Patrick Jfremov-Kustov

Pulborough, UK • patrickjfremovkustov@gmail.com • **patrickjfremovkustov.com**

Profile

Cybersecurity graduate with a First-Class BSc in Computer Science (University of Southampton, 2025) and hands-on experience across enterprise security, cloud security, and penetration testing. CompTIA Security+ certified and ranked in the top 1% on TryHackMe, with proven skills in SecOps, DevSecOps, and offensive security through CTFs and exploitation labs. Experienced in securing cloud infrastructure with Terraform, developing APIs with Python/FastAPI, and integrating security into CI/CD pipelines. Proficient in penetration testing tools including Burp Suite, Nmap, Wireshark, Metasploit, and Kali Linux. Proven communicator with experience delivering security workshops to technology departments and translating complex concepts for diverse audiences.

Experience

Esure Group United Kingdom (Remote)
Security Operations & DevSecOps Jun 2024 – Sep 2024

- Proficient in Python and SQL, leveraging FastAPI for web development and implementing POST endpoints, webhooks and CRUD APIs
- Built cloud infrastructure using Terraform, automating the provisioning and management of AWS resources, including VPCs, security groups, subnets, and EC2 instances
- Developed webhook endpoint for Wiz integration and implemented CSPM controls such as S3 Block Public Access
- Developed CI/CD pipelines (GitHub Actions) and advocated for DevSecOps shift-left security practices, integrating security into the development lifecycle
- Gained hands-on experience with SIEM/XDR (Rapid7), EDR (Crowdstrike), and email gateway security (Mimecast)
- Performed SIEM/XDR (Rapid7) log analysis and initial incident triage, escalating per playbooks and contributing to containment and remediation notes
- Contributed to SecOps operations, including ISO 27001 supplier assurance and phishing email handling, strengthening understanding of security tools and compliance

Starling Bank United Kingdom (Remote)
Onboarding & Acquisitions - Team Member Sep 2023 – Present

- Performed due diligence on a high volume of account applications, verifying documentation against internal/external sources to ensure regulatory compliance and mitigate risk
- Coached and upskilled team members on application review processes, effectively supporting management and improving overall performance
- Designed and delivered workshops to the team on complex areas requiring in-depth knowledge, enhancing accuracy and consistency across operations

House of Veins United Kingdom
Founder & Technical Operations Lead Nov 2022 – Present

- Founded and managed an e-commerce business, gaining hands-on leadership and end-to-end technical ownership
- Implemented security best practices in business operations, including multi-factor authentication, access controls, and GDPR-conscious handling of customer data

Education

University of Southampton Southampton, United Kingdom
BSc (Hons) Computer Science, First Class (1:1) Graduated 2025
Dissertation: "Collaborative Access Control for People with Mild Dementia" - 85%; undergoing publication to an ACM conference (CPSIoTSec 2025)

- Applied the kill chain model to analyse cyber-attacks and evaluate threat actor profiles (Principles of Cyber Security) - 79%
- Developed Python-based Azure Functions for CosmosDB CRUD operations; deployed FunctionApps ensuring seamless cloud service integration (Cloud Application Development) - 79%
- Explored web and cloud application attack/defence strategies, strengthening security knowledge beyond industry standards (Web & Cloud-Based Security) - 76%
- Demonstrated exceptional programming proficiency by achieving 90% in a Java project and 95% in UNIX/SQL databases

The College of Richard Collyer United Kingdom
A-Levels: A* Mathematics; A Computer Science; A Psychology

Leadership & Activities

Cybersecurity Competitions & Community United Kingdom
CTFs & Labs Ongoing

- Ranked in the top 1% on TryHackMe
- Regularly engage in Capture the Flag (CTF) exercises
- Applied a structured pen-testing workflow (reconnaissance, enumeration, exploitation, post-exploitation) across web, network, and privilege-escalation labs

Skills & Interests

Technical: AWS, Azure, Google Cloud, Python, Java, SQL, Bash, FastAPI, Flask, Terraform, GitHub Actions, DevSecOps, SIEM/XDR (Rapid7), EDR (Crowdstrike), Email Gateway Security (Mimecast), VPCs, Security Groups, Subnets, EC2, Load Balancers, CosmosDB, Azure Functions, Linux, OAuth 2.0, Webhooks, NoSQL (Firestore, MongoDB)

Security Tooling: Burp Suite, Nmap, Wireshark, Metasploit, Kali Linux

Frameworks/Standards: OWASP Top 10, ISO/IEC 27001

Languages: English - Native/Bilingual; Russian - Native/Bilingual; Spanish - Conversational

Certifications: CompTIA Security+ (2025); CyberFirst Futures (SCQF Level 5); AWS Cloud Practitioner Course (O'Reilly); *OSCP (in progress)*; *HTB CPTS (in progress)*

Awards: The Ranstad Education ICT Award