Luke Leveque

Louisville, Kentucky / ludicro.professional@proton.me / LinkedIn/In/luke-leveque / GitHub/Ludicro

Experienced student with a demonstrated history of working with forensic and SIEM software as well as real world experience in a SOC environment. Skilled in **Linux**, **Analytical Skills**, **Python**.

Education

University of Louisville
Expected Graduation: May 2025

Bachelor of Business Administration - BBA, Computer and Information Systems - Cybersecurity
        Member of ACM Club – Cyber Defense Team

Morehead State University
Aug 2019 - Jul 2021

High School Diploma, Computer Science
        Graduated the Craft Academy for Excellence in Science and Mathematics based at Morehead University with the Presidential Scholar's Award (GPA > 3.8).

Experience

Palo Alto Networks
May 2024 - Aug 2024

SOC Engineer Intern

- Owned and lead individual incident response activities by analyzing over 300 security alerts and coordinating responses
- Hunted for indications of compromise across multiple technology platforms
- Continuously improved alerting use cases and the threat hunting program
- Collaborated with SOC Automation team to automate tedious activities
- Generated reports detailing security incidents for security leaders and the business
- Demonstrated communication skills in postmortem reviews of incident response activities, to facilitate continuous improvement
- Developed an internal malware auditing system that was able to gather and analyze over 5000 signatures from a week's data using XQL queries, Python, and web APIs.

University of Louisville
Sep 2022 - Dec 2023

Security Analyst Student Assistant

- Assisted in the identification, isolation, and resolution of incidents averaging 7-10 a day.
- Troubleshot issues from customers needing VPN, password management, and other security tools.
- Utilized tools such as Azure Sentinel and Microsoft Defender to monitor, analyze, and respond to threat intelligence.
- Developed an automated Teams alerting systems for specific critical alerts.
- Developed automated data gathering system using active directory and PowerShell to gather and compartmentalize data for easier analysis.

Best Buy – Geek Squad   Aug 2021 - Aug 2022
Consultation Agent & Advanced Repair Agent

- Ensured client issues are resolved in an efficient and timely manner.
- Provided immediate computer assistance from diagnostics to quick repairs.
- Provided knowledgeable technology solutions and support.
- Maintained a friendly, efficient check-in and check-out experience for customers requiring other technical assistance.

Competition Experience

NCL Team Game - Cyber Skyline
> Fall 2021 – U6T6UUBTLB5J – 131st/3909
> Fall 2022 – JWVHPVDWJFN9 – 216th/3926
> Fall 2023 – FHAM10HNEUXA – **11th**/4672
> Fall 2024 – 3Q2XQ2AHK6PE – **12th**/532 (*Experienced Bracket*)

NCL Fall 2022 Individual Game - Cyber Skyline
> Fall 2022 – LG54F8QUDXP9 – 457th/3487
> Fall 2023 – EWCE1DX3HP1U – **230th**/7934
> Fall 2024 – U12B5QK25Q5U – 332nd/8484

Midwest Regionals CCDC - National Collegiate Cyber Defense Competition
> Years 2022 and 2023

Skills
Systems

Operating Systems: **Windows** • **Linux** • Mac

Cloud Environments: AWS • Google Cloud • Azure

Technical

Query Languages: SQL/**XQL**/KQL

Security Analyst/Engineering: **Scripting** • Cloud Security • **Log Analysis** • Networking • Web Applications • SIEM Environments/**XSIAM** •

Python • C/C#/C++ • Java

Professional

Analytical Skills • Presentational • Communication • Teamwork •

Microsoft: **Excel Certified** • Word • PowerPoint

Honors & Awards
Eagle Scout   2020
Boy Scouts of America