Carl Pierre-Louis

Cplouis97@gmail.com
LinkedIn: www.linkedin.com/in/carl-pierre-louis-02332a170

PROFESSIONAL EXPERIENCE

Google *Remote, Florida* January 2026 – Present
Associate Red Team Security Consultant

- Loading….

Neovera *Remote, Florida* May 2024 – December 2025
Information Security Engineer I

- Conduct External Penetration Test Engagements. This includes utilizing OSINT to gather information, scanning external resources, launch phishing campaigns, etc. to identify areas of improvement in client's security posture.
- Show impact through simulated real-world attacks within internal networks. Identifying misconfigurations and vulnerabilities in Microsoft Active Directory, and other running services on Windows and Linux systems. This allows security teams to identify gaps and make improvements to aid in thwarting bad actors.
- Enumerate Thick & Thin clients for potential vulnerabilities or misconfigurations.
- Test wireless networks to ensure they are secure using tools such as aircrack suite & wifite.
- Conduct Vulnerability analysis using tools such as Nessus from an external and internal perspective.
- Work closely with blue teams to identify holes in detection and response procedures through Purple Team engagements.
- Guide clients through engagement process during kick-off meetings, ensuring we operate within scope.
- Write detailed report documenting findings, steps to achieve results and remediation/mitigation recommendation to assist security teams quickly identify and resolve issues.
- Communicate findings with blue teams and executive staff to help clients fully understand impact of results.
- Work independently and on a team to find solutions to customer related issues.

L3Harris *Melbourne, Florida* August 2022 – May 2024
Sr. Assoc. IT Security Analyst

- Threat Hunter, identifying and tracking potential threat actors through their Techniques Tactics and Procedures (TTPs).
- Leveraged Offensive Security mindset to investigate network events for potentially malicious activity.
- Utilized threat Intelligence sources such as AnyRun, MISP, Mandiant, and CISA to aid in identifying activity from threat actors attempting to compromise the network using various ransomware and malware tools such as Emotet, qBot, Maze, and Lockbit to name a few.
- Analyzed logs and network traffic using various tools such as ArcSight and Wireshark, to enhance network security. These tools helped me identify attempts of directory traversal and Local File Inclusion (LFI) among others.
- Document findings and conveyed complex technical concepts to technical and non-technical audiences.
- Lead Security Fundamentals training for over 100 new employees being onboarded.

Carl Pierre-Louis

Cplouis97@gmail.com
LinkedIn: www.linkedin.com/in/carl-pierre-louis-02332a170

Duke Energy *Charlotte, North Carolina* January 2022 – August 2022
Cyber Security Analyst

- Aggressively triaged 400+ events over the course of 6 months
- Investigated events for possible malicious activity using various internal tools such as Enterprise EDR Solution, SIEM tool, IDS & IPS solution, and Email analysis tools.
- Utilized Open-Source Intel (OSINT) to perform further information gathering using tools such as WHOIS, Virus Total, Redirect Checker, and URL scan to name a few.
- Thoroughly documented findings throughout investigation
- Identified malicious or suspicious activity and escalated for further analysis.
- Utilized Pyramid of Pain to prioritize and increase effectiveness of threat intelligence.
- Leveraged MITRE framework to identify tactics and techniques used by attackers to provide a more streamlined approach to investigations.

Microsoft *Charlotte, North Carolina* September 2020 – January 2022
Support Engineer, Azure Bare Metal

- Served as customer internal advocate, collaborating with engineers cross-functionally to troubleshoot customer issues and provide effective solutions.
- Ran test utilizing Azure Virtual Machines to validate functional solutions and provide customers with proof of concept. This allowed me to visually demonstrate to customers how the product worked and give customer recommendations on how to potentially fix issues. Received multiple 'kudos' from customers.
- Contributed to engineer documentation allowing for a more efficient troubleshooting process.
- Empowered customers through the delivery of resources that aided in breaking down tools and features which leads them to rely less on customer support.
- Worked alongside product teams to deliver new features to Azure NetApp, playing a hand in expanding overall functionality.

EDUCATION

Florida Atlantic University, Boca Raton, FL
Bachelor of Science in Management Information Systems May 2019
- *Information Security*

Master of Science in Information Technology Management May 2020

CERTIFICATIONS

Certified Red Team Operator (CRTO) July 2025
Zero Point Security
https://eu.badgr.com/public/assertions/NwUQycsUShOM52htlVKXwA

Offensive Security Certified Professional (OSCP) May 2024
Offsec
https://credentials.offsec.com/184a7a35-7ce9-48e0-9b74-0df870e73f22#acc.fDa8EusJ

Practical Network Penetration Tester (PNPT) Jul 2023
TCM Security
https://certified.tcm-sec.com/6c3f8d12-0aa7-4118-8c45-6d0dff8d6c9c#acc.7qG2cTWa

eLearnSecurity Certified Penetration Tester (eCPPTv2) Mar 2023
eLearnSecurity
https://verified.elearnsecurity.com/certificates/0b3eccdf-caf9-432d-9ccf-24dda21a11a9