ISACA-e2i Tech Talent Youth Connect

31 October 2026

JOB LISTING BOOKLET

As part of our effort to save the environment, please return this booklet at the exit after you have completed **all** interviews.

About e2i (Employment and Employability Institute)

e2i is the empowering network for workers and employers seeking employment and employability solutions. e2i serves as a bridge between workers and employers, connecting with workers to offer job security through job-matching, career guidance and skills upgrading services, and partnering employers to address their manpower needs through recruitment, training and job redesign solutions. e2i is a tripartite initiative of the National Trades Union Congress set up to support nation-wide manpower and skills upgrading initiatives. For more information, please visit www.e2i.com.sg

Content Page

#1 PRICEWATERHOUSECOOPERS RISK SERVICES 3

- 1. Cyber Simulation Associate (July 2027 Intake) 3
- 2. Cybersecurity Associate (July 2027 Intake) 4
- 3. Cybersecurity Audit and Data Protection Associate (July 2027 Intake) 5
- 4. Cybersecurity Senior Associate / Assistant Manager - Offensive Security (Security Testing Delivery) 6
- 5. Cybersecurity Testing Associate (July 2027 Intake) 8
- 6. Operational & Technology Resilience (Business Resilience) Associate (July 2027 Intake) 9
- 7. Red Team Consultant (Associate / Senior Associate / Assistant Manager) 10
- 8. Technology Risk Management Associate (July 2027 Intake) 11

#2 R2 Robotics Pte Ltd 12

- 1. Python Developer (AI-Augmented / Vibe Coder) 12

#3 Red Alpha 13

- 1. AI Engineer 14
- 2. AI Forward Deployment Engineer 14
- 3. AI Marketing 16
- 4. Cloud Engineer 17
- 5. Cybersecurity Engineer 18
- 6. Network Engineer 18
- 7. Software Engineer 19
- 8. Systems Engineer 19

 # e2i services 21

#1 PRICEWATERHOUSECOOPERS RISK SERVICES

PwC's risk services helps organisations to see and act on risk, powering growth and protecting value in a competitive business landscape.

Job Positions	Pre-requisites	Working Hours / Location
1. Cyber Simulation Associate (July 2027 Intake)	**Job Description:** • As a Cyber Simulation Associate, you will be part of a dynamic team of risk management professionals with responsibilities in supporting the team in pre-sales and delivery of cybersecurity-themed exercises to our clients. • Specific responsibilities include, but are not limited to: • Working with the team for the end-to-end conduct of cybersecurity exercises, including exercise planning, scenario development, and reporting. • Conducting current state discovery to understand the client's technology infrastructure, cyber resilience programmes, incident response plans, and scenario-specific playbooks. • Designing exercise scenarios that are relevant to and aligned with the client's specific environment and context. • Engaging relevant business, operational, technical, and management teams in preparing for the cybersecurity exercise. • Providing recommendations to the client on improvements to their existing setup and plans. • Playing a key role in supporting the team during the exercise day conduct. • Involvement in post-exercise debrief/after-action review workshops. • Developing the exercise report and providing observations and recommendations that are meaningful and relevant to the client's context. • Presenting the exercise report and key observations to the relevant stakeholders, tailoring the messages based on the audience. • Proactive support in business development activities such as bid management, proposal formulation, and client presentations, including adhering to internal risk management and compliance policies.	• 5 days • Straits View
	Job Requirement: • A degree in Computer Science, Computer Engineering, Information Technology, or a non-IT degree with a focus on cybersecurity from reputable local or international universities. • A keen interest in helping clients simulate cyber crisis scenarios through the conduct of Table-top Exercises (TTX), Command Post Exercises (CPX), and Ground Deployment Exercises (GDX). • Understanding of various cybersecurity Tactics, Techniques, and Procedures (TTPs) for different cyber threat actors. • Knowledge of cyber incident response and digital forensic investigation requirements.	

Job Positions	Pre-requisites	Working Hours / Location
	• Familiarity with the Cyber Kill Chain Methodology, MITRE ATT&CK Framework, and NIST Cybersecurity Framework (CSF). • A good team player. • Excellent communication, presentation, analytical, and organisational skills. • Ability to work on multiple concurrent projects with tight timelines and competing resources. • Advantageous to have: • Knowledge of technology systems, network and infrastructure, cybersecurity risks, and related control frameworks and practices (COCO, COSO, ISO, ITIL, CMM, COBIT, NIST, SANS, etc.). • Possession of certifications such as CISSP, GCFE, GREM, GCIA, GCIH, EnCE.	
2. Cybersecurity Associate (July 2027 Intake)	**Job Description:** • As an Associate, you'll support delivery of cybersecurity consulting and advisory engagements for clients across multiple industries. • As part of our dynamic team, your responsibilities include but are not limited to: • Support delivery of cybersecurity strategy and governance and CISO advisory related engagements • Conduct technical security assessments such as threat modelling, security architecture review • Provide advisory services related to CII risk assessments, CCoP compliance, CTM, ISO 27001, data protection and security monitoring • Take part in cloud security related engagements including cloud security architecture design, posture assessments, etc. • Support delivery of emerging tech security and risk management related services including "Security for AI" and "AI for Security" related services	• 5 days • Straits View
	Job Requirement: • Bachelor's or Master's degree in Information Technology, Computer Science, Computer Engineering, Cybersecurity, or related disciplines. • Self-motivator with good analytical and communication skills. • Comfortable working in team settings while also demonstrating the ability to quickly learn, adapt and perform effectively as an individual contributor • Strong foundation in cyber / information security concepts and exposure to widely accepted security standards and methodologies such as NIST CSF, Singapore's CTM, ISO 27001, MITRE ATT&CK, etc. • Exposure / understanding of capabilities of various cybersecurity solutions such as DLP, CNAPP, NDR, EDR, PAM, AI Guardrail solutions. • Experience with cloud platforms and workloads such as M365, AWS, Azure.	

Job Positions	Pre-requisites	Working Hours / Location
	• Having obtained at least one cybersecurity / information security related certification such as CISSP, CISA, CRISC or any other relevant certification would be advantageous. • Prior experience working in a professional services firm will be highly advantageous.	
3. Cybersecurity Audit and Data Protection Associate (July 2027 Intake)	**Job Description:** • As an Associate, your responsibilities include but are not limited to: • Collaborate with the team to deliver comprehensive cybersecurity and data protection services to clients. • Support assessments of clients' data protection practices against local regulations (such as PDPA in Singapore) and international standards (e.g., GDPR, ISO 27701, ISO27001, NIST Cybersecurity and Privacy frameworks). • Assist in performing gap analyses and compliance assessments, contributing to detailed reporting and actionable recommendations. • Assist in the planning and execution of technology and cybersecurity audits. • Collaborate with clients' teams to gather necessary audit evidence and documentation, evaluating the design and operating effectiveness of IT controls. • Identify potential risks, vulnerabilities, and areas for improvement within IT systems and processes, preparing clear and concise audit reports, including findings and recommendations for management. • Conducting compliance reviews against technology standards and regulations such as CSA Cybersecurity Codes of Practice (CSA CcoP), ISO27001, and others. • Engage with various tools and technologies used in data security, privacy management, and risk assessment, participating in cyber simulation exercises. • Collaborate across multidisciplinary teams, assisting with the establishment and uplift of data and cybersecurity measures for our clients and supporting projects aimed at enhancing clients' cybersecurity posture.	• 5 days • Straits View
	Job Requirement: • Final-year students or recent graduates in Computer Science, Computer Engineering, Information Technology, Cybersecurity, or related disciplines are encouraged to apply. • Strong fundamentals in information technology, networking principles, and cybersecurity concepts. • Basic understanding of network and cryptography principles, and data loss prevention (DLP) technologies. • Familiarity with cloud security principles and tools (e.g., Microsoft 365, AWS, Azure), common security testing tools (e.g., Kali Linux, Burp Suite, Nmap, Metasploit, Covenant, BloodHound) and database security fundamentals. • Knowledge of data privacy principles, cybersecurity frameworks, and regulations, along with understanding	

Job Positions	Pre-requisites	Working Hours / Location
	common vulnerability classes (e.g. OWASP Top 10), exploitation techniques, and defensive concepts. • Working knowledge of at least one scripting language (e.g., Python, Bash, PowerShell) – the ability to automate and adapt is a plus. • Strong analytical thinking, critical thinking, and problem-solving skills; ability to explain highly technical concepts to non-technical stakeholders. • Excellent interpersonal and communication skills. • Ability to work collaboratively in a team environment, showing initiative and eagerness to learn. • Offensive security certifications such as OSCP, CRT, CRTO, CEH, eJPT, eCPPT, or similar (or working towards them). • Genuine passion for offensive security with active participation in CTFs and contributions to open-source offensive security tools.	
4. Cybersecurity Senior Associate / Assistant Manager - Offensive Security (Security Testing Delivery)	**Job Description:** • End-to-End Security Testing Project Management & Delivery • Own and manage Security Testing engagements end-to-end from scoping, scheduling, resource allocation, execution, quality review, reporting, and closure within strict, time-sensitive deadlines. • Manage multiple concurrent projects simultaneously, ensuring adherence to SLAs, timelines, and quality benchmarks. • Develop and maintain project plans, trackers, and status dashboards for all active engagements. • Coordinate with internal teams (consultants, QA reviewers, threat intelligence) to ensure timely delivery and consistent output quality. • Conduct kick-off calls, weekly status reviews, and post-engagement debriefs with clients. • Proactively identify project risks and delays, escalate where needed, and drive resolution to keep engagements on track. • Ensure all deliverables (reports, presentations, remediation guidance) undergo quality review before client submission. • Define and continuously improve Security Testing delivery processes, templates, checklists, and methodologies for operational efficiency. • Technical Delivery & Consultancy: • Conduct vulnerability assessments and penetration testing (VAPT) across networks, web applications, mobile applications, APIs, cloud environments, and infrastructure. • Perform source code reviews when required. • Collaborate with clients and the threat intelligence team to define assessment objectives, goals, scope, and scenarios. • Simulate cyber-targeted attacks using adversary techniques, tactics, and procedures (TTPs) on client environments where red team engagements are required. • Prepare detailed reports on identified security vulnerabilities, attack paths, and actionable remediation recommendations.	• 5 days • Straits View

Job Positions	Pre-requisites	Working Hours / Location
	• Develop comprehensive and accurate reports and presentations for both technical and executive audiences. • Stay up to date on the latest cybersecurity threats, attack techniques, and industry trends. • Interface with clients to address concerns, issues, or escalations; track and drive to closure any issues that impact service delivery and client satisfaction.	
	Job Requirement: • Bachelor's degree in Computer Engineering/Science, Information Security, or a related technical discipline (or equivalent work experience). • Minimum 3 - 5 years of relevant experience in offensive security / Security Testing, preferably in a consulting or professional services environment. • Proven track record of managing multiple Security Testing projects simultaneously with tight, time-sensitive deadlines. • Hands-on experience in end-to-end engagement delivery - scoping, execution, reporting, and closure. • Experience with effort estimation, scoping, and pricing of security assessment engagements. • Certifications (Required - must have at minimum): • CREST CRT • Certifications (Preferred / Nice-to-Have): • OSCP (Offensive Security Certified Professional) • CREST CCT • GPEN, GWAPT, or equivalent • OSWE, OSED, CRTO, CRTP • PMP / PRINCE2 or equivalent project management certification • CEH (as a baseline) • Technical Skills & Experience: • Experience in at least four of the following: • Performing targeted penetration tests including vulnerability identification, exploitation, and post-exploitation across networks, web apps, APIs, mobile, and cloud. • Strong credentials in wireless, web application, and network security testing. • Setting up and operating red team / penetration testing infrastructure. • Shell scripting or automation of tasks using Python, Perl, Bash, Ruby, or PowerShell. • Thorough understanding of network protocols, data on the wire, and covert channels. • Strong understanding of Unix/Linux/Mac/Windows operating systems. • Familiarity with cloud security assessments (AWS, Azure, GCP). • Experience with compliance-driven VAPT aligned to frameworks such as PCI-DSS, ISO 27001, NIST, SOC 2, HIPAA, etc.	

Job Positions	Pre-requisites	Working Hours / Location
	• Soft Skills & Competencies: • Excellent stakeholder management and client-facing communication skills. • Ability to document and explain technical details in a concise, understandable manner to both technical and non-technical audiences. • Strong organizational and multitasking abilities - comfortable managing competing priorities under pressure. • Commercial awareness and a results-driven mindset for BD contributions. • Proficiency with project management. • Leadership qualities - ability to motivate teams and drive accountability.	
5. Cybersecurity Testing Associate (July 2027 Intake)	**Job Description:** • As an Associate, you'll be exposed to a diverse and technically challenging scope of work across. • Your responsibilities include but are not limited to: • Penetration Testing – you'll learn to identify and exploit vulnerabilities, helping clients secure their assets and protect sensitive data, all while gaining hands-on experience and growing professionally. • Red Teaming – Simulate adversary tactics, techniques, and procedures to test organizational defences, focusing on achieving specific objectives, conducting covert operations, and maintaining long-term access to compromised systems. • Cybersecurity Assessment – Assess clients' security posture through the performance of host configuration review against industry benchmarks, source code reviews, architecture review and cybersecurity risk assessment.	• 5 days • Straits View
	Job Requirement: • Final-year student or recent graduate in Computer Science, Computer Engineering, and Information Technology students from a recognized institution • Strong fundamental knowledge of information technology and cyber security • Knowledge of security testing tools (e.g. Kali Linux, Covenant, Metasploit, nmap, burp suite etc.) • Are keen to develop themselves in the profession. • Are highly motivated, enthusiastic, confident, and creative. • Critical thinking & problem solving. • Possess strong interpersonal and communication skills. • Committed to teamwork and excellence. • Knowledge of scripting programming languages (e.g. bash, python • Penetration testing specific certification such as CEH, CRT, OSCP etc. is an advantage. • Participation in CTF, publicly discovered information security flaws and acknowledged CVE, published research or tool within offensive security domain is an advantage	
	Job Description:	

Job Positions	Pre-requisites	Working Hours / Location
6. Operational & Technology Resilience (Business Resilience) Associate (July 2027 Intake)	• As an Associate, you will be working collaboratively in teams to advise clients around building resilience and sustainability by embedding measures to prevent, respond to, recover and learn from operational disruptions and incidents, with a particular focus on critical services and third parties, technology, data, premises and people. Your core responsibilities will include: • Help our clients develop and implement operational and technology resilience policies, frameworks and standards • Deliver operational and technology resilience reviews (including Business Continuity Management and Disaster Recovery) to assess current state and develop a strategic improvement roadmap • Work with our clients to develop and uplift end-to-end resilience / BCM programmes, from the initial risk assessment and threat/scenario analysis, to business impact assessment, to policy and framework development and the building of playbooks, etc. • Develop and/or implement integrated crisis management structure, protocols and plans to help clients streamline their crisis management process. • Support training exercises to equip organizations with the knowledge to manage their resilience risks and operate their resilience/BCM frameworks. • Work with clients on business continuity and crisis management exercises to help clients validate their resilience capabilities. • Support or lead (where applicable) project workstreams, drawing on your knowledge and experience to support your teammates through knowledge sharing and providing on-the-job coaching where possible.	• 5 days • Straits View
	Job Requirement: • Open to final-year students, fresh graduates, and candidates with up to 2 years of relevant experience in Engineering, Business, Economics, Science, or related disciplines. • 0-2 years of experience working in one or more of the following disciplines: operational and/or technology risk & resilience, business continuity management, disaster recovery planning, technology risk management, or regulatory compliance. The seniority of the candidate commensurate with years of relevant experience and skillset. • Good interpersonal and communication skills, with significant experience in managing complex engagements and stakeholders; business development experience is a plus. • Understanding of resilience and business continuity best practices and protocols, including knowledge of local (e.g. MAS Revised BCM Guidelines) and international BCM standards (e.g. ISO 22301, SS540, EU DORA). • Experience in planning, designing and conducting Table Top Exercises and other business/technology resilience exercises would be beneficial.	

Job Positions	Pre-requisites	Working Hours / Location
	• Associate-level certification in one or more areas of resilience / BCM / DR from a recognised institution such as the Business Continuity Institute (BCI), ABCP, ACRP, etc. would be beneficial.	
7. Red Team Consultant (Associate / Senior Associate / Assistant Manager)	**Job Description:** • We are looking for an experienced offensive security professional to take on a role in delivering end-to-end Security Testing engagements (Red Teaming, Purple Teaming, BAS, Penetration Testing, Cloud Security, AI Security etc.) while contributing to business development efforts. • The ideal candidate combines strong technical expertise in security assessments with proven project management capabilities. • This role sits within our Technology Risk Services practice, where the team helps organizations analyze and strengthen the security posture of their information technology systems and environments. • Red Team consultant should have hands-on experience in offensive security operations along with a solid understanding of attacker tactics, techniques, and procedures (TTPs). • This role combines offensive security expertise with strong communication skills to work closely with blue teams to strengthen monitoring, detection, and response capabilities. • Emulate real-world threat actors and their behaviour through tactics, techniques and procedures (TTPs) on clients' environment. • Conduct purple team exercises in collaboration with blue team to assess detections, improve logging coverage, and enhance response processes. • Use frameworks such as MITRE ATT&CK to map adversary techniques. • Work with PwC's threat intelligence team to support attack simulation/emulations operations. Develop custom tools, payloads and automation scripts to support engagements where appropriate. • Stay updated with emerging threats, adversary tradecraft, and offensive security techniques. • Conducting vulnerability assessment and penetration testing (VAPT) and source code review when required. • Deal with clients to address concerns, issues or escalations; track and drive to closure any issues that impact the service and its value to clients. • Develop comprehensive and accurate reports and presentations for both technical and executive audiences **Job Requirement:** • Bachelor's degree in a technical discipline (or equivalent work experience) • 1-5 years of relevant offensive security experience (depending on the grade A/SA/AM) • Experience in consulting or client-facing cybersecurity roles	• 5 days • Straits View

Job Positions	Pre-requisites	Working Hours / Location
	• Ability to write clear technical documentation and deliver findings to clients or internal stakeholders • Knowledge of detection engineering, hypothesis driven threat hunting, and SOC workflows • Familiarity with adversary emulation plans and intelligence-driven testing • Experience with CI/CD security, container security, and cloud-native environments. • Understanding of malware analysis, reverse engineering, or exploit development is a plus • Minimally possess OSCP / CREST CRT certifications • Candidates with relevant certifications such as OSCP, OSEP, CRTO, CRTE, OSED, CREST CRT/CCT, CARTP/CARTE, Azure/AWS security certifications are preferred	
8. Technology Risk Management Associate (July 2027 Intake)	**Job Description:** • As an Associate, your responsibilities include but are not limited to: • Execute audits and assessments on cybersecurity, IT systems and infrastructure and processes • Collaborate with stakeholders such as clients and managers to identify opportunities to improve their key controls across cybersecurity, business and technology processes • Provide assurance and advisory related services through all major milestones of the sales and delivery lifecycles including identification, proposal development, planning, fieldwork, reporting and debrief processes • Work on specific projects to substantially improve and evolve the capability and quality of the processes, deliverables and thought leadership • Provide coaching and/or conduct training to junior staff to develop communication, analytical and technical skills	• 5 days • Straits View
	Job Requirement: • Final-year students or graduates in Business, Engineering, Computer Science, Information Technology (IT), or a related discipline with an IT focus. • Candidates with IT Audit, Risk, or Controls experience are preferred.. • Demonstrated track record in leading engagements within a professional services or consulting environment, combined with ability to work in teams effectively • Strong verbal and written communication skills • Good presentation skills, both oral and written • Able to work in a fast-paced environment • Good analytical, organizational, and conceptual skills • Excellent soft skills and able to manage stakeholders across multiple disciplines • Excellent project management skills and a demonstrated ability to follow through and complete tasks within tight deadlines	

Job Positions	Pre-requisites	Working Hours / Location
	• Experience in management and/or assessment of adequacy of controls over technology activities at financial institutions is preferred. • Familiar with regulatory requirements such as MAS Notices and Guidelines related to technology, cyber security and outsourcing risk management etc. is a plus • Experience in cybersecurity processes such as vulnerability and threat management, patch management and identity and access management is a plus • Ability to provide recommendations, approaches and good industry practices • Experience in providing regular communication and preparing reports and presentations for clients and senior stakeholders • Good interpersonal skills to successfully interact with internal and external stakeholders such as clients, managers and team members • CISA, CISM, CISSP, PMP or other professional certification is preferred	

#2 R2 Robotics Pte Ltd

R2 Robotics focuses on AI-driven robotics, caregiving solutions, and commercialized automation systems across the Asia-Pacific region (including Singapore, Malaysia, and Australia).

Job Positions	Pre-requisites	Working Hours / Location
1. Python Developer (AI-Augmented / Vibe Coder)	**Job Description:** • Rapid Prototyping: Turn product requirements and "vibes" into working Python applications quickly. Iterate fast, but flag security-sensitive areas before shipping. • AI-Assisted Development: Use AI coding assistants (Cursor, Copilot, etc.) to generate boilerplate, refactor, and debug—while reviewing generated code for insecure defaults, hardcoded secrets, injection risks, and broken auth logic. • Secure Coding Fundamentals: Apply secure coding practices: input validation, output encoding, parameterized queries, proper error handling, least privilege, and safe secrets management. • API & Integration Security: Integrate third-party services and LLM APIs safely—manage API keys via environment variables/secret managers, validate external inputs, and avoid leaking sensitive data in logs or prompts. • Software Fundamentals: Write clean, modular, maintainable code. Understand data structures, algorithms, and design patterns—even when AI helps write them. • Debugging & Verification: Use AI to find bugs, but rely on your fundamentals to verify fixes and ensure they don't introduce security regressions. • Dependency & Supply Chain Awareness: Keep dependencies updated, review package sources, and avoid blindly accepting AI-suggested libraries or install commands.	• Mon to Fri • Paya Lebar

Job Positions	Pre-requisites	Working Hours / Location
	• Collaboration: Work with product and design to ship fast, and with engineering to ensure prototypes don't become insecure production systems.	
	Job Requirement: • Python Proficiency: Solid grasp of Python syntax, data types, control flow, and standard library. • Software Development Fundamentals: • OOP and functional programming concepts. • Git version control (non-negotiable). • Virtual environments and dependency management (venv, poetry, pip). • Basic testing (pytest/unittest) and why it matters. • Security Fundamentals (Required): • Secure coding basics: input validation, output encoding, avoiding injection (SQL/command/template), safe deserialization. • Authentication & authorization basics: sessions, tokens, password hashing (e.g., bcrypt/argon2), least privilege. • Secrets management: no hardcoded keys; use .env, environment variables, or secret managers. • OWASP awareness: familiar with OWASP Top 10 and common web vulnerabilities (XSS, CSRF, SSRF, IDOR, etc.). • Dependency hygiene: understand risks of untrusted packages and outdated dependencies. • AI-specific security awareness: recognize that LLM-generated code may contain insecure patterns, hallucinated packages, or leaked secrets; verify before committing. • The "Vibe Coding" Skillset: • AI literacy: effective prompting to get valid, safe code—not hallucinated nonsense. • Code reading: spot errors, insecure defaults, and vulnerabilities in AI-generated code. • Tool mastery: AI-first IDEs (e.g., Cursor) or plugins (GitHub Copilot). • Web Frameworks: Experience with at least one Python web framework (e.g., FastAPI, Flask, or Django). • APIs: Experience consuming and building RESTful APIs with basic auth and input validation.	

#3 Red Alpha

At Red Alpha, we believe that building a successful technology career takes more than just technical training—it requires the right guidance, practical experience, and a clear career pathway. That's why we've developed our Select – Train – Deploy model, which provides a structured progression from learning to employment.

Whether you're a fresh graduate looking to kick-start your career, an IT professional seeking to deepen your expertise, or someone considering a mid-career switch into technology, our programmes are designed to equip you with in-demand skills across our 6 different technology domains.

Job Positions	Pre-requisites	Working Hours / Location
1. AI Engineer	**Job Description:** • Red Alpha Cybersecurity is hiring AI Engineers who are eager to analyse data, build intelligent systems, and apply AI techniques to real operational challenges through our Digital Specialist Training Programme (DSTP), a structured and fully sponsored pathway. • Whether you're starting out or transitioning into tech, Red Alpha guides you through hands-on training in model development, machine learning, and practical AI application, with deployment into meaningful AI or data-focused roles. • What You'll Be Doing: • Build and fine-tune machine learning models including LLMs, classification, and vision models • Work with foundation models and AI frameworks such as Hugging Face and Ollama Deploy and serve models using vLLM, Nvidia Triton, NIM, and AWS SageMaker Design and query databases using SQL, PostgreSQL, and MongoDB • Perform 1D and 2D data analysis to derive actionable insights • Manage cloud infrastructure on AWS and containerised environments • Apply responsible AI practices and optimise models for production environments • Monitor, integrate, and maintain AI systems across enterprise deployments. **Job Requirement:** • Singapore Citizen or Permanent Resident • No prior experience or degree required • Strong aptitude and passion for the relevant field • Logical and analytical thinking ability	• Mon to Fri • 9am to 6pm • Client-based (deployment)
2. AI Forward Deployment Engineer	**Job Description:** • As a Forward Deployed Engineer (FDE), you will work directly with customers to understand their problems, design the right technical solution, build the critical pieces, deploy them into real environments, and stay accountable until the solution is reliable and usable. • This is a hands-on role across software, data, AI, infrastructure and customer delivery. • What you will own: • Discover, Design & Build Lead technical discovery to understand customer workflows, constraints, data, security boundaries and success criteria • Translate customer problems into technical requirements, acceptance criteria and implementation plans • Design and build production solutions across Python, APIs, backend services, databases, data pipelines and AI-enabled workflows • Make practical architecture trade-offs based on the customer's environment and operational needs • Deploy solutions securely using Docker, CI/CD and cloud infrastructure	• Mon to Fri • 9am to 6pm • Client-based (deployment)

Job Positions	Pre-requisites	Working Hours / Location
	• Work with IAM, networking, monitoring and Infrastructure-as-Code • Troubleshoot real-world production issues and drive them through to resolution • Build with security, observability, rollback and recovery in mind • Run technical discovery sessions, demos, architecture reviews and implementation discussions • Explain technical decisions and trade-offs clearly to technical and non-technical stakeholders • Challenge assumptions respectfully and surface risks early • Keep customers informed and build trust through technical credibility and ownership • Take responsibility beyond ""the code is done" • Harden deployments and resolve remaining issues before handoff • Produce architecture diagrams, documentation and operator runbooks • Ensure customers can understand, operate and recover the solution • Share lessons learned and raise delivery standards across the team	
	Job Requirement: • 4–6 years of hands-on experience across software engineering, backend/platform engineering, data engineering, cloud/infrastructure, solutions engineering or similar • No prior experience or degree required • Proven experience that you can build, reason, communicate and deliver in production • Strong Python and backend engineering fundamentals, including APIs, authentication, testing, error handling and production debugging • Practical experience with SQL and data, including databases, data modelling and ingestion/ETL/ELT Production experience with Docker and cloud environments • Familiarity with Kubernetes, IAM/networking, CI/CD, observability and Terraform or comparable IaC is a strong advantage • Working knowledge of AI/LLM systems, including RAG, tools/agents, evaluations, data access and monitoring • Strong customer-facing instincts and the ability to lead technical conversations and explain trade-offs clearly • High ownership with good judgment around security, access controls, change management and operational safety • Strong engineering judgment, breadth, curiosity and the ability to learn quickly • Comfortable with ambiguity and can turn unclear requirements into assumptions, acceptance criteria and a plan • Stay calm when things break and bring structure to complex problems • Singapore Citizen or Permanent Resident	

Job Positions	Pre-requisites	Working Hours / Location
	• Strong aptitude and passion for the relevant field • Logical and analytical thinking ability	
3. AI Marketing	**Job Description:** • Don't just use AI, build with it. And, become Singapore's next AI Marketer! • Red Alpha, in partnership with Nas.com, is launching a new AI Marketer programme designed to bridge marketing expertise with technical AI capabilities. • We are looking for marketing professionals who want to go beyond using AI tools and learn to build, deploy and own AI-powered marketing systems. • The role begins with a structured, full-time 12-week training programme that takes you from a non-technical starting point to building real automations, integrations and AI workflows. • After training, you'll work across marketing, technology and AI, identifying opportunities to automate repetitive work, improve marketing operations and build systems that deliver measurable business value. • What You'll Do: Understand & Improve Marketing Operations • Map how marketing works across CRM, lifecycle/email, CMS, analytics, advertising platforms and internal data • Identify repetitive work, bottlenecks and opportunities where automation or AI can create value Turn these opportunities into a practical roadmap with clear business outcomes • Build AI & Automation Systems • Build workflows that connect marketing platforms through APIs, webhooks and scheduled jobs Work with SQL and Python to clean, transform and move marketing data reliably • Build AI-powered workflows using LLMs, RAG, tool calling and agentic workflows • Add appropriate human review, approval gates and safeguards where needed • Make Systems Reliable Test and evaluate AI systems using real-world examples and clear quality criteria • Add monitoring, logging, error handling, retries and fallbacks Deploy, document and hand over systems that other people can confidently use • Work With the Business Partner with marketing and business stakeholders to understand problems and define success • Explain what you've built and demonstrate the business impact • Own projects from idea → build → deployment → results **Job Requirement:** • 2–5 years of marketing experience in marketing, growth, lifecycle/CRM, content, performance or marketing operations • No coding experience required. • We'll teach you the technical skills through structured training and AI-assisted development tools • Comfortable learning new technology and working with spreadsheets, platforms, data and systems	• Mon to Fri • 9am to 6pm • Client-based (deployment)

Job Positions	Pre-requisites	Working Hours / Location
	• Strong problem-solving skills: you can break messy problems into steps, test assumptions and persist through debugging • Curious about AI and how it actually works • Strong communication and ownership: you can work with stakeholders and take a project from idea through to something people depend on • We care more about your marketing experience, curiosity and ability to learn than your technical background. • Nice to Have Any of the following is a plus, but not required: Experience administering CRM, marketing automation, CMS, analytics or advertising platforms Spreadsheet formulas, SQL or Python Zapier Make or other automation tools • Personal AI or automation projects Experience experimenting with AI coding assistants or LLM tools • Your First 12 Weeks: You'll go through a structured, build-first programme across Red Alphaand Nas.com: • Weeks 1–4: Technical Foundations Programming, AI-assisted coding, APIs, integrations, databases, SQL and data automation • Weeks 5–7: AI & Marketing LLM applications, RAG, evaluation, marketing operations and the systems behind modern marketing • Weeks 8–10: Build & Deploy AI workflows, automation engineering, production reliability and deployment • Weeks 11–12: Real-World Deployment Identify a high-value marketing problem, build a solution, deploy it, measure the results and hand it over to the business • Singapore Citizen or Permanent Resident • No prior experience or degree required • Strong aptitude and passion for the relevant field • Logical and analytical thinking ability	
4. Cloud Engineer	**Job Description:** • Red Alpha Cybersecurity is hiring Cloud DevOps Engineers who are eager to architect, deploy, and manage cloud environments through our Digital Specialist Training Programme (DSTP), a structured and fully sponsored pathway. • Whether you're new to the field or making a career switch, Red Alpha provides hands-on training with cloud platforms, automation, and infrastructure fundamentals, with deployment into meaningful cloud or infrastructure roles.: • Design and deploy cloud infrastructure on AWS and Azure Implement CI/CD pipelines and GitOps workflows using FluxCD • Build and manage containerised environments using Docker and Kubernetes • Write automation scripts in Python and Bash Provision and manage infrastructure as code using Terraform, CloudFormation, and Ansible • Manage project workflows using Jira, Confluence, and Agile planning tools	• Mon to Fri • 9am to 6pm • Client-based (deployment)

Job Positions	Pre-requisites	Working Hours / Location
	• Implement DevSecOps practices and security management across cloud environments Monitor and maintain system observability using the Elastic Stack **Job Requirement:** • Singapore Citizen or Permanent Resident • No prior experience or degree required • Strong aptitude and passion for the relevant field • Logical and analytical thinking ability	
5. Cybersecurity Engineer	**Job Description:** • Red Alpha Cybersecurity is hiring Cybersecurity Specialists who are eager to launch their career in cybersecurity through our Alpha Specialist Training Programme (ASTP), a structured and fully sponsored pathway. • Whether you're a fresh graduate or making a career switch, Red Alpha equips you with practical skills, industry-recognised certifications, and deployment into meaningful cybersecurity roles. What You'll Be Doing: • Undergo hands-on training in cyber defence, incident response, threat intelligence, and offensive security • Work across both public and private sector cybersecurity roles upon deployment Apply skills in penetration testing, threat hunting, security operations, and incident response • Support security engineering, GRC, and SOC functions depending on placement • Collaborate with teams on security architecture and red team operations • Conduct vulnerability assessments and digital forensics investigations • Perform malware analysis and reverse engineering • Develop and present strategic security reports to stakeholders **Job Requirement:** • Singapore Citizen or Permanent Resident • No prior experience or degree required • Strong aptitude and passion for the relevant field • Logical and analytical thinking ability	• Mon to Fri • 9am to 6pm • Client-based (deployment)
6. Network Engineer	**Job Description:** • Red Alpha Cybersecurity is hiring Full Stack Infra Engineer who are eager to design, implement, and maintain robust and secure infrastructure across LAN, WAN, and cloud environments. • You'll be involved in both project-based work and the daily operations of mission-critical systems, with opportunities to grow into advanced roles across networking, infrastructure, and cybersecurity. • What You'll Be Doing: Design, implement, and maintain LAN, WAN, WLAN, VPN, and firewall systems • Configure and deploy network appliances, routers, switches, and load balancers (e.g. Cisco, Fortinet) • Conduct vulnerability assessments and support remediation across network layers	• Mon to Fri • 9am to 6pm • Client-based (deployment)

Job Positions	Pre-requisites	Working Hours / Location
	• Troubleshoot network performance issues and ensure minimal downtime • Work closely with clients and teams to generate system specs and present architecture solutions • Plan, execute, and monitor IT infrastructure setup and upgrades (on-prem and virtualised) • Manage and maintain Windows, Unix/Linux servers, virtual machines, and databases (e.g. SQL Server, Oracle) Perform routine preventive maintenance and respond promptly to system alerts and issues • Support operational systems to meet SLA requirements • Participate in change management, disaster recovery, and patch management processes	
	Job Requirement: • Singapore Citizen or Permanent Resident • No prior experience or degree required • Strong aptitude and passion for the relevant field • Logical and analytical thinking ability	
7. Software Engineer	**Job Description:** • Red Alpha Cybersecurity is hiring Software Engineers who are eager to design, build, and test applications through our Digital Specialist Training Programme (DSTP), a structured and fully sponsored pathway. • Whether you're a fresh graduate or making a career switch, Red Alpha equips you with practical coding experience, engineering best practices, and industry-relevant skills, with deployment into software development roles. • What You'll Be Doing: • Develop applications using Java and C++ fundamentals Build frontend interfaces using HTML, CSS, JavaScript, and React.js • Develop backend services using Python and Node.js Write shell scripts and work within Linux environments • Containerise and deploy applications using Docker • Apply secure programming practices across the software development lifecycle Leverage AI tools to enhance software development workflows • Collaborate with teams on real-world software engineering projects	• Mon to Fri • 9am to 6pm • Client-based (deployment)
	Job Requirement: • Singapore Citizen or Permanent Resident • No prior experience or degree required • Strong aptitude and passion for the relevant field • Logical and analytical thinking ability	
8. Systems Engineer	**Job Description:** • Red Alpha Cybersecurity is hiring Full Stack Infra Engineer who are eager to design, implement, and maintain robust and secure infrastructure across LAN, WAN, and cloud environments. • You'll be involved in both project-based work and the daily operations of mission-critical systems, with opportunities to	• Mon to Fri • 9am to 6pm • Client-based (deployment)

Job Positions	Pre-requisites	Working Hours / Location
	grow into advanced roles across networking, infrastructure, and cybersecurity. • What You'll Be Doing: Design, implement, and maintain LAN, WAN, WLAN, VPN, and firewall systems • Configure and deploy network appliances, routers, switches, and load balancers (e.g. Cisco, Fortinet) • Conduct vulnerability assessments and support remediation across network layers • Troubleshoot network performance issues and ensure minimal downtime • Work closely with clients and teams to generate system specs and present architecture solutions • Plan, execute, and monitor IT infrastructure setup and upgrades (on-prem and virtualised) • Manage and maintain Windows, Unix/Linux servers, virtual machines, and databases (e.g. SQL Server, Oracle) • Perform routine preventive maintenance and respond promptly to system alerts and issues • Support operational systems to meet SLA requirements • Participate in change management, disaster recovery, and patch management processes	
	Job Requirement: • Singapore Citizen or Permanent Resident • No prior experience or degree required • Strong aptitude and passion for the relevant field • Logical and analytical thinking ability	

e2i services

e2i Services

- Career Coaching & Job Matching
- SkillsFuture Advice

• For Career Coaching

Are you at a career crossroad? Engage a career coach to nurture your career and be well-equipped with newfound skills as you embark on a new career or navigate a career change.

You can also reach them at the following centres (By appointment only):

e2i Career Centre (DNI)

Devan Nair Institute
for Employment and Employability
80 Jurong East St 21 Level 2
Singapore 609607

Operating Hours (DNI)

Mondays: 2:30pm – 5:00pm
Tuesdays – Fridays: 9:00am – 5:00pm
Saturdays: 9:00am – 1:00pm

Nearest MRT: Jurong East

e2i Career Centre (OMB)

1 Marina Boulevard,
#B1-03
Singapore 018989

Operating Hours (OMB)

Mondays: 2:30pm – 5:00pm
Tuesdays – Fridays: 9:00am – 5:00pm
Saturdays: 9:00am – 1:00pm

Nearest MRT: Raffles Place, Downtown

e2i Career Centre (OTH)

ServiceSG Centre Our Tampines Hub,
1 Tampines Walk,
#01-21
Singapore 528523

Operating Hours (OTH)

Mondays: 2:30pm – 5:00pm
Tuesdays – Fridays: 9:00am – 5:00pm
Saturdays: 9:00am – 1:00pm

Nearest MRT: Tampines

Jobs and Skills Centre

Locations	Address	Operating Hours* (With effect from 1 September 2023)
Bishan Community Club	Level 1, Reading Room	Mondays: Closed Tuesdays to Fridays: 10am to 5.30pm

Locations	Address	Operating Hours* (With effect from 1 September 2023)
	51 Bishan Street 13, S(579799)	Saturdays: 10am to 2pm Sundays and Public Holidays: Closed
Ci Yuan Community Club	Level 4, Multi-Purpose Room 5, 51 Hougang Avenue 9, S(538776)	Mondays, Tuesdays, Thursdays & Fridays: 10am to 5.30pm Wednesdays: Closed Saturdays: 10am to 2pm Sundays and Public Holidays: Closed
Clementi Community Centre	Room 01-06, 220 Clementi Avenue 4, S(129880)	Mondays, Wednesdays and Fridays: 10am to 5.30pm (Virtual/Phone Coaching) Thursdays: 10am-5.30pm (Face-to-Face Coaching) Tuesdays: Closed Saturdays, Sundays and Public Holidays: Closed
The Frontier Community Club	Level 2 Room 205, 60 Jurong West Central 3, S(648346)	Mondays, Tuesdays, Thursdays & Fridays: 10am to 5.30pm Wednesdays: Closed Saturdays: 10am to 2pm Sundays and Public Holidays: Closed
Social Service Office @ Bukit Merah	3779 Jalan Bukit Merah, #01-01, S(159462)	Mondays to Fridays: 9am to 5pm Saturdays, Sundays and Public Holidays: Closed
Social Service Office @ Queenstown	40 Margaret Drive, #02-01, S(140040)	Mondays to Fridays: 9am to 5pm Saturdays, Sundays and Public Holidays: Closed
Teck Ghee Community Club	861 Ang Mo Kio Avenue 10, #02-03, S(569 734)	Mondays, Wednesdays to Fridays: 10am to 5.30pm Tuesdays: Closed Saturdays: 10am to 2pm Sundays and Public Holidays: Closed

Locations	Address	Operating Hours* (With effect from 1 September 2023)
Toa Payoh West Community Club	Level 3, Music Room 1, 200 Lorong 2 Toa Payoh, S(319642)	Mondays to Thursdays: 10am to 5.30pm Fridays: Closed Saturdays: 10am to 2pm Sundays and Public Holidays: Closed
Yew Tee Community Club	20 Choa Chu Kang St 52, #03-05, S(689286)	Mondays to Wednesdays, Fridays: 10am to 5.30pm Thursdays: Closed Saturdays: 10am to 2pm Sundays and Public Holidays: Closed

The following centres are supported by a job kiosk where you can explore career resources virtually.

Locations	Address	Operating Hours*
Clementi Community Centre KIOSK	Level 1, 220 Clementi Avenue 4, S(129880)	Mondays to Fridays: 10am to 5.30pm Saturdays: 10am to 2pm Sundays and Public Holidays: Closed
Hong Kah North Community Club KIOSK	Level 1, 30 Bukit Batok Street 31, S(659440)	
Whampoa Community Club KIOSK	Level 1, 300 Whampoa Drive, S(327737)	
Yuhua Community Club KIOSK	Level 1, 90 Boon Lay Way, S(609958)	

NTUC Job Security Council's Telegram Channels

Be alerted daily on the latest job vacancies from hiring companies. Subscribe to JSC Telegram channels today! If you don't have Telegram, get more info on how to download the app at https://telegram.org/

Jobs Alert for PMET
e.g. Engineers, Managers, Executives, Technicians

Join Our Telegram
https://www.e2i.com.sg/JSCTelegram/PMET

Jobs Alert for non-PMET
e.g. Temp jobs, operators, packers, etc

Join Our Telegram
https://www.e2i.com.sg/JSCTelegram/Non-PMET