About ThreatDefence

ThreatDefence is a rapidly growing Australian cybersecurity vendor, delivering industry-leading threat detection and response services to a global market. We are looking for a DevOps Engineer to join our technical team and support our local and international customers. In this role, you will be responsible for maintaining our backend platforms and ensuring uninterrupted service delivery.

The ideal candidate is a highly motivated technologist with a strong passion for cybersecurity, exceptional troubleshooting skills, and solid foundational knowledge in DevOps and infrastructure management.

Key Responsibilities

* Manage Linux-based production, test, and development environments (installation, configuration, and testing).
* Deploy and manage Docker and Kubernetes clusters.
* Maintain high system availability through proactive monitoring and best practices.
* Lead new system deployments, upgrades, and modifications.
* Oversee AWS cloud environments, including EC2 instances and S3 storage.
* Diagnose and troubleshoot technical issues and performance bottlenecks.
* Automate tasks through extensive scripting (Bash, Python).
* Design and maintain patch management and version control processes.
* Develop system architecture with a focus on performance and security.
* Ensure comprehensive technical documentation is maintained.
* Collaborate with development teams on application updates and changes.
* Champion new technologies to enhance the environment.
* Work with Elasticsearch and Logstash clusters (log parsing, performance optimization, troubleshooting).
* Manage CI/CD pipelines and related activities.
* Develop tools for ETL and automation testing (Python).
* Comply with internal secure software development policies and procedures.

Candidate Profile

A successful candidate for this role should have:

* Hands-on experience with Linux operating systems (essential).
* Proficiency in scripting (Bash, Python).
* Experience with monitoring platforms such as Zabbix, Grafana, and Prometheus.
* Practical knowledge of Docker and Kubernetes.
* Exposure to cloud environments (AWS).
* Understanding of IP networking fundamentals (IP, DNS, routing, firewalls, load balancing).
* A solid grasp of security principles, including access control, security protocols, vulnerability management, and incident response.
* Experience with packet capture tools and analysis.
* Strong troubleshooting and problem-solving skills for resolving complex incidents.

Qualifications & Experience

* Tertiary degree in Computer Science, Cybersecurity, or a related field.
* 4-7 years of relevant IT experience in DevOps, infrastructure, or security-focused roles.