LME
A H E

JOB DESCRIPTION

GENERAL INFORMATION:			
Department: Information Security	**Line Manager** Information Security Service Lead	**Job Title:** Junior Security Engineer	**Name:** TBC
Working Hours: Mon – Friday 09:00am – 6:00pm 08:00am – 5:00pm	**On-Call Requirement:** Yes	**Corporate Title:** Officer - F	**Reporting Line:** Service Lead -> Head of Information Security -> CTO

JOB DESCRIPTION:

About the London Metal Exchange

The London Metal Exchange is the world centre for the trading of industrial metals – the majority of all non-ferrous metal futures business is transacted on our platforms.
Last year, 149 million lots were traded, equating to $15 trillion and 3.5 billion tonnes notional, with a market open interest high of 1.9 million lots.

A member of HKEX Group, the LME brings together participants from the physical industry and the financial community to create a robust and regulated market where there is always a buyer and a seller, where there is always a price and where there is always the opportunity to transfer or take on risk – 24 hours a day.

Investors value the LME as a vibrant futures exchange but also for its close links to industry. The possibility of physical delivery via the world-wide network of LME-approved warehouses makes it the perfect hedging venue for industry and provides a reference price they trust.

The Exchange provides producers and consumers of metal with a physical market of last resort and, most importantly, with the ability to hedge against the risk of rising and falling world metal prices.

Overall Purpose of Role
This role is an entry-level position within the Information Security team at the London Metal Exchange (LME). This role supports the secure delivery and operation of infrastructure and applications, identity and access management (IAM), and secure configuration management, with a strong focus on automation across each discipline.

The successful candidate will work closely with IT Engineering, Security Operations, and Infrastructure teams to ensure that security controls are effectively implemented and maintained across LME's platforms. This is a hands-on role ideal for early-career professionals with a strong interest in security engineering, DevOps practices, and technology aspects of IAM.

Key Responsibilities:

Security Engineering & Automation
- Assist in the deployment and maintenance of security tools and platforms (e.g., E-Mail Security, DLP, SIEM, Endpoint Protection).

- Develop and support the automation of security tools, configuration, and updates using scripting (e.g. Python, PowerShell, Bash, NPM).
- Contribute to Infrastructure as Code (IaC) efforts using Terraform or Ansible.
- Help monitor and maintain secure configurations across Windows, Linux, and kubernetes environments.

Identity & Access Security
- Assist in implementing role-based access controls (RBAC) and least privilege principles in code.
- Help automate IAM workflows and integrate identity controls into CI/CD pipelines.
- Support the implementation of access controls and enforcement of least privilege across platforms and services.
- Help automate access governance workflows and integrate identity-related controls into development and operational pipelines.
- Assist in access reviews and the secure onboarding/offboarding of users and systems.

DevOps Integration
- Contribute to the integration of security controls into CI/CD pipelines (e.g., SAST, DAST, secrets management).
- Collaborate with engineering teams to embed security into build and deployment processes.
- Participate in the development of secure, scalable, and resilient infrastructure solutions.

Operational Support
- Provide support for incident response and troubleshooting related to security tooling and access controls.
- Provide support for Red/Blue team testing and penetration testing.
- Help maintain documentation, standards, and procedures related to security engineering and platform protection.
- Participate in on-call and weekend support rotations as needed

Qualifications Required:
- A University degree or equivalent qualifications in a STEM subject such as Computer Science, or Engineering and/or Information Systems.
- Desirable: Entry-level certifications such as CompTIA Security+, Microsoft SC-900, or AWS Cloud Practitioner.

Required Knowledge and Experience:
- Up to 2 years of experience in IT, security engineering, or DevOps (internships or academic projects included).
- Basic understanding of:
    - IAM concepts and tools (e.g., LDAP, oAuth, IdP).
    - Networking and security protocols (TCP/IP, HTTPS, DNS, Firewalls, Proxy).
    - Operating systems (Windows, Linux/Unix, Kubernetes).
    - Scripting or programming (Python, Bash, PowerShell).
    - CI/CD tools and cloud platforms (e.g., Ansible Tower, Bitbucket, Hashicorp Vault, Pipelines, AWS, Azure)
    - Security Tooling (e.g. EDR, SIEM, Antivirus)

Personal Qualities:
- Curiosity about emerging threats and technologies
- Ability to assess and prioritize tasks/risks
- Attention to detail
- Enthusiastic about security engineering and automation.
- Strong analytical and problem-solving skills.
- Effective communicator with good documentation habits.
- Team-oriented, proactive, and adaptable in a fast-paced environment.
- Willingness to learn and grow within a critical infrastructure environment.
- Commitment to continuous learning