Vinula Kasthuriarachchi

+61404781574 vinulakas.98@gmail.com www.linkedin.com/in/vinula-kasthuriarachchi-7b3130154

Cyber Security graduate with a Master of Information Technology (Cyber Security) from the University of South Australia and a software engineering background. Practical experience in cyber risk assessment, cybersecurity governance, infrastructure security, and network segmentation through hands-on work across operational IT environments at the National Railway Museum. Strong analytical, stakeholder engagement, and problem-solving skills developed through technical project work and customer-facing roles, with a strong interest in cyber operations, governance, risk management, and infrastructure security.

Core Competencies

Governance, Risk & Compliance (GRC)

- Security posture assessments aligned to NIST CSF and ISO 27001
- Risk identification, control gap analysis, and treatment planning
- Policy, procedure, and incident response plan development
- Control mapping and traceability to business objectives
- Information privacy awareness and secure data handling principles

Risk Reporting, Data Analysis & Monitoring

- Risk assessment facilitation and mitigation planning
- Risk register documentation and control traceability
- Compliance monitoring and documentation updates
- Preparation of structured risk summaries for stakeholders
- Supporting risk awareness and training activities
- Data analysis to identify operational risk trends and anomalies
- Preparation of risk insights using structured datasets and reporting tools

Security Operations & Incident Response

- SOC alert triage and incident investigation
- Log analysis (Windows Event Logs, Sysmon, Splunk)
- Malware triage and static analysis fundamentals
- Network traffic analysis using Wireshark
- MITRE ATT&CK mapping and attack chain analysis
- Risk-based incident classification and documentation

Technical Tools & Technologies

- SIEM: Splunk
- Vulnerability Assessment: Nessus
- DFIR: Wireshark, Microsoft Sysinternals
- Cloud Platforms: Microsoft Azure, AWS
- Identity & Access: Active Directory, Microsoft Entra ID
- Endpoint Security: Microsoft Defender (basic exposure)
- Programming: Python, JavaScript, Java
- Web Technologies: ReactJS, Node.js
- Security Testing Exposure: Burp Suite, mitmproxy
- Sophos Firewall (exposure)
- Microsoft 365 Administration (basic exposure)
- Network Segmentation & VLAN Concepts
- Network Topology Mapping

Relevant Experience

Cyber Security Volunteer — National Railway Museum
03/2026 – Present
Adelaide

- Conducting cybersecurity assessments across operational IT environments, identifying risks related to network architecture, access control, infrastructure exposure, and operational dependencies.
- Developed asset inventories, software application inventories, network topology documentation, and stakeholder-friendly infrastructure diagrams across servers, NAS systems, CCTV infrastructure, workstations, and networking equipment.
- Designed a proposed segmented network architecture separating User, Server, and CCTV environments, including conceptual traffic restriction and access control logic to reduce unnecessary exposure.
- Collaborated with museum stakeholders and external service providers to support VLAN-based network segmentation planning, Sophos firewall architecture review, infrastructure validation, and implementation preparation activities.
- Assessed identity and access management practices, reviewed MFA adoption opportunities, and developed recommendations aligned with operational requirements and volunteer-based user constraints.
- Developed cybersecurity governance documentation including access management procedures, acceptable use standards, software governance controls, cybersecurity awareness material, implementation validation documentation, and cybersecurity improvement roadmaps.

Cyber Security Analyst (Capstone Project) — National Railway Museum, 02/2025 – 07/2025
University of South Australia (Obtained High Distinction) Adelaide

- Conducted structured cyber risk assessments across 6–8 operational systems, identifying 20+ risk scenarios and mapping controls to NIST CSF and ISO 27001 categories.
- Performed threat modelling to analyse attack vectors and define mitigation strategies aligned to organisational risk appetite.
- Developed governance artefacts, including an Incident Response Plan, Security Policy, and structured Risk Register.
- Contributed to a 12-month cyber security uplift roadmap by prioritising remediation initiatives based on risk impact and feasibility.
- Engaged stakeholders to translate technical risks into clear, business-aligned recommendations.

Practical Security Experience

- Achieved 120/120 accuracy in CrowdStrike Falcon Complete practical assessment.
- Performed SOC-style alert triage across enterprise-like environments, analysing logs to identify potential indicators of compromise.
- Investigated suspicious scripts, automation misuse, and simulated attack chains.
- Conducted malware static analysis and indicator identification.
- Analysed network traffic captures to identify anomalous behaviour and intrusion patterns.

Additional Professional Experience

Team Member, *Woolworths* 10/2023 – present
Acting Assistant Department Manager (5-week secondment) Adelaide, Australia

- Trusted to perform Acting Assistant Department Manager responsibilities during management leave, overseeing team coordination, task allocation, and operational decision-making in a fast-paced environment.

Software Engineering Consultant (Front-End Technologies), *Evolza* 03/2023 – 07/2023
Colombo, Sri Lanka

- Delivered technical solutions and facilitated client training sessions on system functionality and best practices.
- Collaborated with stakeholders to translate business requirements into structured technical implementations.
- Provided post-deployment support and process guidance to ensure operational stability.

Software Engineer - Intern, *Kavithi Group* 07/2022 – 01/2023
Colombo, Sri Lanka

- Primarily worked as a Front End Developer on the company's main projects, such as ERPNext and Blynxx Quizz App.

Software Engineer - Intern, *iiH Solutions (Pvt) Ltd.* 07/2020 – 07/2021
Colombo, Sri Lanka

- Primarily worked in the Front End Development team and worked on the company's main project "Infirma" for a year. The language used was ReactJS.

Customer Service Associate, *Dialog Axiata PLC* 10/2017 – 02/2018
Colombo, Sri Lanka

- Managed high-volume customer interactions in a regulated telecommunications environment.

Education

Master of Information Technology (Cyber Security), *University of South Australia* 07/2023 – 07/2025
Selected Coursework: Risk Management and Governance | Enterprise Security | Security Architecture and Engineering | Security Operations | Australian Cyber Law and Digital Evidence

BEng. (Hons) Software Engineering with Industrial Placement (Upper Second Honors), 01/2018 – 07/2022
University of Westminster

Certifications

CompTIA Security+ (In Progress)

References

Can be provided on request.