Curriculum Vitiate – Rob Page

linkedin.com/in/rnpage/ https://robertpage.uk

Personal Profile

I am a multi-disciplined cybersecurity professional with experience in offensive and defensive security, threat intelligence, malware analysis, DFIR, and consultancy. I'm driven by a passion of solving complex problems and a thirst for improving processes by leveraging automation. I have communicated complex topics to diverse audiences, including C-Suite executives and government ministers.

Certifications

Certification	Status
DipHE in Computer Forensics & Security	Current (Merit)
CISSP	Expired, Renewal in Progress
SSCP	Current
Recorded Future Certified Threat Intelligence	Current
Splunk User & Power User	Current
NCSC Industrial Control Systems Security	Current
CREST Practitioner Intrusion Analyst	Current
CREST Registered Threat Intelligence Analyst	Expired, No current renewal plans
CREST Practitioner Security Analyst	Expired, No current renewal plans

Technologies

SIEM: Splunk, Elastic & Sentinel; **EDR:** CrowdStrike, Microsoft Defender for Endpoint, Elastic Agent; **NDR**: Darktrace; **SOAR:** Dimisto, The Hive, Cortex, Node-RED; **Vulnerability Scanning:** Nessus, Qualys Cloud; **Threat Intel:** Recorded Future, MISP, XForce, BitSight; **General:** Vagrant, Ansible, Python, PowerShell, JavaScript, Rust, Docker, Kubernetes, AWS, Office 365 Admin, MacOS, Windows, Linux.

Personal Projects

Developed cybersecurity tools, including LeakSeek.io (data breach identification), SpotSpoof.com (detects IDN/Punycode and similar domain names), and HeaderAudit.com (security header detection).

Employment History

Founder – MatchedRisk April 2024 – Current

As the founder of MatchedRisk, I created a platform that enables insurers to assess cybersecurity risks within 30 seconds during the quotation phase. The platform also matches identified risks with tailored products and services to mitigate or eliminate them.

Key achievements:

- Integrated RAG-assisted Large Language Models (LLMs) to analyse cybersecurity policies and identify weaknesses.
- Leveraged OSINT to uncover breaches and misconfigurations, enhancing risk profiles.
- Built tools to analyse internet-facing infrastructure in real-time, identifying vulnerabilities.
- Partnered with cybersecurity vendors to cross-sell solutions that mitigate risks.

MatchedRisk is developed using Python (Flask, FastAPI), LangChain (GPT/Claude), RabbitMQ, PostgreSQL, and PyQt, packaged with PyInstaller.

Founder & Director – seem.io July 2023 – April 2024

As the founder of seem.io, I aimed to make cybersecurity accessible to micro and small businesses by developing a Security Information and Event Management (SIEM) system with AI, orchestration, and ticket management.

Key achievements:

- Designed a custom query language with detection rules and template inheritance for data enrichment and automation.
- Gained proficiency in batch/stream processing with Bytewax (Python), Flink (Scala), and Kafka.
- Developed expertise in Rust and Scala for the backend, stream processing, and log collection agent.
- Integrated LLMs (LLaMA & GPT) to simplify alert triage and investigation for users.

The MVP tech stack included a React frontend, Rust API (Rocket), Kafka, Flink, RabbitMQ, PostgreSQL, Memgraph, and MongoDB, deployed on a Proxmox cluster with Ceph storage and Kubernetes for container management.

Principal SOC Analyst – Arcturus Security September 2020 – July 2023

I had the unique opportunity to establish a Security Operations Centre (SOC) from the ground up, designing and implementing core processes to launch a new MSSP service. I utilized open-source tools and developed Python APIs for automated reporting, phishing analysis, and artifact enrichment, contributing to CREST accreditations for both SOC and Incident Response.

After the launch, I oversaw the Incident Response service and served as Principal SOC Analyst, focusing on:

- Training and developing SOC staff.
- Coordinating threat hunting activities.
- Managing the detection ruleset.

I responded to diverse cybersecurity incidents, including ransomware attacks across various platforms and network topologies, with a strong emphasis on insurance-driven cases.

Cyber Security Consultant / Information Security Specialist – NHS Digital January 2018 – June 2020

In these roles, I contributed to securing critical NHS services by advising on cybersecurity requirements, assessing threats and risks, and developing detection and response strategies. Key achievements include:

- Advising internal programmes on cyber risks across the development pipeline and analysing threats across the NHS using custom Python scripts for non-intrusive data analysis.
- Serving as a technical lead in the Cyber Security Operations Centre (CSOC), coordinating incident response activities with NHS and government partners, and maturing CSOC processes.
- Leveraging offensive security expertise for threat hunting, attack path mapping, and external threat analysis.

Highlights:

- Contributed to the adoption of NCSC Active Cyber Defence products (e.g., PDNS and vulnerability scanning).
- Delivered technical demonstrations to C-suite executives and government officials.
- Presented at healthcare and cybersecurity conferences.

- Developed a chatbot for vulnerability remediation advice and frameworks for Cyber Essentials and HSCN IT Health Checks.
- Organized and executed tabletop and live training scenarios.

Penetration Tester - Sec-1 June 2015 – July 2017

During my time at Sec-1 I worked on the following projects types:

- External and Internal Web Application assessments (including PCI DSS 11.3),
- Internal Network assessments (including PSN IT Health Checks),
- Social Engineering (Telephone, Physical Access, OSINT and Phishing)
- Mobile Application assessments (Android, iOS),
- Router and Firewall assessments and rule set audits,
- Wireless assessments,
- Dynamic and static code analysis (web, compiled applications)
- Cyber Essentials (basic and Plus).

In addition to the above roles, I was the **Vice President of the Leeds Beckett Hacking Society** and the **Leeds OWASP Chapter** - where I presented several talks and lectures. Additionally, I have presented at various cybersecurity conferences such as **BSides** and **Securi-tay**.