David Rankin

hi@davidr.co – linkedin.com/in/davidr-au

PROFESSIONAL SUMMARY

Senior SOC Analyst and 2IC with experience across SOC, NOC, and consulting functions. Currently leading the Melbourne SOC team for a managed security services provider and providing onsite SOC technical leadership to a major Victorian government department. Skilled in high-volume triage, investigation, and detection engineering using Microsoft Sentinel, Defender, and related platforms. Recognised for adaptability, early progression into senior responsibilities, and delivering measurable improvements in SOC governance, operational efficiency, and customer security outcomes.

SKILLS

Security Platforms: Microsoft Sentinel, Microsoft Defender suite, Entra ID (Azure AD), AlienVault/LevelBlue
Detection & Engineering: KQL-based analytic rule design, detection logic refinement, watchlist-driven enrichment, alert template development, playbook automation
SOAR & Automation: Microsoft Logic Apps, Sentinel playbooks, triage workflow automation, data enrichment pipelines
Incident Response & Threat Management: Investigation, containment, proactive hunting, incident coordination, evidence-based reporting
Governance & Compliance: Essential Eight uplift, ISO 27001 exposure, SOC reporting & metrics
Professional Skills: Stakeholder communication, customer advisories, technical documentation, team leadership, project coordination

PROFESSIONAL EXPERIENCE

OneStep Group, Melbourne | October 2022 – Present

Senior SOC Analyst & 2IC | (July 2025 – Present)

- Promoted to 2IC of the national SOC; lead the Melbourne team, overseeing priority incident response, escalations, and process improvements.
- Embedded with a major Victorian Government department, maturing Sentinel detection engineering and automation; achieved a 60% false-positive reduction and provided strategic uplift advice.
- Mentored analysts and established standardised training and documentation, reducing dependencies and lifting national team capability.
- Supported the CISO in delivering the organisation’s first ISO 27001 internal audit, gaining practical experience in control assessment and compliance evidence preparation.
- Advanced detection and automation in Sentinel and Defender by onboarding new log sources, enhancing playbooks, and developing cross-platform workflows (Sentinel, FreshService, AlienVault APIs).

SOC Analyst | (Jan 2024 – June 2025)

- Led end-to-end incident management for 15+ customers across diverse sectors, including government, enterprise, and healthcare, using a broad toolset (Sentinel, Defender, LevelBlue, Mimecast, Check Point, Palo Alto).
- Spearheaded detection engineering initiatives, playing a lead role in false positive reduction through rule tuning and suppression logic that improved the signal-to-noise ratio and analyst workflow efficiency.
- Independently delivered an Essential Eight–aligned audit response, managing evidence collection and controls validation with minimal support to ensure a successful outcome and preserve partner status
- Presented monthly governance reports and service analysis to customers, driving data-backed recommendations to streamline daily operations and strengthen security coverage.

SOC / NOC / Service Desk Analyst | Jan 2023 – Jun 2024 **(Secondment & Permanent Role)**

- **Initial Engagement and Monitoring:** Delivered network and security monitoring services across diverse customer environments, supporting triage, incident response, and continuous service availability. Operated FortiGate, FortiAnalyzer, FortiManager, CradlePoint NetCloud, and Microsoft security platforms to validate failover events, analyse network metrics, and identify security anomalies.
- **Structured Incident Response & Trust:** Participated in major incident response, applying structured severity assessments and coordinating service restoration across IT operations and leadership. Coordinated with WAN service partners and stakeholders to expedite resolution of network and security incidents, maintaining strong customer trust.
- **Contained Security Incidents:** Collaborated with the SOC to investigate and contain security incidents, executing remediation (account isolation, MFA re-enrolment) and collecting digital evidence for HR-led staff investigations.
- **Process and Knowledge Management:** Authored over 100 internal knowledge base articles, creating a single source of truth that improved team consistency, efficiency, and reduced reliance on tribal knowledge.
- **Compliance Foundation:** After the departure of the program lead, I took sole responsibility for completing and delivering the Essential Eight–aligned audit response, managing controls validation and documentation to ensure a successful submission and preserve partner status.

KEY CERTIFICATIONS

- Microsoft Certified: Security Operations Analyst (SC-200)
- CompTIA Security+
- CompTIA Network+
- Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900)
- Microsoft Certified: Azure Fundamentals (AZ-900)
- Full list on LinkedIn