SEBASTIAN STANICI

(+44) 7450 859 962 – London, United Kingdom – stanicisebastian@gmail.com – GitHub – LinkedIn

WORK EXPERIENCE

JPMorgan Chase June 2023 - Present
Red Team Operator, Associate *London, United Kingdom*

- Principal responsibilities include scoping operation calls, producing OSINT reports on the external and internal perimeter of the targets, actively exploiting misconfigurations and vulnerable systems along with writing and presenting reports to senior stakeholders.
- I also run cyber security tabletop exercises, build operation-critical infrastructure and research latest tactics, techniques and procedures to ensure the team adapts to the current threat landscape.

JPMorgan Chase Sept 2020 - May 2023
SOC Analyst, Associate *London, United Kingdom*

- Main activities are to respond, investigate and remediate incoming security events to keep the company safe from cyber threats and attacks using Splunk for SIEM, CrowdStrike, OSINT tools.
- Other side projects I worked on were related to JavaScript deobfuscation techniques, threat hunting for different attack paths which are tested through red or purple teaming, mentoring new analysts into fully joining the team and developing AWS cloud scripts to assist with sandboxing malware.

School of Computer Science, University of Birmingham Oct 2018 - Apr 2020
Java Teaching Associate *Birmingham, United Kingdom*

- Aided the Masters-level Java programming course by holding tutorials, shared lectures and laboratory sessions for postgraduate students to help build up their Java, networks and software engineering skills.

JPMorgan Chase June - Aug 2019
Software Engineering Intern *Bournemouth, United Kingdom*

- The role involved developing features for a trending product ensuring the secure software design of projects with technologies such as Java, Angular and TypeScript.
- My involvement in the Cyber and Technology Controls department also represented taking part in a global Capture The Flag event between cyber security interns where I achieved the first place.

SKILLS

Security tools	UNIX shell/powershell, Burp, Cobalt Strike, Metasploit, Kali Linux
Infrastructure	Windows Active Directory, UNIX, Win32 API, Ansible, Terraform
Cloud	Amazon AWS, Microsoft Azure/Entra ID, Google Cloud (GCP)
SIEM	Splunk, ElasticSearch, CrowdStrike Falcon LogScale
Programming	Java, C#, C/C++, Python, Bash, Golang, VBA, Assembly
Databases	MySQL, MariaDB, PostgreSQL, MongoDB, RavenDB

EDUCATION

University of Birmingham, United Kingdom *Sept 2017 - July 2020*
BSc Computer Science - First-Class Honours GPA: 4.25

Relevant modules:	Computer security	Network security
	Systems architecture	Software engineering
	Professional computing	Data structures and algorithms

CERTIFICATIONS, TRAINING AND PROJECTS

Advanced Evasion Techniques and Breaching Defenses (PEN-300) training Present

· Currently training on advanced penetration testing techniques against mature cyber security controls and bypasses of security mechanisms designed to block attacks.

NotSoSecure Hacking Cloud Infrastructure training June 2023

· Cloud infrastructure (AWS, Azure, GCP) vulnerabilities and security misconfigurations course
· Learned how to identify the attack surface exposure created by cloud-based services such as virtual machines (VMs), buckets, container as a service (CaaS) platforms, and serverless functions.

Offensive Security Certified Professional (OSCP) certification Nov 2022

· Demonstrated the ability to use persistence, creativity, and perceptiveness to identify vulnerabilities and execute organized attacks through the Offensive Security PEN-200 course.
· Shown outside the box thinking while managing both time and resources.

Antisyphon Training - SOC Core Skills September 2021

· The course covered core security skills in a SOC such as searching external/internal hosts along with their network segmentation, using SIEM tools to understand system (Windows/UNIX) logs, packet captures, network logs as well as triage, investigation and remediation steps.

RAF Association Connections for Life volunteering website Oct 2020 - July 2021

· A team of volunteers from JPMorgan Chase have gathered in their free time to develop a website for the Royal Air Force Association to find volunteers across the UK who could connect with RAF veterans.

Industrial Control Systems product vulnerability disclosed Sep 2019 - Apr 2020

· A white-box vulnerability assessment has been conducted on an ICS product owned by a market-leading vendor as part of the university final year project.
· A new authentication vulnerability has been found, ethically disclosed to the vendor and fixed in the immediate update of the product through work alongside my professor and their PhD student.

EXTRA-CURRICULAR ACTIVITIES

Running a tabletop exercise with a fictive security incident at BSides London 2023 while giving career advice to cyber security enthusiasts and students learning about the industry

Volunteering on company's Corporate Responsibility days to preserve the fauna and flora of parts from the United Kingdom

Actively teaching programming, cyber security and software engineering concepts to students from levels ranging from Year 3 to Masters degree

Taking part in cyber security and software engineering conferences such as Black Hat or BSides

Using cyber security learning platforms such as HackTheBox, TryHackMe and Proving Grounds to develop practical penetration testing skills

Actively taking part in hackathon and capture the flag events

Managed the University's Computer Science Society as a member of the operating committee

PERSONAL HOBBIES

Mentoring, long-distance running, yoga, non-fiction books, racket sports, skiing, helping others

REFERENCES

Available upon request.