



# A Day in the Life

*at Kick ICT*

I joined Kick ICT in August 2023, and since then, it's been a steady stream of new experiences. No two weeks are the same—unless I'm doing reports... then there's a strong sense of déjà vu. I currently work a four-day week, mainly focusing on Kick Secure, where I help maintain and improve our customers' security posture.

My role involves carrying out remediation tasks such as configuring Conditional Access policies and ensuring our clients' email security aligns with Microsoft's standards—this includes setting up DMARC, DKIM, and SPF records for their domains. This often means I'm in direct contact with customers via email or calls to explain what's happening or request access to their DNS control panels, things like that.

A significant part of my role involves auditing logs—both within Microsoft portals and on end-user devices—to identify anomalies or security alerts. If I detect something concerning, like a malicious file on a user's machine, I follow procedure by isolating the device to prevent further spread and escalating it to a specialist in the team for further investigation.

I've also had the opportunity to work with Fortinet firewalls, which was a highlight for me. These are used widely across the industry (or at least they should be). I configured one from scratch with support from my colleague David. After many rules, settings, and testing, we completed the setup—and the following week, I visited a customer site in Edinburgh to swap out their old firewall with our new and improved configuration.

I work closely with a great team in the office, including a university friend, Dario, another consultant, Ben, and two senior team members—David Paine (CISSP certified) and Stuart Beattie, who knows more about scripting and automation than I thought was possible. I also get involved in on-site work, which varies from laptop setups and networking fixes to Azure migrations and general support tasks. This range has massively broadened my technical skill set.

I regularly work within Microsoft portals such as Entra, Microsoft 365 Admin, Security, Purview, Exchange, and SharePoint. I also use third-party tools like DMARCian to monitor email flows, helping identify spoofing or phishing attempts. Another key tool is RocketCyber, which provides endpoint detection and response capabilities across our customer base (very handy for real-time threat visibility and alerting). We also use our own internally developed Kick Secure Portal, built by Stuart Beattie. This central hub gives me access to everything I need—from internal notes and security scores to audit details and customer contacts.

Outside of technical work, Kick ICT has a great location at Strathclyde Business Park, which offers woodland walks and several nearby lunch spots. Personally, I usually bring my own food and enjoy lunch in the kitchen area—often followed by a quick game of ping pong in the games room. It's a great way to reset and get the steps in.

Kick also promotes personal and professional development. We recently attended a seminar focused on transforming bad habits into good ones, which gave a refreshing take on productivity and mindset. We also complete monthly KnowBe4 training sessions covering cyber security awareness (phishing, malware, etc.) and wellness tips such as correct posture and monitor positioning. It's short, useful, and relevant.

In summary, I've really enjoyed my time at Kick ICT so far. It's been a fantastic place to develop my skills, contribute meaningfully to customer security, and work with a talented and supportive team. I look forward to continuing this journey and building on what I've learned.

*-Kacper Lewandowski*



**Kick**