**Lee Ward****l.ward@netwkr.net** **Personal Website:** [**https://netwkr.net**](https://netwkr.net) **LinkedIn:** [**http://uk.linkedin.com/in/wardlr**](http://uk.linkedin.com/in/wardlr)

**Professional Summary**A seasoned IT Professional with over 16 years’ experience in system administration, cybersecurity and network management. Passionate about engineering solutions, learning complex systems, exploring cutting-edge technologies and outcomes that give businesses a competitive edge.

**Key Technology & Skills**

– TCP/IP, UDP, Inter-VLAN Routing, DHCP, DNS, NAT, hardware & software firewalls, Enterprise Wifi
– Microsoft Windows Server (including Active Directory & Group Policy) & Client Proficiency
– Microsoft Azure, Entra ID (formerly Azure AD) general use
– Threat hunting, OSINT, vulnerability scanning, remediation
– Cybersecurity platforms: SIEM, XDR, NDR
– Linux (Debian, Ubuntu) proficiency
– HCL BigFix Lifecycle, including patching, software distribution and management.
– TOPdesk, JIRA Service Desk (with an interest in Kanban)

**Other Technologies (Mixed confidence)**

– Database: Microsoft SQL Server, MySQL, ElasticSearch
– Visualization: Grafana, Kibana
– Development: Python, PHP (8.2+), Javascript, HTML5 & CSS3
– Automation: Ansible, Bash, Powershell & Batch scripting.

**Training**

– Axelos: ITIL Foundation v4, On-prem, 2019
– Microsoft: Microsoft SQL Server 2016: Querying Data with Transact-SQL, At-home, 2019
– Microsoft: Microsoft SQL Server 2014, At-home, 2019.
– Microsoft: Deploying & Managing Windows 10 Using Enterprise Services, On-prem, 2016.
– Microsoft: Configuring and Installing Windows 10
– Microsoft: Microsoft Office 365 Jumpstart, At-home, 2011
– Cisco: Administering Cisco Unified Communications 7, QA London, 2009.

**Professional Experience**

**IT Security Senior Engineer**Aston University, Birmingham | 2023 - Present

– Governance, Risk & Compliance: Lead, implement & enforce university policies, assist and organize work to prepare the university for accreditation, for example Cyber Essentials renewal.
– Effective communication: Work with stakeholders at all levels including external partners and law enforcement and communicate our craft in ways that makes sense for everyone.
– Document effectively: Create clear and concise documentation for end users, and internal team use for systems and procedures, and develop ways to automate burdensome tasks, reduce errors.
– Use existing organizational knowledge alongside experience to create…

…organization-specific solutions to weaknesses or threats to the business, and update where necessary.
– Utilize experience in SIEM, XDR, NDR platforms and prior system administration experience and expertise with Windows, macOS & Linux, Microsoft Exchange, Active Directory, Entra ID, MECM/BigFix Lifecycle to quickly discover and hunt threats to the organization, and remediate quickly or organize P1 remediation with appropriate teams.
– Information protection: Complement the work of our legal team in communicating, advising and enforcing technical measures for the protection of information.
– DFIR: Use prior system administration experience to acquire information from systems, capture and examine packet capture logs utilizing Wireshark, recover data where physically possible and preserve. Lead technical incident response, quickly ascertain and document events and coordinate response and remediation and post-mortem.
– Pick up new, little-used or unknown technology quickly: Quickly learn and adapt to situations as business or team requirement arises.
– Approachable and seek to build rapport: Teach, pass on knowledge, communicate our craft in a way that empowers staff and students to recognize threats and report them.
– Arrange and work with partners to coordinate regular independent testing of systems and infrastructure and test security suites to ensure systems respond correctly.

**> IT Security Officer**Aston University, Birmingham | 2018 - 2023

– Governance, Risk & Compliance: Assist in implementation and enforce university policies, assist and organize work to prepare the university for accreditation, for example Cyber Essentials renewal.
– Effective communication: Work with stakeholders at all levels including external partners and law enforcement and communicate our craft in ways that makes sense for everyone.
– Document effectively: Create clear and concise documentation for end users, and internal team use for systems and procedures, and develop ways to automate burdensome tasks, reduce errors.
– Use existing organizational knowledge alongside experience to create organization-specific solutions to weaknesses or threats to the business, and update where necessary.
– Utilize experience in SIEM, XDR, NDR platforms and prior system administration experience and expertise with Windows, macOS & Linux, Microsoft Exchange, Active Directory, Entra ID, MECM/BigFix Lifecycle to quickly discover and hunt threats to the organization, and remediate quickly or organize P1 remediation with appropriate teams.
– Information protection: Complement the work of our legal team in communicating, advising and enforcing technical measures for the protection of information.
– Digital Forensics & Incident Response: Acquire and catalogue evidence, use prior system administration experience to acquire information from systems, recover data where physically possible and preserve. Perform incident response, quickly ascertain and document events and respond and remediate.
– Pick up new, little-used or unknown technology quickly: Quickly learn and adapt to situations as business or team requirement arises.
– Approachable and seek to build rapport: Teach, pass on knowledge, communicate our craft in a way that empowers staff and students to recognize threats and report them.

**> IT Support Engineer**Aston University, Birmingham | 2014 - 2018

– Provide second-line IT Support for whole university: Respond to technical issues in a human way, build rapport, learn legacy, proprietary or unusual hardware or systems and be approachable.
– Plan, implement and configure new systems and services, and create & update documentation: Learned line of business and instrument systems, their interfaces, software, and documented this to pass this knowledge on to other engineers.
– Build rapport throughout the business: Became a known technical contact for the Colleges of Engineering and Physical Sciences (then Engineering and Applied Science), and Health and Life Sciences (then Life and Health Sciences). Continued to foster my existing working relationships with key stakeholders.
– Use prior system administration experience to effectively hunt down and troubleshoot to reach root cause for faults and remedy as appropriate.

**> Assistant Distributed Systems Engineer**Aston University, Birmingham | 2012 - 2014

– Provide second-line IT Support for whole university: Respond to technical issues in a human way, build rapport, learn legacy, proprietary or unusual hardware or systems and be approachable.
– On-hand to jump on first line and helpdesk during abnormally high load and provide a friendly face to visitors to the helpdesk. – Learn new organizational knowledge to allow me to tailor support provided in line with organizational expectations.
– Build and deploy systems, deploy required software in line with end-user expectations and verify on deployment.
– Use prior system administration experience to effectively hunt down and troubleshoot to reach root cause for faults and remedy as appropriate.

**> IT Support Technician**Walsall Academy, Walsall | 2007 - 2012

– Provide first and second-line IT Support to all areas of business: Respond to all technical issues, build rapport and be approachable.
– Learn new organizational knowledge to allow me to tailor support provided in line with organizational expectations.
– Pick up new technologies, and take on responsibility where there were gaps in our capability to reduce reliance on outsourcing.
– Assisting the senior technician with the proof-of-concept testing, deployment, and P2V migration to VMware vSphere alongside external support service.
– Assisting the senior technician with the proot-of-concept testing, deployment of Citrix XenServer, XenDesktop and XenApp alongside external support service.
– Take on responsibility for physical Cisco-based network core and edge, work alongside external support service to deploy the academies first Wifi network.
– Take on responsibility for Cisco-based Voice-over-IP system, work alongside external support service to migrate legacy Callmanager and Unity publisher and subscriber to Unified Communications Manager Business Edition 7.
– Onboard and support the academies first Linux-based estate, and become advanced support for existing systems.