John Paul J. Pamintuan

Johnpauljpamintuan@gmail.com   linkedin.com/in/johnpaulpamintuan
github.com/JohnPaulPamintuan   johnpaulpamintuan.netlify.app   +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 **Technical 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

Google Cybersecurity Professional Certificate — equips beginners with essential cybersecurity skills, covering network security, threat detection, incident response, and security tools, preparing them for entry-level roles like Security Analyst or SOC Analyst.

CompTIA 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, making it valuable for entry-level roles in cybersecurity.

ISC² - 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.

The 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.

The 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.

The 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.

The 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.

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.

Creating a Cybersecurity Home Lab
- Cybersecurity Home Lab: Building, Attacking, and Defending Virtual Environments

Threat Detection & Response
- Splunk SIEM in Action: A Guide to Data Ingestion, Analysis, and Real-Time Security Monitoring
- Network Threat Detection with Suricata

Vulnerability Management:
- Scanning Tools: Used Nessus to identify and analyze system vulnerabilities
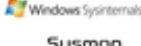
Python:
- Basic Automation Project

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

Skills	Associated Project
Windows Defender: Skilled in implementing Windows security measures, including antivirus management, firewall rule optimization, and proactive threat mitigation strategies	[Windows Security](#)
Active Directory Management: Demonstrated expertise in setting up, configuring, and managing Active Directory environments, including user and group management, organizational unit structuring, and access control.	[Active Directory Lab](#)
Security Monitoring: Proficient in using Splunk, Sysmon, TCPdump, and Wireshark for network traffic analysis, centralized log management, and telemetry data visualization to detect and analyze potential security threats.	[Detection Lab](#)
Network Traffic Analysis: Skilled in capturing, filtering, and interpreting packet data using TCPdump and Wireshark to identify anomalies and optimize security configurations.	[Detection Lab](#)
Linux File System Management: Proficient in navigating and managing Linux file systems using Bash commands, including directory traversal, file creation, permissions management, and process control.	[Unix Security](#)
Windows Event Log Analysis for Incident Detection: Experienced in leveraging Windows Event Logs and Event Tracing for Windows (ETW) for security monitoring, incident detection, and troubleshooting. Proficient in using Get-WinEvent and related tools for parsing and filtering logs to detect suspicious activities and security threats.	[Detection Lab](#)
Virtualization: Configuring virtualized environments with VirtualBox for secure testing.	[Home Lab](#)
Malware Analysis: Safely executing and analyzing malware in isolated virtual machines.	[Home Lab](#)
Vulnerability Assesment: Conducted vulnerability scans using Nessus to identify system weaknesses, analyze security risks, and provide actionable remediation recommendations.	[Vulnerability Lab](#)
Network Security: Implementing secure VM network configurations (NAT, Internal Network).	[Home Lab](#)
Offensive Security: Conducting reconnaissance with Nmap and crafting payloads using msfvenom.	[Home Lab](#)
Incident Monitoring: Configuring Sysmon for detailed telemetry and analyzing logs with Splunk.	[Home Lab](#)
Home Lab Design: Establishing sandboxed environments for cybersecurity research.	[Home Lab](#)

Tools

Network Security Tools	TCPDUMP WIRESHARK NMAP VirtualBox VirtualBox **NAT** **INTERNAL-NETWORK** **HOST-ONLY NETWORK**
Endpoint Security Tools	Microsoft Defender for Endpoint Windows Sysinternals Sysmon Microsoft Event Viewer **Get-WinEvent**
Threat Detection Tools	splunk> SURICATA
Vulnerability Tools	Nessus vulnerability scann
Scripting and Automation Tools	PowerShell python
Offensive Security Tools	Metasploit
Penetration Testing Operating Systems	KALI LINUX
Directory Services and Access Control Tools	Active Directory

Work Experience

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 (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

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