Robert Lowery

Detection Engineer & Security Researcher

rob@lowery.tech • lowery.tech • github.com/0xrob • uk.linkedin.com/in/robert-lowery-a282bb138 • London, England, United Kingdom • lowery.tech/pubkey.asc

PROFILE

Security researcher and detection engineer working at the offensive-informed end of defence: understanding how real intrusions work, then building the detection that catches them at scale.

Cyber analyst by trade, with a background spanning offensive and defensive security, now leading threat detection for a national programme across UK government.

Publish independent research at lowery.tech on threat hunting, malware development and detection engineering.

EXPERIENCE

Technical Lead — X-gov Detection Engineering **Oct 2025 – Present**

Government Cyber Coordination Centre (GC3) · Contract • Hybrid

- Lead detection for a UK government programme set out in the Government Cyber Action Plan.
- Build custom AI pipelines that ingest vulnerability and CTI data from multiple sources, normalise it, and generate detections across several query languages.
- Built strict validation processes for detection content, testing detections at scale against true-positive logs in multiple SIEM languages.
- Further programme work is not publicly disclosable.

Lead Detection Engineer **Mar 2025 – Jan 2026**

Foreign, Commonwealth and Development Office · Contract

- Built the department's detection-as-code platform, including its CI/CD pipeline.
- Built detections protecting critical UK government infrastructure.
- Matured the detection engineering function and led upskilling across the team.

Lead Security Engineer **Aug 2023 – Present**

Cabinet Office · Contract

- Developed and implemented detection-as-code CI/CD pipelines using Splunk security content, contentctl and a custom Python library.
- Built scalable detection content based on data models.
- Developed SOC KPIs for the detection function and presented them to key stakeholders.
- Drove the SOC maturity journey, implementing change at scale through DLP, architectural change and detective monitoring improvements.
- Mentored junior analysts and upskilled team members.

SOC Lead **Aug 2021 – Aug 2023**

CyberProof / UST · Full-time

- Led the Middle Europe security monitoring and detection team, mentoring analysts and supporting complex investigations.
- Built a threat hunting platform from scratch on an exclusive contract with a Fortune 100 client.
- Developed tailored threat hunting packages from MITRE TTPs, using a MITRE heatmap I built to expose use-case gaps.
- Hunted advanced in-memory threats using anomaly-based detection and CTI-driven hypotheses across a large network estate.
- Represented the blue team in purple team exercises, building queries to detect techniques designed to bypass industry-leading EDR.
- Performed complex incident response investigations at scale and reported hunting KPIs to stakeholders.

SOC / Information Security Analyst **Nov 2019 – Aug 2021**

London Stock Exchange Group (LSEG) · Full-time • London Area, United Kingdom

- Monitored and protected highly regulated environments, securing legacy and unpatched infrastructure against advanced attack.
- Developed advanced monitoring for SWIFT payment infrastructure to meet best practice in a highly regulated banking environment.
- Applied threat modelling and a defence-in-depth approach across EDR and network monitoring.
- Proactively hunted anomalous activity and tuned known-good behaviour to surface lateral movement and other ATT&CK TTPs.

- Investigated breaches end to end: timeline reconstruction, remediation, reporting and stakeholder communication.

MDR Cyber Security Analyst **Sep 2018 – Nov 2019**
Reliance ACSN · Full-time

- Investigated alerts daily, delivered tuning recommendations and built new detection rules.
- Advised customers on enforcing security policy through technical controls.
- Worked to PCI-DSS, ISO 27001 and NIST 800-63 from a security compliance perspective.

SKILLS

Detection Engineering Detection-as-code · CI/CD pipelines · Splunk contentctl · Sigma · KQL · MITRE ATT&CK mapping · Data-model-based content · Alert triage & tuning

Threat Hunting Hypothesis-driven hunting · ATT&CK heatmapping · CTI-led hunting · Microsoft Defender for Endpoint · Jupyter / msticpy · In-memory anomaly hunting

SIEM & Security Platforms Microsoft Sentinel · Splunk · LogRhythm · QRadar · EDR / AV tooling · Proxy & email gateway

DFIR & Malware Analysis Incident response at scale · Timeline reconstruction · FTK · Volatility · YARA · Static & dynamic analysis · Windows internals · Reverse engineering

Offensive Security Red team tradecraft · Purple teaming · Sliver & Covenant C2 · Custom loaders & stagers · Direct syscalls (SysWhispers) · HTML smuggling · EDR & AV evasion research

Frameworks & Compliance PCI-DSS · ISO 27001 · NIST 800-63 · NCSC endpoint baselines

Platforms & Tooling Python · C / C++ · PowerShell · Windows & Linux hardening · Active Directory · Azure / Microsoft 365 security

PUBLISHED RESEARCH

- Threat Hunting with Jupyter Notebooks to Detect Advanced Threats — Part 1: Setting up msticpy with MDE
- Threat Hunting with Jupyter Notebooks to Detect Advanced Threats — Part 2: Custom Queries and a Host Investigation Notebook
- Stopping Blue Teams From Obtaining Payloads via Browser-Based Virtualisation Detection and HTML Smuggling
- Building a Custom Shellcode Loader with SysWhispers to Utilise Direct Syscalls
- Building a Custom Shellcode Stager with Process Injection to Bypass Windows Defender
- Using Covenant and Excel 4.0 Macros to Bypass Windows Defender
- Using a Database of 100 Million+ Breached Passwords to Secure a Linux Server / Endpoint for an SME
- Using a Password Filter to Create a Banned Password List without Azure AD on Windows
- Creating a Malware Analysis Lab for Dynamic Analysis

CERTIFICATIONS

- LogRhythm 330 — Certified Engineer, LogRhythm SIEM
- LogRhythm 310 — Cyber Analyst
- CompTIA Security+ (2018)
- CrowdStrike Engineer (2019)
- Microsoft — Windows Server 2016: Advanced Virtualisation
- Microsoft — Windows Server 2016: Advanced Networking
- Microsoft — Azure Virtual Machines
- CS50, Harvard University (online)
- Autopsy Hands-On Course

EDUCATION

MSc Cyber Security **2017 – 2018**
University of West London
Grade: 1st

BSc Criminology and Forensic Science **2014 – 2017**
University of Essex