Job Description

Senior SysOps Engineer (L3)

Reporting to: SysOps Team Lead

Location: Cape Town or Johannesburg (Office Based)

Roles and Responsibilities

We are looking for an experienced and technically strong Senior SysOps Engineer. In this hybrid senior technical and leadership role, you will serve as the primary L3 escalation point for complex technical issues while actively contributing to operational excellence, automation, security, and continuous improvement across our managed services environment. You will combine deep hands-on expertise with our core toolset (N-able, Intune, Microsoft Defender, Entra ID, Acronis, Mimecast, Meraki, etc.) with the ability to mentor the team, drive proactive solutions, and help lead the SysOps function. If you thrive on solving challenging problems, building efficient systems, and developing both technology and people, this is the role for you.

Key Responsibilities:

Technical Escalation & L3

- Act as the final escalation point within the SysOps team for complex technical issues that L1/L2 cannot resolve.
- Perform deep troubleshooting, root cause analysis, and advanced diagnostics across servers, networks, M365, Entra ID, Azure, and client environments.
- Diagnose and resolve issues involving Active Directory/Entra ID, networking protocols (TCP/IP, DNS, DHCP), cloud platforms, and security tools.
- Provide timely and effective updates to clients and internal stakeholders during major incidents.

Automation & Continuous Improvement

- Design, implement, and maintain automation workflows using PowerShell, Python, Azure Automation, and RMM platforms (especially N-able).
- Identify opportunities to reduce manual effort and drive self-healing systems and proactive monitoring.
- Optimise and enhance our existing toolset (N-able, Intune, Microsoft MDE, BitDefender, Qualys, Acronis, Mimecast, Meraki, etc.) for greater efficiency and scalability.
- Champion the adoption of emerging technologies and best practices.

Security & Compliance

- Ensure adherence to security standards and frameworks (Microsoft best practices, CIS, NIST).
- Oversee vulnerability management, patching, and incident response in collaboration with the SOC team.
- Implement and manage security controls using Microsoft Defender suite, Conditional Access, and other endpoint/cloud security tools.

Systems Administration & Optimisation

- Manage and optimise servers, Active Directory/Entra ID, Microsoft 365, Azure, and hybrid cloud environments.
- Ensure high availability, performance, and reliability of client infrastructure.
- Conduct proactive maintenance and system optimisation activities.

Team Leadership & Mentoring

- Support the SysOps Team Lead in day-to-day team management and leadership.
- Mentor and develop L1 and L2 engineers, providing technical guidance, training, and knowledge sharing.
- Conduct technical reviews, 1-2-1s, and contribute to performance feedback and professional development.
- Help foster a culture of accountability, innovation, documentation, and continuous improvement.

Reporting, Metrics & Knowledge Management

- Contribute to defining and tracking team KPIs aligned with business and client goals.
- Develop and maintain custom dashboards and reports (especially in N-able).
- Use data-driven insights to identify trends, recurring issues, and automation opportunities.
- Ensure high-quality documentation and knowledge base ownership across the team.

Service & Project Delivery

- Help manage IT support projects, upgrades, migrations, and deployments.
- Ensure adherence to ITIL principles and defined SLAs.
- Collaborate with other teams (SOC, Consulting, Commercial) to align technical delivery with business needs.
- Participate in strategic and operational initiatives alongside other Support Team Leads.

Experience

- 7+ years in IT support or systems administration, with at least 3+ years focused on advanced/L3 technical issues.
- 1–2+ years of experience in a team lead, deputy lead, or mentoring capacity (or strong readiness to step into a second-in-command role).
- Deep hands-on experience with N-able (highly advantageous), Microsoft ecosystem (Intune, Entra ID, M365, Defender), and RMM/automation tools.
- Strong automation and scripting skills (PowerShell and/or Python required).
- Solid understanding of cybersecurity principles, vulnerability management, and cloud/hybrid environments (Azure preferred).
- Experience working in a managed services provider (MSP) environment is a strong advantage.

Skills

- Exceptional technical troubleshooting and problem-solving abilities.
- Strong scripting and automation mindset.
- Excellent communication and interpersonal skills, with the ability to explain technical concepts clearly.
- Leadership potential and ability to mentor and develop others.
- Data-driven approach with good analytical and reporting skills.
- Ability to manage multiple priorities and work effectively under pressure.
- Fully fluent in English (spoken and written), with a professional demeanour and high personal integrity.

Qualifications

- Bachelor’s degree in IT, Computer Science, or a related field (or equivalent experience).
- Microsoft Certified: Azure Administrator Associate (AZ-104) and/or Microsoft Certified: Azure Security Administrator Associate (AZ-500) – Highly desired
- Microsoft Certified: Azure Devops Expert
- Microsoft Security Operations Analyst (SC-200) or equivalent.
- ITIL Foundation (or higher) certification.
- CompTIA Security+ or equivalent.
- Additional certifications such as CCSP, CCNA and/or vendor-specific (N-able, Meraki, etc.) are a plus.