Position Description

Job Title

Senior Cyber Engineer
Permanent Full Time

Location

This role supports flexible working arrangements, including a hybrid model with the option to work from both the office and home. Candidates from **Western Australia** and **South Australia** are especially encouraged to apply.

Key Purpose

The Senior Cyber Engineer is responsible for providing technical leadership to our support team and delivering Identity technical solutions in conjunction with senior consultants and Directors.

About Us

We are a leading implementation partner specialising in Identity and Access Management, Privileged Access Management, and Identity Governance. We are a forward-thinking team of cybersecurity professionals driven by the desire to secure all apps and users.

We help businesses secure their environments by using modern tools, expert knowledge and a pragmatic approach.

We are rapidly becoming SA's best-known IAM provider and are a trusted partner to our clients in Adelaide and across the country. Our reputation is built on being knowledgeable, highly experienced, effective and reliable.

Our team is everything. Hand-picked, high performing, driven and as smart as they come.

- We have grown since rapidly since 2019 and we will continue to attract the A-grade talent we need to grow and be the best.
- We have customised training plans to meet our people's needs whilst enhancing the capability of our business.
- We have fun and get the job done.
- We mentor and vet our staff to grow them into autonomous stars.
- We will help you achieve your professional goals and grow into being an IAM expert.

We are always looking for awesome, talented people to join our A-grade team.

About You

You will be responsible for delivering specialised Identity Security consultancy services to a number of our valued clients.

This will include a mixture of complex technical work, strategy and project planning, and mentoring and leading more junior staff. You will have exceptional customer engagement skills, and a passion for complex problem solving. You will be a critical thinker with a strong technical acumen. Familiarity with the identity security domain is vital. We are looking for experience with IGA, IAM, and PAM systems and principles.

We work heavily with IAM platforms including - Okta, Entra, SailPoint, Saviynt, CyberArk, Delinea, SilverFort and CrowdStrike and experience in some of these technologies is a must. Importantly, the concepts that these platforms support – Zero Trust Architecture, password management, MFA, SSO, contextual access, risk-based auth, roles, HR as a master, automated provisioning and privileged management must be well understood.

Strong recent experience with Active Directory, AAD, AAD Connect and m365, device management and device authentication is essential.

Identity systems connect with everything, so understanding IAM in a larger digital context is crucial. Experience with any of the following is necessary - SIEMs, SAP, SuccessFactors, Workday and ServiceNow.

Communication is key. You will need to manage expectations of our customers autonomously, including the ability to engage with a range of stakeholders and explain complex ideas clearly and effectively.

Your written communication skills must be on-point, as a large part of this role will communicating those complex ideas in documents including architecture, technical designs, strategies, options analysis, presentations and tender responses.

Key Responsibilities and Outcomes

The Senior Cyber Engineer is responsible for delivering quality solutions and support to clients:

1. Proactively engaging with key external stakeholders and Subject Matter Experts (SMEs) to understand their requirements, business direction and technical landscape.
2. Evaluating new technologies and solutions in consultation with key vendors.
3. Managing client relationships at an operational level. You won't be expected to manage contracts, but you will be required to maintain relationships. Particular emphasis is on communicating with stakeholders as to the status of requests in a timely and professional manner.
4. Generating high quality documents and diagrams including requirements and design documents, architecture diagrams and models, test plans, detailed test cases, as-built, risk assessments, implementations, and project plans.
5. Performing system configuration, functional and integration testing, and deploy solutions.
6. Providing technical support to clients and maintenance of deployed technologies.
7. Reporting on progress, billable hours and deliverables including weekly time writing.
8. Working autonomously to troubleshoot complex technical issues and report on resolution.
9. Identifying existing and potential issues and design matters in overall system and solution architecture.
10. Assisting with completing tender documents for prospective clients.
11. Providing leadership and work guidance to less experienced personnel.
12. Assisting in other duties as given by the Directors and Identifly senior staff.
13. Delivering client outcomes with high quality and according to timelines.
14. Interacting with clients, suppliers and other employees professionally at all times.

Team Leadership

Team Leaders will be responsible for the following capabilities for their direct reports:

1. Providing leadership and mentoring.
2. Accountable for leave management.
3. Managing staff performance reviews.
4. Accountable for work assignment.
5. Developing training plans.
6. Dealing with other HR matters as they arise.
7. Contributing to company goals.

Working Relationships

This role will work closely with internal and external key stakeholders to understand the business and technical needs of our clients, including the deployment and maintenance of technology solutions for our clients.

This role will work closely with clients, Project Managers, Security Managers, IT Managers, Technical SMEs and Security resources to deliver complete solutions for our clients including decisions around appropriate technologies to use.

Skills and Experience

Experience

- 15+ years IT experience.
- 7+ years in Identity/Security or Infrastructure domains.
- Knowledge and experience working with IDaaS solutions (Okta and Entra).
- Knowledge and experience working with PAM solutions (CyberArk and Delinea).
- Expert knowledge of IAM domains (Access, Authentication, Provisioning, Governance).
- Knowledge of authentication, password management, MFA, SSO and adaptive security.
- Knowledge of Cyber Security Frameworks and Best Practices (NIST, SACSF) (desirable).
- 5+ years of customer facing role, dealing with internal or externals customers regularly.
- Must have a proven track record of successfully engaging with stakeholders.
- Nice to have SIEM, M365, Ping, Forgerock, SuccessFactors, WorkDay, PeopleSoft, NetIQ, ServiceNow.
- Experience with JIRA and agile delivery frameworks.

Skills

- Ability to quickly communicate complex ideas around a technical topic, ideally on the fly on a whiteboard.
- Excellent analytical skills, and ability to engage with a range of stakeholders to understand requirements.
- Excellent written skills with a proven track record of delivering complex and detailed design documents.
- Ability to identify security risks and issues with current or designed deployments.
- Access management hands on technical experience (Okta, Azure, Ping, SailPoint).
- Hands on technical experience with Privileged Access Management (CyberArk, Delinea).
- Hands on technical experience with Identity Governance and Administration (IGA) platforms (SailPoint, Saviynt).
- Skills or at least an understanding of Public cloud management (Azure, AWS, Google).
- Automating solutions and migrations using scripting (PowerShell, Python, Java, JS, SQL etc.).
- System administration skills and understanding of Active Directory, LDAP, RADIUS and ADFS (desirable).
- Integration methods such as API, web-services, database connections, SCIM.
- Professional and effective client liaison.
- Strong verbal and written communication.
- Excellent personal presentation.
- Excellent time management and prioritisation of tasks.
- Ability to work in a dynamic team environment or autonomously.
- Outstanding attention to detail.
- Leadership skills with experience in managing and developing diverse teams.
- Experience in leading collaborative and high-performance work environment.
- Strong track record of setting and achieving team goals, conducting performance reviews, and mentoring team members.

Performance Goals

ID	KPI	Metric		
1	Deliver client outcomes with high quality and according to agreed timelines.	1.	Delivered within agreed timeframe 100% of the time unless variance agreed.	
		2.	Feedback provided to Identifly only reflects high quality performance.	
		3.	All project outcomes met, for all projects.	
2	Complete assigned work with < 5% variance on estimates.	1.	Tracked hours are aligned with agreed estimates and do not exceed more than 5% of estimates.	
3	Manage relationships with clients, suppliers and other employees professionally at all times.	1	No substantiated complaints received from Clients, Suppliers and other Employees.	
		2	Feedback provided to Identifly only reflects high quality performance.	
		3	All feedback provided by Client, Supplier, and other Employees reflects positive professionalism.	
4	100% of your worktime will be accountable as per the following metrics. *Exceptions will be made including learning and training, events and leave.*	1	Client Billable between 85-95%	
		2	Maximum of 15% Team Leadership, internal meetings, Internal Technical Meetings (FLYAT) and BD.	
5	Team Productivity and Efficiency, Team Leadership.	1	Ensure work is allocated to direct reports and maximise team utilisation.	
		2	Mentor and develop skills for reports.	