Insert Name

|  |  |  |  |
| --- | --- | --- | --- |
| Address | Phone number | email address   |  | | --- | |  | | Profesional Summary |   (Remove – Your CV should be in 3rd person, if you don’t have experience in IT or cybersecurity translate what skills you bring to the table)  \*Insertname\* is an experienced Registered Nurse with more than 12 years of dedicated service in the healthcare industry. Now embarking on a transition into the field of Cybersecurity, this is due to his love of computers. Insertname extensive background in nursing positions him as a unique asset with cross-over skills. Throughout his career, Insertname has thrived in high-paced, high-stress clinical and managerial roles. His ability to maintain composure and make calculated decisions in challenging situations has consistently ensured the correct and timely course of action.  Insername has a well-established record of offering unwavering support and mentorship within the workplace. Notably, he has devised innovative tools aimed at risk mitigation and workflow enhancement, demonstrating his commitment to improving safety and efficiency. Drawing upon his honed skills from the mental health sector, \*Insername\* excels in facilitating productive, clear, and concise conversations, often delving into complex and sensitive subjects.  Some guy's approach is rooted in a compassionate, person-centred ethos that he carries into every professional endeavour. His experience, motivation, and adaptability make him a valuable addition to any team, ready to contribute effectively in the dynamic field of Cybersecurity. | |
|  | |
| Skills (Remove – Highlight your main skills, no more than 8, again if there is cross over add them) | |
| * Digital forensics * Penetration testing * Team Lead and Managementr * Training and Development | * Log analysis and SIEM Management * Governance, Risk and Compliance * Change management * Project management |
| |  | | --- | |  | | Work history | | |

## Company | Position (Example)

Jan 2022 - Present

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.

**CYBER SECURITY BOOTCAMP – SYDNEY UNIVERSITY | Student**

November 2022 – May 2023

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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Technical Proficiencies (Remove – Add software or technology that you are good at not that your aware of) | | | * SEIM   + Splunk   + Sec Onion * Vulnerability assessments   + OWASP Zap   + Nessus * Forensic   + Autopsy | * Cloud   + Microsoft Azure   + Amazon Web Services * Operating systems   + Linux   + Kali Linux   + Windows | | |
| EducationCertification: SEC+, CISSPMonash University - Bachelor of ScienceSydney University – Grad Cert in Cybersecurity (Finish Dec 2024)Training | |
| * TCM Practical Ethical Hacking * TCM Practical Web Application Security and testing * Adult Education Principles - Northern Sydney LHD | * ECcouncil C++ For Pentesters * Plain English Academy - Plain English writing * Hack the Box (Ongoing) * Try Hack Me (Ongoing) * Splunk basics (Ongoing) |

**Projects**

**Web application and hardening** | Cybersecurity Bootcamp

 The project was to create and secure a web application

* Using Azure I deployed a docker container with the framework for the web page. Then I was able to bind a self-signed certificate to the site. Finally using the Web Application Gateway, Azure Front Door and Security Centre Recommendations I was able to secure and protect the site from malicious actors.

**Penetration Testing** | Cybersecurity Bootcamp

* The project was to perform a penetration test on the fictitious Rekall Corporation
* As a team we completed a capture the flag exercise across the companies 3 domains of its website, Linux servers and Windows Servers. Utilizing a number of tools including Foxy Proxy, Burpsuite, Metasploit, Google Dorking, Nmap, Nessus and other Vulnerability scanning and exploiting tools.

**Building a Security Monitoring Environment** | Cybersecurity Bootcamp

* The project was to utilise a SEIM to monitor the fictitious Virtual Space Industries
* Utilizing Splunk and additional Splunk Add-Ons I was able to monitor the company's logs to detect a brute force attack. The style of techniques and location of origin for the attack were all able to be determined via the dashboards I had created.

**References available on request.**