Mark Cardiff

3 Ellensborough Grove, Kiltipper, Dublin 24. **mark.cardiff@gmail.com**
Mobile Number: 087 900 6701 **www.linkedin.com/in/mark-cardiff**

PERSONAL PROFILE

A dedicated and results-oriented professional with a strong passion for IT, specializing in Security. With a proven track record in problem-solving and a comprehensive understanding of security operations, I thrive in challenging environments. Currently serving as the Team Lead in Presidio's EU Security Operations Centre (SOC), I effectively lead a team while driving operational excellence and client satisfaction. Looking to further enhance my expertise and contribute to the advancement of network security while pursuing new opportunities for professional growth.

KEY SKILLS AND CERTIFICATIONS

- **SIEMs:** QRadar, FireEye Helix, Palo Alto XSOAR
- **EDR:** FireEye HX, Blackberry Cylance Protect & Optics
- **Ticketing Systems:** Connectwise and Brightgauge
- **CompTIA IT Fundamentals, Network+, Security+, CYSA+**
- **IBM Certified Security Analyst**
- **Security Blue Team Level 1**
- **TryHackMe Top 1%**

EDUCATION AND TRAINING

2017 – 2019 **DBS, Aungier St, Dublin.**
HDip Computing (Infrastructure and Networking)

2012 – 2013 **DBS, Aungier St, Dublin**
Diploma in Business Management

2003 – 2009 **DIT, Bolton St**
BEng in Structural Engineering

WORK EXPERIENCE

July 21 – Present **SOC Team Lead - Presidio**
Responsibilities include:

• Supervising and leading a team of 25 analysts in the Security Operations Centre, providing guidance, mentorship, and escalation support for L1, L2, and L3 analysts.
• Managing day-to-day monitoring of SIEM/EDR systems for multiple clients across diverse industries, ensuring timely detection and response to security incidents.
• Investigating and documenting security events, employing analytical skills to determine the severity and impact of incidents, and reporting findings to clients.
• Conducting regular meetings with clients on a monthly/weekly/daily basis to discuss incidents, provide incident reports, and address their concerns or inquiries.
• Coordinating and leading weekly meetings and daily scrums with the SOC team, fostering collaboration, sharing knowledge, and aligning priorities.
• Collaborating with cross-functional teams to onboard new clients to the SOC, conducting initial assessments and overseeing the setup of monitoring systems.
• Continuously refining and improving use cases to optimize the SOC's detection and response capabilities.

Sept 19 – July 21 **SOC Analyst - Presidio**

Sept 05 - Sept 19 **Superquinn/SuperValu Knocklyon**
Ambient / Scanning Team Leader

INTERESTS

- Technology and IT: I have a home lab that I have used help in my studies for Certifications and to learn more about the systems we use in the SOC.
- Car Mechanics and Restoration: I enjoy working on my cars to improve and restore them, figuring out how things work and getting them going again.
- Fine Scale Modelling: A hobby that requires attention to detail and patience.