Daniel Byers BSc (Hons) MSc

Over the past decade, I have acquired a wide ranging and deep understanding of core Cybersecurity concepts from professional experience, formal academic study, and self-driven learning. With practical experience in both offensive and defensive domains, my skill-set can be applied in any purple team environment. I can bring expertise to discussions in regards to compromising and defending critical systems, and am familiar with performing tasks related to both. This experience includes such things as incident response, administration of network IDS, performing investigations to aid customers during active breaches, analysing logs and network traffic for anomalies, threat hunting, penetration testing, digital forensics, and more. Since January 2024, I have been working as a Detection Engineer, which has entailed producing and maintaining detection rules for QRadar, advanced threat research of known exploited vulnerabilities, assisting in preparation for a MITRE Engenuity assessment, and spearheading the project to create runbooks for day-to-day operations.

I have an extensive understanding of programming, with professional experience in multiple high and low level languages. This knowledge greatly helps me in many areas of Cybersecurity as I can quickly produce useful tools to support day-to-day operations or scripts to automate repetitive tasks. My understanding of regular expressions enables me to parse logs with ease, I can reverse engineer binaries to understand malware, analyse vulnerabilities in software, write custom exploits, and perform all tasks related to software maintenance. Most recently, I have improved the capabilities of an EDR sensor by conducting research of malicious activity and then realising it as detection logic in C++, including utilising eBPF for kernel-level visibility. Most of my projects are displayed on a website that I developed, which is written in Ruby on Rails and hosted on Google Cloud Platform.

A lifetime of computer use has given me a strong set of problem solving abilities when using modern operating systems. Initially in Windows, but for the last ten years mainly in Linux. Now, the vast majority of the systems in my home network are Linux-based, and I run Linux on my work machines. I have a love of operating systems theory, and enjoy learning about the internals, or experimenting with advanced features.

I am a very quick learner and have no reservations about admitting the limitations to my knowledge and/or asking for help when required. In fact, I like to be the least skilled person in the room so that my potential for learning is maximised. This does not mean that I shy away from teaching; having to pass on knowledge is the best way to highlight gaps in my own. To this end, it is common to find me engaged in discussion with colleagues after they have sought my assistance. I realise that I am human and will make mistakes, so am not afraid of accountability. I enjoy watching (and attending if possible) talks/conferences related to computing and participating in group meet-ups/Hackathons/Capture the Flags. Overall, I have a wide knowledge and passion for computer theory and operation, with confidence that anything I don’t know, but need to, I can learn. Outside the virtual domain, I am an avid reader, enthusiastic gamer, novice Japanese speaker, and eager world explorer.

Daniel Byers BSc (Hons) MSc

Email: work@danielbyers.net

Phone: (+44|0) 7949 358 152

Bright, talented, natural problem-solver with excellent self-discipline and the ability to work with the minimum of supervision, under pressure, and well within a team. Care is taken in any situation to ensure quality is delivered and correct focus is placed on priorities in complex environments.

Key Skills

Threat Hunting

Security Research

Penetration Testing

Incident Response

Malware Analysis

Linux, Windows

Ruby, Python, PHP

C, C++, Java, Rust

Assembly

HTML, CSS, JavaScript

PostgreSQL, MySQL

BASH, PowerShell

Networking

Cryptography

Digital Forensics

Artificial Intelligence

Cloud Engineering

Basic Japanese

Employment History

Detection Engineer
IBM, January 2024 – Present

EDR Researcher & Developer
WithSecure, September 2021 – December 2023

Cyber Security Analyst
AlertLogic, April 2020 – August 2021

Software Developer
Seamless, June 2019 – September 2019 (internship), October 2019 – April 2020 (employee), June 2020 – November 2020 (consulting)

Software Developer
Umbrellar Cloud Hosting, September 2015 – June 2016 (internship), June 2017 – December 2017 (consulting)

Software Developer
Practice Loan Company, Lichfield, September 2016 – September 2017

Education & Qualifications

LPIC-1
Linux Professional Institute, October 2024

Google Cloud Platform: Associate Cloud Engineer
Google, August 2024

Cyber Security Analyst+
CompTIA, August 2022

Cyber Security MSc
Passed with Merit, University of Birmingham, September 2018 – December 2019

Computer Science BSc
1st Class Honours, Manchester Metropolitan University, September 2013 – July 2017

Access to Higher Education Diploma in Computing
Passed with 8 Distinctions, 4 Merits, Lincoln College, September 2012 – July 2013

General Certificate of Education (Advanced Subsidiary)
English Literature and Physics, September 2008 – July 2009

'Design and the Web' Certification
Open University, 2008

General Certificate of Secondary Education A-C
English*2, Maths, Science*2, ICT*2, Design Technology, RE, Business,
Cordeaux High School, 2004 - 2007

Full Clean UK Driving License **References available on request**