

Usama Ghawji

• [linkedin.com/in/ughawji/](https://www.linkedin.com/in/ughawji/) • usamaghawji.com • +1 (416) 877-4388 • u.ghawji@gmail.com •

EXPERIENCE

SOC Analyst Intern

June. 2019 - Sept. 2019

Johns Hopkins Aramco Healthcare | Aramco, KSA

- Constructed informative dashboards and reports in **SPLUNK** based on use cases to identify vulnerabilities
- Engineered **SPLUNK** threat detection queries in order to cover areas of the **MITRE ATT&CK** framework and further cyber threat hunting capabilities.
- Conducted packet analysis via **Wireshark** to identify malicious traffic and network troubleshooting
- Implemented phishing awareness campaign resulting in a **40% decrease** in failed phishing attempts

Co-Founder, Director of Operations

Aug. 2020 - Present

Lassonde Security Club | Toronto, CAN

- Created and implemented cyber security-specific workshops, tools, and guest speakers for university students.
- During a workshop, explained to students the basics of **Wireshark** including UI, capture filters, and analyzing network
- Grew traffic by performing user research and designing graphics resulting in **100% growth** in 5 months

Financial & Data Analyst

Sep. 2018 - Sep. 2020

Excel Lassonde | Toronto, CAN

- Created **Microsoft Excel/Power BI** reports to reveal trends in the data and make it meaningful
- Established a new **Excel** reporting system to improve availability and accuracy of data
- Organized and presented data in a way that both technical and non-technical people can understand.

EDUCATION

York University - Lassonde School of Engineering | Honours BSc - Computer Science

Expected April 2022

- Experience Venture Award | YSpace
 - Awarded for excellence in disruptive innovation, entrepreneurial thinking, and leadership skills

CERTIFICATIONS

- **Splunk Fundamentals 1** - April 2021
- **Splunk User Behavior Analytics (UBA)** - May 2021
- **CompTIA Security+** - *Expected December 2021*

PROJECTS

- **Social Engineering**
 - Used the **SEToolkit** in **Kali Linux VM** to clone websites like Facebook and Gmail.
 - Conducted a simple Watering Hole Attack to perform credential harvesting
- **NFT Collection** | [The Humanoids](#)
 - Worked in a team of three to launch a 10,000 NFT collection - **sold out in under 3 minutes**
 - Applied user-research, CRM strategies, and social-media marketing, to grow the Discord community from 200 members to **over 47K** members in less than 2 months.

SKILLS

- **Softwares:** Splunk, Wireshark, Power BI, Microsoft Suite, Palo Alto Traps
- **Languages:** MySQL, Python, HTML, CSS, Java, Javascript
- **Frameworks:** ISO 27001, MITRE ATT&CK, Cyber Kill Chain
- **Knowledge:** GRC, Incident Response, CIA, Social Engineering, SDLC, Risk Management, TCP/IP, Networking, Agile