

BULK UP YOUR DEFENDER TODAY



DETECTION RULE AND THREAT HUNT DEVELOPMENT FOR NHS WALES USING SENTINEL AND KQL

Windows Defender is an excellent antivirus solution, but industry standards mean it's slow to update, and a globally applicable set of rules and policies just isn't good enough in the modern cyber climate. To this end, this project aims to deliver industry specific, threat intelligence informed detection rules and threat hunts which will bolster the defences of NHS Wales using Microsoft Sentinel, with a focus on phishing protection and supply chain compromise.