Liam Rees

linkedin.com/in/liam-rees

SUMMARY

I've taken the decision to move on to a new chapter in my working life to pursue my interest in Cyber Security full time. This is why I'm reskilling with CAPSLOCK to become a cyber security practitioner, undertaking a 16 week intensive training course and working towards 4 security certificates.

Due to my profound interest in computing and technology; having designed, developed and maintained a number of websites, as well as having experience in Python and Linux, teaching both programs in secondary school settings, where I also used Raspberry Pi to develop units of work that helped instil computational thinking.

I was a primary and secondary school computing teacher with over 13 years experience, which has provided me with many transferable skills. For instance excellent communication and problem solving skills, capability to work calmly and methodically under tight deadlines and pressure, work independently and collaboratively as part of a team. As well as having the aptitude and commitment for continuous learning and always producing work to the highest professional standards.

CERTIFICATION

- **PGCE in ICT/Computing.**
  Bradford College (2008-2009)
- **Masters (MSc) in Multimedia application and IT/Computing.**
  University of Teesside (2001-2002)
- CCSK - Certificate of Cloud Security Knowledge (Studying)
- CompTIA Security+ (Studying)
- ISO 27001 Foundation Certificate (Studying)
- CISMP (Certificate in Information Security Management Principles) (Studying)

SKILLS

- HTML/CSS
- Python
- Linux
- Adobe Photoshop
- Communication
- Customer Service
- Interpersonal Skills
- Leadership
- Management Skills
- Problem-Solving
- Time Management
- Transferable Skills

Labs Completed

Tackling labs across Linux, Windows, cloud, endpoint protection, offensive & defensive security. Using tools such as Wireshark, Powershell, SSH, Metasploit, and others. Tracks completed; SOC Analyst 1, Microsoft Security Core, Threat Hunter, and Cloud Security. Tools used include Splunk, QRadar, MS Defender, Powershell, Suricata, Linux sylog, and many others.

Professional Experience

Trainee Cyber Security Consultant
CAPSLOCK
09/2022 - 02/2023 *Remote, liveclasses*

Intensive 5-month cyber security training and workplace readiness programme. Actively solving real cyber security problems as part of a team. Areas covered;

- Security culture & awareness + understanding business
- Security by design(architecture, GRC, cloud,3rd party assurance)
- Access control (IAM/PAM)
- Offensive & defensive security
- Business continuity, resilience & incident response

Key Stage 2 Class teacher and Computing Lead.
The Ingrow and Long Lee Federation
05/2015 – 07/2022 *Long Lee*

To fulfil the professional responsibilities of a teacher, as set out in the School Teachers' Pay and Conditions Document

Key responsibilities include:
- Co-ordinating and overseeing teaching staff with computing
- Coaching, mentoring and developing all staff within the computing curriculum
- Updating the Head Teacher and governing body regarding the computing curriculum and development plan
- Creating a learning environment which developed resilience, confidence and independence

Computer Science Lead teacher.
Our Lady & St John Catholic College.
08/2009 – 05/2015 *Blackburn*

Key responsibilities include: producing schemes of work for key stage 3 including computer hardware, HTML, Scratch, Python, app programming and Kodu. For Key stage 4 I have developed schemes of work for Python/ Linux activities and all areas of the OCR Computing GCSE.

Head of Department for Computer Science.
Our Lady & St John Catholic College.
08/2012 - 08/2013 *Blackburn*

Key responsibilities include; selecting courses and schemes of work for key stage 3 & 4, lesson observations of department members, analysis of assessment data, mentoring NQT, attending local area head of department and SLT meetings. Chairing department meetings and ensuring a smooth running of the Computing department. During my time as head of department, the department achieved 67 % A to C for the Edexcel GCSE ICT qualification.

Liam Rees

CYBER SECURITY EXPERIENCE

What I'm doing at CAPSLOCK
600+ hour course with live, instructor-led classes

I study at CAPSLOCK 20+ hours a week over 5 months. It's a CIISec accredited course.
We work towards solving real cyber security problems within a simulated cyber security workplace, mainly as part of a team. Below are the projects covered and work I've produced.

Security Culture & Business Understanding

- Reviewed the effectiveness of the existing information security awareness efforts and created a report highlighting areas for improvement
- Formulate a high level plan to reduce the risks associated with phishing, showing measurable results within the next 6 months
- Developed an understanding of how security relates to business objectives

Security by Design

- Created a new cyber security governance structure which described the organisational structure, roles & responsibilities important to monitoring, addressing, and escalating risk & compliance issues.
- Developed a security strategy, describing the steps involved in building a security framework, addressing requirements identified in legislation.
- Reconfigured the cloud services to meet security standards outlined by consultants and produced a report to present to management.
- Developed BYOD technical controls and related processes.
- Investigated supply chain security assurance processes. Produced recommendations for improvement.

JML & Access Control

- Investigated an Active Directory and highlighted potential nonconformities and anomalies.
- Developed a joiners, movers, leavers policy.
- Created a stakeholder matrix and plan for stakeholder engagement and a dissemination plan regarding the JML Policy project.

Offensive & Defensive Security

- Scoped & conducted a pen-test, producing a report highlighting the tests performed, vulnerabilities discovered and corrective actions.
- Investigated and chose 3 open source tools which could be used by the IT team to develop their offensive testing capability. Provided the IT manager with an analysis report of the tools chosen.
- Planned the development of a new threat intelligence team, detailing new processes and how the team will fit into the current governance structure.
- Prepared and delivered an argument to the Board as to why a full-scale SOC implementation is needed with cost-benefit analysis.

Incident Management and Business Continuity

- Developed a strategy to implement detection and monitoring capability on a limited budget.Analysed tool capability, highlighted new processes and performed a cost-benefit analysis.
- Developed an organisation-wide incident response plan, using all skills learnt throughout the course to date. Tailored to the needs of the organisation, based on relevant industry standards and contractual obligations whilst integrating other relevant organisational processes such as Business Continuity, Disaster Recovery, Crisis Management, etc.

SKILLS-BASED LEARNING

Impact Skills
- Professional Communication
- Working in a high-performance team
- Research & Resourcefulness
- Presenting & Public Speaking
- Problem Solving
- Report Writing
- Working under time pressure

Culture
- Ethics
- Policy, Process, Procedure
- Social Engineering
- Understanding Business & Cyber
- Security culture & Awareness

Risk
- Supply Chain Security
- Threat Intelligence
- Outsourcing
- Governance
- Physical Security
- Business Resilience
- Laws, Regulations & Standards
- Risk Management
- Management Information & Metrics

Process
- Audit
- Forensics Fundamentals
- Incident Management
- IAM/PAM

Technology Fundamentals
- Threat Hunting
- SOC
- Industrial Controls Systems & IoT
- Security Architecture
- Applied Cryptography
- Cloud Security & Infrastructure
- Pen-Testing
- Endpoint Protection
- Malware
- Application Security (SDLC)
- Operating Systems
- Basic Scripting
- Network Fundamentals
- Big Data & Emerging Technologies