TNP
the networking people

connectivity
consultancy
engineering

JOB DESCRIPTION

Senior Network Security Specialist

Responsible to:	Security Architect
Direct Reports:	None
Salary:	£50,000 to £68,000 plus benefits

TNP Overview

TNP supplies independent consultancy allowing large organisations to design, build and operate their own networks and security solutions, supported by the expertise that TNP has to offer.

A large proportion of TNP's customer-base is public sector, currently offering services to Local Authorities, Health, Educations and Police/Blue Light services, including provision of Wide Area Networks, Local Area Networks, Wireless LAN and Security. Underpinning this, TNP operates its own carrier class ISP network providing high speed Internet access across the UK.

We want to make sure we have the best people for the job and provide genuinely equal opportunities for our people to thrive.

Our recruitment process is designed with inclusion and equity at its core, and we encourage all our employees to work to deliver TNP's mission which is to be:

> ***"The trusted long-term partner to public sector, delivering excellent outcomes in connectivity and security"***

Underpinning this are TNP core values that encourage and support staff to work within a behavioural framework of:

- ***People First, All In it Together***
- ***Never Stop Evolving***
- ***Do the Right Thing Always***
- ***Take Action Be Accountable***

Role Overview

To design, implement and support network security architecture at customer premises, and support the TNP Operations Team with any network security requests as a point of technical escalation. This includes leading a technical project throughout its entire lifecycle, from the gathering of requirements and presentation of solution at the pre-sales stage, through detailed design and ensuring smooth implementation, then ongoing overall technical responsibility for the customer and their solution.

Candidates must have a keen interest in network security coupled with an in-depth knowledge and working experience of modern network and systems security architecture including Firewalls, Unified Threat Management, Web Filtering, Email Security, Web Application Firewalls, Authentication (2FA/SAML), VPN, SDWAN, and SASE. You will also have an understanding of other relevant areas of networking such as LAN/WAN design, router/switch configuration and a general solid foundation of networking fundamentals.

You should have an avid interest in computer and network security, a logical approach to problem solving, planning and good written and verbal communications skills. Detailed knowledge of IP, network security, unified threat management, communications media and networking equipment are essential.

As a Fortinet Expert Partner, TNP would value candidates that have design and practical experience of Fortinet's security portfolio, including the FortiGate UTM platform, SDWAN, ZTNA and SASE.

Mentoring new technical staff throughout their career at TNP and assisting the Operations Manager in the development of training programmes is a key part of the role.

Main Duties

1. Design, implement and support network security architecture including Firewalls, Unified Threat Management, Web Filtering, Email Security, Web Application Firewalls, Authentication (2FA/SAML), VPN, SDWAN, and SASE for TNP's customers both remotely and at their premises.
2. Augment network security infrastructure with automated SecOps tooling, tuning solutions providing SIEM, SOAR, and XDR functions to modernise SOC capabilities and provide scale for TNP's customers both remotely and at their premises.
3. The preparation and presentation of security architecture designs and technical implementation plans both within the organisation and to external customers; this includes attendance, and potentially leading, of pre-sales meetings via web conference or onsite.
4. Remote and onsite security audits/health checks, including preparation and presentation of reports.
5. Technical management and overall technical responsibility for nominated Customers or nominated Customer Solutions.
6. Working pro-actively to review and improve nominated Customer environments as new compliance frameworks, best practice guides, attack vectors or new technologies emerge. This includes the technical design, presentation to the customer and leading the implementation.
7. Document new solutions and assist with the development of a training programme. Lead relevant internal technical training sessions with TNP technical staff. Where required, deliver technical content to customers.
8. Advise and assist customers in gaining and maintaining accreditation for relevant compliance frameworks, including but not limited to, PSN Code of Connection, PCI-DSS, ISO27001 and Cyber Essentials. This may involve advising the customer as the compliance requirements change and/or providing recommendations and follow-up actions following an official audit or health check.
9. Working within customer requirements to design & deliver relevant projects within agreed timescales.
10. Undertake 3rd line support via email and telephone. Perform remote diagnostics, resolution and dispatch to an appropriate team member if appropriate. Where necessary, undertake 3rd line support on site at customer premises
11. Provide long-term mentoring to nominated technical staff, assisting with their personal and technical development
12. Attendance and reporting to appropriate internal and external meetings, with overall technical responsibility for nominated internal and external projects.

13. To work to appropriate service levels with defined quality of service metrics that will enable you to maintain and demonstrate high quality of service provision.
14. To maintain high levels of professional conduct, including but not limited to, cooperative engagement in tasks set, the exercising of initiative to suggest through line mangers improvements to the service provided, and clear and professional styles of communication at all times.
15. To pro-actively maintain relevant technical accreditations and industry knowledge, via attendance of webinars, conferences, news feeds, online learning. Keep up to date on relevant new technologies, developments and products; and, where necessary, undertake a detailed evaluation.
16. Provision of technical support for network and system faults, as directed, ensuring prompt rectification. This will require 24x7 call-out rota working and may include participation in a 3rd line 24x7 call-out rota to act as an escalation point for the on-call engineer.
17. Arranging and performing of planned out-of-hours maintenance on TNP or customer infrastructure as required.
18. Such other duties appropriate to the grade as may be directed by the Board of TNP or by its nominated representatives.

Special Conditions

- The company's 24x7 support commitments will require participation in a rota based, on-call system that will result in call-outs outside of standard working hours.
- Enhanced Disclosure and Barring Service (DBS) is a condition of initial appointment.
- Non-Police Personnel Vetting (NPPV3) clearance to be achieved within probationary period.
- A full UK driving licence

Contacts

Name/organisation	**Reason**	**Approximate Frequency**
Security Architect or nominated representative	Day to day management, directions & instructions	Daily
Security Architect	Performance monitoring	Weekly
Security Architect	Reviews	Quarterly
TNP Internal	Team work	Daily
TNP Technical Teams	Provide mentoring to nominated technical staff throughout their career at TNP	Daily
TNP Operations Desk	To accept escalated faults and queries.	Daily
Customers & Partners	Design, installation, audits, presentation of reports, fault investigation and rectification; liaison and problem solving,	Daily
Customers	Day-to-day technical account management	Daily
Commercial Team	Gathering of requirements and producing customer pre-sales designs, costings and bid reviews	Daily
Customers/Commercial Team	Working alongside the Commercial Team, or in some cases independently, to present technical solutions to the Customer and address any queries	Daily
Network providers & Hardware Vendors	Fault escalation and support	As Required

Person Specification

Criteria	Essential / Desirable	Application form / Interview
Relevant professional-level qualifications in the field of network security, including Fortinet NSE4, 7.	Essential	Application Form
Commitment for ongoing professional development to achieve additional relevant qualifications such as Fortinet NSE 5, 6, 8.	Essential	Interview
Relevant professional-level qualifications in the field of networking (Cisco CCNA/CCNP, Juniper JNCIA/JNCIS/JNCIP)	Desirable	Application Form
Full UK Driving License	Essential	Application form
Detailed working knowledge of network security architecture and general TCP/IP networking and L2/L3 protocols	Essential	Application form / Interview
Experience of designing and leading the implementation of security architecture solutions, including acceptance testing, troubleshooting and detailed documentation	Essential	Interview
Demonstrable experience of technical report writing	Essential	Interview
Demonstrable detailed knowledge of modern enterprise security stack, including but not limited to, UTM, ZTNA, SD-WAN, modern authentication methods (e.g. SAML) & remote access solutions.	Essential	Application form / Interview
Experience in configuration and deployment of Fortinet security platform	Essential	Interview
Experience with SEC-OPS toolset technologies such as SIEM, SOAR, XDR.	Desirable	Interview
Practical knowledge of wider automation tooling such as infrastructure as code, configuration management, APIs, playbooks, templates (e.g. jinja) or scripting (e.g. python, ansible, terraform)	Desirable	Interview
Working knowledge of the design and configuration of enterprise cyber security solutions	Essential	Interview
Previous experience of working with the public sector (directly or as a consultant)	Desirable	Application Form
Knowledge of relevant security compliance frameworks, such as PSN Code of Connection, PCI-DSS, ISO27001, IG Toolkit and Cyber Essentials	Essential	Interview

Excellent communication skills, both written and verbal coupled with an ability to maintain confidentiality.	Essential	Application form / Interview
Enthusiasm and a demonstrated capability for problem solving, with an ability to identify, prioritise and focus on key issues.	Essential	Application form / Interview
Ability to work both independently and as part of a team, with no day-to-day supervision. Commitment to approaching tasks with flexibility, proactivity and completion to a high quality of workmanship.	Essential	Application form / Interview
A flexible approach to areas of work which will include participation in an out-of-hours on-call rota as well as work outside of standard office hours.	Essential	Interview
Commitment to undergo further training through operational requirements and personal development	Essential	Interview