Curriculum Vitae

# Oliver Queen

# Cybersecurity Consultant

# 2 February 2020

COMMERCIAL IN CONFIDENCE

**CONTACT DETAILS**

Phone:

EMAIL:

|  |  |  |  |
| --- | --- | --- | --- |
| DETAILS | | | |
| **Candidate Name** | Oliver Queen | | |
| **Employer** |  | | |
| **Position** | Cybersecurity Consultant | | |
| **Availability** | 4 Weeks | **Resides** | Melbourne, VIC, AU |

|  |
| --- |
| OVERVIEW |
| * Oliver is a Cyber Security Leader with over 20 years of successful experience in the ICT Industry. His experience from System Administrator/Engineer to leading and developing the Cyber Security capability. * He is recognised consistently for performance excellence and contributions to successes in ICT and security industry. Oliver’s strengths are in leadership, security development and project management. * He is an extremely versatile and adaptable person, with a broad range of experience in both technical support and operation planning. * He can resolve problems quickly, delivering high levels of stakeholders’ satisfaction. As a proficient Cyber Security Leader, Oliver is strategic in organising and executing projects and tasks, whilst incorporating the expectations of a client, team or the individual. He effectively trains users and support process improvements to a large range of systems and software. * Oliver is well-versed in business practices and IT standards such as ITIL, NIST, government equivalents and Rail communication standards. * He has spoken at multiple cyber security conferences, such as B-Sides, CyberCon and various summits. |

|  |
| --- |
| EDUCATION & QUALIFICATIONS |
| * Certificate: GEVA, GSOM, GSLC, GSTRT, ISO27001 Lead Auditor. * Charles Sturt University – Master in Cyber Security (finish Dec 2024) |

|  |
| --- |
| REGISTRATIONS & COMPETENCIES |
| * Incident Response / Management - RAAF * SANS 500 Windows Forensics Analysis * SANS 504 Hacker Tools, Techniques, Exploits, and Incident Handling * SANS 572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response * SANS 508 Advance Incident Response, Hunting & Forensics * SANS 415 A Practical Introduction to Cyber Security Risk Management * SANS 530 Defensible Security Architecture and Engineering * SANS 460 Enterprise and Cloud Threat and Vulnerability Assessment * SANS 560 Network Penetration and Ethical Hacking * SANS 551 Building and Leading Security Operations Centers * SANS 512 Security Leadership Essentials for Managers |

|  |  |
| --- | --- |
| EXPERIENCE | |
| **Jan 21 – Current** | **Company | Position (Example)** |
|  | Software and Data is an Australian enterprise specialising in web application hosting and security.   * Deployed Splunk across the network, configuring the indexers, deploying forwards, and creating reports and dashboards. Provided comprehensive education and training on Splunk functionalities, limitations, and applications. * Conducted vulnerability assessments and scanning using OWASP Zap and Nessus on web applications and the network. Expertly configured scans to avoid service disruption, offering detailed reports and educational support. * Managed PCI DSS compliance, including assessments, policy reviews and amendments, educating the organization, and overseeing policy implementation.   **Key Achievements:**   * Creation of polices and procedures for compliance. |
| **Nov 22 – May 23** | **CYBER SECURITY BOOTCAMP – SYDNEY UNIVERSITY | Student** |
|  | The course is constructed to take a student from no experience to a proficient SOC analyst. The bootcamp is conducted over 24 weeks. The course is split into 3 main sections. It also includes 4 Project deliverables.   1. IT Administration. This covers Linux, Windows Servers and Clients, networking and security, cloud, and web development and coding languages Bash, PowerShell and Python. This Project gets the students to create a web application using the Azure platform. 2. Offensive operations. This includes Penetration Testing, on web applications, Linux and Windows clients, and Windows servers. The main operating system the students learn on is Kali Linux. The project is in the form of a capture the flag. 3. Defensive operations and career preparation. This includes SIEM training on Splunk, introduction to Digital forensics and two projects. Building, and configuring a SIEM, this includes rule sets and finally a research project.   **Key Achievements**   * Achieving a 98.26 final grade * Developing and handing over a resource guide for students based off the resources and information provided by the educators. It has continued to be used after i completed the course. |