PHILLIP GESTRO

Senior Cybersecurity & Infrastructure Security | Identity | Risk & Delivery

Wellington, New Zealand | 022 454 4303 | Phillip.Gestro@ecloudsolutions.co.nz

LinkedIn | Professional portfolio

Professional Profile

Senior infrastructure security and cybersecurity consultant with more than 20 years of experience across enterprise Microsoft systems, hybrid identity, operational networks, cloud and client-facing technical delivery. My security work combines strategic advice with hands-on engineering: strengthening access controls, reviewing architecture, improving monitoring and supporting incident response. My background includes nine years advising ECLOUD clients and seven years as CentrePort's ICT Technical Lead.

I develop practical security decisions grounded in the complexity of the underlying environment. At CentrePort I improved Microsoft 365 and Active Directory security, coordinated managed detection onboarding, supported incident investigations, and prepared security strategies, maturity reviews and independent testing. Earlier consulting work covered technology risk, privacy, business continuity, regulated cloud solutions and ransomware recovery. I can challenge suppliers, identify dependencies and take agreed improvements through implementation, validation and handover.

Security Architecture & Hands-On Engineering

- **Identity and privileged access.** Strengthen Microsoft 365, Active Directory and hybrid identity using MFA, Conditional Access, least privilege and secured remote access.
- **Security architecture and assurance.** Develop practical cyber strategies, design reviews, risk decisions, maturity assessments and penetration-testing and segmentation readiness.
- **Detection and response.** Coordinate managed detection onboarding, investigate security events, improve monitoring and support response and recovery activities.
- **Security in critical infrastructure.** Integrate segmentation, operational technology and Private 5G security requirements with suppliers, network engineers and system owners.

Professional Experience

ICT Technical Lead | CentrePort Limited | Jun 2019 - Aug 2026

Led practical cybersecurity improvements across CentrePort's Microsoft platforms, identity, operational networks and hosted infrastructure, combining strategy and technical architecture with hands-on controls, testing and specialist-provider coordination.

- **Turned security risks into architecture decisions, testing and management actions.** Developed CentrePort's cybersecurity strategy and maturity reviews, translated identity and network risks into practical hardening and remediation, and led CentrePort-side Arctic Wolf managed detection onboarding across six locations. Coordinated independent penetration-testing and network-segmentation readiness, separating delivered controls from proposed work and outstanding decisions.
- **Completed CentrePort's Microsoft 365 and Exchange hybrid transition.** Following the initial vendor phase, personally completed the remaining Exchange Online mailbox migration, configured Azure AD Connect and Exchange hybrid services, deployed the replacement hybrid server and retired legacy Exchange infrastructure. Implemented MFA, Conditional Access and Defender security controls. Strengthened privileged access and account-lockout protection, helping identify and block a brute-force attack; investigated and restored a failed MFA control for Remote Desktop Services.
- **Led CentrePort-side integration of New Zealand's first commercial Private 5G network.** Turned Tū Ātea's network design into a supportable CentrePort environment, leading hands-on integration across existing network and security infrastructure, server-room and fibre readiness, radio-access sites and field connectivity. Coordinated design interpretation, specialist suppliers, testing and commissioning to connect the vendor-delivered platform to the port's operational systems.

- **Shaped hosting decisions and led migration delivery.** Assessed cloud, private hosting and infrastructure renewal options against cost, security, resilience and recovery. Recommended the ASI hosting direction and led CentrePort-side technical planning, service-provider dependencies, implementation, cutover and validation.
- **Modernised operational networks and engineering standards.** Delivered workplace, tenancy and marine-network improvements, including a dedicated network for Rail Isolation. Established field-cabinet, fibre acceptance and testing standards, alongside a dual-contractor model to improve traceability, reliability and delivery assurance.
- **Directed suppliers while retaining technical ownership.** Challenged designs and scope, defined technical work packages and acceptance criteria, coordinated specialist engineers and contractors, and produced clear implementation, troubleshooting and operational handover documentation.
- **Led the Shed 39 relocation and established CentrePort's digital infrastructure foundation.** Designed the four-rack server-room environment and led the complex relocation of staff and ICT services from two existing sites into Shed 39. Directed infrastructure deployment, specialist suppliers, migration, cutover and commissioning while maintaining business continuity and decommissioning the former locations. The new environment became the foundation for subsequent Private 5G, field-network and workplace improvements.
- **Converted Private 5G infrastructure into operational services.** Took the vehicle-fleet service from bench build and controlled pilot into production rollout; led the reusable Reefer Tower delivery model and CCTV cabinet and pole deployment standard; and delivered Gallagher-controlled vehicle gate and intercom connectivity. Further CCTV and crane work remained staged within the programme.

Consulting and Enterprise Assignments

Senior Technical Consultant | ECLOUD | May 2010 - Jun 2019

Held responsibility for client technology strategy, infrastructure, cybersecurity and operational support across government, health regulatory, industrial, education and commercial organizations. Worked directly with senior leaders while remaining closely involved in technical design, implementation, escalation and recovery.

- **Connected security advice with service recovery.** Prepared cybersecurity strategies, security-risk and privacy assessments, cloud-readiness reviews and business-continuity plans. Supported practical security improvements and commercial-client ransomware response and recovery.
- **Designed and validated regulated cloud solutions.** Led government and regulatory cloud design work, built off-network proofs of concept, resolved architecture and integration issues and progressed solutions through security-risk, governance and design-authority review.
- **Advised a broad client portfolio.** Supported an All-of-Government agency, health professional regulators and industrial and education clients, alongside a portfolio exceeding 300 private-sector organizations. Developed technology roadmaps, risk-based priorities and practical investment and delivery recommendations.
- **Combined consulting with hands-on engineering.** Designed, built, migrated and supported Microsoft server and collaboration platforms, Active Directory, Exchange/Microsoft 365, virtualization, hybrid hosting and enterprise networking. Troubleshot complex identity, application, platform and operational dependencies for clients.
- **Managed commercial and supplier decisions.** Worked with executives, finance teams and providers on business cases, RFI/RFP inputs, procurement, contracts, licensing, hosting and support choices, identifying delivery risks and challenging unclear costs or ownership.
- **Explained decisions and transferred knowledge.** Translated technical and regulatory requirements into clear recommendations, implementation plans and operational guidance; coached engineers and users, drawing on earlier Microsoft Certified Trainer experience.

Enterprise Contract Assignments | Comsmart via ECLOUD | Dec 2014 - Jun 2019

Recurring assignments undertaken while employed by ECLOUD, totalling approximately three years across Revera, NZX, CTAS and CentrePort, alongside work for Comsmart direct clients.

- **Delivered enterprise infrastructure projects.** Worked with architects and application vendors to implement secure data-centre, virtualization, Microsoft server and Revera Apollo local-cloud platforms, taking designs through build, integration and technical validation.
- **Built and integrated Microsoft application services.** Hands-on builds and troubleshooting across Active Directory, Windows Server, IIS, SQL Server, Certificate Services and Remote Desktop Services; resolved identity, network, vendor and application dependencies.

- **Improved operational security and supportability.** Reviewed technical builds, implemented Group Policy and privileged-access hardening, investigated complex infrastructure faults and contributed clear delivery and handover records.

Earlier Career

- **Occupational Therapy Board of New Zealand | IT Administrator (2007 - 2010).** Led public-facing practitioner-registration platform infrastructure and managed technical support, planning and suppliers for health regulatory operations.
- **TelstraClear | Microsoft Windows Systems Engineer (2006 - 2007).** Delivered enterprise Active Directory recovery and migration work and supported Microsoft, Citrix and communications platforms.
- **BOSIT | Network Engineer (2004 - 2006).** Designed, implemented and supported Microsoft systems, networks, wireless and backup services for Wellington clients.
- **Avonmore Tertiary Institute | Microsoft Certified Trainer (2004).** Delivered Level 5 and Level 6 computing-support training, preparing adult learners for Microsoft, CompTIA A+ and Network+ qualifications. Held Microsoft Certified Trainer status for three consecutive years and taught MCSA material to people already working in the IT industry.

Technical Skills and Delivery Expertise

Hands-on security: Active Directory hardening, Entra/hybrid identity, Exchange Online security, MFA and Conditional Access, Defender for Office 365/Identity, privileged remote access and network segmentation.
Strategy and resilience: Cybersecurity strategy and maturity, risk/privacy assessment, Arctic Wolf MDR onboarding, incident escalation, ransomware recovery support, testing readiness, disaster recovery and multi-vendor security delivery.

Qualifications and Professional Development

National Diploma in Computing Engineering (Level 6). Historical certifications include MCSE, MCSA | Messaging, MCP, Microsoft Certified Trainer, CompTIA A+, Network+ and Linux+. Passed Microsoft exams SC-100 (Cybersecurity Architecture) and MS-500 (Microsoft 365 Security Administration). Technical Writing and Train the Trainer certification through Auldhouse.