Doney Biju John

Information Systems & Cybersecurity / Technologist

Email: doneybiju@gmail.com
Phone: +370 617 92782
LinkedIn | GitHub | Portfolio

Summary

Entry-level SOC / Security Operations candidate with hands-on labs in alert triage, log analysis, and incident documentation (TryHackMe SOC L1, LetsDefend). Familiar with TCP/IP, DNS, HTTP(S), Wireshark, and Linux CLI; basic Python/SQL for investigations. Built Nmap/OpenSCAP compliance scanning and Google Workspace RBAC + audit-logging access governance automation.

Education

B.Sc. Information Systems and Cybersecurity — Vilnius University (Sep 2022 – Jan 2026 expected)

Experience

Cybersecurity Intern — Extramus 07/2025 - 10/2025 — Italy

- Supported security assessments and access reviews, documented findings and remediation actions.
- Investigated CEO-impersonation phishing and documented indicators and user impact.
- Assisted with improving security controls/policies and tracking adherence with stakeholders.
- Investigated suspicious access/events and escalated with clear incident notes and timelines.
- Contributed to security tooling evaluation and produced short recommendations based on requirements.

Cybersecurity Analyst (Forage) — TATA 05/2025 – 06/2025 — Online

- Performed SIEM-style alert triage on simulated phishing, suspicious logins, and malware indicators.
- Wrote incident documentation: impact, evidence, containment suggestions, and escalation messages.

Shuffler — Evolution 10/2024 – 06/2025 — Lithuania

- Followed strict SOPs and quality standards in a fast-paced, shift-based environment.
- Escalated issues quickly and communicated clearly in English across a multicultural team.

Projects

Google Workspace Access Governance Automation

- Automated onboarding/offboarding-style access changes; implemented RBAC logic, audit logging, and customizable notification emails.

Security Policy Compliance Checker

- Containerized scanner using Nmap/OpenSCAP; generated compliance outputs suitable for reporting.

Certificates

- Google Cybersecurity Professional Certificate: Coursera
- Zendesk Customer Service Professional: LinkedIn
- TryHackMe — SOC Level 1 Path: TryHackMe

Skills

- SOC / IR: alert triage, incident documentation, phishing analysis, escalation workflows
- Networking: TCP/IP, DNS, HTTP(S), packet analysis
- Systems: Linux CLI, Windows fundamentals
- Scripting: Python basics, SQL basics
- Tools/Concepts: vulnerability scanning basics, IDS/IPS concepts, compliance scanning (Nmap/OpenSCAP)