John Paul J. Pamintuan

Johnpauljpamintuan@gmail.com www.linkedin.com/in/johnpaulpamintuan
https://github.com/JohnPaulPamintuan www.mywebsite.com ☎ +420 734 611 026
Pardubice, Czech Republic

Cybersecurity Professional

Contents

Overview

I am a dedicated cybersecurity professional, 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.

With a strong foundation in both offensive and defensive security strategies, my focus lies in automation, orchestration, and secure deployment of cybersecurity solutions. My hands-on expertise includes **network traffic analysis**, **firewall configuration**, and advanced **Windows event monitoring** using tools like **TCPdump**, **Wireshark**, **Sysmon**, and **Event Tracing for Windows (ETW)**. Recent projects involve configuring and updating **Microsoft Defender** and Firewall, administering **Linux system**s, and managing **Active Directory** environments to build resilient cybersecurity defenses.

Driven by a commitment to growth and improvement, I am currently studying **Python** skills to deepen my technical expertise. I actively engage with platforms like **Hackthebox**, **Coursera's hand-on projects**, and **Try Hack Me** to continually hone my skills

I hold some certifications certifications including the **Google Cybersecurity Certificate**, **CompTIA Security+**, and **Coursera certifications** like (**Palo alto's network cybersecurity**, **IBM's cyber security fundamental**, **Splunks** and **Cisco's security operation center (SOC)**. I am committed to continuous learning and skills development.

My previous roles, from luxury hospitality service to **IT intern**, have strengthened my adaptability, team collaboration, and customer engagement skills. In every project, I prioritize clear communication, stakeholder alignment, and ensuring that I meet milestones effectively and deliver results that meet and exceed expectations.

I would like to improve myself within the **Cyber Security field** in order to become the ultimate **Penetration Tester**. I always keep a close eye to newly discovered **vulnerabilities** and like to challenge myself with unsolved weaknesses. I am someone who wants to make the world a more secure place for the next generation, even if it goes unnoticed.

Key Achievements

- G**oogle Cybersecurity Professional Certificate** — is a hands-on program designed to build foundational cybersecurity skills and apply industry-standard practices.
    - Learned essential cybersecurity frameworks and structured defense strategies.
    - Gained experience in securing both Windows and Linux environments against common vulnerabilities.
    - Practiced identifying and mitigating network threats using practical, hands-on methods.
    - Incident Response: Developed skills in detection, containment, and recovery.
        - This certification equipped me with essential skills in cybersecurity, readying me to protect systems and communicate risks effectively in professional environments.

- C**ompTIA Security+ certification** — provides a foundational understanding of cybersecurity, focusing on securing networks, systems, and data. It covers key areas such as threat identification, security technologies, risk management, identity and access control, and cryptography. Security+ emphasizes hands-on skills for assessing and mitigating risks, making it valuable for entry-level roles in cybersecurity.
    - **Key Areas**: Threats, Attacks, and Vulnerabilities, Security Tools and Technologies, Network and Application Security, Identity and Access Management, Risk Assessment and Incident Response and Cryptography and Data Protection.

- I**SC^2 - CC (Certified in CyberSecurity) certification** — is an entry-level credential focused on essential cybersecurity knowledge and skills. It's designed for those new to the field, covering core concepts like security principles, access control, network security, and incident response. The CC certification helps build a solid foundation for future advancement in cybersecurity roles.

- **The Security Analyst Fundamentals IBM Specialization on Coursera** — provides foundational training for aspiring cybersecurity analysts. The specialization covers essential skills for monitoring, detecting, and responding to cybersecurity incidents, using tools and techniques widely adopted in the industry.

- T**he Palo Alto Networks Cybersecurity Foundation course on Coursera** — introduces fundamental concepts of cybersecurity, focusing on key areas such as threat prevention, network security, and the role of firewalls in protecting systems. It's designed to provide learners with essential skills to understand and navigate the cybersecurity landscape.

- T**he Splunk Search Expert Specialization on Coursera** — is designed to teach learners how to effectively search, analyze, and visualize data within Splunk, a leading platform for operational intelligence. This course focuses on developing advanced skills in Splunk's search language and leveraging its capabilities for real-time data analysis and security monitoring.

- T**he Cisco's Security Operations Center (SOC) course on Coursera** — provides an in-depth look into the roles, responsibilities, and processes involved in operating a Security Operations Center. It covers core aspects of SOC operations, including monitoring, incident detection, and response, along with the use of various security technologies and strategies to protect organizations from cyber threats.

- T**he Google Cloud Cybersecurity** — provides foundational knowledge and practical skills for securing cloud environments. It focuses on Google Cloud's security features, best practices for protecting cloud-based infrastructures, and understanding common cloud threats. The course is ideal for those seeking to specialize in cloud security and secure data and applications in Google Cloud.
    - **Key Areas:** Introduction to cloud security principles, risks, and challenges. Overview of Google Cloud security tools such as Identity and Access Management (IAM), encryption, and monitoring. Securing Google Cloud networks using Virtual Private Cloud (VPC), firewalls, and secure connectivity. Implementing monitoring, logging, and alerting systems for detecting and responding to incidents in the cloud environment.

Cybersecurity projects

GitHub **Profile: https://github.com/JohnPaulPamintuan**

- **Microsoft Windows Defender & Windows Firewall**
  - Microsoft Windows Defender Antivirus and Firewall

- **Linux System Administration**
  - The commands commonly used for navigating and filtering the File System

- **Network traffic Analysis and using TCPdump and Wireshark**
  - Utilized TCPdump to capture and analyse TCP traffics
  - Utilized Wireshark to analyse HTTP/S and RDP traffic

- **Microsoft Active directory**
  - Setting up Microsoft Active Directory using Virtual Machine
  - Configured groups and performed basic administrative tasks with Microsoft Active Directory: Resetting User's Passwords + Unlock

- **Windows Event log analysis using Sysmon and Tracing for Windows (ETW)**
  - Using Sysmon and Event logs to detect and analyse malicious activity on Windows Server including identifying DLL hijacking
  - Introduction to ETW (Event Tracing for Windows): Basics for Cybersecurity Detection
  - Utilized Get-Win Event cmdlet to analyse Windows Event Logs
  - Skills Assessment - Windows Event Logs & Finding Evil - HackTheBox.

- **Splunk**
  - Utilized data analysis software and visualization tools to interpret security events

- **Python**
  - Basic Automation Project

- **Breach Response Case Studies:**
  - Case Study: Spear Phising Attack

Skills

Hard Skills	Associated Project
• Windows Event logs Analysis and detection	Detection Lab
• Network Traffic Monitoring and Detection	Detection Lab
• Active Directory	Configuration Microsoft AD
• Incident Response Planning and Execution	Soc Automation Lab
• Security Automation with Shuffle SOAR	Soc Automation Lab
• Linux systems (Ubuntu/Debian-based)	Unix Security
• Vulnerability Management	Qualys/Nessus
• Python	SOC automation Lab

Soft skills

- **Analytical Thinking** :
  - **Problem Solving** : Ability to approach and solve technical issues methodically, applying logical thinking to identify and address root causes.
  - **Attention to Detail** : Careful attention to detail when analyzing security incidents and documenting findings
- **Project Management** :
  - **Task Management** : Experience in managing tasks and projects, ensuring that goals are met within set deadlines.
  - **Collaboration** : Comfortable working with teams,providing support and sharing knowledge to achieve common objectives
- **Continuous Learning** :
  - **Ongoing Education** : Commitment to continuous learning and staying updated with the latest cybersecurity trends and tools.
  - **Adaptability** : Willingness to learn new skills and adapt to new challenges in a dynamic work environment.
- **Communication :**
  - **Technical Reporting :** Capable of preparing clear and concise reports on security incidents for both technical and non-technical audiences.
  - **Community Involvement :** Active participation in cybersecurity communities, contributing to discussions and learning from peers.

Tools

- **Network Security Tools**

WIRESHARK TCPDUMP python™ Nessus vulnerability scanner

- **Endpoint Security Tools**

Microsoft Defender for Endpoint Windows Sysinternals Sysmon

- **SIEM Tools**

splunk>

Work Experience

- **Technical Support - RAINBOW DISPLAY SYSTEMS s.r.o. Pardubice, Czech Republic 2024 :**

Cooperating with a technical supervisor on identification, analysis, and resolution of IT related problems in small networks with several tens of machines.

  - Client support: Provided technical support to clients, troubleshooting and resolving hardware and software issues in a timely manner.
  - Maintenance of Company Hardware Assets: Managed and maintained the company's hardware assets, including regular updates, repairs, and replacements to ensure optimal performance
  - Analysis of Network and PC issues.

- **Cyber Security Student | Self-Taught | Various Courses 2023 :**
  - Engaged in studying and applying cybersecurity principles through certifications and hands-on projects.
  - Focused on network security, system administration, and threat analysis.
  - Continuously learning and developing skills to detect, analyze, and mitigate cybersecurity threats in various environments.
  - My current focus is on mastering Python to enhance my technical abilities further.

- **Service Professional – in three luxurious, 4 star-rated hotels and a Michelin starred restaurant:**

1. **Parco dei Medici Bettoja (4 Stars + L Hotel)**
2. **Bettoja Hotel Mediterraneo and Hotel/Restaurant Massimo d'Azeglio (4 stars Hotel).**
3. **Enoteca La Torre (Michelin 2 stars restaurant) Rome, Italy :**
   - Delivered exceptional dining experiences by providing attentive and personalized service, managing guest needs, and ensuring a high standard of food and beverage quality.

- **Assistant Manager – Spiller, Milan, Italy :**
  - Assisted in overseeing daily restaurant operations, ensuring smooth and efficient service.
  - Managed staff schedules, training, and performance evaluations to maintain high service standards.
  - Coordinated with kitchen and front-of-house teams to ensure timely and accurate order fulfillment. Monitored inventory levels, ordered supplies, and managed vendor relationships to ensure cost control.Monitored inventory levels, ordered supplies, and managed vendor relationships to ensure cost control.
  - Prepared and analyzed financial reports, including sales and expense reports, to track performance.
  - Handled customer inquiries, resolved complaints, and ensured a positive dining experience. Developed and executed marketing strategies to attract and retain customers.

- **Receptionist – Hotel Central Lodge, Rome, Italy :**
  - Welcomed and assisted guests with check-in/out, ensuring a seamless and pleasant experience.
  - Coordinated reservations, appointments, and guest services efficiently
  - Collaborated with housekeeping and other departments to ensure guest satisfaction.

- **Summer Job as Assistant Lifeguard – in 3 beach resorts in Fregene, Italy :**
  - Maintained cleanliness of the beach area, regularly removing debris and ensuring a safe environment. Set up and arranged sunbeds and umbrellas for guests, ensuring a comfortable beach experience. Provided friendly customer service by addressing guest inquiries and need

Education

- **Cyber Security Fundamentals**, MOOC (massive open online course) 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