JOHN PAUL J. PAMINTUAN

Phone: +420 734 611 026
Email: Johnpauljpamintuan@gmail.com
Linkedin: linkedin.com/in/johnpaulpamintuan
Github: https://github.com/JohnPaulPamintuan
Website: https://johnpaulpamintuan.netlify.app

Pardubice, Czech Republic

Resume,
Skills & Projects

In a nutshell

- Cybersecurity professional passionate about safeguarding people, businesses, and systems in today's connected world. Energized by the challenge of defending data, networks, and systems against evolving threats, I blend problem-solving, continuous learning, and ethical responsibility to create safer digital environments. Driven by a commitment to growth and improvement, I am quick to adapt, eager to tackle new challenges, and currently advancing my Python skills to deepen my technical expertise. Fluent in English, Italian, and Tagalog, I bring flexibility, resilience, and a global perspective to every task."

Key Achievements — Certifications

- Google Cybersecurity Professional Certificate
- CompTIA Security+
- ISC2 - CC (Certified In CyberSecurity)
- Security Analyst Fundamentals IBM Specialization
- Palo alto Networks Cybersecurity Foundation
- CIsco's Security Operation Center (SOC) Certification
- Google Cloud Cybersecurity
- Splunk Search Expert Specialization
- Infosec's Python For Cybersecurity

Key Projects on Github

- **Microsoft Windows Defender & Windows Firewall**
  - This project demonstrates the configuration of Windows Defender and Windows Firewall to enhance security through antivirus management, firewall optimization, and proactive threat mitigation.
- **Network traffic Analysis and using TCPdump and Wireshark**
  - These projects demonstrate my expertise in network traffic analysis using TCPdump and Wireshark, focusing on capturing, filtering, and interpreting packet data for network troubleshooting, anomaly detection, and security optimization.
- **Linux System Administration**
  - This project showcases my ability to navigate and manage the file system using Linux commands and the Bash shell, including file manipulation, directory management, and automation for system administration.
- **Microsoft Active directory**
  - This project demonstrates my ability to set up and manage Active Directory, including user/group management, OU structuring, and access control for secure and efficient resource management.
- **Windows Event Log Analysis using Sysmon and Tracing for Windows (ETW)**
  - This project demonstrates the use of Windows Event Logs and Event Tracing for Windows (ETW) for security monitoring and incident detection. It focuses on analyzing event logs using tools like Get-WinEvent to detect suspicious activities and troubleshoot security issues.

- **Creating a Cybersecurity Home Lab**
  - This project demonstrates the process of setting up a basic home lab for cybersecurity, focusing on creating a secure and isolated environment for testing and learning. It includes configuring virtual machines, networking setups, and sandboxing techniques to facilitate safe experimentation and research.
- **Threat Detection & Response**
  - This project demonstrates the application of Splunk and Suricata for effective threat detection and response. It involves centralized log management, parsing network traffic, creating dashboards, and leveraging Search Processing Language (SPL) to analyze security data and identify incidents.
- **Vulnerability Management**
  - Conducted vulnerability scans using Nessus to identify system weaknesses, analyze security risks, and provide actionable remediation recommendations.
- **Python**
  - Python for Cybersecurity: basic task automation.

Skills

- **Security Analysis**: Windows Event Logs, Network Traffic Monitoring (Wireshark, TCPdump), Sysinternals Sysmon
- **Systems & Tools**: Active Directory, Windows Defender, Virtualization (VirtualBox), Linux (Kali & Ubuntu/Debian)
- **Incident Response & Management**: SIEM (Splunk), Incident Detection, Threat Mitigation, Windows Firewall Configuration
- **Network Security**: Secure VM Networking (NAT, Internal Network), Offensive Security (Nmap, Msfvenom)
- **Automation & Development**: Python for Cybersecurity Automation, Task Scripting
- **Home Lab Design**: Building Sandboxed Environments for Malware Analysis and Cybersecurity Research

Tools

- **Network Security Tools**:
  - **TCPdump**, **Wireshark, Suricata** (Network Traffic Analysis)
  - **Nmap** (network scanning), **VirtualBox/VMware** (Isolated Environments, Penetration Testing)
  - **NAT/Internal Network** (Secure Network Testing)
  - **NESSUS** (Vulnerability Scanning Tool)
- **Endpoint Security Tools**:
  - **Windows Defende**r (Antivirus Management)
  - **Sysmon** (System Monitoring), **Get-WinEvent** (Log Retrieval)
  - **Event Viewer** (Log Analysis)
- **Threat Detection Tools**:
  - **Splunk** (SIEM Tool: Log Ingestion, Analysis, and Incident Detection), **Suricata** (IDS/IPS Tool)
- **Scripting & Automation**:
  - **PowerShell** (Task Automation, Log Parsing)
  - **Python** (Scripting, Security Automation, Network Analysis)
- **Offensive Security**:
  - **Metasploit** (Penetration testing, Payload Creation)
  - **Kali Linux** (Pen-testing OS with Pre-installed Security Tools)
- **System Administration**:
  - **Active Directory Users and Computers** (User/Group Management, Access Control)

Work Experiences

Technical and Cybersecurity Experience:

Technical Intern (Cybersecurity Focus)
RAINBOW DISPLAY SYSTEMS s.r.o. – Pardubice, Czech Republic (2024)

- Collaborated with technical supervisors to identify, analyze, and resolve IT issues within small networks.
- Provided client support by troubleshooting and resolving hardware and software issues in a timely manner.
- Managed and maintained company hardware assets, ensuring regular updates, repairs, and replacements for optimal system performance.
- Conducted network and PC issue analysis, implementing solutions to enhance security and reduce vulnerabilities.

Cybersecurity Student | Self-Taught
Various Courses – (2023)

- Studied and applied cybersecurity principles through certifications, labs, and hands-on projects.
- Focused on network security, system administration, and threat analysis.
- Developed skills in detecting, analyzing, and mitigating cybersecurity threats across different environments.
- Currently advancing technical expertise by mastering Python for enhanced cybersecurity automation and problem-solving.

Hospitality Experience:

Service Professional
Parco dei Medici Bettoja, Bettoja Hotel Mediterraneo & Massimo d'Azeglio (4-Star Hotels), Enoteca La Torre (Michelin 2-Star Restaurant) – Rome, Italy

- Delivered exceptional guest experiences with personalized service in luxury and fine-dining environments.
- Ensured high food and beverage standards and seamless service delivery.

Restaurant Manager
Spiller – Milan, Italy

- Oversaw daily operations, staff management, and cost control.
- Coordinated front-of-house and kitchen teams for efficient service.
- Managed inventory, vendor relations, and financial reporting.
- Developed marketing strategies to enhance customer retention and revenue.

Receptionist
Hotel Central Lodge – Rome, Italy

- Facilitated smooth check-ins/outs and managed reservations.
- Ensured guest satisfaction by coordinating across departments.

Education

- **Cyber Security Fundamentals**, MOOC Program at University of London, 2024
- **Tourism and Hospitality Management** at Cristoforo Colombo State Technical Institute for Tourism, 2020

Languages

- Filipino (Tagalog): Native speaker
- English & Italian: Fluent in comprehension, writing, and speaking
- Spanish: Conversational, enhanced through frequent interactions with international tourists
- Czech & French: Basic proficiency (scholastic level)

Interest

- Self-Education
- Dedicate personal time to staying up-to-date with the latest trends and advancements in the IT security field.
- My current focus is on mastering Python to enhance my technical abilities further.
- Enjoy engaging in physical activities, including sports and participating in team-oriented endeavors.
- Find fulfillment in traveling and exploring countryside trails, embracing the opportunity to discover new places and cultures.
- Enjoy the serenity of nature through peaceful beach strolls and long walks, finding solace and relaxation in the rhythmic waves and calming landscapes

COVER LETTER BY

John Paul J. Pamintuan

Cybersecurity Professional

Dear Recruitment Team,

I am writing a letter of interest in regards to the position in your company. Your company is known for its innovation, professionalism, and results-driven marketing strategy, which is why I am certain I would make a valuable addition to your team. I would be interested in learning more about the company and available opportunities, so I have enclosed my resume for your consideration.

I am confident that my experience in this field will be an asset to your company. As you will see on my resume, I have a proven record of achievements, which will allow me to make major contributions to your company.

I look forward to speaking with you to discuss how my experience and abilities match your needs. I will call you on the day of the week to see what day and time fit your busy schedule. Don’t hesitate to contact me at your phone number or contact me by email at your email address should you have any questions. I look forward to speaking with you.

John Paul

John Paul J. Pamintuan