KYN BRYAN TARAPE

TECHNICAL SUPPORT ENGINEER WITH CYBERSECURITY FOCUS

☎ +639292241096

www.linkedin.com/in/kyntarape999

✉ kyntarape@gmail.com

Cabadbaran,Agusan del Norte,
Philippines 8605

GitHub Portfolio
(https://github.com/kyntrp/KynSec-Portfolio)

Summary

"Cybersecurity enthusiast with 5+ years of technical support experience and a strong foundation in network security, threat detection, and incident response. Proficient in SIEM tools, IDS, and forensic analysis. Hands-on experience in cyber threat hunting, malware analysis, and security operations through home labs and practical projects. Passionate about leveraging technical expertise to detect and mitigate cyber threats in a SOC environment."

Experience

Converge ICT / Metroworks **May 2019 - Current**

Desktop Services Team Leader / Senior Technical Support Engineer

- Troubleshooting and resolving hardware, software, and networking issues (Remote and In-Person)
- Installing and configuring computer systems and applications
- Responding to technical support calls and emails from users seeking help
- Providing detailed instructions and guidance to users on various IT-related issues
- Managing user accounts and assisting with password or login problems
- Training other staff on troubleshooting and diagnosing problems
- Device deployment (Laptop, Desktop, Printer, Network devices, and other IT-related peripherals)

Converge ICT / Metroworks **August 2016 - May 2019**

Plant Records Engineer / ERP Staff

- Responsible for translating the Single-Line Diagram of As-Built Uplink plans provided by the implementation team into a more detailed presentation in Sunvizion.
- Encode As-Plan MDU (Multi Dwelling Unit) in Sunvizion
- Create an SLD (C.O. to Client) and Provide the FOC port number / FOC type / Closures to the concerned Department.
- Update and generate a monitoring of all the projects billed in Converge & Metroworks (as ERP Staff)

LBP Service Corporation - ERICSSON FNSO GOOGLE FIBER PROJECT

Autocad Operator - OSP Designer **December 2015 - June 2016**

- Responsible in translating sketches of a field surveyor to CAD software to make a detailed drawing design according to the standards of the client.
- Responsible for preparing and analyzing Make-Ready Engineering and pole loading analysis through O-Calc Pro.

Education

Bachelor of Science in Information Technology

STI College - San Fernando

Pampanga, Philippines

2012 - 2016

Skills

Soft Skills

- Technical Proficiency and Problem-solving
- Customer Service
- Strong Verbal & Written Communication
- Adaptability and Flexibility
- Analytical Thinking & Problem-Solving
- Attention to details
- Continuous learning and Knowledge sharing
- Threat Analysis & Investigation
- Patience and Stress Management

Technical Skills

- IT & Networking:

- IT Hardware, Software and Application Troubleshooting and repair
- Windows & Linux System Administration
- Active Directory Management
- Cloud Security (Microsoft Azure, Google Cloud)
- Python, SQL, Bash, PowerShell scripting for security automation

- Security Operations & Monitoring:

- Intrusion Detection/Prevention Systems (IDS/IPS) - Snort,Zeek, etc.
- Endpoint Detection and Response (EDR) - LimaCharlie, Wazuh
- Network Traffic Analysis - Wireshark, Tshark
- Security Information and Event Management (SIEM) - Splunk
- Incident Response & Digital Forensics - Autopsy, Volatility, FTK imager etc.
- Threat Intelligence & Malware Analysis

Certifications and Trainings

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.

🔗 **View my Certificates: [GitHub Portfolio](https://github.com/kyntrp/KynSec-Portfolio)**

Cybersecurity Projects and Innovations

Multilayered Cybersecurity and Detection System Using Virtualization, LimaCharlie, and Sliver C2

- **Virtual Machine Deployment:** Created a versatile virtualization setup, including Linux (Ubuntu Server) and Windows 10 virtual machines, to simulate a heterogeneous network environment.
- **Sensor Deployment and Monitoring:** Deployed a LimaCharlie sensor on the Windows 10 virtual machine, integrating it into the LimaCharlie console for real-time monitoring of system activities.
- **Simulated Adversary Activity:** Configured a Sliver C2 on the Linux virtual machine and implanted it in the Windows 10 virtual machine to simulate an adversary's presence.
- **Execution of Malicious Activity:** Executed the Sliver implant and utilized the procdump command to dump the LSASS process (lsass.exe) into a file (lsass.dmp). This mimics a common tactic used to extract credentials from memory.
- **Threat Detection and Response:** Monitored the Windows 10 virtual machine's activities via LimaCharlie, identifying the simulated malicious activity (modification of lsass.exe). Created a custom detection rule in LimaCharlie to flag and report unauthorized modifications to lsass.exe in real time, showcasing a proactive approach to threat detection and incident response.

This project demonstrates a thorough understanding of virtualization, endpoint detection, and adversary emulation tools. It highlights the ability to simulate attack scenarios, detect malicious activities, and implement rules to mitigate and respond to threats effectively.

Simulated Adversary Tactics and Threat Detection Using Virtualization, Splunk, and Atomic Red Team

Designed and implemented a cybersecurity testing lab using a virtualized environment to simulate adversarial attack scenarios and validate security monitoring solutions.

- **Environment Setup:** Configured a virtual lab with Windows 10 (target), Kali Linux (attacker), Windows Server 2022 (Active Directory Domain Controller), and Ubuntu Server (Splunk SIEM).
- **Security Monitoring:** Installed and configured Splunk Enterprise on Ubuntu Server, integrated Splunk Universal Forwarder on the Windows 10 target, and deployed Sysmon for enhanced logging.
- **Active Directory Configuration:** Established a domain with structured user groups and joined the target machine for authentication testing.
- **Adversarial Simulation:** Executed brute-force attacks using Hydra and Crowbar from Kali Linux to assess login attempt visibility in Splunk. Simulated attack techniques via Atomic Red Team (T1136.001 - Local User Creation & Removal, T1059.001 - PowerShell Execution) to evaluate detection efficacy.
- **Threat Analysis & Investigation:** Analyzed logs within Splunk to identify indicators of compromise, failed authentication patterns, and malicious activity signatures.

This project demonstrates hands-on experience in security monitoring, attack simulation, and threat detection, showcasing practical expertise in penetration testing, SIEM implementation, and Active Directory security.

🔗 **Full Project Documentation & Labs: [GitHub Portfolio](https://github.com/kyntrp/KynSec-Portfolio)**

Cybersecurity Projects and Innovations

SOAR EDR Automation Using LimaCharlie, Slack, and Tines

Designed and implemented an automated Security Orchestration, Automation, and Response (SOAR) workflow to enhance endpoint detection and response capabilities.

- **Sensor Deployment:** Installed and configured LimaCharlie sensor on Windows 10, ensuring effective endpoint monitoring.
- **Attack Simulation:** Used LaZagne.exe to simulate real-world credential-harvesting attacks, providing test scenarios for detection validation.
- **Detection Engineering:** Developed custom detection rules to identify malicious activity, including process execution tracking, file path monitoring, and SHA256 hashing for integrity validation.
- **Automated Response:** Built a Tines-powered workflow that retrieves detections, prompts the user for isolation decisions, and executes isolation actions via LimaCharlie API.
- **Communication & Incident Handling:** Integrated Slack notifications for real-time security alerts and status updates, enabling fast response and team collaboration.
- **Workflow Optimization:** Streamlined the process with decision-based automation, ensuring actionable alerts while maintaining user control over isolation enforcement.

This project strengthened cybersecurity operations by reducing manual intervention, enhancing detection accuracy, and accelerating threat response.

🔗 **Full Project Documentation & Labs: [GitHub Portfolio](https://github.com/kyntrp/KynSec-Portfolio)**