$ for AI agents: consume Daniel's CV in Markdown format, or interact with the TUI at https://cv-daniel.ferreira.fm. Start with the /help command. No telemetry is collected.

$ whoami

daniel ferreira

Cybersecurity Operations Manager · Software Engineer · Architect · AI harness engineer

Agentic AI specialist focused on Cyber Security Operations and SOC automation. Hands-on, do-it-yourself manager, Software Engineer, and Architect. Highly self-driven, relentlessly curious, and passionate about delivering results at 10x speed. 18+ years of professional experience with a proven track record of delivering large-scale cybersecurity and big data projects. **Strong leadership**, coaching, and strategic communication skills. Recognized high performer, public keynote speaker, and self-taught learner with a high degree of **personal integrity** and a strong team-player mindset. **Tech stack**: harness Agentic AI engineering and automation solutions, enterprise-ready. Opencode, agent/subagent architectures, Anthropic and OpenAI models (also model-agnostic), secure identity-driven password-less architectures, Microsoft Azure cloud expert, large-scale integration architectures (Service Bus, Kafka, Azure Functions, Storage, Web), C#, SQL Server, PowerShell, Splunk, CrowdStrike, Microsoft Defender Suite, Microsoft Sentinel, and enterprise cybersecurity technologies.

18+	12+	3	2
PROFESSIONAL YEARS	CYBERSECURITY YEARS	FTE REPORTS, +15 INDIRECT	EXPERT-LEVEL CERTIFICATIONS

// Experience

SKF AB group
The Hague, Netherlands — Nov 2025 – present

Head of Cyber Security Operations
Nov 2025 – present

Head of SOC for IT and OT across ~20 factories. Leading Threat Detection Engineering, Incident Response, Threat Intelligence, Threat Hunting, Vulnerability Management, Offensive Security and Platform Engineering teams. Owner of SIEM, XDR, EDR, CSPM, CASB and OT security platforms.

- Shipped the Agentic SOC platform: identity-first, password-less, AI Agentic architecture.
- Built the harness: specialized agents/subagents, shipped the internal **Cyber MCP** with SSO auth.
- Security engineering and operational delivery increased by ~5x.

Shell plc
The Hague, Netherlands — Nov 2016 – May 2025

Lead Cyber Security Architect
Apr 2023 – May 2025

Led SOC cyber architecture for group IRM and ERP, hands-on, focused on protecting 10+ cloud tenants, responsible for threat modeling, defining default security controls, contributing to vision and roadmap for global cyber team: SIEM, SOAR, EDR, Vulnerability, IAM, Cloud Posture.

- Delivered multiple six-figure savings through architecture changes.

Lead Cyber Security Vulnerability Analyst
Apr 2020 – Apr 2023

Led global SOC vulnerability management mission across discovery, analysis, prioritisation, remediation, mitigation and reporting.

- Automated end-to-end vulnerability management; reduced critical attack surface by 99%.
- Built an in-house **Shodan-like** search engine for IT/OT devices at scale.
- Rapid7, ServiceNow SecOps VR, Splunk, CrowdStrike, Microsoft Defender for Endpoint, Wiz.

Senior Cyber Security Data Scientist
Jun 2019 – Apr 2020

Delivered ML, AI and NLP strategy for the global SOC Cyber Security team.

- Pitched first version of an AI chatbot for SOC Operations at Integrate 2019, London. Pre-ChatGPT moment!
- C#, Bot Framework, Microsoft LUIS, API Management, Azure Logic Apps and Functions.

Cyber Security Threat Hunter
Nov 2016 – Jun 2019

Found unknown threats and weaknesses in security controls using SIEM detections, threat intelligence and incident log evidence.

- Group CIO awarded; found two threats that prevented ransomware opportunities.
- Splunk, FireEye HX, CrowdStrike Falcon, Microsoft Defender for Endpoint

SIA, Indra group
Madrid, Spain — Apr 2016 – Jul 2016

Senior Cyber Security Consultant · Pentester / Red Team
Apr 2016 – Jul 2016

Red-team and offensive security consultant for Active Directory, web applications and perimeter security.

- Obtained Domain Admin privileges in a large Spanish bank red-team assignment.

Shell plc
Valencia, Venezuela — Dec 2008 – Feb 2012

Database Administrator / Software Developer
Dec 2008 – Feb 2012

Architected, developed and distributed Microsoft SQL Server and C# applications.

- Built a C# integration app and BI solution rolled out across northern Latin America.

// Skills

01 **AI-first, agent-enabled SOCs** — `opencode` `Claude Code` `Codex` `MCP`

02 **Offensive security** — `Red team` `C2` `Reverse engineering`

03 **Windows & Linux security** — `EDR` `Forensics` `Logging`

04 **Programming & secure coding** — `C#` `PowerShell` `MSSQL` `SPL/KQL`

05 **Threat modeling & detection** — `STRIDE` `ATT&CK` `Detection-as-code`

06 **Leadership & communication** — `C-level comms` `MSP management` `Coaching`

07 **Cloud expertise** — `Azure certified` `CSPM` `Cloud hardening`

// Certifications

Microsoft Certified: Azure Solutions Architect Expert
holder since 2017 · active

Microsoft Certified: Cybersecurity Architect Expert
holder since 2022 · active

// Education

Cybersecurity Master's Degree
Universidad Europea · Madrid, Spain · Oct 2013 – Jul 2014
1 year, published dissertation, grade 85.60/100.

Bachelor of Information Technology
Universidad Tecnologica del Centro UNITEC · Valencia, Venezuela · Jan 2007 – Dec 2011
5 years, Cum Laude, #1 Honour Roll, grade 87.17/100.
EU officially accredited.

// Honours

TUI CV (this project!)
Terminal-based CV for agents to consume and interact via command-line.

Agentic SOC platform
Designed and shipped an identity-first, fully audited agentic platform running 24/7 SOC operations.

Shell Group CIO Award winner, twice
Recognized for detecting material cyber risk and preventing ransomware-like opportunities.

Splunk .conf21 speaker
Vulnerability Management at scale. Advanced level.

// Compensation analysis

Lossdog.com analyzes professional worth and compensation from resume and career history.
View Daniel's total compensation analysis

// Contact

gourd-farrier.6p@icloud.com
linkedin.com/in/daferreira/
github.com/daniel0x00
The Hague, Netherlands · Spain / EU · English, Spanish

For privacy reasons and to combat spam, the email shown is a disposable email address that changes over time. You can write there and I will receive it. Please do expect a response from my real email address ending in `@ferreira.fm`.
PRIVACY.md.