Kyn Bryan Tarape

kyntarape@gmail.com | https://www.linkedin.com/in/kyntarape999 | https://github.com/kyntrp/KynSec-Portfolio | +639292241096 | Cabadbaran, Agusan del Norte, Philippines 8605

WORK EXPERIENCE

Converge ICT / Metroworks **Pasig City/Agusan del Norte**

Desktop Services Team Leader / Senior Technical Support Engineer *May 2019 - Present*

- **Diagnosed and resolved complex hardware, software, and networking issues** both remotely and on-site, ensuring minimal downtime and high user satisfaction
- **Installed, configured, and optimized computer systems and applications** across diverse environments, tailored to user and business requirements
- **Provided responsive technical support via calls and emails**, delivering clear, actionable solutions to end users and stakeholders
- **Created detailed user guides and delivered step-by-step instructions** to assist users with IT-related issues, enhancing self-service capabilities
- **Managed user accounts and resolved authentication issues**, including password resets, access control, and login troubleshooting
- **Trained junior staff and peers on diagnostic techniques**, fostering a culture of knowledge sharing and technical excellence
- **Prepared, hardened, and configured IT devices**—including laptops, desktops, printers, routers, and tablets—for deployment, with asset documentation and user onboarding
- **Built and configured fully functional LAN/WAN networks** from the ground up for regional offices and business centers, including switch, router, and access point deployment with secure connectivity and structured cabling.

Plant Records Engineer & ERP Staff *Aug 2016 - May 2019*

- **Translated Single-Line Diagrams (SLDs) of As-Built Uplink plans** into detailed network documentation using Sunvizion, supporting accurate infrastructure mapping and implementation tracking
- **Encoded Multi-Dwelling Unit (MDU) As-Plans** into Sunvizion, ensuring precise data entry and alignment with field deployments
- **Created end-to-end SLDs from Central Office to Client**, including assignment of FOC port numbers, FOC types, and closure details for coordination with implementation and operations teams
- **Updated and generated project billing reports** for Converge and Metroworks as part of the Finance ERP team, ensuring accurate tracking and timely documentation of completed infrastructure projects
- **Demonstrated adaptability by transitioning from technical engineering to ERP support**, bridging gaps between departments and contributing to operational efficiency during resource-critical periods

LBP Service Corporation - ERICSSON FNSO GOOGLE FIBER PROJECT **Pasig City**

Autocad Operator - OSP Designer *Dec 2015 - Jun 2016*

- **Converted field surveyor sketches into detailed CAD designs**, ensuring compliance with client standards and specifications for Outside Plant (OSP) infrastructure
- **Prepared and analyzed Make-Ready Engineering (MRE) plans**, including pole loading assessments using O-Calc Pro to support safe and efficient network deployment

EDUCATION

STI College - San Fernando Pampanga **Pampanga, Philippines**

Bachelor of Science in Information Technology *Graduation Date: May 2015*

SKILLS SUMMARY

Soft Skills : Critical Thinking & Problem-solving, Customer Service Excellence, Verbal & Written Communication, Adaptability & Flexibility, Attention to Detail, Continuous Learning & Knowledge Sharing, Threat Investigation & Analysis, Resilience Under Pressure

Technical skills	:	Hardware & Software Troubleshooting, Network Administration, Firewall Management, Windows & Linux System Administration, Active Directory Management, Cloud Administration (Azure, GCP), Python, SQL, Bash, PowerShell Scripting
Security Operations & Monitoring:	:	Intrusion Detection & Prevention Systems (IDS/IPS): Snort, Zeek Endpoint Detection & Response (EDR): Wazuh, LimaCharlie Network Analysis: Wireshark, Tshark Security Information & Event Management (SIEM): Splunk Incident Response & Forensics Threat Intelligence & Malware Analysis

CERTIFICATIONS & TRAINING

TryHackMe-SOC lvl 1

- Hands-on experience in SIEM monitoring, endpoint security, threat analysis.

SC2-Certified in Cybersecurity (CC)

- Security principles, access controls, network security, incident response.

LinkedIn Learning-Become an IT Security Specialist

- IT Security Foundations and core concepts, Operating System Security, Network Security and Network Communications, Cybersecurity with Cloud Computing, Cybersecurity Foundations:Computer Forensics, Basic Vulnerability Management, Threat Modeling, Artifical Intelligent,Ethics and softskills for Security Professional, 'Governance, Risk, and Compliance' (GRC)

Cyberdefenders Blue Team Labs Participation

- Engaged in realistic, browser-based labs simulating real-world cybersecurity scenarios, enhancing skills in threat detection, incident response, digital forensics, and malware analysis

PROJECTS AND INNOVATIONS

SOAR & EDR Automation | LimaCharlie, Slack, Tines

- Built an automated SOAR workflow to enhance EDR using LimaCharlie sensors, Slack alerts, and Tines orchestration.
- Simulated credential-harvesting attacks (LaZagne.exe) to validate custom detection rules.
- Engineered detections for process tracking, file path monitoring, and SHA256 integrity checks.
- Automated endpoint isolation via LimaCharlie API with user-driven decisions.
- Integrated Slack for real-time alerts and incident updates.
- Reduced manual response time and improved detection accuracy through decision-based automation.

Threat Simulation Lab | Splunk, Atomic Red Team

- Deployed a virtual lab: Windows 10 (target), Kali Linux (attacker), AD Domain Controller, and Splunk SIEM.
- Configured Splunk Enterprise and Universal Forwarder; deployed Sysmon for enriched logging.
- Simulated MITRE ATT&CK techniques (T1136.001, T1059.001) using Hydra, Crowbar, and Atomic Red Team.
- Analyzed Splunk logs for IOCs, failed logins, and malicious patterns.
- Demonstrated hands-on skills in SIEM deployment, threat detection, and AD security testing.

Endpoint Threat Detection | LimaCharlie, Sliver C2

- Created a virtualized lab with Windows 10 and Ubuntu Server to simulate adversary behavior.
- Deployed LimaCharlie sensor for real-time endpoint monitoring.
- Executed Sliver C2 implant and LSASS memory dump (procdump) to emulate credential theft.
- Developed custom LimaCharlie rule to detect unauthorized LSASS modifications.
- Showcased proactive threat detection and incident response in a controlled lab environment.