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 — June 2023 – Currently

- **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 — June 2022 – April 2023

- **Monitoring and Interpretation:** Watched active channels/dashboards on platforms like ServiceNow, Elastic, and Splunk, replaying and interpreting events to detect potential security incidents.
- **Documentation and Reporting:** Created annotations, reports, and cases to document incidents and their resolution, ensuring accurate record-keeping.
- **Incident Investigation:** Effectively utilized ServiceNow, Elastic, and Splunk platforms, including channels, event graphs, annotations, cases, and reports, to promptly investigate and resolve security incidents. Proficient in pattern recognition to identify potential complex cyberattacks, escalating issues as needed.
- **Recommendations for Improvement and Troubleshooting:** Identified improvements for the service, efficiency, and quality, Developed and documented troubleshooting techniques for efficient resolution of common security issues.
- **Service Level Agreement Compliance:** Ensured compliance with defined service level agreements regarding response time and customer notification, maintaining high standards of service delivery.

Education

Institut Tecnològic de Barcelona — 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** 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.**

Languages

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