detexian

Detexian Pty Ltd
114 Highett Road, Highett, VIC 3190
info@detexian.com
ABN 30 626 231 598

Aug 21 2018

To whom it may concern

Business case for a stay over 3 months | Tracy Ray Reed

Evidence about the nature, size, duration and importance of a project to the local community and any potential impacts to the business/community should the project not be able to proceed, including employment opportunities for Australian workers

No matter how strong the defense, cybersecurity breaches happen. Real time cyber surveillance is essential to contain issues promptly and minimize damages. However, this is currently out of reach for the average small-medium business in Australia as existing solutions are too complex and costly. Under the newly introduced Notifiable Data Breaches (NDB) scheme that requires businesses to report breaches, cyber surveillance is needed more than ever. Detexian makes it easy for small-medium businesses by providing a cost-effective online solution, eliminating hardware and lengthy complex configurations, and doing all the heavy lifting data mining work for system administrators.

According to a Frost & Sullivan study commissioned by Microsoft, cyber security incidents could cost Australian businesses $29 billion dollars per year. Small and medium businesses (SMB) are most vulnerable as attack targets because the majority of them are ill-equipped to mitigate cyber risks, vulnerabilities and intrusions. A study by Ponemon on the State of Cybersecurity in Small & Medium Businesses states that only 14% of SMB consider themselves effective at mitigate cyber risks, vulnerabilities and attacks. This means the majority of SMB are struggling to protect themselves.

While at Stanford Business School, Detexian's co-founders identified that the primary reason for SMB's ineffectiveness is over-reliance on off-the-shelf perimeter defense that only block known threats while being unable to monitor in real-time for abnormal and suspicious activity that form more advanced, unknown threats. This inability is in turn due to lack of budget and know-how. Existing advanced threat detection solutions are mostly enterprise offerings, hence too complex and costly for SMB to deploy.

To alter this grim status-quo, the co-founders created Detexian to pioneer a unique way to detect intrusions by monitoring log data with artificial intelligence. This approach drastically reduces the cost of monitoring, previously only affordable for enterprise businesses, and allows companies to minimize damages caused by breaches, which are usually exacerbated by late detection. As shown in this Cisco Infographic report, 33% of organisations are unable to identify a breach within 2 years.

Detexian validated the problem with experts at Stanford for twelve months before entering into a competitive selection and due diligence process to receive seed funding from lead investor, Sydney-based Right Click Capital Growth Fund. The decision to relocate to Melbourne was based on the growth opportunity, as Melbourne is set to become a leading hub for cybersecurity, as acknowledged by the Victorian Government.

There are significant positive opportunities for the Melbourne community linked with the success of Detexian. While there is a shortage of qualified and experienced cybersecurity staff, as outlined in the Australian Cyber Security Skills Shortage Study, there is a great need for enterprise grade solutions for small and medium businesses. Detexian provides a solution by automating time consuming and laborious roles, allowing cybersecurity professionals time and money to develop in other areas and achieve a higher level of protection and more effective response rate to threats and intrusions. Experts within Australian companies, according to leading IT strategy insight site 'CIO', are eager to adopt technology which can automate tasks such as data monitoring, as companies are inundated with data and there is a clear need for team collaboration to solve more complex issues, currently restricted by the time-consuming tasks.

The artificial intelligence which Detexian is developing has the potential to solve a significant and global industry problem, affording SMBs visibility and advanced effective risk management, protecting businesses and consumers. Having gone through stringent screening and due diligence processes, and being backed by institutional investors, if Detexian were unable to proceed, it would not only impact current employees and investors, but also a significant opportunity loss for the Australian community.

<u>Evidence that specialist advice/expertise from overseas is required – this may include evidence from an employment agency of a shortage of similarly qualified persons in Australia</u>

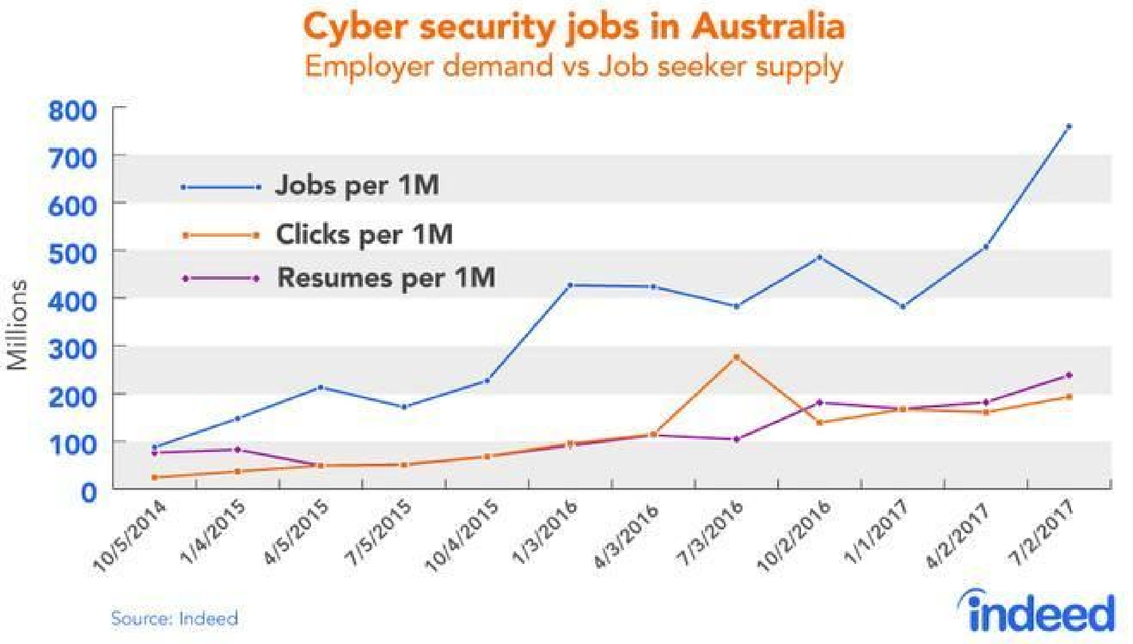

Chart 1. Source: Indeed.

Chart 1 from Indeed shows that demand for cyber security jobs significantly outstrips supply. Since 2014, the number of jobs advertised has been 2-4 times the number of clicks and resumes submitted by interested applicants.

Refer to chart 2. AISA (Australian Information Security Association) published an industry survey in which more than 78% AISA member respondents believe there is a shortage of qualified cybersecurity workers for positions in Australia.

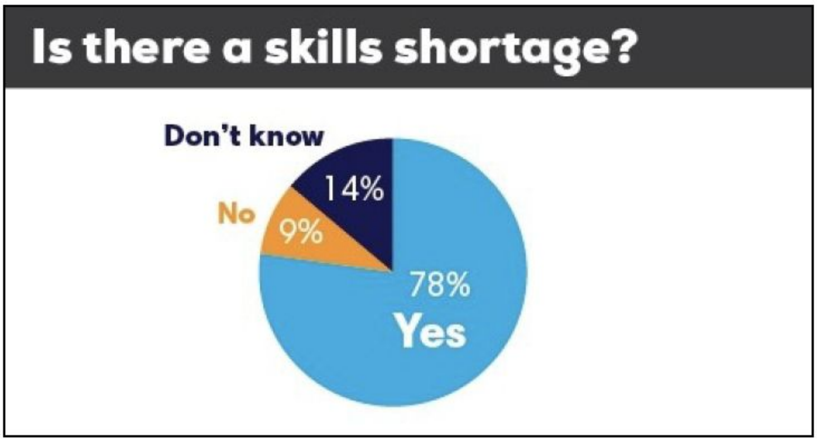

Chart 2. Source: Australian Information Security Association.

AustCyber, an Australian Government's Industry Growth Centre initiative, predicts around 11,000 additional cyber workers will be required to fill technical and non-technical positions over the next decade – and that's just to meet business-as-usual demands. AustCyber points to a serious cybersecurity skills shortage as one of the key three challenges that limits the growth of the Australian cybersecurity industry.

"While universities have recently begun to introduce several new study courses, they will unlikely produce enough graduates to meet industry demand in the near future. It is also questionable whether the industry will be able to draw workers with related skills from areas outside of cyber, as pathways for professional and transitional training are not currently sufficient."

Whether there are contractual obligations relating to the installation/servicing of a piece of equipment; any evidence provided by the applicant's proposed employer that they have tried unsuccessfully to hire an Australian to do the proposed work (for example, evidence of job search, training programs, letter of support from relevant union)

There is no installation/servicing of a piece of equipment to be done here.

The technology stack on which Detexian's products are being built was created by Tracy Reed, the visa applicant and Chief Technology Officer (CTO) of Detexian Inc, the parent company of Detexian Pty Ltd. As CTO, Tracy directs the technology development and the products based entirely on his experience and security expertise which he shares with the team.

Tracy's expertise has been accumulated from his 25 years of experience in the security and technology industry. This is not something which can be locally reproduced or trained for in time to meet the current need for security tools such as Detexian in order to take advantage of the hot security market opportunity. Without Tracy, the project will not exist and would not go forward at this stage.

The number of Australians being employed on the project and/or by the business

There are 3 Australians employed by the business, namely Tran Huynh (CEO), Vinod Subramanian (Systems and Development Director), and Katherine Goff (Digital Marketer).

The time available for an Australian to be trained to do the proposed work over a longer period

It is impossible to train an Australian or anybody to replace Tracy Reed to do the proposed work because Tracy has a unique combination of skills, intellectual property from his 25 years of experience, passion to make a difference to SMB cybersecurity and willingness to take a lower than market compensation to come to Australia to work on a startup venture. The entire Detexian security concept was created by Tracy. Without him, the project will not go forward.

As quoted from the aforementioned AISA survey, someone of Tracy's calibre is considered a "mythical unicorn" given his rare combination skillset of ethical hacking, scripting abilities, web application knowledge, public speaking and training experience. His dedication to the mission, including his willingness to relocate is clear, and his specific skillset is impossible to train or replace.

For a brief overview of his publications, presentations, achievements, and network, please see this Google search: https://www.google.com/#&q=tracy+reed+linux

We believe that Tracy's presentation, workshop, and teaching experience would be of great benefit to the Australian cybersecurity community and is both unique and impossible to replicate. We have already engaged with several educational and community groups to organise presentations, workshops, and keynote speaking events when he arrives. Please see the following links for more information regarding his past experience:

https://www.socallinuxexpo.org/scale/16x/speakers/tracy-reed
https://extension.ucsd.edu/about-extension/tracy-reed

Open Web Application Security Project presentation on log-based web app attack detection:
https://www.meetup.com/Open-Web-Application-Security-Project-San-Diego-OWASP-SD/events/158734172/

2017: 20 hour Linux Training Course for Skydriver IT, covering Linux fundamentals

KPLUG presentations on the following topics:
SSH security (Jul 2014)
Log based web app attack detection (Jun 2014)
TAILS: The Amnesiac Incognito Live System (security/anonymity tool) (Apr 2014)
Logstash: Centralized logging with a searchable interface for system administration, security, and general troubleshooting (Jun 2013)
Scribus Desktop Publishing Application on Linux (Oct 2011)
SSH security (Jul 2011)
GPG and SSH (Jun 2011)
Introduction to MySQL (May 2005)
Asterisk PBX
SELinux
OpenVPN
ATA over Ethernet

Large scale wireless security survey in San Diego, war flying research:
http://arstechnica.com/features/2002/08/warflying/
http://www.computerworld.com/article/2577318/mobile-wireless/war-flying--wireless-lan-sniffing-goes-airborne.html
http://www.g4tv.com/articles/39432/warflying-for-wi-fi/
http://www.ultraviolet.org/treed/writings/display.php3?document=warflying

"Silence On The Wire" computer security book review:
http://www.groklaw.net/articlebasic.php?story=20060618140712984
(War flying research features in this book)

Tracy Reed citations:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwifkIm9qv_cAhVriIQKHRsTAmkQFjAAegQIBxAB&url=https%3A%2F%2Fideamensch.com%2Ftracy-reed%2F&usg=AOvVaw1ZGOmOy3LEgaMIz9kzAiQH
https://ideamensch.com/tracy-reed/
https://ideamensch.com/wp-content/uploads/2017/04/TracyReed1.jpg
https://www.securitymagazine.com/authors/2287-tracy-reed
https://www.welivesecurity.com/2011/12/19/what-would-a-credit-card-breach-cost-your-company/
https://www.nextadvisor.com/blog/finding-a-hipaa-compliant-web-host/
https://www.esecurityplanet.com/trends/article.php/3933491/Is-Linux-Really-More-Secure-than-
https://www.sharefile.com/blog/wp-content/uploads/sites/2/2017/09/data_security.jpg
https://www.networkworld.com/article/3191804/security/healthcare-records-for-sale-on-dark-web.html
https://images.techhive.com/images/article/2016/12/medical_records_laptop_doctor-100699858-

Published piece:

https://www.securitymagazine.com/articles/87943-payment-data-compliance-12-major-requirements-of-the-pci-data-security-standard