DAVID CLARKE

Cyber Security Professional / People Leader / Cloud Security Advocate

🚠 **Melbourne**
🌐 **Australia**
🏠 **Also available remotely**
@ dave@david-clarke.id.au
📱 +61 Please reach out to me privately (email/keybase) if you require my mobile #

🏠 david-clarke.id.au
🔥 KeyBase - davidclarke_au
🔑 PGP - 1234 E339 C30C C855
t Blog
in linkedin.com/in/davidclarkeau
○ GitHub - davidclarke-au
🦊 GitLab - davidclarke-au
🐦 @davidclarke_au
M david-clarke-au.medium.com
🐦 Click me? ◎ Click me?

A Little Bit About Me 🐾

I **loathe** writing CV's, but I understand why it's required, hence why it's now in a 🔀 Code Repository. Simple to update, modern, backed up and demonstrates many technical skills right off the bat.

I honestly think you should get a good picture of who I am, what I do and what might be a good future fit for me from the links above. OSINT ☺

This CV is ordered deliberately. In my opinion, in order of importance.

Starting with me, an informal and honest introduction. 😬

Followed by what I work on day to day and am responsible for, my skillset and what I'm passionate about.

Followed by my work history.

Followed by my training and education.

What I love doing is **TALKING** to people…. So please feel free to get in contact with me and setup a chat.

Anyway, all the boring stuff below…

Skillset / Passions / Areas of Interest 👍

Cyber Security **Culture, Awareness & Uplift**
Cyber Security **Leadership**
Cyber Security **Strategy**
Cyber Security **Evangelist** (is there a non-religious equivalent? If so, that….)
Cloud Security, with preference to aws

Working with clients to assist in **Security maturity uplift** and continual service improvement

BugBountys - from a client (SaaS) side though, assisting companies doing the **initial discovery** and beginning their **journey into Bug Bounty programs** via BugCrowd, HackerOne, Cobalt.IO etc…

Data Centre - have historically completed a significant amount of work and large projects in **Data Centres**. Always something I've enjoyed.

Experience 💼

CyberCX

SOC Operations Manager - VIC - Managed Security Services

In my role as SOC Operations Manager (VIC) MSS I am responsible for overall delivery, performance and continual service improvement of Managed Security Operations Centre (SOC), Security Information and Event Management (SIEM), Vulnerability Management System (VMS), Managed Endpoint Detection & Response (MEDR) and Digital Forensics & Incident Response (DFIR) offerings.

The SOC Operations Manager (VIC) MSS is a key member of the MSS leadership team in the region. The Manager - SOC Operations (VIC) MSS leads the activities and management of the Managed Security Services operations team in the region, positioning CyberCX as Australia's greatest force of cyber security professionals.

Senior Service Delivery Manager

In my role @ CyberCX I am responsible for

Service Delivery Management - Managed SIEM, SOC, VMS, MEDR, DFIR
Service Transition - Project -> BAU
Service Delivery Governance
Service Level Risk Management

Security Operations Management:
Lead and Owner of SecOps Process & Procedures
Lead and Owner of SecOps Governance
Continual Service Improvement
Enhancement and Innovation
Service Activation and Onboarding
Bridge between Service Delivery and Security Operations

CyberSecurity Project Management

PreSales engagements for CyberCX portfolio offerings

Enosys Solutions

Senior Service Delivery Manager

(this role folded into CyberCX in July 2020)

In my role @ Enosys I am responsible for

Service Delivery Management - Managed SIEM, SOC, VMS, MEDR, DFIR
Service Transition - Project -> BAU
Service Delivery Governance
Service Level Risk Management

Security Operations Management:
Lead and Owner of SecOps Process & Procedures
Lead and Owner of SecOps Governance
Continual Service Improvement
Enhancement and Innovation
Service Activation and Onboarding
Bridge between Service Delivery and Security Operations

CyberSecurity Project Management

PreSales engagements for Enosys portfolio offerings

2016 – 2019

PageUp

Head Of Security & Compliance

I was promoted into this global role to ensure PageUp's IT Assets are secured by best of breed technology, practices and processes whilst maintaining compliance with relevant contractual and industry obligations in order to accelerate the growth of PageUp. Growing the team was also an important function in this role.

Create, maintain and operate PageUp's cyber security strategy leveraging appropriate technology, threat information, training and operational processes in order to reduce the likelihood of business critical security breaches.

Track and communicate technology risk to the business in order to ensure the leadership team are adequately informed to make decisions on resource allocation, budgets and risk mitigation.

Support the growth of the business in all targeted markets by externally promoting PageUp's security platform USP to clients, prospects and the wider market. Ensure PageUp gains/maintains appropriate security credentials and certifications to leverage in promotion of USP.

Manage and maintain a security technology budget with appropriate spend to meet the needs of the operation and implementation of the cyber security strategy

Champion and embed a culture of security awareness and practices in order to enable autonomous teams to progress unimpeded whilst ensuring security of outcomes delivered.

ISO Compliance & Security Officer

My role at PageUp at a high level boils down to maintaining and constantly improving PageUp's Information Security Management System (ISMS) ensuring PageUp People's security practices meet the needs of its clients and industry standards.

Key tasks include -
maintenance of ISO 27001 certification
manage information security risks (identify, assess, document, propose treatments and manage action plans)
work with other team members to implement a variety of information security controls
conduct regular checks on the effectiveness of security controls
arrange regular information security meetings and audits

document clear and concise procedures and configuration standards to meet policy and audit requirements

regularly review and update information security policies

process information security incident reports and any suggestions for information security improvements

develop information security awareness material and run awareness sessions

work with other team members to assess the information security risks related to new initiatives and identify appropriate controls

develop information security responses to tenders and client queries

monitor security threats and bulletins

monitor data privacy threats and bulletins

perform Adhoc duties as assigned

2012 - 2016

VicSuper

Analyst IT Security & Operations

The purpose of the role is to provide technical expertise and assistance in security operations, projects, infrastructure and daily business needs.

There is a high degree of complexity in the role, balancing projects, vendor management, change management, problem management and incident management.

Security Operations Project Management/Coordination IT Operations administration Stakeholder management ServiceDesk Support SOE/desktop management

IT Infrastructure Specialist

The purpose of the role is to provide technical expertise and assistance in projects, infrastructure and daily business needs.

Pre 2012

Previous Work History

Previous work history before 2012 can be provided on request or visible on my LinkedIn

Blogs & Articles 〰

Dates stated on articles - Ongoing

Links: LinkedIn **in** - Medium **M** - Other

📑 **Tackling MFA for AWS Organization Member Accounts** - **in** - **M**

With the recent advice published by AWS around best practice for MFA on AWS Organisations (not a typo 🌐😊) management and member accounts, I thought it would be a good chance to write up how I tackled this previously and hopefully provide some guidance for others.

🌍 **GDPR & PageUp Security** - **M**

The aim of this article is to talk though some key GDPR terms and the parts of the GDPR that matter to our clients and how we are addressing them.

🔑 **PageUp Passwords — Housekeeping and Best Practice** - **M**

A short piece on password best proactive for SaaS and the options that PageUp provided for clients. SSO vs Non-SSO.

📦 **AusPost Parcel Lockers — Hardening Required M** - 📑

I wanted to call this piece AusPost Parcel Lockers - Insecure by Design but we agreed to change it. A write up on a discovered Security weakness and the follow ups, disclosures etc.

🔒 **PageUp Disabling TLS 1.0 𝐌**

A blog discussing the reason for the disablement of TLS 1.0, who, what, when, why etc…

𝕐 **Deleted your Yahoo! Account? Check again… 𝐌** - 📧

A write up of the mess that was deleting a Yahoo account post their Security Incident.

G **G Suite + SPF, why bother? 𝐌**

A piece on the very frustrating shortcomings and insecurities of GSuite SPF and DKIM implementation, which was thankfully fixed.

🎸 **Stevie Ray Vaughan — Cast of Thousands 𝐌**

Eh, not tech related, but a passion piece.

Training 📖	My **preferred way of learning** is on the job, with smart, driven and passionate people!	Ongoing

AWS Security Fundamentals   2016

This self-paced course is designed to introduce you to fundamental cloud computing and AWS security concepts including AWS access control and management, governance, logging, and encryption methods. It also covers security-related compliance protocols and risk management strategies, as well as procedures related to auditing your AWS security infrastructure.

Nessus Deployment — Tenable University

Nessus Scanning — Tenable University

Nessus Analysis and Reporting — Tenable University

ITIL-F HDAA, Melbourne   2011

This certification verifies that support center professionals possess the knowledge of the ITIL® framework necessary to support an ITIL initiative. ITIL Foundation certified individuals have demonstrated their awareness of the ITIL processes and terms and satisfied the prerequisite requirement for pursuing additional ITIL certifications.

Education 🏛

Customised Course, EXCOM Education, Melbourne, VIC, AUS.   2005-2006
Given my previous credits earned in my diploma, I sat a customised course at EXCOM Education which consisted of the CompTIA A+ Hardware and Software Course and the Career Builder Course. Once completed I was hired by EXCOM.

Diploma of eBusiness Support, Computer Power Training Institute, Melbourne, VIC, AUS.   2004-2006
The course provides the comprehensive training needed in today's business world to develop and support electronic business solutions. Completion of the course includes the attainment of two of the industry's highly sought, globally recognised vendor certifications:Microsoft Certified Professional and either a CompTIA i-Net+ or Red Hat Linux Certified Technician certification.

VCE, Successfully completed Year 12 and achieved my VCE, State School FTW.   2003

Conference activity 👤   2019

BSides Melbourne 2019

Speaker, Strengthening Security in a Post-Incident World.

I spoke @ the inaugural BSides Melbourne 2019 on "Strengthening security in a post-incident world"

The structure of my talk was to talk about the incident, who we are, the legislative landscape that we faced, the challenges we saw and how to strengthen security from the lessons we learnt, both technical and non technical.

The goal of the talk was to share with the wider Security community what happened, share knowledge and leanings, and give attendees easy to implement suggestions for potential uplift at their own companies.

Interests ⛺

Come on, we covered this above… OSINT. Hit up my **t** then we can talk ◎ or 🍺 or 🏁 or ⛰ 🚶

Languages 🔤

Native: English
Basic: None, yet, hopefully Italian soon :)

Personal ℹ

Birth date: I'm likely applying for a Security role, so adding this should fail me instantly. Plus you don't need this information at this stage of the recruitment process anyway.
Citizenship: Australian Citizen
Family: Married, Dad to one

References 👥

Available on request only..

Source

git | LAST COMMIT | FEBRUARY | LICENSE | MIT

Clone away, help yourself..