



Erin Connolly

JUNIOR SECURITY ANALYST

Egham, United Kingdom | erin.connolly@gmail.com | +44 7382 094 517 | linkedin.com/in/erinconnolly-sec

PROFILE

Cybersecurity graduate from Royal Holloway, University of London with SOC experience from a summer placement at **NCC Group**. Triageed over **120 alerts per shift**, escalated 8 confirmed security incidents, and wrote 6 SIEM correlation rules. Holds **CompTIA Security+** certification. Placed in the **top 10 at the National Cyber Security Challenge** (2024).

EDUCATION

BSc (Hons) Computer Science (Information Security) in Computer Science (Information Security)

Royal Holloway, University of London, Egham

Sep 2022 – Jun 2025

SKILLS

- SIEM (Microsoft Sentinel, Splunk)
- Endpoint Detection (CrowdStrike Falcon)
- Network Analysis (Wireshark, tcpdump)
- Vulnerability Scanning (Nessus, OpenVAS)
- KQL & SPL (SIEM Query Languages)
- Python (Security Scripting)
- Linux Administration (Kali, Ubuntu)
- MITRE ATT&CK Framework
- Incident Triage & Escalation
- Phishing Analysis
- Active Directory Security
- Log Analysis & Forensics

LANGUAGES

- English - Native

REFERENCES

James Kettle

SOC Team Lead, NCC Group
james.kettle@nccgroup.com, +44 7700 900 291

EXPERIENCE

SOC Analyst (Summer Placement), NCC Group, Manchester

Jun 2024 – Sep 2024

Summer placement in the Security Operations Centre providing managed detection and response services to corporate clients.

- Triageed an average of **120 security alerts per 8-hour shift** using Microsoft Sentinel and CrowdStrike Falcon
- Escalated **8 confirmed incidents** to Tier 2 analysts, including 2 phishing campaigns and 1 ransomware precursor
- Wrote **6 SIEM correlation rules** in KQL (Kusto Query Language) to detect brute-force login attempts across client tenants
- Produced **4 incident reports** for clients with root cause analysis, timeline reconstruction, and remediation recommendations

IT Student Helper (Part-time), Royal Holloway IT Services, Egham

Sep 2023 – May 2024

Part-time first-line support for the university's IT services.

- Resolved **300+ support tickets** covering Wi-Fi connectivity, password resets, and software installation
- Assisted with the rollout of **multi-factor authentication** to 12,000 student accounts over a 6 week period

CERTIFICATIONS

CompTIA Security+, CompTIA

Mar 2024 – Mar 2027

Microsoft SC-200: Security Operations Analyst Associate, Microsoft

Jan 2025 – Jan 2026

PROJECTS

Lateral Movement Detection (BSc Dissertation)

Sep 2024 – May 2025

Built a machine learning classifier to detect lateral movement patterns in Windows event logs.

- Trained a **Random Forest model** on 2.3 million simulated log entries, achieving **91% precision and 87% recall**
- Tested against **4 MITRE ATT&CK lateral movement techniques** (Pass-the-Hash, PsExec, WMI, RDP hijacking)
- Received **72%** and was nominated for the ISG Best Dissertation prize

National Cyber Security Challenge 2024

Mar 2024 – Jun 2024

Competed in the national CTF competition run by the Cyber Security Challenge UK.

- Placed **top 10 nationally** out of 1,200+ participants across all rounds
- Solved challenges in **cryptography, forensics, web exploitation, and reverse engineering**
- Invited to the **Masterclass final** at a secure government facility

EXTRA CURRICULAR ACTIVITY

President – Royal Holloway Cybersecurity Society

Sep 2024 – Jun 2025

Led a society of **85 members**. Organised weekly CTF practice sessions, **4 industry speaker events**, and a trip to BSides London attended by 12 students.

Volunteer – CyberFirst (NCSC Schools Programme)

Jul 2024 – Aug 2024

Assisted NCSC instructors on a **5-day CyberFirst course** for 30 sixth-form students, running practical labs on networking and cryptography.

TryHackMe – Top 3% globally

Jan 2023

Completed **140+ rooms** on TryHackMe covering penetration testing, forensics, and SOC fundamentals. Currently ranked in the **top 3%** of all users globally.