

A DAY IN THE LIFE OF A NETWORK DEFENCE RESEARCHER

I joined CESG straight out of University and started my career in the Intrusion Detection research team within Network Defence. The Network Defence team works with many other agencies, at home and abroad, to help keep HM Government communications and IT systems safe from hackers and other threats. This is achieved by undertaking cutting edge research and developing new solutions and services.

Before starting here, I hadn't really had much experience with electronic attack or malware. Today, much of my time is spent analysing the threat to HMG networks and IT systems, whether that's examining the latest 0-days or reverse-engineering malware to discover its intent. This work is technically challenging and very much hands-on. I also spend time working with CESG's analysts, developing new analytical tools to help them when commercial solutions are not available.

At first the learning curve was quite steep, but the area is extremely inclusive and I benefited greatly from the experience of my peers. Another advantage is the areas provision for training and it's commitment to keeping staff up to date with technology. Since joining I've attended several of the big security conferences and conventions all over the world.

As the frequency and complexity of attacks increases, crafted to penetrate specific networks or applications, so does the necessity for advanced detection techniques. The need to protect government assets requires advanced solutions. Our team researches, develops and maintains state-of-the-art Intrusion Detection Systems for both the host and network.

As a whole the work is current, fast-moving and challenging. It's also rewarding to see my work making a real difference to the security of the UK.