PAUL SMITH - CURRICULUM VITAE

PAUL@PASE.LTD
MANCHESTER

PERSONAL STATEMENT

A highly motivated IT Specialist with over 30 years' experience of which the last 25 years have been within Information Security.

I specialise in the areas of Information Security Platforms, Operational Running, Monitoring, Management and Analytical Work.

I have a background that covers most recently Vulnerability Assessment, Network Detection Response and Log Management encompassing the configuration, support, and monitoring of Vendor Specific Platforms, being TENABLE (Security Center and Nessus), DARKTRACE (NDR) and SYSLOG (NG)

And previously Intrusion Prevention/ Detection Systems, Anti-Virus Systems, Security Information Event Management/Audit Log Assurance Systems, as well as Apple macOS, Microsoft and Linux operating systems and Forensic Investigation Work.

I have experience in varying customer-facing, operational and strategic roles.

I have successfully worked on infrastructure, consolidation, migration, transition, and development projects.

I am accustomed to communicating at all levels within the business in the resolution of complex security challenges. I combine common sense, with problem solving to deliver quality, risk managed, IT Security and Cyber-Security Day-to-Day Run and Maintain Solutions

MAJOR ACHIEVEMENTS

- Setup, configuration, management and knowledge expertise of numerous Tenable Security Center and Tenable Nessus Vulnerability Management Platforms for varying projects and customers.
- Related internal and external Blue Team Vulnerability Assessment work in line with NCSC Cyber Essentials test specifications.
- Compliance and security audits involvement to ensure PCI and Cyber Essentials accreditation.

EMPLOYMENT HISTORY

July 2016 – January 2025: (Hybrid)

SERCO SECURITY TOOLING / SECURITY OPERATIONS

Position: Security Tooling SME, Vulnerability Assessment Specialist.

DUTIES

- Setup, management and configuration of TENABLE Security Center and TENABLE Nessus Vulnerability Management Platforms for Security Operations and Security Tooling Departments.
- Ongoing internal and external Blue Team Assessment work in line with NCSC Cyber Essentials Test Specifications.
- Providing Subject Matter Expertise to Serco's 3rd line tooling support staff and relevant customer user-base.
- Secondary role Supporting Darktrace Network Detection Response, Cortex XDR and SYSLOG NG Platforms for use by Serco Cyber Operations.
- Use of SolarWinds and Excel for operational automation analysis / investigation tasks.
- On Site Vulnerability Assessments at Serco Justice, Immigration, Leisure, and Transport Facilities as part of the Security Operations Center Function.
- Symantec Endpoint Protection Manager Management for Security Operations.
- ArcSight Proof of Concept for Security Operations.
- Commission of Mcafee ESM (NITRO) SIEM Enterprise Security Manager for Lincoln County Council.
- Commission of Mcafee ePolicy Orchestrator (EPO) AV Management for Lincoln County Council.

1996 – 2016: (Hybrid)

COMPUTER SCIENCES CORP (BAE SYSTEMS) CYBERSECURITY UK SOC

Positions: Information Security Specialist / Desktop Support Analyst

DUTIES

- Various security operational and setup functions in Chesterfield SOC Campus (Hybrid).
- Two Secondments to BAE SYSTEMS IT Security (Warton)
- Development of Mcafee Network Security (Intrushield), Sourcefire (Firepower), Snort and ISS (Realsecure) Intrusion Protection Platforms for related customers.
- 3rd Line Desktop Support for BAE SYSTEMS (Woodford) User-base.

Prior 1996: (On Site)

National Rivers Authority / Environment Agency (3rd Line Desktop Support)
Manweb Scottish Power (3rd Line Desktop Support)
Racal Datacom (3rd Line Desktop Support)

KEY SKILLS

- Operational day to day run and maintain of Tenable's Vulnerability Management Platforms for Vulnerability Management Functions relating to CVSS.
- Handling escalations from support teams and providing training.
- Business Practise Vulnerability Assessments.
- Dash-boarding and reporting in relation to Standards, Guidelines, Policy, Prioritisation and Risk Reduction Requirements.
- Continuous health checks and service improvement processes from a strategy, usability and reporting perspective.
- Administration and configuration of Security Tooling and Tenable Products.
- Comprehensive high level and detailed low level documentation, work instructions and knowledge base creation.
- Working with the customers and key stake holders to ensure the services meet requirements.
- Providing support and expertise of Tenable.SC Vulnerability Platform for audits.

EDUCATION

Tenable University

Security Center and Vulnerability Management Platform Training.

Qualys

Vulnerability Management Foundation Training.

Darktrace

Threat Visualizer Administration and Cyber Engineer Training.

Microsoft

Azure Security Engineer Associate Training (AZ500) and Azure Fundamentals (AZ900).

CompTIA

Security+ and PenTest+ Training.

SecurityBlue.Team

BTL2 Training.

ISC2

CISSP Training.

EC-Council

Certified Ethical Hacker v4 Qualification.

ITIL 4

Sir Thomas Boteler COE High School

7 GCSE Passes