Mykola Nesterenko

Senior Technical Security Analyst

United Kingdom

contact@cybernester.com | +44 7 950 999 787

Website: https://cybernester.com | LinkedIn: https://www.linkedin.com/in/m-nester/

Professional Summary

Cybersecurity professional with extensive experience in designing and implementing robust security solutions for cloud environments. Currently overseeing the strategic aspects of a SIEM platform migration at Lloyds Banking Group, where I assist management of the transition from Splunk to Google SecOps and re-implement current detection controls to adhere to current industry standards. Having progressed from a Cybersecurity Engineering Intern to a Senior Technical Security Analyst, I integrate technical expertise with leadership to strengthen our security posture. My initiatives have contributed to a 10% improvement in overall team performance and a 15% increase in cloud threat detection coverage.

Professional Experience

Senior Technical Security Analyst

Lloyds Banking Group, London, UK

09/2023 – Present

- **SIEM Platform Migration:** Overseeing the strategic process of migrating our SIEM platform from Splunk to Google SecOps. I coordinate with cross-functional teams to ensure that the migration aligns with updated security standards.
- **Cloud Security Enhancements:** Developing and implementing detection controls for Microsoft Azure and Google Cloud Platform environments, which has resulted in a 15% improvement in threat detection coverage.
- **DevSecOps Leadership:** Directing multi-platform code promotion procedures, ensuring the seamless integration of security within the software development lifecycle.
- **Innovation & Mentorship:** Leading innovation initiatives within the Chief Security Office and mentoring colleagues, contributing to a 10% improvement in overall team performance.

Cybersecurity Engineer (Intern)

Lloyds Banking Group, London, UK

05/2023-09/2023

- Assisted in enhancing the SIEM system across multiple platforms with a primary focus on Google Cloud Platform.
- Designed and implemented security controls that reduced false positives by 4% and improved monitoring capabilities.
- Awarded the Group's Innovation Challenge for significant contributions to security initiatives.

Laboratory Teaching Assistant

Abertay University of Dundee, Dundee, UK

09/2022 - 05/2023

- Assisted in delivering modules on Computer Hardware, Operating Systems, and Digital Forensics, contributing to an improvement in student performance by 8%.
- Provided support in explaining complex technical concepts, selected for this role based on academic excellence.

Education

BSc (Hons) Ethical Hacking, First Class (GPA 4.35/4.5)
Abertay University of Dundee, Dundee, UK
09/2019 – 05/2023

- **Relevant Modules:** Secure Software Development, Malware Analysis, Digital Forensics, IoT & Cloud Secure Development

Projects

SIEM Platform Migration (2025-Ongoing, Lloyds Banking Group)

- Currently leading the migration from Splunk to Google SecOps, rewriting a significant number of detection controls using YARA-L.
- Collaborating closely with cross-functional teams to review, prioritise, and refine detection controls to ensure compliance with modern security standards and effective threat mitigation.

CSO Coins Project (2025, Lloyds Banking Group)

- Led the development of a colleague reward platform, overseeing vendor engagement, design approval, manufacturing logistics, and the creation of an interactive web application for seamless user interaction.

New Ways of Working (2024, Lloyds Banking Group)

- Championed the adoption of an Agile Scrum framework to streamline legacy processes, significantly boosting team productivity and collaboration while fostering a culture of continuous improvement.

Unified Mobile Malware Analysis Framework (2022–2023, Abertay University)

- Developed a standardised methodology and pre-configured virtual machine framework for Android malware analysis optimised for Apple Silicon platforms using an ARM Kali VM.
- Earned exemplary evaluations (Grade A+) for innovation and thorough research.

Android Malware Analysis Report (2022, Abertay University)

- Established a secure environment for analysing both live and static Android malware samples, producing a comprehensive report commended for its depth and precision.

Skills

- **Programming Languages:** C++, Java, Swift, PHP, Python
- **Cloud Platforms:** AWS, Microsoft Azure, Google Cloud Platform
- **Security Tools & Platforms:** Splunk (including Splunk Cloud), Azure Sentinel, SentinelOne, Google SecOps.
- **Operating Systems & Tools:** Unix-based systems, Command Line Tools, Jenkins
- **Cybersecurity Expertise:** Malware Analysis & Reverse Engineering, Digital Forensics, Secure Software Development, DevSecOps, Web Application Penetration Testing
- **Additional:** Report Writing, Project Management

Languages

- **English:** Bilingual Proficiency
- **Russian:** Native
- **Ukrainian:** Bilingual Proficiency
- **Bulgarian:** Limited Working Proficiency

References

Available upon request