Suraj Rimal

13/234 Trower Road, Wagaman NT, 0810
M: 0476 155 697 • E: surajrimal403@gmail.com

PROFESSIONAL PROFILE

LINKEDIN

Highly skilled and results-driven Cybersecurity Officer with a proven track record of implementing robust security measures to safeguard critical digital assets and protect against evolving cyber threats. Possessing knowledge in network security, vulnerability assessment, and incident response, I am dedicated to ensuring the confidentiality, integrity, and availability of sensitive information. Adapt at collaborating with cross-functional teams, I have a reputation for effectively mitigating security risks and fostering a culture of cybersecurity awareness within organizations. With a strong ethical mindset and a commitment to continuous learning, I strive to stay at the forefront of the ever-changing cybersecurity landscape.

EDUCATION & QUALIFICATIONS

- **Diploma of Information Technology** | *Australian Catholic University, Sydney, 2016 – 2017*
- **Bachelor's in information and communication Technology** | *University of Sunshine Coast, QLD 2017 – 2019*

CERTIFICATIONS

- **Microsoft Certified: Security Operations Analyst Associate (SC-200)**
  https://learn.microsoft.com/api/credentials/share/en-gb/surajrimal-6789/E36C6C17F5D99500?sharingId=9E6C3D7C01EE2D54

- **Microsoft Certified:** Security, Compliance, and Identity Fundamentals (SC:900)
  https://www.credly.com/badges/5a7aecba-5a33-4c83-a390-5c9f82b5f4f1/public_url

- **(ISC)2: Certified in Cybersecurity**
  https://www.credly.com/badges/8f65bd84-29e2-4aca-8ee6-8d3e856fc32f/public_url

- **Currently Learning from TryHackMe and willing to pursue CompTIA security +**

TRAINING & SKILL DEVELOPMENT

Enabling your team to innovate with the Essential Eight- Attended Microsoft Webinar on 27th July 2023.

Intro to Service Management with ITIL® 4 | April 2023
- Certificate ID: ASXc0hFwASQoYIE_W3puEY6aNYzn

Completed IT Help Desk Training | *September 2020*
- *Certificate ID: AQtr2zITGe29Lw7mtFriWy5HEotR*

Completed Learning Office 365 (Microsoft 365) | *September 2020*
- *Certificate Id: AeaUf-8gnOo_v7r_1WjDDwiqU2EB*

ACS Professional Year Program | *Navitas Professional, Darwin, 2020*

LICENCES / PERMITS

Open Driving License

Working with Children

Certificate III in Individual support

Member of Australian Computer Society (ACS)

TECHNICAL SKILLS

Understanding of network protocols (TCP, IP, HTTP, HTTPS, FTP, SMTP, DNS, SSH, ICMP, IMAP etc)

Network Security (IPS/IDS, NGFW, WAF, VPNs**.)**

Operating System | Windows, Linux

Endpoint Security (Device control, Application Whitelisting/Blacklisting, MDM, EDR, XDR DF, DLP, Encryption)

Security Tools (Antivirus software, firewalls, IDS/IPS, SIEM, VPNs, Wireshark, Nessus Professional, DigiCert)

Security Information and Event Management (SIEM) |Falcon Logscale & MS Defender 365

Basic Unix/ Linux Command and regex and willing to Learn more

Cyber Threat Intelligence

Basic Digital Forensics Skills

Incident Response and Handling

Cloud Security Fundamentals

Data Loss Prevention (DLP)

Security Awareness Training

Risk Management

NON-TECHNICAL SKILLS

Continuous Learning

Critical Thinking and Problem-Solving

Communication & Collaboration

Teamwork.

Ethical Mindset

Adaptability

Hobbies

- **Participating in local cyber meetups to stay updated on industry trends and expand professional networks.**
- **Volunteering at a local community.**
- **Enjoy assisting fresh graduate with job search and guidance.**

CORE COMPETENCIES

- Proactive thinking and utilising strategic planning, analytical skills, and ability to anticipate change to implement innovative solutions and deliver exceptional customer satisfaction.
- Keen to share knowledge and transfer skills to develop capabilities of team members as well as add value to the organisation and make a difference.
- Effective oral and written communication skills to ensure clear and accurate communication and presentation to business and technical audiences, engaging corporate stakeholders from all levels.
- Operate with professionalism and integrity in all aspects of every role including conduct, appearance, compliance and working in the best interests of the client and the public.
- Dedicated to continuous learning and self-development, highly trainable and able to receive constructive criticism.
- Highly flexible and adaptable, capable of learning and developing new skills rapidly to contribute to organisational efficiency and productivity.

EMPLOYMENT HISTORY

IT Security Officer | *Charles Darwin University, NT* // May 2023 – present

- Create and manage incident tickets for each security alert or incident, documenting relevant details such as the nature of the incident, actions taken, and resolution status.
- Analyze security alerts to identify patterns, trends, and potential indicators of compromise (IOCs).
- Creating tickets and escalate the security incidents to the Tier 2 and Team Lead if needed or to different teams.
- Monitor user access logs and activities to identify any unusual or suspicious behaviour that may indicate a security incident.
- Analysing and determining malicious files and emails on sanboxie or Isolated VMware.
- Continuously monitoring, responding, and investigating security incidents and alerts generated by various security systems, such as intrusion detection/prevention systems (IDS/IPS), firewalls, anti-virus, and other security technologies.
- Use SIEM tools to collect, correlate, and analyze security event data for detecting and responding to security incidents., such as Falcon Logscale & Microsoft 365 Defender to detect potential threats or suspicious activities.
- Develop and implement incident response plans for incident such as Spam, Malware, Phishing, Ransomware, Data Theft etc.
- Responding to Cybersecurity Alerts & Advisories received from CISA, ACSC, bleeping computers etc & coordinate and assist in the remediation of identified vulnerabilities.
- Participating in SOC working groups, meetings such as Perth Joint Cyber Security Centre.
- Stay up to date with industry trends and advancements in cybersecurity.
- Staying informed about current cybersecurity threats, tactics, and procedures.
- Planning and implementing security measures that ensure the safety of data, systems and networks.
- Reviewing and managing user access privileges to systems, applications, and data to prevent unauthorized access.
- Conducting cybersecurity training sessions for employees to raise awareness about security best practices and potential threats.
- Effectively communicating security concepts and risks to non-technical stakeholders.
- Enforcing the organization's security policies and guidelines and promoting compliance among employees.
- Understanding & knowledge of Essential Eight, NIST Framework, Defence in Depth, Security principals and Concepts (CIA), Unified Cyber Kill Chain framework & MITRE ATT&CK Framework.
- Prepare regular reports for management and stakeholders.
- Document and report on security incidents, including actions taken and lessons learned.

IT SUPPORT OFFICER | *Charles Darwin University, NT* // Jan 2022 – May 2023

- Resolving client queries regarding applications and systems.
- Secured server and network devices; provided assistance in procuring orders and installing end-user devices in accordance with ICT policies and standards.
- Maintained proper documentation, review and update of relevant ICT procedures and resources on a regular basis to ensure efficient continuity of ICT processes.
- Working with a ticketing system to monitor and resolve service desk issues promptly.
- Managing access, securing systems, providing support/training to the clients, identifying the technical problem and implementing solutions.
- Proposing and documenting new ideas and solution design to improve business efficiency and client experience.
- Installed hardware in accordance with current procedures, and ensured it was operational and available for the intended use throughout the school.

ICT OFFICER | *Katherine South Primary School, NT* // August 2020 – December 2021

- Maintain, configure, and perform reliable operation of computer systems, network servers, and virtualisation, including virus protection and eradication.
- Install and upgrade computer components and software, manage virtual servers, and integrate automation processes, where required.
- Troubleshoot hardware and software errors by running diagnostics, documenting problems and resolutions, prioritising problems, and assessing impact of issues.
- Provide documentation and technical specifications to school staff for planning and implementing new or upgrades of IT infrastructure.
- Perform or delegate regular backup operations and implement appropriate processes for data protection, disaster recovery, and failover procedures.
- Lead desktop and helpdesk support efforts, ensuring all desktop applications, workstations, and related equipment problems are resolved in a timely manner with limited disruptions.
- Develop, maintain IT resources of the organisation, critical to the daily operation of the learning institution.
- Report on metrics regarding usage and performance and suggest changes and improvements for maintenance or protection.
- Perform other duties such as creation and publication of the school's online newsletter, outage management, IT training for school staff and students, re-imaging and creation of custom images.

Project:

- Successfully completed and launched an online canteen system.

SUPPORT WORKER(Part-Time) | ANGLICARE NT | March 2020 – Dec 2021

- Provide direct support and care in accordance with the client's service plan.
- Establish appropriate and effective working relationships with clients, maintaining professional boundaries always.
- Respect and support the personal preferences of clients when providing services, ensuring dignity, privacy and confidentiality always.
- Assist clients to access activities and outings that facilitate community inclusion and meet personal interest and needs.
- Monitor the client's well-being, behaviour and circumstances and report changes to the coordinator immediately.
- Complete case notes, attendance records, communication books and other administrative tasks accordingly.
- Ensuring service provision is culturally appropriate for each individual client.
- Interact and communicate with other team members.

Received Compassionate Award Certificate from Anglicare NT.

REFERENCES

Scott Beven Deputy Director ITMS-CDU *T: +61 8 8946 6712* *M: 0438 855 692* *E: scott.beven@cdu.edu.au*	**Jacqui Paull** *Business Manager-Katherine South Primary school)* *M: 043871057*	**Jess Mulkerrins** ICT Service & Experience Champion *T: 08 8946 7004* *E: jess.mulkerrins@cdu.edu.au*