purplecon sydney 2024

everything you need to know about cyber in 20 minutes or less*

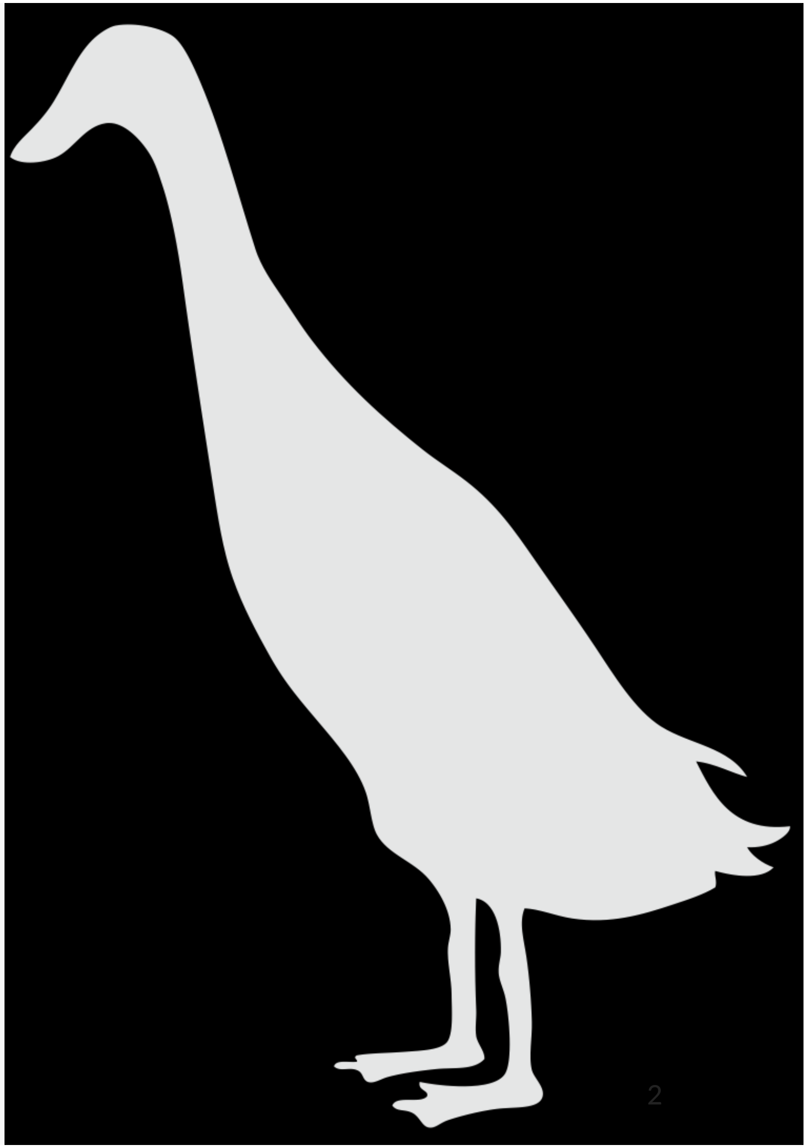
*or more

whoami

Liam O’Shannessy

Executive Director
Security Testing & Assurance VIC/TAS
CyberCX

linkedin is a hellplace
RIP infosec twitter
I guess mastodon is it now for social media?
@liamo@mastodon.social



what even is

cyber?

security operations

tools & tech

- specific tools eg EDR
- overview tools eg SIEM
- vuln detection

processes

- correlate signals
- respond / don’t?
- trends?
- intel
- compliance / cost - log retention etc.

people

- security operations centre (SOC)
- working as a team
- humans

security operations versus…

threat hunting

- SOC might threat hunt in response to:
  - a new 0day
  - an incident
- SOC can suffer from *sample bias*

incident response

- SOC will do initial response - lock down a host / account
- initiate IR process

digital forensics & incident response

digital forensics

- what happened?
- driven by:
  - legal?
  - HR?
- evidence quality & chain of custody

incident response

- what is the current state of play?
- phases:
  - identification
  - containment
  - eradication
  - recovery

IR - the forgotten phases

- preparation
- crisis comms
- lessons learned / intel

cyber intel

~~intel means having a threat feed of Indicators of Compromise (IoC's)~~ in 2010

past, present, future

- threats and threat actors
- understand the past and present
- forecast the future?

intel everywhere

- security ops
- incident response
- offensive security
- governance and risk
- strategy

why

- threats evolve
- so what? what next?

offensive security

pentesting is

- discovery and identification of vulnerabilities
- limited in scope and duration
- analysis of vuln impact
- noisy

pentesting is NOT

- following the tactics, techniques and procedures of real-world adversaries
- vulnerability scanning
- a good test of detection & response

ideal pentesting

- risk-informed scope
- open book
- intel-driven

offensive security + cute colour coding

red teaming

- following the tactics, techniques and procedures of real-world adversaries
- assesses not just vulns but detection & response
- takes time

purple teaming

- red + blue
- open book
- automated vs manual

testing considerations

- what environment?
- scope?
- how often?
- when?

AppSec

"push security left"

appsec

- ~~“leave security till last”~~
- integrating security into all parts of the ~~software~~ development lifecycle

secure SDLC phases

- analysis / design:
  - threat modelling
  - security requirements
  - supply chain
- implementation / verification
  - automated testing (SAST/DAST/SCA)

also

- security training
- security champions
- ProdSec?
- Infrastructure as Code

identity and access management (IdAM)

identity

- who is this person/system and how do they prove it?
- proving it via something:
  - you know
  - you have
  - you are

access management

- process & mechanism for managing access to a system

considerations

- multi-factor auth
- phishing-resistant auth

identity and access management (IdAM) - more

privileged access management (PAM)

- securing admin & system access
- additional risk = additional controls
- can passwords be avoided? press button access
- approval workflows

work lifecycle management (LCM)

- joiners/movers/leavers
- integration with HR systems
- role-based access controls (RBAC)

workforce identity governance and administration (IGA)

- require approval / report for access levels that may raise risk - “toxic combinations”
- access reviews

governance, risk & compliance

- what? policies
- how? standards & procedures
- why? risks
- frameworks

- compliance - because you gotta

- frameworks are guidance, not gospel
- people

cyber strategy

“what is the perfect amount of cyber?”

aims

- enable the organisation to achieve their goals securely*
- *without overinvestment

how

- business impact identification / assessment
- critical assets
- information / insights / analysis

considerations

- people and process over technology

everything?

... no

Infrastructure

How we secure our datacentres, networks, nodes, cables, clouds, containers

Architecture

Secure design patterns. Well-Architected Framework

SaaS

and the various other aaS's

Communication

Privacy / Safety / Reliability

.

Education / Training / Awareness

.

nobody has all the answers. security is team game. working together, we’ve got this

thank you to these legends

Amanuel Wolde - Security Operations

Jay Banerji - DFIR

Cyber Intel - Katherine Mansted

AppSec - errbufferoverfl

IdAM - Meredith Begg

Leon Li - GRC

Strategy - Lachlan McGrath