Christiaan de Wet

Security Engineer | Researcher | Developer

I built my career foundation on system administration, and later gaining broad knowledge in Cyber Security, alongside certifications and qualifications which practically validate my 20 years of experience. While navigating life through H, J, K, and L, I enjoy to tinker and constantly explore all sorts of technologies in my spare time, and I find great satisfaction in writing code and developing applications.

christiaan.dewet@gmail.com | +44 7311 991910 | Oxfordshire, UK

christiaan-de-wet | CryDeTaan | CryDeTaan

Skills

Brain archive; some current and past skills, tools and / or familiarities:

Red Teaming and Pentesting	Bloodhound, Burp Suite, CobaltStrike, Guardara (FuzzLabs), Kali
Reverse Engineering	Radare2, Immunity Debugger, OllyDbg, Ghidra, IDA
AI/ML	LLMs (Claude, Bedrock), Embedding models & vector search, Claude Code (Skills, Commands, MCP), Agentic workflows
(Web) Development and Tooling	Bash, C#, GoLang, Javascript, PHP, Python, dnspy, Docker, Git, Nginx, Postman
Database	MySQL, Snowflake, Neo4j
Cloud and Cloud native	AWS, AWS Lambda, Azure, Azure Functions, Cloudformation, Kubernetes, Terraform
Security products	Checkmarx, CyberArk, Cybereason, Fortify on Demand, Splunk, Snort, SonarQube, Tenable, Websense
Enterprise	Windows, Active Directory, Exchange, PostFix, and many more
I like(d) to tinker with	Arduino, Arch, Home Assistant, i3WM, RaspberryPi

Recent Experience

Founder & Lead Developer

Mar 2021 – Present

Mailphantom · E-mail privacy SaaS

SaaS offering which protects your email privacy by using unique email addresses online.

- Automated testing and deployment (GitHub Actions)
- Design and build the entire web application (Laravel, VueJS)
- Follow DevOps strategies to maintain the application and infrastructure

Security Engineer - Lacework Labs | Software Engineer - Code Sec

Feb 2023 – Aug 2026

Fortinet (Acquired Lacework) · Cloud security company

Providing security subject matter expertise to drive improvements within the Lacework Platform

- Developed and improved SAST and SCA features (GoLang, Java, GitHub Actions)
- Developed and patented (US12407702) internal tooling for dynamic CVE Data collection (Laravel, VueJS)
- Developed cloud-based composite alert detections from Threat Intelligence (Python, Sigma, Snowflake, Neo4j)
- Developed CWE categorisation and consolidation pipeline using LLM and embedding models (Python, Bedrock)
- Developed baseline framework to compare Lacework vulnerability evaluation engine against CVE Data sources (Python)
- Developed PHP language support for the SAST engine (GoLang, Semgrep)
- Developed PHP language support for the Code Aware Agent (GoLang)
- Developed PR Comment features and improvements for Code Security CI/CD Apps(GoLang, Java)
- Established a SAST Taxonomy for SAST detections
- Established an Attack Simulation program to test and validate detections (Terraform)
- Performed novel research on Living Off the Land vulnerability detection and presented at BlackHat USA 2023.
- Support and drive Vulnerability Management features to improve CVE data efficacy (GoLang)

Sr. Manager - Penetration Testing and Security Research

Feb 2020 – Jan 2023

Becton, Dickinson and Co. (BD) · Medical device manufacturer

Led the Penetration Testing and Security Research team and perform Security Research against BD's medical products and infrastructure.

- Define and embed Penetration Testing and Security Research as a formal phase of BD's Secure SDLC, with methodology and standards aligned to the NIST Cybersecurity Framework and UL 2900
- Develop proof of concept exploits to demonstrate impact of vulnerabilities (python, bash)
- Perform manual code review to discover vulnerabilities within large code bases (C#, PHP, Java)
- Perform Penetration Testing & Security Research on BD's products using emerging technologies such as Kubernetes and cloud native applications
- Provide guidance on secure architecture design and DevSecOps within CI/CD pipelines
- Support developers in their SDLC through threat modelling and guidance for mitigating emerging threats
- Utilise SAST, SCA, DAST and fuzz testing in the Secure SDLC verification and validation stage (Checkmarx, FoD)
- Team Leadership, Mentoring, and Career Planning

Student Admin
Jun 2018 – Jan 2020

Offensive Security (OffSec) · Cyber Security training provider

Provide support and improvements for the highly coveted OffSec Labs and Exams

- Developed a plagiarism detection system using machine learning (spaCy NLP)
- Provide assistance in building new lab and exam machines
- Provide guidance to students during their lab time
- Provide Linux, VPN, Virtual Machine technical support
- Used the opportunity to up-skill, and learn from those who build Offsec and obtain two additional Offsec certificates
- Write technical documentation for new lab and exam machines

Penetration Testing Team Lead
Oct 2017 – Jun 2018

Capitec Bank · Retail Bank

Establish the Offensive Security and Red Teaming function

- Develop and define engagement methodologies and frameworks aligned to ISO 27001 and PCI-DSS testing requirements
- Implement automated source code analysis (SonarQube)
- Plan and execute on security assessments on internal environments, producing control framework assurance evidence
- Support Incident Response team during investigations, particularly where new TTPs were discovered

Penetration Tester/Security Engineer
Apr 2014 – Sep 2017

Investec Bank · Investment Bank

Improve Security posture through initiatives, projects, and red team and penetration testing exercises

- Advise internal infrastructure teams on designs and implementation strategies of new systems
- Design and implement CyberArk to manage all local Admin accounts, enforcing least privilege required by ISO 27001 and PCI-DSS
- Design and implement global Splunk infrastructure, delivering centralised logging controls required by ISO 27001 and PCI-DSS
- Develop security monitoring detections and strategies from Threat Intelligence
- Plan and execute on security assessments on internal environments
- Research vulnerabilities, reverse engineer targeted malware and write associated internal advisories
- Support Incident Response team during investigations, particularly where new TTPs were discovered

Technical Support Engineer and Services Manager
Apr 2010 – Mar 2014

Performanta Technologies · Cyber Security service provider

Design, implement and manage multiple security technology domains and products, as well as Technical and operational management and support of the services department

- Served as Information Security Officer and Consultant for multiple large organizations
- Conducted R&D on emerging security threats and solutions
- Implemented Data Loss Prevention solutions at Royal Bank of Scotland and Standard Bank SA
- Advised sales teams on technical markets and trends throughout the sales lifecycle

Certificates

(GCPN) GIAC Cloud Penetration Tester
GIAC (SANS) | Candidate ID : 24212070

(OSWE) Offensive Security Web Expert
Offensive Security | OSID: 15591

(CISSP) Certified Information Systems Security Professional
(ISC)2 | Career ID: 437270

Neo4j Certified Professional
Neo4j Graph Academy

(OSCE) Offensive Security Certified Expert
Offensive Security | OSID: 15591

(OSCP) Offensive Security Certified Professional
Offensive Security | OSID: 15591

CompTIA Security+ & Network+ Certifications
CompTIA | Career ID : COMP001007205511

Publications

Living Off the Land Attack
An overview of Living Off the Land (LOTL) attack techniques
Lacework Labs — Mar 2024

How to Protect Against "Living Off The Land" Attacks
A talk on how to protect against Living Off the Land attacks.
BlackHat USA 2023 — Aug 2023

Protect containers from Living Off the Land (LOTL) attacks
How to protect containers from Living Off the Land (LOTL) attacks: A step-by-step guide
Lacework Labs — Mar 2024

Abstract Entropy
A blog I add some content to from time to time
Christiaan de Wet — Jan 2020

Awards

BD Star Award — May 2021
BD Information Security
Monthly award given to individuals who made significant contributions.

BD Annual Excellence Award 2021 — Dec 2021
BD Information Security
Annual award given to an individual who made significant contributions for the year.