Cyber Security Expert

Experience: Intermediate - Senior

Role Overview

The cyber security expert is responsible for driving DevOps practices, ensuring secure, scalable, and efficient delivery pipelines, and maintaining the company's overall information security posture. The role bridges development, operations, and security to deliver high-availability systems, while enforcing compliance with organizational and regulatory requirements.

Key Responsibilities

DevOps

- Design, implement, and maintain CI/CD pipelines for applications and infrastructure.
- Manage on-premise and cloud environments (Azure & AWS) with Infrastructure as Code (Terraform, ARM/Bicep).
- Oversee monitoring, logging, and alerting systems (CloudWatch, Azure Monitor, Prometheus, Grafana, Seq).
- Optimize cost, scalability, and performance across cloud and hybrid workloads.

Cloud & Systems Management

- Manage deployments for frontend (.NET Blazor, Django, React) and backend (.NET Core, Python, Node.js) services.
- Oversee databases (PostgreSQL, SQL Server, MongoDB) including HA, backup, and security.
- Implement containerization and orchestration (Docker, Kubernetes, ECS/AKS).
- Ensure secure integration of application services (API Management, App Gateway, ALB/WAF).

SpecCon Holdings

Key Responsibilities

Information Security

- Define, implement, and enforce ISO 27001-aligned policies, controls, and procedures.
- Manage identity and access management (Azure AD, IAM, SSO, MFA, Conditional Access).
- Conduct vulnerability management, penetration testing coordination, and risk assessments.
- Lead phishing simulation campaigns, awareness programs, and incident response.
- Ensure compliance with regulatory standards (GDPR, POPIA, HIPAA if applicable).
- Oversee Key Vaults, Secrets Management, and PKI/SSL management.

Collaboration & Governance

- Work with business unit heads to identify security and operational gaps.
- Provide regular reports on infrastructure health, costs, risks, and compliance status.
- Support ISO consultants, auditors, and external partners in security/compliance reviews.

Required Skills & Expertise

Core Technical Skills

- Cloud Platforms: Azure (preferred), AWS (working knowledge).
- IaC: Terraform, ARM/Bicep, Ansible.
- CI/CD: Azure DevOps, GitHub Actions, Jenkins.
- Containers & Orchestration: Docker, Kubernetes (AKS/EKS).
- Scripting/Automation: PowerShell, Bash, Python, Go (basic).
- Networking & Security: VPC/VNet, VPNs, Firewalls, WAF, IAM/AD.
- Databases: SQL Server, PostgreSQL, MongoDB.
- Monitoring/Logging: CloudWatch, Azure Monitor, Prometheus,
- Grafana, Seq.
- Version Control: Git (GitHub, GitLab, Azure Repos).

SpecCon Holdings

Requied Skills & Expertise

Security Skills

- Risk management, vulnerability assessment, penetration testing (coordinating with third parties).
- Strong knowledge of ISO 27001, NIST CSF, CIS Benchmarks.
- Security tools: Defender, GuardDuty, CloudTrail, WAF, SIEM solutions.
- Encryption, PKI, certificate lifecycle management.

Leadership & Soft Skills

- Team leadership and mentoring.
- Vendor and stakeholder management.
- Strong documentation, reporting, and presentation skills.
- Incident response and crisis management.

Certifications (Required / Recommended)

Cloud / DevOps

Required:

- Microsoft Certified: Azure Administrator Associate (AZ-104)
- Microsoft Certified: Azure Solutions Architect Expert (AZ-305)

Recommended:

- HashiCorp Certified: Terraform Associate
- Kubernetes Certified Administrator (CKA)
- AWS Certified Solutions Architect Associate

How To Apply

Short-listed applicants may be requested to participate in the relevant assessments and competency-based interviews to assess the best fit for the position. Valid and relevant documentation will be requested.

Send your CV to hr@speccon.co.za If you are not contacted within two weeks, please consider your application unsuccessful.

SpecCon Holdings