Pentest practice lead and cybersecurity professional with extensive leadership experience and strong interest in ethical hacking, penetration testing and research. Hard working, inquisitive, curious, and technically minded. Experienced in bash and python scripting, Kali Linux, Metasploit, Burp Pro, and various C2 platforms.

Army Veteran of the Iraq and Afghanistan Wars.

WEBSITES

https://www.example.com
https://medium.example.com
GITHUB: https://github.com/example

CERTIFICATIONS

ISACA - CISM
Offensive Security – OSCP
ZeroPoint Security - CRTO
eLearnSecurity – eCPTX
eLearnSecurity – eWPTX
TCM Academy - PNPT
ISC2 - SSCP
EC-Council - C|EH
CompTIA – Pentest+, Security+

SKILLS

Network Penetration Testing
External Penetration Testing
Web Application Penetration Testing
Social Engineering
Organizational Leadership
Security Consultation
Scripting

JOE HEYO

Red Team Lead

EDUCATION

Random University
Master of Science, Cybersecurity and Information Assurance 2022
Bachelor of Science, Cybersecurity and Information Assurance 2019

Random State Community College
Associate of Applied Science, Advanced Technical Studies 2013

EXPERIENCE

Company Name – Red Team Lead (previous Senior Penetration Tester)
March 2021–Present
Red Team Lead Penetration Tester responsible for ensuring high quality results in full spectrum security assessments, including web application, external, cloud, and internal penetration testing, phishing, social engineering, and more. Communicates effectively with clients throughout project creation, testing, and delivery. ***Discovered CVE-2022-xxxxx during a client web assessment of a third-party application.***

Company Name - Security Engineer
October 2020–March 2021
Penetration tester conducting web application, external and internal penetration testing, phishing, social engineering, and more. Create trending security content for prospective clients. ***Discovered CVE-2020-xxxxx during a client web assessment.***

Title, Random Company Name before entering field
2016–2018
Short description of job.

OFFENSIVE TOOLS

ToolName – Description of tool(s) you have created
ToolName – Description of tool(s) you have created
ToolName – Description of tool(s) you have created

TEACHING AND EDUCATION

Course Name – Where course is located
Course Name – Where course is located

CVE'S

2020-xxxxx, 2021-xxxxx, 2021-xxxxx, 2021-xxxxx, 2021-xxxxx, 2022-xxxxx, 2022-xxxx, 2022-xxxx, 2022-xxxxx, 2022-xxxxx, 2022-xxxx

Cyber McCyberface

Cyber McCyberface is currently one of the Co-Founders of Cyber Company having previously been the Technical & Operations Director of Old Company, an NCSC and CREST accredited Cyber security company that employed 15 fully time staff and 3 contractors, which he co-founded in 2016. Within his role at Old Company he managed and worked within the professional services team to ensure quality delivery in a many different cyber security projects. He has performed multiple purple team engagements and over 200 penetration tests on multiple platforms, including Mobile, AWS, Azure and web applications. He has delivered Cyber Security training for Space University in both Singapore and Malaysia, and regularly provided advanced Cyber Security training for Old Company's key clients. He is the lead consultant for several of Old Company's key clients, within the highly regulated areas of medical technology, financial technology, and local government. These projects include, PCI-DSS, ISO27001, Penetration Testing, Read Teaming and the application of different frameworks such as NIST and CIS. He has externally accredited CREST CRT and the NCSC approved Cyber Scheme CSTL(Web) approved certification's as well as security clearance. He was the chapter leader of the Antarctica OWASP chapter in 2016/2017 and is a co-creator of ConCon, Antarctica's annual Cyber security conference, a professional Cyber Security conference which has over 400 attendees every year and has run since 2014.

Cyber McCyberface – My House – XXXXXXX – McCyberface@company.co.uk

Qualifications & Training

- **2010-2011 – Big Time University,** PgCert Learning and Teaching in Higher Education
- **2008-2009 – Big Time University,** MSc Computer Networks - Distinction
- **2004-2007 – The University of Antarctica**, BSc (Hons) Biomedical Sciences
- **Industry Accreditation**: CREST CRT, Cyber Scheme CSTL(web), SANS – GWAPT, Cisco - CCNA, Cisco - CCAI

EXPERIENCE

Co-Founder/Partner Cyber Company – September 2022-Present

My current role at Cyber Company involves several key areas, from client engagement all the way through to delivery. I have delivered several successful Cyber Security engagements for companies in various sectors, all which have had the goal of raising their overall security posture and capabilities.

Co-Owner & Technical/Operations Director Old Cyber Company – Cyber Security Consultancy Company March 2016- September 2022

As the technical director of Old Company I led many different cyber security projects with the assistance of my team. I was responsible for hiring all member of my team over the 7 years designed and developed and crucially delivered several new cyber security services. Within this time I successfully led the team to complete projects in PCI-DSS, Penetration Testing, Red and Purple Teaming, Phishing Campaigns, GPDR/DPO2018, several gap analysis frameworks, such as cyber essentials, 27001, NIST and CIS.

Space University – Special Visiting Lecturer Sept 2016 – Present

I work for the Space University as a special visiting lecturer on their MSc in Cyber Security and Management. Whilst teaching for Warwick I bring together my industrial and teaching experience to provide students with a transferable knowledge and skills.

Big Time University – Senior Lecturer in Information System Security Sep 2009 – January 2018

I am currently a senior lecturer in the information security and. In this role my teaching focuses in the area of information security, more specifically the teaching of offensive security testing, building secure systems and the management of information security. I focus on grounding my teaching in both my research and professional consultancy to ensure students get a fully rounded experience which will enable them to develop both their theoretical understanding and practical skills. I have spent the last few years working with academia and industry to try to bridge the skills gap in cyber security. This has led me to create a local Antarctica OWASP chapter, create a cyber-security conference in Antarctica (Attendance of 450 people), ConCon and hosted a CTF competition with the National Cyber Security Challenge in October 2016, 2022 and 2023

Computacenter, London – Technical pre-sales Consultant - July 2007 – June 2008

Employed within technical pre-sales I was responsible working with new business clients, working with numerous vendors and their products (Cisco, HP, IBM and EMC) and advising clients on the best technologies to implement. Throughout my time at Computacenter, I dealt with a variety of clients and consultants, my specialist interest being that of computer networking and security.

SKILLS

Cyber Security Expertise	I have completed over 200 penetration tests, testing many different technologies, including modern and legacy web applications, multiple cloud platforms (AWS, Azure), more traditional infrastructure and stand alone IoT devices. I pride myself on the result of these engagements and always strive to provide a report and post test meeting which places the findings and risk within the context of the system and the organisation. My background in educations lends itself to deep but concise explanations to empower and educate those responsible to fixing the systems. I have also conducted several IT Health Checks and I personally hold the Cyber Scheme Team Leader (web) certification with security clearance, so am deployable as a CTL for Web. Furthermore I have experience of all major penetration testing tools and even developed my own vulnerable application which I used for teaching whilst working at the University. I have also taken several companies through their PCI-DSS compliance, helping them not only reach the required level but ensuring the baseline of security extends beyond the requirement. I have experience working with QSA's, dealing with ASV's. In my time at Old Company I have experience in working in large teams and performing initial gap analysis's and subsequently project managing the implementation of the required Cyber Security standards, including NIST, Cyber Essentials, 27001 and CIS. I have interviewed numerous employees in many different organisations to understand where their gaps lie, not only within the required standard but in a more general cyber security approach. As I appreciate many standards use generic language which can be used to ignore certain areas of cyber security, even when important. I am also familiar with many existing and newer architectures, such as Azure and AWS. I am also very aware of the numerous challenges these new technologies and architectures have, such as a lack of centralised user management and a lack of centralised logging and monitoring capability. In addition, I am also aware of the challenges legacy systems can present an organisation, they can be integral to the running of an organisation but also present many issues when it comes to the risk their outdated technology introduces. Through my extensive career, I've prioritised not just the technical accuracy but also the interpretive quality of over 200 penetration test reports. My unique blend of cybersecurity and educational experience ensures that my reports and post-test briefings are comprehensive yet comprehensible. They serve to educate as well as inform, enabling organisations to not just meet but exceed their cybersecurity benchmarks. With a proven proficiency in facilitating the implementation of Cyber Security standards, I deliver reports that provide actionable insights, drawing from an in-depth understanding of both modern and legacy systems
Learning, Teaching & Assessment	I have had experience in teaching students at all levels (4-7). Further to this I have had experience teaching UK students and overseas students. Each group I understand may require different approaches and I have developed skills in this area, such as adapting my language to ensure the students understand and the ability to use different examples and analogies to explain concepts and principles. More specifically the assessments I have developed vary from very practical hands on assessments where the students are required to practically solve issues or accomplish tasks, (e.g parameter manipulation) to assessments which require the combination of theory and practise (e.g creation of an IDS rule), to more theoretical assessments which are built upon real life case studies (e.g implementation of a policy based security control) which provides the students with context and meaning. I also led the design on Old Company's CREST CRT course and was a key developer of several courses we delivered for the ABC group. These courses were built from the ground up and were designed to provide attendees with the latest in domain knowledge. Throughout my time at Old Company I continued to teach, delivering modules for Big Time University and delivering Old Company's CRT course.
Management and Team Leading	Over the past 6 years I have hired, managed, and developed my team at Old Company. I always lead from the front and delegate and support when appropriate. Over the past 6 years my team has remained largely the same, thus we have not suffered much attrition and staff turnover. I believe this is in part due to the selection of the right individuals and the culture I have helped created within the team.

	As Old Company is a consultancy company I have also worked alongside numerous, clients, regulators and external parties, actually having involvement in two specific instances with the ICO auditors when a client was being investigated by them. I try to empower my team, but ensure they are fully supported should they need assistance or backing, I like giving people opportunities to prove themselves. For example, we had a junior member of the team apply for a senior position, although they did not get the role I made a point of occasionally letting them lead an internal meeting, to show I had faith in them and give them a controlled opportunity to develop their skills.
Communication	Whilst working at Old Company I have developed my communications skills in such a way that I can present information to different audiences, for example I have delivered the results of several gap analysis and penetration tests to both senior management and those staff members who needed to implement the results of the reports. I'm also familiar with conflict management, as working as a consultant you can sometimes be seen as a threat, I have developed several techniques to help reduce any fears and encourage collaboration. For example, when working with IT providers, I ensure they have visibility of our road map and project plan, and I ensure I take their input into timeframes and expectations, by encouraging their input, they feel more like part of the team, rather than an outsider who is to be judged by our work. Working as a senior University lecturer has given me an opportunity to develop and further my communication skills considerably. Having to present different types of information, ranging from hard technical facts to softer more methodological information has been an interesting journey for me. I have developed techniques which have enabled me to do this, by grounding the hard technical facts in real work examples I have found the students to be more interested and engaged. For the softer information I have found engaging the students with examples and getting them to play the roles of clients and developers has seen them engage further. In 2013 I visited India and Sri Lanka on a recruitment visit, I toured Universities in both Countries giving lectures and running tutorials for their students. Hence I have experience with international travel, recruitment and engagement.
Problem Solving	All aspects of my current role involve some kind of problem solving, and I rarely go one day without at least one significant problem to tackle. Fortunately I relish problems and get real enjoyment out of solving them. Typical problems I face in my current role 1. Constant changing cyber security environment, I find one of the biggest challenges within cyber security is the constantly changing environment, whether that be regulation changes, technical advancements or even political shifts. Fortunately I have enough experience to be able to find the common themes within this changing environment, and due to my passion for learning I really enjoy applying myself to these new challenges. For example when AWS (Amazon Web Services) began to take off, I had very little experience working within this environment, however after taking a Udemy course, contacting several trusted peers, I found myself in a position where I could apply my more general technical cyber security skills to this new technology. 2. Staff management issue's, I have had issues which range from staff refusing to work onsite to issues with pay parity. In any of these challenges I ensure I have the full information and set to work on trying to find a workable solution which all parties can be comfortable with, should no such solution exist I ensure that the staff member with the issue is made aware the reasons why they cannot be accommodated to minimise any ill feelings. 3. Working in cyber security consultancy I am involved with many challenges when it comes to performing the consultancy, this can range from not being able to access the people, process or systems we need, an unexpected gap in the capability of the organisation or even a unexpected shift in deadlines and priorities. In these instances I explore the options available, seek council from those involved if appropriate and make the best decision available, whilst ensuring all stakeholders understand the reality. I find it much easier to deal with a problem in its infancy than risk allowing it to grow out of control.

John Smith *Global SOC Lead*

UK | john.smith@test.com | -

PROFILE

I am a Global SOC Lead passionate about increasing SOC maturity and operational effectiveness. I am committed to helping organisations identify and establish a well-aligned maturity strategy for their security operation centre. This includes defining a target operating model that ensures measurable progress. Additionally, I have extensive experience in responding to various security incidents in large enterprises. My passion for continuous professional development drives me to study topics related to my profession and beyond, including business administration, criminology, and business risk management.

PROFESSIONAL EXPERIENCE

06/2023 – present

Global SOC Lead
[Redacted]
As the global security operations lead at [Redacted], I oversaw the management of the function. I gave senior management greater visibility into operations while developing strategies to improve the process.

- Acting as a lead incident responder in significant security incidents
- Built SOC maturity strategies in line with agreed target operating models.
- Provided guidance and consultancy to other business functions about security best practices.
- Established sprint cycles to implement required changes for prioritised maturity requirements.
- Structured training plans and mentorship for analysts and engineers.

04/2022 – 06/2023
Portsmouuth

SOC Client Lead
[Redacted]
Responsible for consulting leading accountancy firms and financial institutions on security operation best practices, assisting them in technical security maturity and process improvements.

- Leading the on-boarding, deploying and integrating various security solutions to provide clients with a managed detection and response capability.
- Produce critical documentation such as incident response plans, playbooks, and operating manuals.
- Acting as a dedicated Incident handler for clients, coordinating the response efforts of both parties.
- Acting as SOC manager for clients and the intermediary between customer and service provider.

12/2021 – 04/2022
[Redacted]

UK SOC Lead
[Redacted]
Responsible for leading the UK team and delivering the SOC service to our customer base, the lead incident handler for ransomware attacks and high priority cyber incidents.

- Managed and delivered the training for the global team.
- Producing documentation that aligns with policies that help the team deliver value to our customers and meet expectations.
- Built the Strategic IR Response plan for the MSSP with a RACI chart to ensure all members of the SOC team are aware of actions and responsibilities.
- Advised the global head of security operations on issues and provide solutions aligned with the strategy.

12/2020 – 12/2021
[Redacted]

T2 SOC Analyst
[Redacted]

07/2020 – 2020
[Redacted]

Cyber Security Engineer
[Redacted]

04/2019 – 2020
[Redacted]

T2 SOC Analyst
[Redacted]

05/2018 – 03/2019
[Redacted]

Junior SOC Analyst
[Redacted]

Further experience available on request

ORGANIZATIONS

08/2022 – present

[Redacted]
Security Operations Management Content creator
Producing content for a future course that aims to help improve security operations by informing potential and current managers of maturity techniques, best practice related to the organisation and business management philosophy in relation to SOC.

[Redacted]
Security+ Instructor
CompTIA Security+ Instructor and study group host with a high degree of first-time passes from students.

CERTIFICATES

CySA+
Achieved May 2020

eJPT
Achieved September 2020

Blue Team Level 1
Achieved September 2020

Splunk Fundementals
Achieved September 2020

Crowdstrike Falcon Adminstrator
January 2021

SecureOnix Architect
Achieved January 2021

Sumo Logic Adminstrator
February 2021

CISM
February 2022

SC-200
October 2022

AWARDS

The Iron Division Commanding Officers Award for Excellence
British Army

PUBLICATIONS

2023

[Redacted]
A Newsletter dedicated to my research around security operations, security operations maturity, risk management and more to inform and demonstrate my knowledge to a broader audience.

[Redacted]
In Development
A book dedicated to informing people how to become an effective SOC professionals through different kinds of thinking and approaches to common issues.