

EMMANUEL INVENTOR DIAZ, *CompTIA Security+, H3CNE-RS+*

Senior Infrastructure, Networking & Cybersecurity Professional

Bacolod City / Mandaluyong City, Philippines | Fully remote (AEST hours); flexible to hybrid in Metro Manila

Mobile: 09173260064 **Email:** emmanuel.inventor.diaz@gmail.com

LinkedIn: linkedin.com/in/emmanuel-diaz-801a6555

Credly: credly.com/badges/1c593016-410c-427b-aaa0-69f828257616



PROFESSIONAL SUMMARY

Senior infrastructure, networking and cybersecurity professional with 10+ years designing, securing and operating a 24/7 multi-site network for a 1,000-bed government hospital. Acts as the senior technical escalation point across many departments, owning infrastructure, security tooling and ISP relationships, with added experience in ISO internal auditing and ICT procurement inspection. Has delivered projects end to end, from planning through deployment, testing and handover, including a SOC built from scratch (Wazuh, Shuffle, Proxmox) and a 10Gbps fiber backbone upgrade. Experienced at explaining technical risk to non-technical stakeholders, deciding what to resolve, delegate or escalate, and reducing repeat issues through automation and documentation.

CORE COMPETENCIES

- **Infrastructure Design & Implementation:** WAN/LAN design, Layer 3 switching (H3C, Cisco), VLAN segmentation, OSPF, BGP, VPN, SD-WAN, Wi-Fi (Omada), multi-ISP load balancing and failover, fiber plant, Proxmox virtualization, Ubuntu Server.
- **Cybersecurity & Risk:** Next-gen firewalls (Sophos, pfSense, OPNsense), SIEM/SOAR (Wazuh, Shuffle), incident response, ransomware prevention, security risk assessment, RA 10173 (Data Privacy Act) compliance, audit support.
- **Technical Leadership & Communication:** Escalation ownership, staff training and mentoring, stakeholder briefings for non-technical audiences, technical evaluation of vendors and hardware, documentation and handover.
- **Operations, Continuity & Automation:** 24/7 high-availability operations, DR/BCP testing, SOAR workflow automation, monitoring and logging, continuous process improvement.

KEY PROJECTS & TECHNICAL IMPLEMENTATIONS

- **SOC Deployment from Scratch:** Architected and deployed an automated Security Operations Center on Proxmox, hosting Ubuntu Server VMs for Wazuh (SIEM) and Shuffle (SOAR). Integrated the two through webhooks to automate threat detection and route real-time breach alerts to Slack.
- **10Gbps Network Backbone Upgrade:** Led the backbone modernization, deploying fiber optic duplex transceivers across a 5-kilometer span to connect the main server room to administrative departments and medical wards.
- **Multi-ISP Load Balancing & Failover:** Implemented and tuned traffic distribution and failover across 4 ISPs on a Sophos firewall for 1,400+ concurrent users.
- **Network Rationalization & VLAN Segmentation:** Designed a managed-network architecture to replace unmanaged switches and separate clinical (EMR/HIS), administrative, voice, CCTV, wireless, server and guest traffic into dedicated VLANs, improving security, visibility and central management.

PROFESSIONAL EXPERIENCE

Network Administrator & Cybersecurity Analyst

January 2016 – Present

Corazon Locsin Montelibano Memorial Regional Hospital (1,000-bed Level-3 Government Tertiary Hospital)

- **Technical ownership & escalation:** Independently manage the hospital-wide network across multiple buildings and satellite clinics, supporting about 600 workstations, 200 network printers, 100 Wi-Fi access points, 100 VoIP devices and 100 CCTV devices on 17 Layer 3 switches with a 3Gbps internet link and 10Gbps backbone. Own complex network and security escalations for critical financial and clinical systems (PhilHealth eClaims, billing, payroll, procurement), with zero unplanned downtime.
- **Infrastructure design & implementation:** Design, deploy and test network and server infrastructure from planning through handover, and review the existing environment for resilience and efficiency gains (backbone upgrade, ISP failover, VLAN segmentation).
- **Cybersecurity & risk:** Designed and enforce the security architecture protecting health and financial records of 500,000+ patients, with zero major NPC or COA findings. Mitigate and block over 1.2 million attack attempts annually through firewall rule optimization and continuous traffic analysis, and built the SOC that supports detection and response.

- **Automation & process improvement:** Automated threat detection and alert routing with Wazuh, Shuffle and Slack, reducing manual monitoring and speeding up response.
- **Training & mentoring:** As IT Office Training Coordinator, develop curriculum and deliver technical training on network operations, cybersecurity awareness and data privacy to technical and non-technical staff.
- **Internal audit & compliance:** Served as an IQEA Internal Quality and Environmental Auditor (ISO 9001:2015 and ISO 14001:2015) from July 2024 to January 2026, conducting compliance audits and driving process improvements for ICT systems.
- **ICT procurement inspection:** Served as a member of the ICT Inspectorate Committee, carrying out technical verification and compliance testing of incoming enterprise hardware and services.
- **Business continuity:** Run quarterly disaster recovery and business continuity tests to keep a round-the-clock environment resilient.

CERTIFICATIONS

- **CompTIA Security+ (SY0-701)**
Certified: June 16, 2026 – Valid until: June 16, 2029
- **H3CNE-RS+ (H3C Certified Network Engineer – Routing & Switching Plus)**
Certified: January 20, 2026 – Valid until: January 20, 2029
- **OCNA-Wireless (Omada Certified Network Administrator – Wireless)**
Certified: November 18, 2025 – Valid until: November 18, 2028
- **Sophos Firewall Specialist; Sophos Cybersecurity Technical Specialist**
- **ISO 9001:2015 and ISO 14001:2015 Internal Auditor**



EDUCATION

- **Bachelor of Science in Computer Engineering, 2006 – 2011**
University of St. La Salle, Bacolod City, Philippines

ADDITIONAL INFORMATION

- **Performance:** Rated "Very Satisfactory" in formal annual government performance evaluations, 2016–2025.
- **Remote readiness:** Home office with dedicated high-speed internet and backup power, and experience with remote and asynchronous collaboration. Able to work Australian business hours (8:30 AM–5:30 PM AEST).