James Mockford – CV

I am an Operational Technology (OT) Cybersecurity Specialist with over 7 years' experience in both IT and OT environments. With a background in protecting critical infrastructure, I specialise in building security architectures that effectively bridge the gap between IT and OT environments. My technical expertise spans vulnerability assessment, threat monitoring, and incident response across industrial control systems. I'm seeking opportunities that allow me to tackle complex security challenges while continuing to grow as a security professional.

Technical Skills

- **OT/ICS Security**: SCADA, PLC, DCS, IoT/IIoT, ICS protocols
- **Network Security**: Firewalls, Network Segmentation, IDS/IPS, Tenable, Claroty
- **Penetration Testing**: Kali Linux, Nmap, Metasploit, Wireshark, x64dbg
- **SIEM & Log Management**: Sentinel, LogRhythm, AlienVault, Wazuh, Defender
- **Languages / Scripting**: Python, Bash, PowerShell
- **Networking**: Industrial network architectures, LAN/WAN technologies, Mobile Communications, APIs
- **Compliance Frameworks**: IEC62443, NIST SP 800-61, NIST SP 800-82, NIS2, ISO27001, CE+

Career Summary

Wessex Water (Feb 2024 - Present)

OT Cyber Security Specialist (Dec 2024 - Present)

As an OT Cybersecurity Specialist, I secure industrial control systems and SCADA networks, implementing targeted security controls that protect critical operational technology.

- Delivered guidance for enterprise-wide OT initiatives including Claroty deployment, NIS2 regulatory compliance, and secure-by-design implementation.
- Spearheaded Claroty platform management, including design and implementation of a custom monitoring and alerting system that enhanced visibility and incident response capabilities across the OT environment.
- Served as technical authority on cross-functional working groups, contributing expertise to shape organisational OT security standards, governance frameworks, and strategic roadmaps.
- Architected and implemented comprehensive OT vulnerability management program, establishing standardised processes for vulnerability identification, prioritisation, remediation, and reporting.
- Conducted security assessments including device audits and penetration tests to evaluate security posture of new OT equipment, resulting in significant improvements to overall security stance.

Cyber Security Operations Lead (Feb 2024 - Dec 2024)

As Cyber Security Operations Lead at Wessex Water, I oversaw daily cyber security operations across our IT and OT environments.

- Led complete transformation of security monitoring capabilities, managing end-to-end migration from LogRhythm to Microsoft Sentinel from initial tender and procurement through deployment and implementation. This initiative significantly enhanced threat visibility while reducing alert fatigue, resulting in 60% improvement in both Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) metrics.
- Developed custom rules, alerts, and incident response playbooks for both IT and OT incident scenarios.

james.mockford@outlook.com | 07778 024479 | jamesmockford.co.uk

- Contributed to critical documentation including Cyber Incident Rapid Response Handbook, Dynamic Security Posture Playbook, and Cyber Incident Response Plan covering both IT and OT environments.
- Led BAU operations for key security tools: Defender, LogRhythm, Sentinel, Claroty, Tenable, Cofense, Proofpoint, and Hornbill.
- Engineered advanced, custom Python-based security dashboards integrating multiple security systems into a cohesive "single pane of glass" solution. This executive-level reporting platform translated complex security metrics into actionable intelligence for leadership, enabling data-driven strategic decisions.

Blueskytec (April 2022 - February 2024)

Network Penetration & Test Analyst

As a Network Penetration & Test Analyst at Blueskytec, I specialised in identifying vulnerabilities within critical infrastructure and industrial control systems, offering tailored cybersecurity solutions to clients.

- Conducted penetration tests on OT environments, including PLCs, SCADA systems, and ICS devices for clients such as Schneider Electric, Saudi Aramco, Shell (Nigeria LNG), DSTL (MoD), and Associated British Ports.
- Applied MITRE ATT&CK framework for ICS to identify and mitigate OT-specific threats.
- Demonstrated live OT cyber-attacks at industry events, highlighting vulnerabilities in industrial systems.
- Architected and constructed comprehensive Industrial Control Systems (ICS) testbed environment, replicating production infrastructure for secure penetration testing and validation of internally developed security products.
- Established and managed complete enterprise infrastructure from ground zero, including designing network architecture, implementing multi-layered firewall protection with granular policy management, deploying Office 365/Exchange environment, and creating specialised servers (file system, Git version control, WSUS patch management).

BMT Defence & Security UK (September 2016 - April 2022)

ICT Analyst (Apr 2020 - Apr 2022)

As an ICT Analyst, I was responsible for implementing and maintaining enterprise IT infrastructure, ensuring security, reliability, and compliance with MoD standards.

- Administered and maintained enterprise network infrastructure including routers, firewalls, and web servers.
- Provided Tier-3 level technical support, resolving complex infrastructure and security issues.
- Mentored junior and trainee analysts on system administration and security practices.

Junior ICT Analyst (Feb 2018 - Apr 2020)

- Provided comprehensive tier 1-2 IT support to over 1000 employees across multiple locations.

ICT Apprentice (Sep 2016 - Feb 2018)

- Supported and documented key IT systems, with a focus on SharePoint environments.

Education & Certificates

- ISA/IEC 62443 Cybersecurity Fundamentals Specialist (March 2025)
- ISA/IEC 62443 Cybersecurity Design Specialist (April 2025)
- ITIL v4
- CompTIA A+

- CompTIA Network+
- Windows Server 2019 Administration
- City & Guilds Level 3 Diploma in Information Systems
- Level 3 Extended Diploma in Information Technology (Bath College)

Professional Development & Extracurricular Activities

- Active participant on TryHackMe platform, enhancing practical cybersecurity skills.
- Regular contributor to open-source projects on GitHub.
- Alumnus of the START incubator program.
- Practitioner of Brazilian Jiu-Jitsu.

james.mockford@outlook.com | 07778 024479 | jamesmockford.co.uk