Mike Minion

mikeminion@googlemail.com

Highly skilled SecOps Engineer with experience in professional services and regulated manufacturing covering all areas of Cyber Security. Adept in protecting computer systems and securing data in hybrid environments via zero trust access. Hands on experience in SOC management, incident and containment. Proven experience of applying new security controls to hybrid environments covering Public Cloud (AWS, Azure) and On-Premises.

- *SSCP studying*
- ITIL Level 3
- PRINCE2 Foundation
- MA Film - University of Aberdeen
- CISCO IT Essentials 1 & 2
- Advanced Diploma Level 3 ICT Practitioners
- NVQ Level 3 Information Technology

- Azure Active Directory
- CISCO Meraki Firewalls
- CISCO Umbrella
- Mimecast
- Qualys Cloud Suite
- Qradar / Senseon
- Ruby, Powershell, Bash Scripting
- Windows Server & Linux (Kali, Debian derivatives)

February 2021 - *Current*
SecOps Engineer at Huntswood CTC

Member of the SecOps Team, carrying out project work, and protecting Huntswood CTC estate. Hybrid environment AWS, Azure & on prem with sites in the UK & South Africa. Responded to SOC incidents working alongside 3rd party QRadar, implemented problem and policy fixes. Predeployment reviews for projects.

Projects Completed

- CISCO Any Connect Zero Trust Migration
- Build Machine security and performance benchmarking (Qualys and CIS)
- Annual Pentest Management and Delivery
- Review and implementation of security GPOs for desktop applications
- Office 365 Security Hardening (macro implementation, global policies, etc)
- Various Email Integrity Projects (Phishing Campaigns, SpamTitan implementation)
- Netskope Publisher update process & updated the process of using Netskope Rest API v2
- Scripting in Powershell and Shell for reporting and interrogation
- Cloud Estate Security Analysis and Remediation (detection, reporting, patching, etc)

Tools:

- Netskope
- Trend AV & Trend Phish Insight
- Qualys (VMDR, Benchmarking, Patching, Asset Management, Scans & Reporting)
- QRadar
- Mimecast
- Spamtitan

- Windows Sandbox
- Kali Lunix
- Azure sign logs/AWS Cloudtrail
- Wireshark
- App any run/url scanner io/virus total/cisco talos
- Security scripts in retrieving information
- SolarWinds Event Manager

October 2020 -Jan 2021
Divisional Security Analyst at Kingspan

Security Analyst within Kingspan Panels a major part of the Kingspan Group. Tasks are focused on ensuring the safety of the Kingspan Group’s Estate through monitoring, remediation and preventative work. Responded to escalated security incidents raised internally and via SOC escalations. Worked with third parties like Qualys to ensure the Kingspan Estate remains secure across Cloud and on Premises.

Originally part of Infrastructure Engineering covering the installation, running and maintenance of all compute, storage, networking, firewalls and virtualised infrastructure for all of Kingspan. Responsible for security, deployment and reliability concerns.

Projects Completed

- Cisco Umbrella scheduled reporting
- Implemented Qualys Scan Pipeline for new deployments
- Completed Qualys onboarding and initial vulnerability resolutions
- WSUS and SAP Security reviews & remediations
- Meraki WiFi Deployment and Hardening
- SolarWinds Orion Migration & Upgrade
- Promark Decommissioning

November 2018 – October 2020

Divisional IT Infrastructure Engineer at Kingspan Panels

Member of the 3rd line team, which provided Infrastructure support to the Kingspan panels estate along with working on projects. For existing hardware/software: compute, storage, networking, firewalls, telephony, physical & virtual infrastructure. Triaged alerts and tickets through the helpdesk via SolarWinds. The estate is expanded globally, with offices and factories in different locations and having different setups. Support was also provided for legacy systems that were out of support.

Projects/Works Complete

- Qualys Scans configuration to scan assets to determine how secure they were on the network
- Meraki Wifi deployment in office and factory’s, within the division
- Phone migration in Sydney from ISDN to SIP
- Applied scheduled maintenance [Forcepoint] firewalls bringing the estate in line with compliance
- Ensured Orion (Solar Winds) ran and monitor the estate correctly
- Decommissioning & migration of legacy systems on the estate

October 2017 - August 2018
Senior Technician at IT Centric

Looked after clients based worldwide. Managed administration within the help desk, and provided support to colleagues, while completing projects. Senior Technical support for any major incident. Clients included Police Scotland, Lloyds Bank and more

Technical Stack

- Office 365 & Azure
- Windows Server 2012 / 2016
- SharePoint 2010
- CISCO Networking

October 2015 - October 2017
Network Technician at Pulsant

Network Technician for a leading MSP to Financial Services, E-Commerce, Legal and other firms. Acted as one of front line the Engineers across numerous accounts delivering custom solutions and SME support to clients.

- Network setup, development and troubleshooting across cloud, on-premises and third party solutions
- System and Network Security Management - penetration testing, solution hardening, etc
- Scripting and Automation for solutions and monitoring
- Incident Management, Resolution and Remediation - from investigation to implementing fixes
- Management of Deployments, Rollouts, Maintenance and Upgrade Scheduling
- Project: Configured the dr suite roll back process

May 2015 - October 2015
IT Engineer at DunedinIT

IT Engineer at DunedinIT providing support for medium sized businesses. Implemented and led a number of networking focused projects as an external SME covering Cloud technologies, Thin Clients, custom web solutions and more

March 2015 - April 2015
Full Stack Developer at House of Bruar

Short Term role providing development services to a Scottish Retailer. Provided frontend development alongside SQL database development. Migrated company data from an Excel spreadsheet to a fully serviced SQL database including integration with the frontend website.