Umar Mohammad Riaz

r.umar.mohammad@gmail.com | linkedin.com/in/umar-mohammad-riaz | github.com/mr-umar

Work Experience

Cipher | A Prosegur Company — cipher.com

L2 Detection and Response Analyst (Full-time) — June 2023 – September 2024

- **Management and investigation of alerts from customers:** Monitored and assessed alerts from security systems such as Microsoft Sentinel and XDR, leveraging SIEM and OSINT tools, alongside Microsoft Azure, Proofpoint, and Elastic, to investigate and report security incidents comprehensively.
- **Dashboard monitoring:** Continuously supervised dashboards using platforms like Microsoft Sentinel and Elastic to ensure real-time visibility and rapid response to security events.
- **Management of Use Cases and evaluation of rules and behavior for improvement:** Developed and managed use cases, evaluated existing rules and behaviors, and implemented improvements to enhance security posture, leveraging tools such as Microsoft XDR and Azure.
- **Improvement and creation of use cases:** Enhanced and developed use cases using KQL (Kusto Query Language) and Logic Apps to improve threat detection and response strategies.
- **Interlocution with CSM and Integrator:** Communication with Customer Success Managers (CSMs) and Integrators to ensure effective communication and coordination for security initiatives.

Proficio — proficio.com

L1 Cyber Threat Analyst (Internship for my studies at ITB) — June 2022 – May 2023

- Monitored security dashboards (ServiceNow, Elastic, Splunk) to detect incidents.
- Created reports and documented incidents for accurate tracking.
- Investigated and resolved threats, escalating complex cases.
- Recommended improvements and developed troubleshooting techniques.
- Ensured compliance with SLAs for timely responses.

Education

Polytechnic University of Catalonia (UPC) — upc.edu

Bachelor's degree in Telecommunications Technologies and Services Engineering (Telecommunications Engineering) — September 2024 – June 2028

First-year student with a focus on applied mathematics, physics, and communication technologies, gaining a solid foundation in signal theory, linear algebra, and the fundamentals of telecommunications

Institut Tecnològic de Barcelona (ITB) — itb.cat

Higher Vocational Education in Networked Computer Systems Administration, Specializing in Cybersecurity — September 2021 – May 2023

Proficient in networked computer systems administration with a strong emphasis on cybersecurity.

Skills and Qualifications

High knowledge of **operating systems and network** administration.
Great **Python** and **C** Programming/Scripting skills.
Experience with **Elastic, Splunk SIEMs and Microsoft security solutions (XDR, Sentinel, Azure).**
Strong skills in cyber threat intelligence **analysis and reporting.**
Cyber defense **techniques, adversary tactics, techniques, and procedures.**
Experience with **OSINT** Techniques.
Knowledge in **ITIL, MITRE, MISP, NIST and other threat intelligence platforms.**

Languages

- **English -** B2
- **Spanish -** Native
- **Catalan -** Native
- **Urdu -** Native

Interests

- Computers, technology, and video games.
- Passionate about exploring new technologies and gaming trends.