- Cisco Network Essentials
- Fortinet: Technical Introduction to Cybersecurity
- Introduction to Cybersecurity (Cisco)

## EDUCATION

### BS Computer Engineering

Rizal Technological University | 2018 - 2023