



CURRICULUM VITAE · CONTRACT DELIVERY

Joshua Paul Gardner

Cyber Security Operations · Architecture · Infrastructure

18 years across ICT operations and cyber security. Security operations design and management, vulnerability management, EDR/NDR/SIEM tooling, incident response, security architecture and advisory — built on a deep infrastructure and networking foundation across on-premises and cloud estates.

Engagement basis	Outside IR35 · statement of work, defined deliverables, substitution and control retained by supplier
Contracting entity	Avertory Limited · UK limited company · Companies House 16542620
Business insurance	Professional indemnity and public liability available on request
Location	Guernsey / UK · remote-first, on-site as scoped
Contact	josh@avertory.com · avertory.com

Version 1.0 · September 2026 · Avertory Limited · UK professional services

PROFILE

Contract cyber security specialist

Senior cyber security practitioner with 18 years of ICT operations and security experience, currently operating as InfoSec Senior Technical Analyst for a Guernsey-based international insurance group. Prior to that, ten years leading MSP and MSSP business units — designing, building and running Security Operations Centres and delivering vulnerability management, EDR, NDR, SIEM and security posture programmes for local government and private-sector clients.

Engagements are delivered through Avertory Limited on an outside-IR35 basis: fixed scope, written deliverables, supplier-controlled working methods and a right of substitution. Typical assignments are security operations build-out, vulnerability management programmes, platform implementation (SentinelOne, Orca Security, Qualys), security architecture reviews and interim InfoSec leadership.

Item	Detail
Contract roles	Security Operations Lead · Vulnerability Management Consultant · Security Architect · InfoSec Technical Analyst · Interim Security Manager
Engagement models	Statement of work, fixed-scope delivery, retained lifecycle support, day-rate consultancy
IR35 position	Outside IR35 — supplier controls how, when and where work is performed; deliverable-based SOW; substitution permitted; no integration into client hierarchy
Sectors	Insurance and financial services, local government, professional services, mining and industrial, education
Availability	Confirmed per engagement in writing · UK, Channel Islands and remote

CAPABILITY

Core skills

Capability	Level
Cyber security operations design, implementation and management	Advanced
Vulnerability management and attack surface reduction	Advanced
Security monitoring, detection and tooling (SIEM, EDR, NDR)	Advanced
Incident response and threat intelligence analysis	Advanced
Security architecture, advisory and consulting	Advanced
Infrastructure management (on-premises and cloud)	Advanced
Solutions architecture and solution design	Advanced
Cyber security pre-sales (local government and private sector)	Advanced
Operations management and service governance	Advanced
Governance, compliance and audit support (ISO 9001, ISO 27001)	Advanced

EXPERIENCE

Work history

InfoSec Senior Technical Analyst

2024-02 – Current

Utmost Group · Guernsey, UK

- Vulnerability management and risk surface reduction.
- Security monitoring, detection, and tooling.
- Incident response.
- Threat intelligence and analysis.
- Security advisory, architecture, and projects.
- Governance, compliance and audit support.
- Leadership, training, and knowledge sharing.

IT Operations & Security (Remote from 2019)

2014-01 – 2024-01

Icon Information Systems (Pty) Ltd · Durban, KZN, South Africa

- Leadership role focused on developing and delivering security and infrastructure solutions for clients.
- Day-to-day management of Managed Service Provider (MSP) and Managed Security Service Provider (MSSP) business units.
- SOC design, implementation and management with a focus on vulnerability assessments, automated penetration testing, security posture assessments, SIEM, EDR, NDR tools and policy reviews.
- Vendor engagement and liaison across various products and services.
- Internal and external cyber security pre-sales.
- Advisory and management roles in disaster recovery and business continuity services to various clients.
- Implementation and management of internal ISO standards including 9001 and 27001:2013.
- Top-level management of developer teams and client requirements.

Technical Operations Manager

2013-08 – 2014-06

Siyatya General Trading · Durban, KZN, South Africa

- Managed online portals for delivering training programmes and resources.
- Designed client solutions for data backup and security, online presence, social media marketing, and system automation.
- Managed client support request processes and assisted support teams in prioritising mission-critical requests.
- Consulted on business acquisitions regarding ICT components covering audits, upgrades, maintenance, and other client requirements.

EXPERIENCE

Work history (continued)

Trainer – Networks Engineering

2012-05 – 2013-08

Richfield (previously PC Training and Business College) · Durban, KZN, South Africa

- Adapted training plans for client needs while keeping timelines, budgets and objectives in mind.
- Scheduled and taught in-class and online courses to increase learning opportunities.
- Supported distance and online learning via a Moodle-based web portal with content delivery via video sessions or Q&A.
- Assessed student needs to develop effective training plans.
- Contributed to development of the network engineering curriculum and training content.
- Provided one-to-one and interactive training sessions with assessments to determine competence.
- Handled over 200 daily students, switching between classes while maintaining a positive attitude.

Systems Administrator

2008-08 – 2012-02

Freda Rebecca Gold Mine · Bindura, Mashonaland Central, Zimbabwe

- Provided comprehensive training to internal and off-site users to optimise systems maintenance and resolve recurring issues.
- Drafted backup and recovery policies and procedures ensuring systems and network availability for over 350 users.
- Designed and implemented systems, network and user security policies.
- Administered and troubleshoot servers, networks (LAN, WAN, VPN), printers and applications.
- Initiated and managed a fibre backbone and wireless fail-over project for two remote sites back to head office.
- Planned and implemented complex internet and intranet applications on multiple platforms.
- Technical implementation of ERP system upgrade (Sage AccPac).
- Spearheaded inventory control measures to maintain IT equipment, supplies, tools and replacement parts.

CREDENTIALS

Education and certifications

Credential	Awarding body	Period
Fortinet – Network Security Analyst: Cyber Security	Fortinet	2019-05 – 2022-04
AWS Certified Cloud Practitioner / Cloud Computing	Amazon Web Services (AWS)	2019-03 – 2022-03
CompTIA Security+	CompTIA	2015-02 – 2018-02
BSc Computer Science	Bindura University of Science Education, Zimbabwe	2005-08 – 2009-12

CONTRACTING

How engagements are structured

Work is contracted business-to-business between the client (or agency) and Avertory Limited. The structure below is written into every statement of work so the engagement stands up to an outside-IR35 assessment.

Status test	How the engagement is structured
Control	Avertory Limited determines how, when and where the work is performed. The client specifies outcomes, not working methods or hours.
Substitution	A suitably qualified substitute may be provided at the supplier's cost, subject only to reasonable security vetting.
Mutuality of obligation	No obligation to offer or accept further work once the deliverables in the statement of work are complete.
Part and parcel	No line-management responsibility, no appraisals, no staff benefits, no place in the client organisation chart.
Financial risk	Fixed-price or milestone-based delivery where scope allows; supplier carries rework risk and its own equipment, tooling and insurance.
Business on own account	Avertory Limited delivers to multiple clients and partners, holds its own brand, website and business insurance.

Typical contract deliverable	Output
Vulnerability management programme	Asset baseline, scan and authentication coverage, risk-based prioritisation model, remediation workflow and reporting pack.
Security operations build-out	Detection and monitoring design, tooling deployment, playbooks, escalation paths and operating rhythm.
Platform implementation	Deployment plan, configuration baseline, integration set, validation evidence and handover documentation.
Security architecture review	Current-state assessment, gap register, prioritised remediation roadmap and design decisions.
Interim InfoSec support	Advisory capacity, audit and compliance support, incident response readiness and knowledge transfer.

Contract enquiries: josh@avertory.com · Avertory Limited · Companies House 16542620 · avertory.com