Curriculum Vitae

MATTHEW **RYDING**

Cumbria (Preston) – Willing to relocate · +44 7885 911534 · Full Driving Licence
matryding@gmail.com · www.linkedin.com/in/matthew-ryding

Qualification Summary

GIAC:	GSOC/SEC450 - BLue Team Fundamentals
Comptia:	Network+ (N10-007) Security+ (SY0-501) CySA+ (CS0-002)
DHS-ISC:	US CISA - Industrial Control Systems Incident Response Team Certification
ITILv3:	ITIL Foundation for ITSM
Splunk:	Splunk Fundamentals 1

Technical Skills

Tools/ Technologies:	LogRhythm, Darktrace, Digital Guardian, Splunk, Snort, Cisco AnyConnect VPN, VLAN, Port Security (802.1x), OSI Model, TCP/IP, DNS, DHCP, Cisco/Palo Alto Firewalls, Network Policy Server, Wireshark, NMAP, Netstat, Nessus, OpenVAS, Active Directory, Group Policy, Blackberry UEM (MDM), Azure, Virtualisation, Office 365 Administration, SharePoint, Microsoft Teams, DLP, Citrix XenApp, SCCM, Ivanti, ServiceNow, Asset Management
Frameworks:	Lockheed Martin Cyber Kill Chain, MITRE ATT&CK, OWASP Top 10, ISO 27001, GDPR, NIST SP800-53, NIST SP 800-30, Cyber Essentials, PCI-DSS, CIS Top 20 Controls, IEC 62443, NIST SP 800-82,
Operating Systems:	Windows Server 2008-2016, Windows XP-10, Kali Linux, MacOS, Android, iOS

PERSONAL SUMMARY

I am a keen and fast learning cyber professional with previous experience in the IT industry supporting secure accounts. I have taken part in CompTIA's CyberReady initiative over the last 6 months where I worked towards multiple industry recognised qualifications alongside getting hands-on experience taught by UK CNI Professionals – This experience includes tools used across the industry such as Nessus, AlienVault, Windows Firewall, Snort, etc. I have also learnt about various attack frameworks such as MITRE ATT&CK, Diamond Model of Intrusion, and the Lockheed Martin Cyber Kill Chain.

I possess excellent communication skills in both communicating technical subjects to non-technical people, as well as using technical language where necessary. Having worked in a 1st and 2nd line environment in the past, I have improved my ability to solve complex problems given a set of

information, as well as work with colleagues and other teams closely to come together and analyse root causes.

EXPERIENCE

SEPT 2022 - PRESENT

DIGITAL FORENSICS AND INCIDENT RESPONSE SUPERVISOR, SELLAFIELD LTD.

After excelling in my analyst role, I was promoted to DF&IR Supervisor where my main responsibilities are to lead a small shift team of analysts and provide SME advice on cyber security matters to assist in legal and business conduct. Responsibilities include:

- Act as a point of escalation for cyber security incidents, and responding within defined policies and regulations
- Train a shift of CSOC analysts to ensure that standards are met and knowledge is share around the team
- Lead in tuning the cyber tooling to increase efficiency of incident detection and response
- Use forensics knowledge and tools to deliver forensically sound evidence to regulators upon request
- Overseeing technical implementation of cyber security tooling
- Providing advice and guidance to internal and external stakeholders on matters of cyber security, digital forensics, and incident response to ensure threats and risks are identified to reduce impact and consequence

SEPT 2021 - SEPT 2022

CYBER OPERATIONS SECURITY ANALYST, SELLAFIELD LTD.

In this role I was responsible for day to day monitoring of various cyber security tools to identify potential threats, and ensuring they are responded to and correctly escalated. Responsibilities include:

- Aid in development of detection rules, signatures and IOCs
- Producing succinct, detailed, and accurate technical reports in a timely fashion
- Documenting and reviewing documentation regarding best practice around incidents
- Gathering intelligence on the current threat landscape from external sources, and writing semi-technical reports for management
- Used mailboxes to monitor incoming spam for email-based threats, and to communicate best practices for users

The tools I used and gained hands-on experience with include: SIEM, IPS/IDS, EDR, Firewalls, Proxies, AV, DLP, Network Monitoring

JUNE 2016 – SEPT 2021

2ND LINE DESKTOP ENGINEER, DXC TECHNOLOGY

At DXC Technology, I am an engineer responsible for remote incident resolution and identifying patterns in commonly reported issues for a wide range of technologies, including things with a focus on security such as ensuring users adhere to AUPs, managing an Endpoint Security database, auditing user permissions and ACLs, handling data with a 'Secret' marking, patching (Including visiting client sites to rebuild servers in a data center after an attack), and ensuring devices are kept within a secure configuration.

My main duties included:

- Providing training to 1st and 2nd line agents in a live helpdesk environment
- Adhering to ITIL aligned processes regarding incident and problem management
- Providing remote end-user support, including software installs and break/fix support
- Maintain a knowledge base by writing, and approving knowledge articles

- Following NIST SP800:88 standards when handling the destruction of data
- Ensuring that devices have the latest AV definitions to meet NAC requirements

JUNE 2015 – JUNE 2016

ASSET MANAGEMENT, DXC **TECHNOLOGY**

I was responsible for overseeing the CMDBs of multiple companies to ensure data accuracy, consolidating old and redundant processes to save time, and communicating with on-site engineers and suppliers to obtain reliable information.
This role involved optional self-teaching moments that allowed me to go above and beyond what was required, this included teaching myself how to create MS Access databases so that I could configure and re-tool existing databases with the goal of increasing automation.
My main duties included:

- Analysing large amounts of data to spot trends
- Using MS Access and Excel to process large datasets to create reports
- Worked with on-site engineers to build acceptable metadata standards
- Create and evaluate workflow documentation

EDUCATION

FEBRUARY 2018

HIGHER LEVEL APPRENTICESHIP IN IT, SOFTWARE, WEB & TELECOMS PROFESSIONALS LEVEL, 3AAA ACADEMY

JUNE 2016

ADVANCED LEVEL APPRENTICESHIP IN IT, SOFTWARE, WEB & TELECOMS PROFESSIONALS LEVEL 3, 3AAA ACADAMY

REFERENCES

Available upon request