ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Cyber Education Awareness & Influence

Enabling Security in DevOps

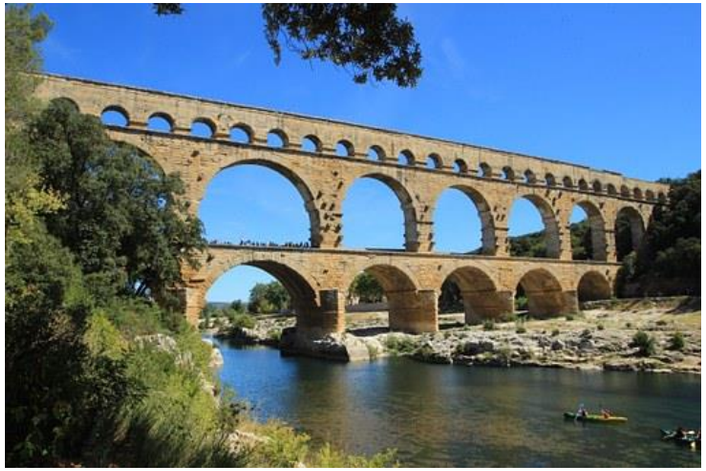
Suzi Dyke, Telstra

The need for speed - Moving to Agile, DevOps delivery...

How DevOps teams can view security

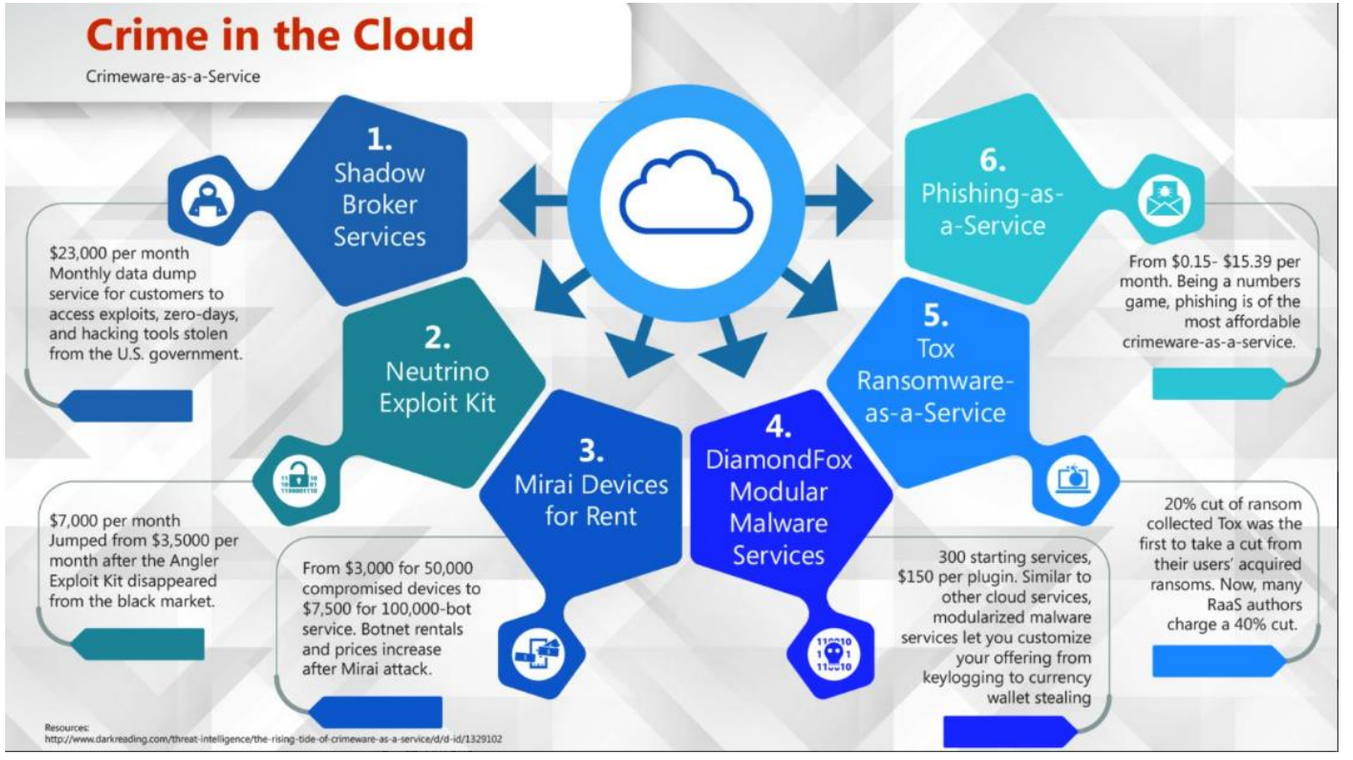
How security teams can view DevOps

Collaboration.

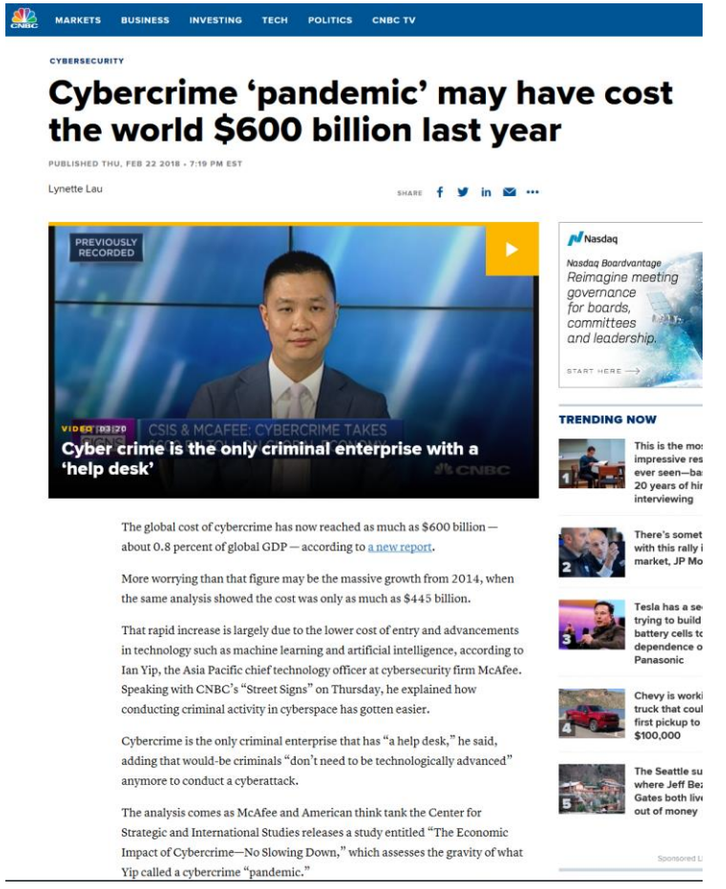


The industrialisation of crime…

Increased threat landscape…



Increasing business impacts…



1. https://www.darkreading.com/threat-intelligence/the-rising-tide-of-crimeware-as-a-service/d/d-id/1329102 & https://www.linkedin.com/company/the-cyber-security-hub/?feedView=images
2. https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html

Increasing regulatory controls...

Mandatory Data Breach Notifications

A number of States in the US have had data breach notification laws in place for some time.
The European Union, as well as New Zealand, have both introduced breach notification laws.
On 16 June 2015, Canada passed legislation to introduce a national mandatory data breach notification scheme. Australia implemented mandatory data breach notifications on the 22 February 2018.[1]

EU General Data Protection Regulation (GDPR)

The regulation will fundamentally reshape the way in which data is handled across every sector, from healthcare to banking and beyond**.**
GDPR was enforced on 25 May 2018 – and organisations that are not compliant could now face heavy fines.
Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location.
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).
The conditions for consent have been strengthened.
Under the GDPR, breach notifications are now mandatory[2]

1. https://www.oaic.gov.au/privacy/notifiable-data-breaches/
2. https://eugdpr.org/

DevOps Security Strategy

Highly empowered and accountable DevSecOps teams

Operating in a self-sufficient, autonomous manner

Delivering resilient, customer-centric and secure solutions

Education, Awareness & Influence

Highly empowered and accountable DevSecOps teams

Operating in a self-sufficient, autonomous manner

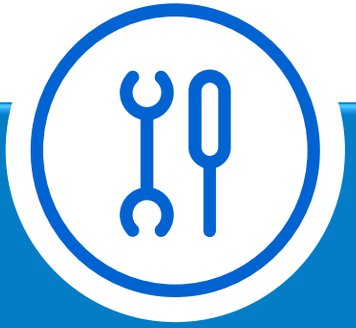
Delivering resilient, customer-centric and secure solutions

People

Security education, awareness & influencing behavioural change

Process

Training on processes & linkage to Security Capability Maturity Model



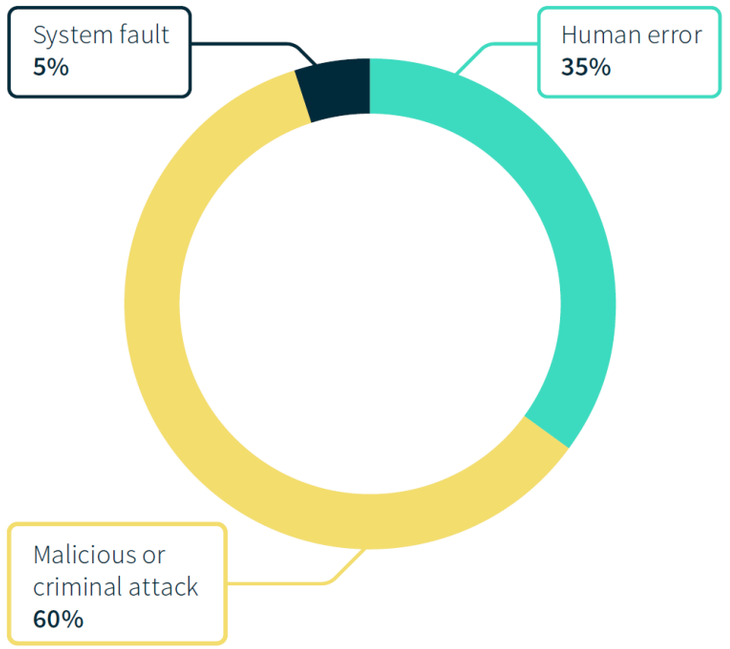
Technology

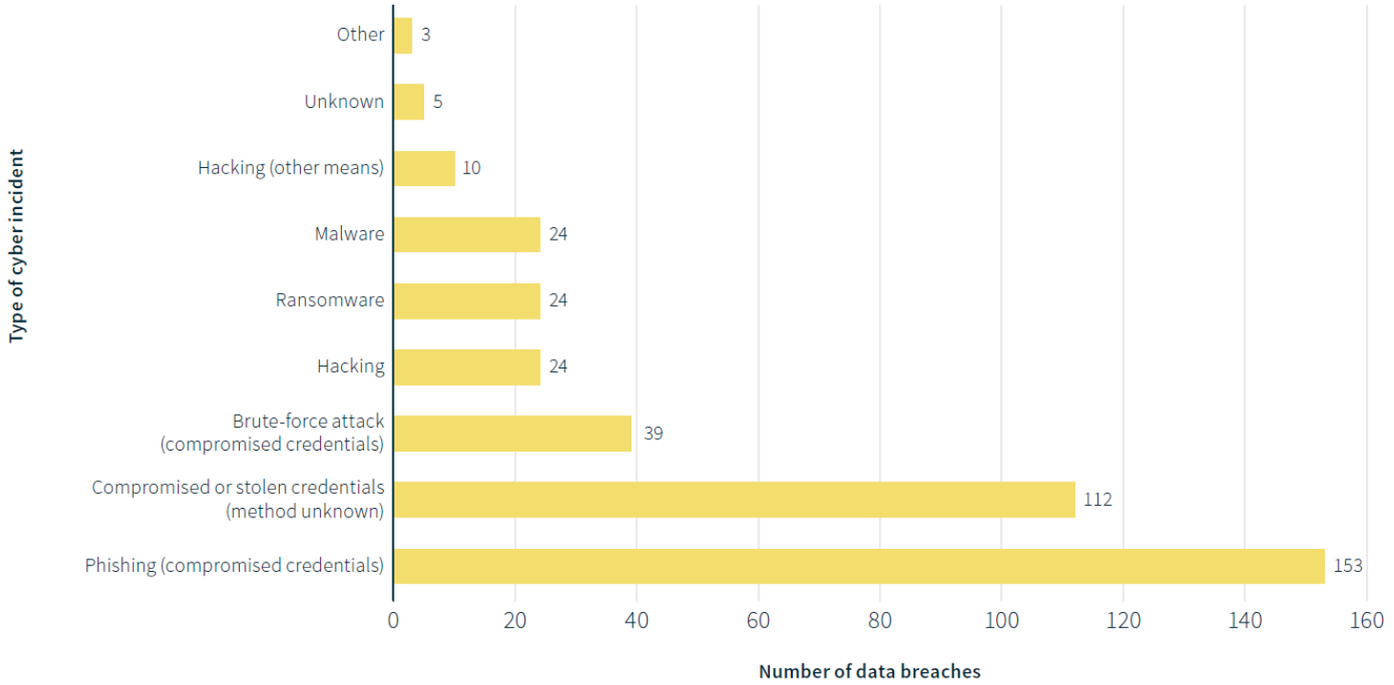
Training on security tooling usage

CYBER SECURITY IS AS MUCH ABOUT PEOPLE AS IT IS TECHNOLOGY

Even the best technical security efforts can be undermined by a weak security culture. Security needs to be everybody's responsibility

- Human error was a major source (35 percent) of reported breaches[1].
- Of those attributed to 'malicious or criminal attack', a significant number involved a human factor, such as tricking employees to click on a phishing email or to disclose passwords[1].





1: OAIC Notifiable Data Breaches Scheme: 12-month Insights Report (May 2019)

Cyber Awareness

The Business

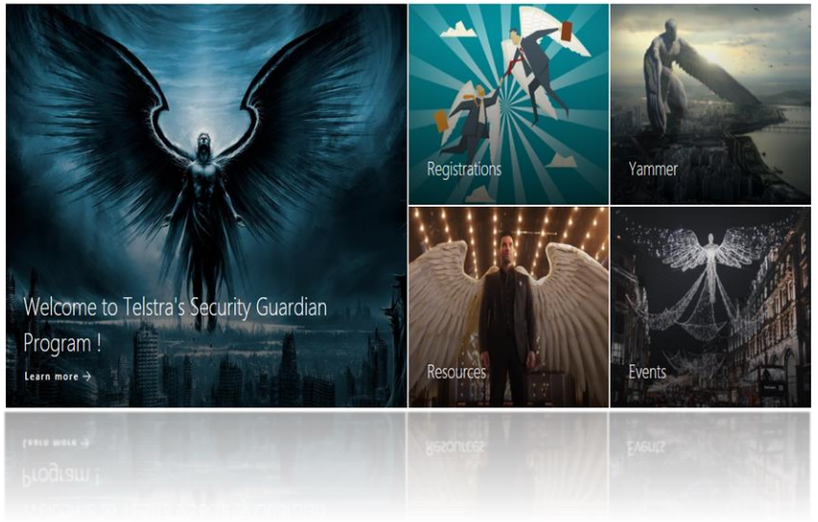
Security awareness is driven by the

Evangelist Program

Product Owners/Scrum Masters

Security knowledge & awareness is driven by the

Security Guardian Program



DevOps Teams

Security knowledge and awareness is driven by the

Security Champion Program

Business

Technical

Cyber Awareness for new Graduates

Business Awareness

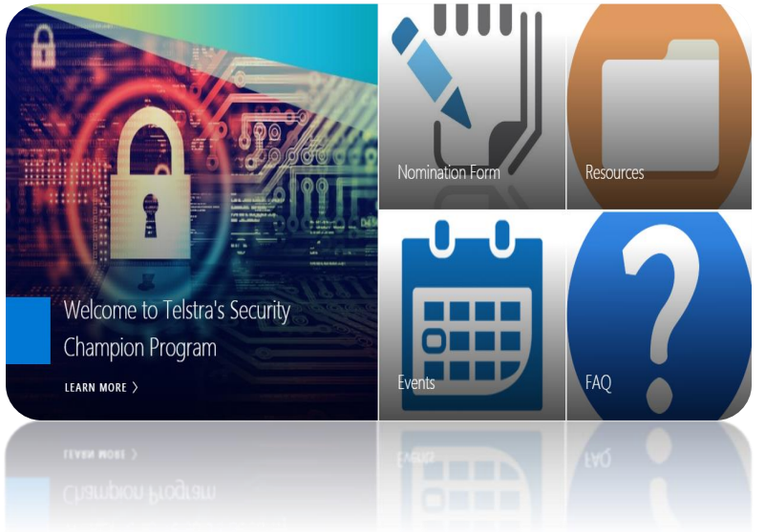
Security awareness is driven by enrolment in the Evangelist Program

Graduates run their own Secure Coding Tournament

Secure Coding tournament driven by graduate program

DevOps team Awareness

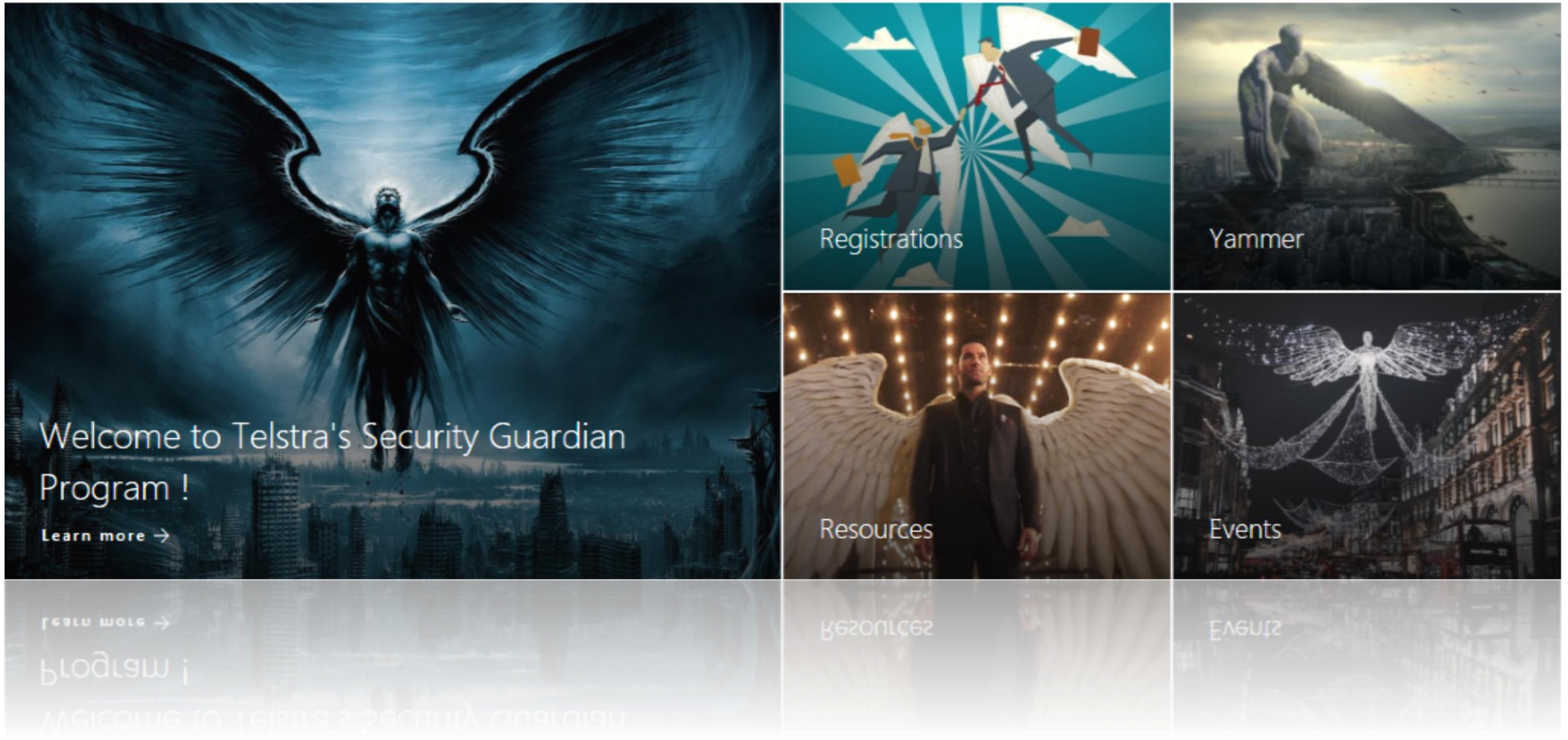
Security knowledge is driven by enrolment in the Security Champion Program



It is proposed that new graduates will be enrolled in the Evangelist and Security Champion Programs as part of their graduate training

Business Focus — Technical Focus

Security Guardians – Piloting



Security Champion Program

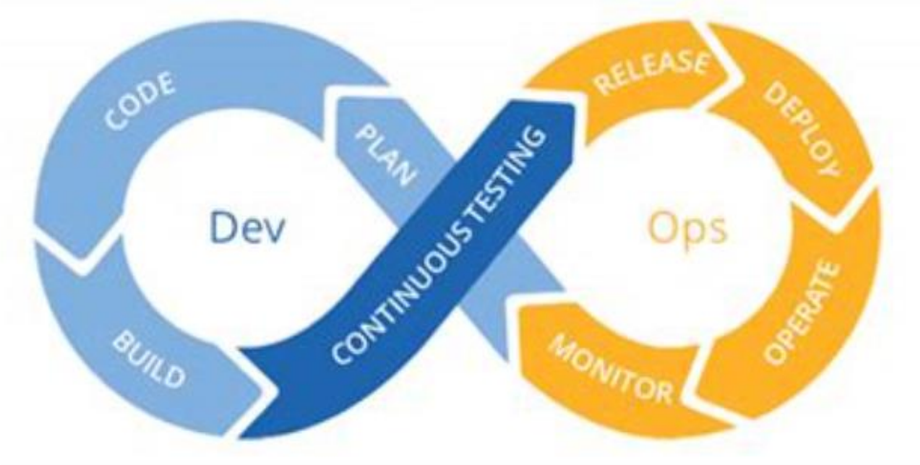
Creating a culture and capability of security within DevOps teams

- Create a culture of security
- Uplift team skills
- Liaison for Cyber Security > 2-way relationship
- Understand priorities for Security Assessments
- Identify and prioritise vulnerability resolution
- Oversee integration with automated security tools

Security Champion Program Training Scope

Security Champions Globally

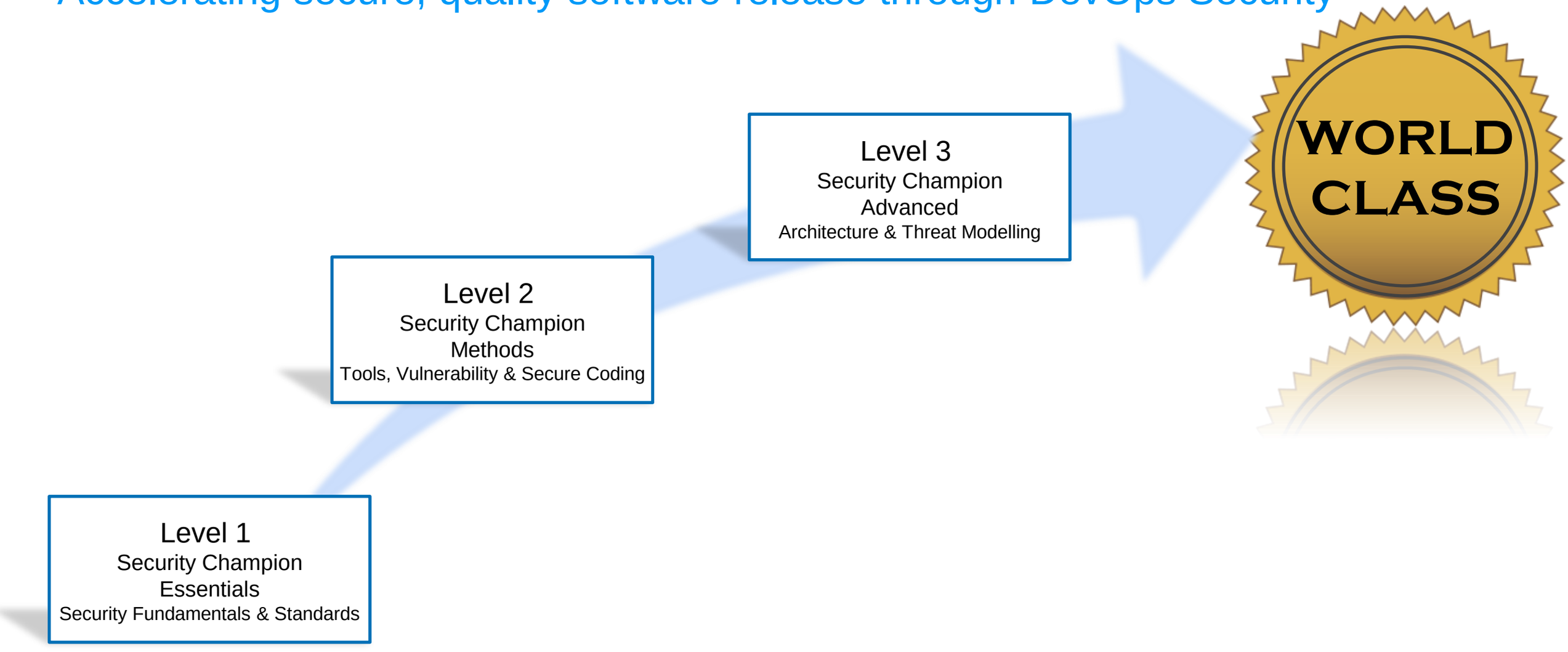
Security across the full DevOps Lifecycle



Security is integrated within each phase of the DevOps lifecycle

Security Champion Accreditation

Accelerating secure, quality software release through DevOps Security

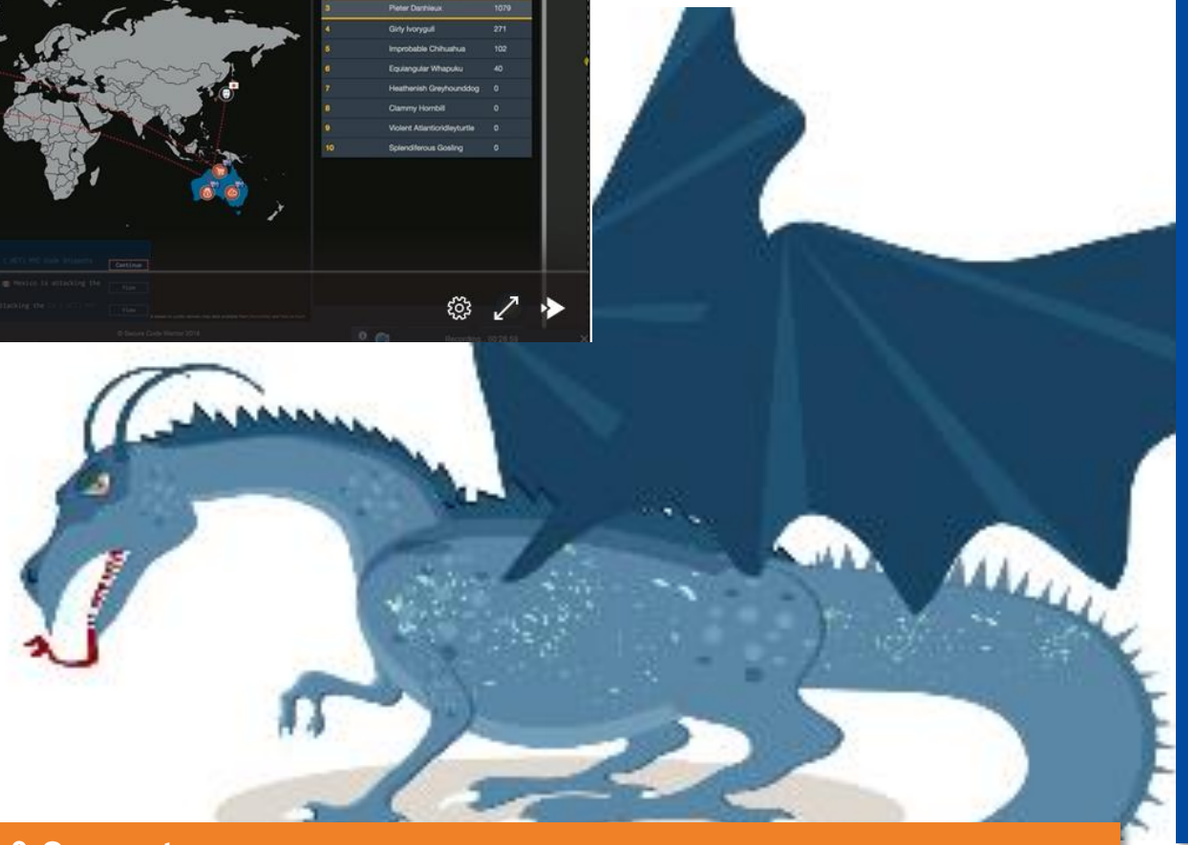


Security Champion SharePoint – Live and growing

(Includes support resources)

Security Champions Tournaments and Talks

Security Champions Tournaments



Cyber Security "Brown Bag" Education Sessions

Date	Topic	Attendees
Jul 2018	The A-Z of Application Security	181
Aug 2018	TSSR and Cyber Risk Management	194
Sept 2018	Vulnerability & Penetration Testing – from 20 000 feet	195
Oct 2018	Secure Code, Break/build and Jetpack	159
Nov 2018	Security Architecture & Standards	136
Dec 2018	The Red Team	143
Jan 2019	* Walk through of real-world attacks	126
Feb 2019	Continuous Vulnerability scanning	93
Mar 2019	Creating Abuse test cases	144
Apr 2019	* Container/Docker image security	157
May 2019	* Removing secrets from code repositories. Credential Management in CI/CD pipelines (AMP/PCF)	91
Jun 2019	* Best practice for security logging and feeding SIEMs	120
Jul 2019	Threat Modelling	155
Aug 2019	* Transport Layer Security – Ciphers and hash algorithms	154
Sep 2019	Socrates to Security Breaches	55
Oct 2019	Patching and vulnerability remediation	140
Nov 2019	Cyber Awareness	-
Dec 2019	Automating policy compliance in cloud environments	-

Communication & Support

Security Champion SharePoint site, with resources to support DevOps teams

Security Champion Distribution list for updates and notifications

Security Champion Yammer group where DevOps teams can ask Cyber Security questions

Security Champion Engagement, Recognition and Rewards

Coffee Catch-ups

Meetups between Cyber Security and the Security Champions

Recognition

Certificates presented as Security Champions complete levels 1, 2 & 3

Level 1 Certified Security Champion

Level 2 Certified Security Champions

Hall of Fame for tournament winners

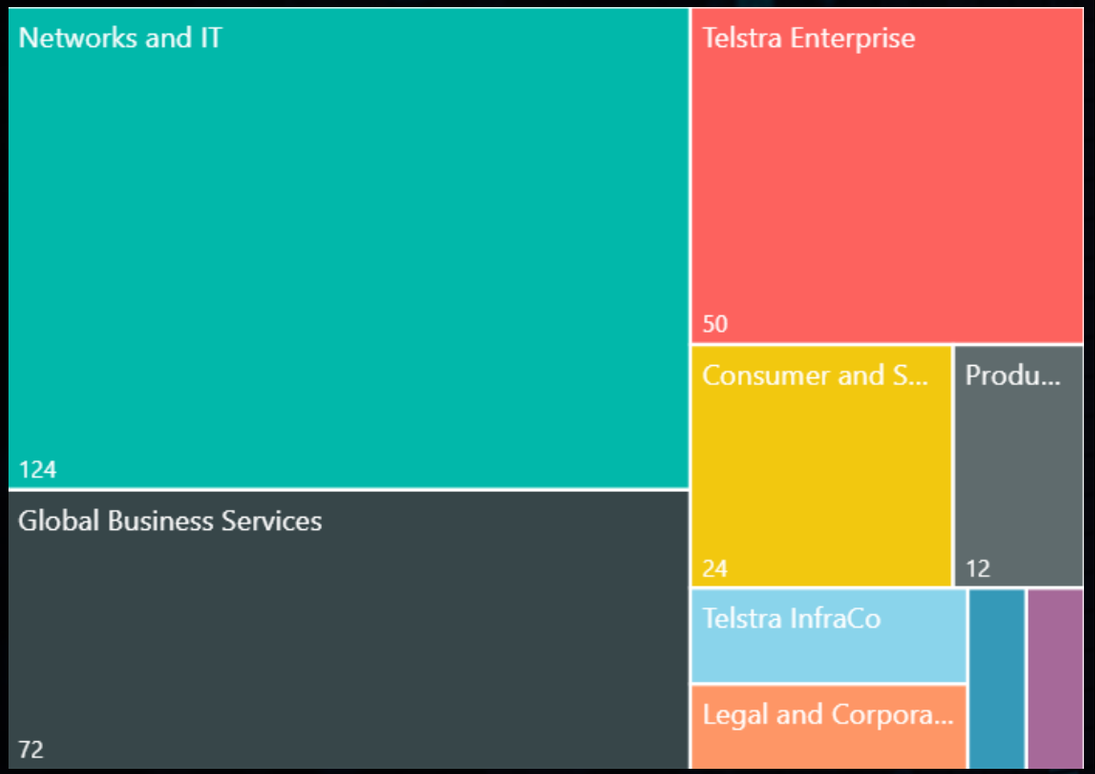
Global Security Champion Tournament

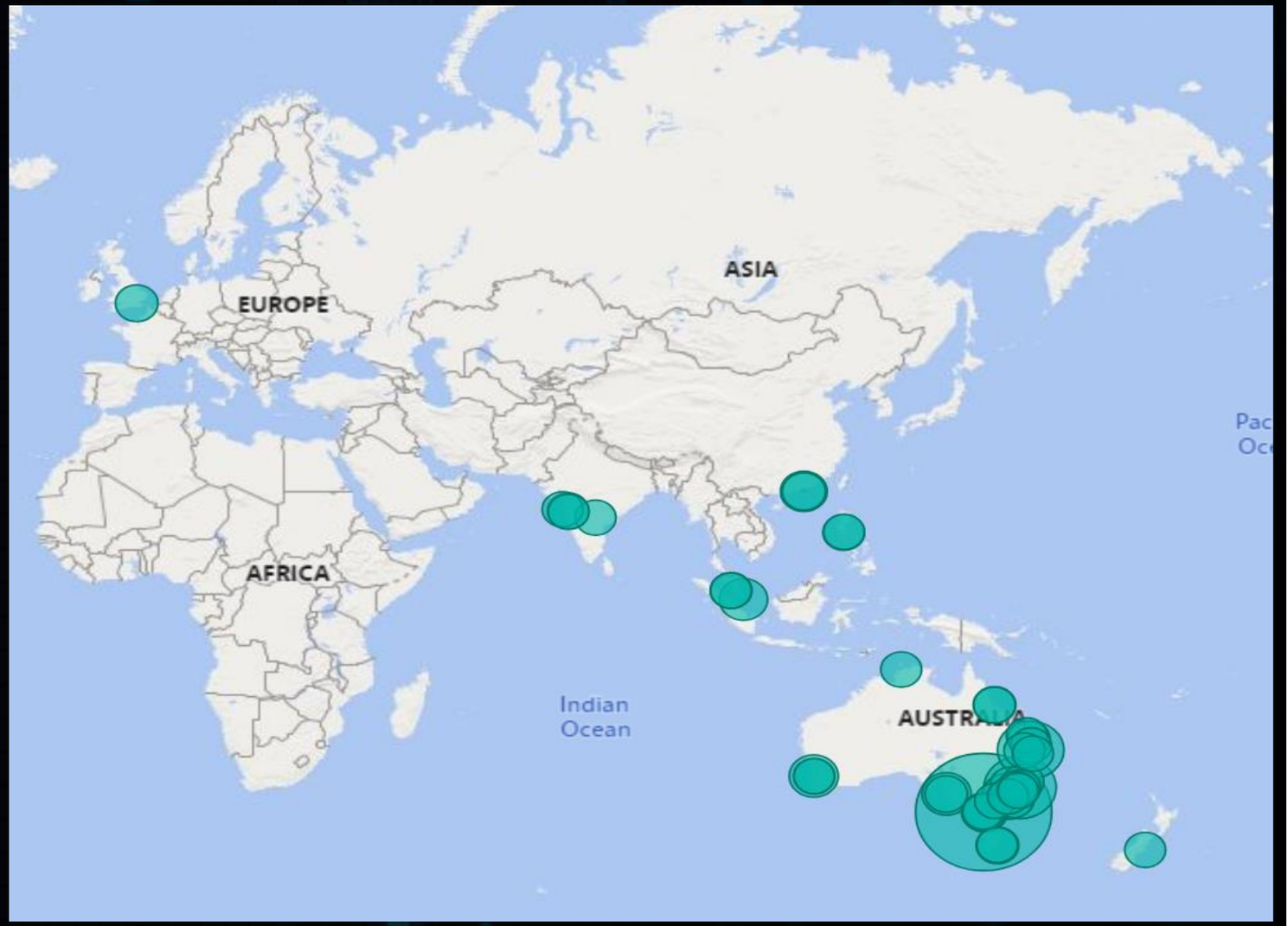
Security Champion Outstanding Achievement Awards

For the individual that delivered security outcomes in FY19, they were awarded 1st Prize, second Prize, third Prize and prizes for honourable mentions.

CYBER SECURITY EVANGELIST PROGRAM

The program now comprises almost 350 members from all states and territories, 8 countries and all BUs.



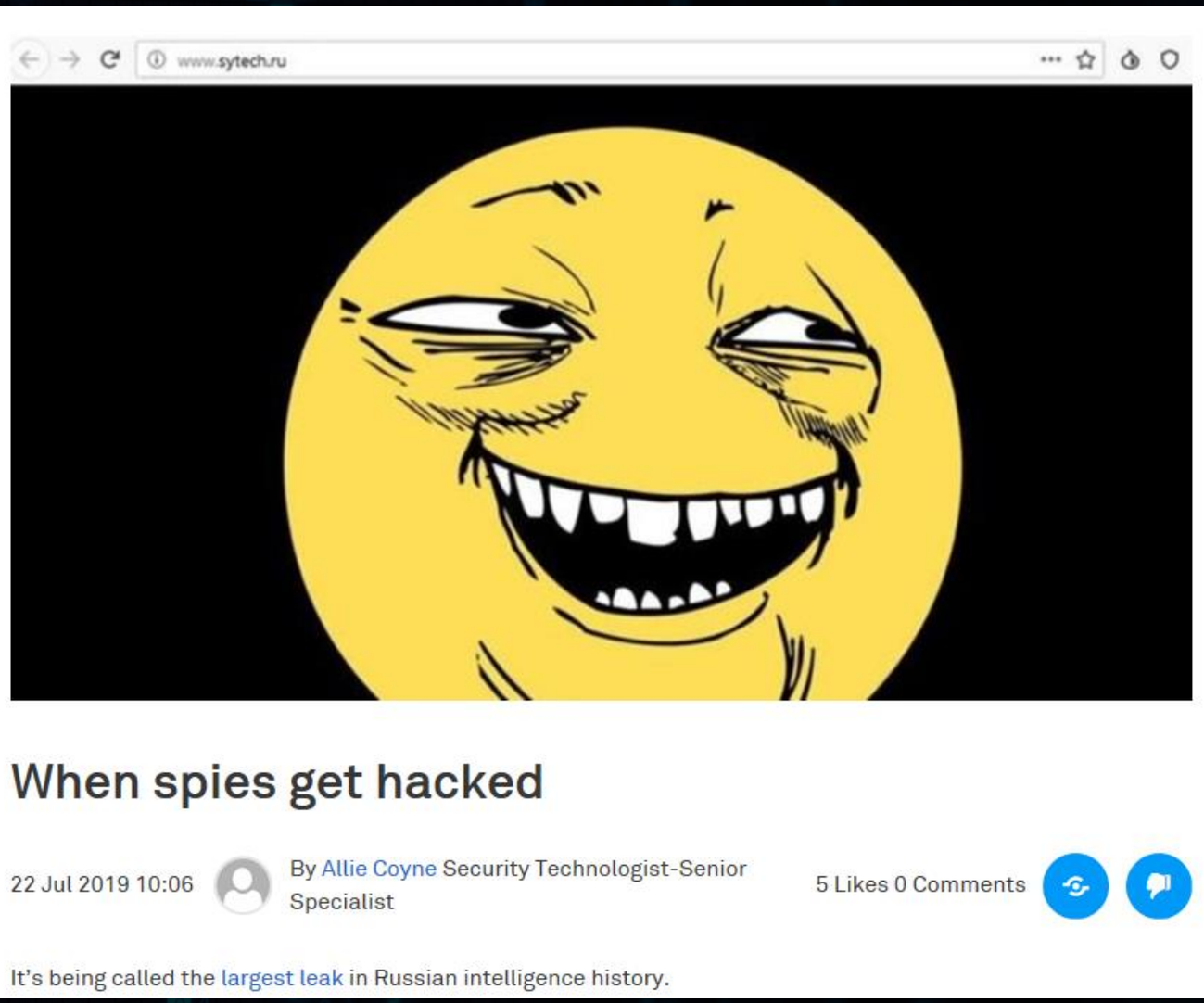


WHAT'S IN IT FOR THEM?

- Monthly **information sessions** with security SMEs
- A monthly '**debrief**' informing them of the latest threats impacting Telstra
- The opportunity to request security **awareness services**, including targeted phishing drills, team briefings & a tour of the CTRC
- Access to a thriving and engaged **community** of security enthusiasts
- ...and **merch** from the 'merch store' (posters, wallpapers, banners & an email sig block generator)

DECODED

DECODED launched in late 2018 and now has over 500 subscribers.



Observations…

- ❑ Creation of security education programs identifies security gaps
- ❑ Attendance links to feedback
- ❑ Effective security awareness is greater than just DevOps
- ❑ Customisation makes training relevant
- ❑ Gamification makes learning fun and get buy-in
- ❑ Consider maintenance
- ❑ Consider limitations (time zones, budget, geography etc)
- ❑ Metrics for learnings

There are many pieces that need to come together!

Outcomes…

- ❑ 20-30% improvement in secure coding skills (based on Secure Code Warrior data *% from when the developers started at the beginner skill level, to when the developers complete the skilled skill level)*
- ❑ DevOps Team say they didn't think much about security while delivering but now they do
- ❑ Stakeholders liked the program so much they are planning to create testing champions, automation champions etc.
- ❑ Improved relationship between IT and Security

We need to team to succeed!

What now? Capability is still rolling out…

- ❑ Ongoing engagement - tournaments, meetups, brown bags etc
- ❑ Customisation for different domains
- ❑ Updates driven by data/feedback/change
- ❑ New training on emerging threats & technologies/capabilities

We are still on our journey and have lots of work to do going forward!

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

StateFarm

GOLD SPONSORS

vmware

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XebiaLabs

cloudbees

Carnegie Mellon University Software Engineering Institute

TIGERA

CONTINO

NowSecure

MEDIA SPONSORS

DZone

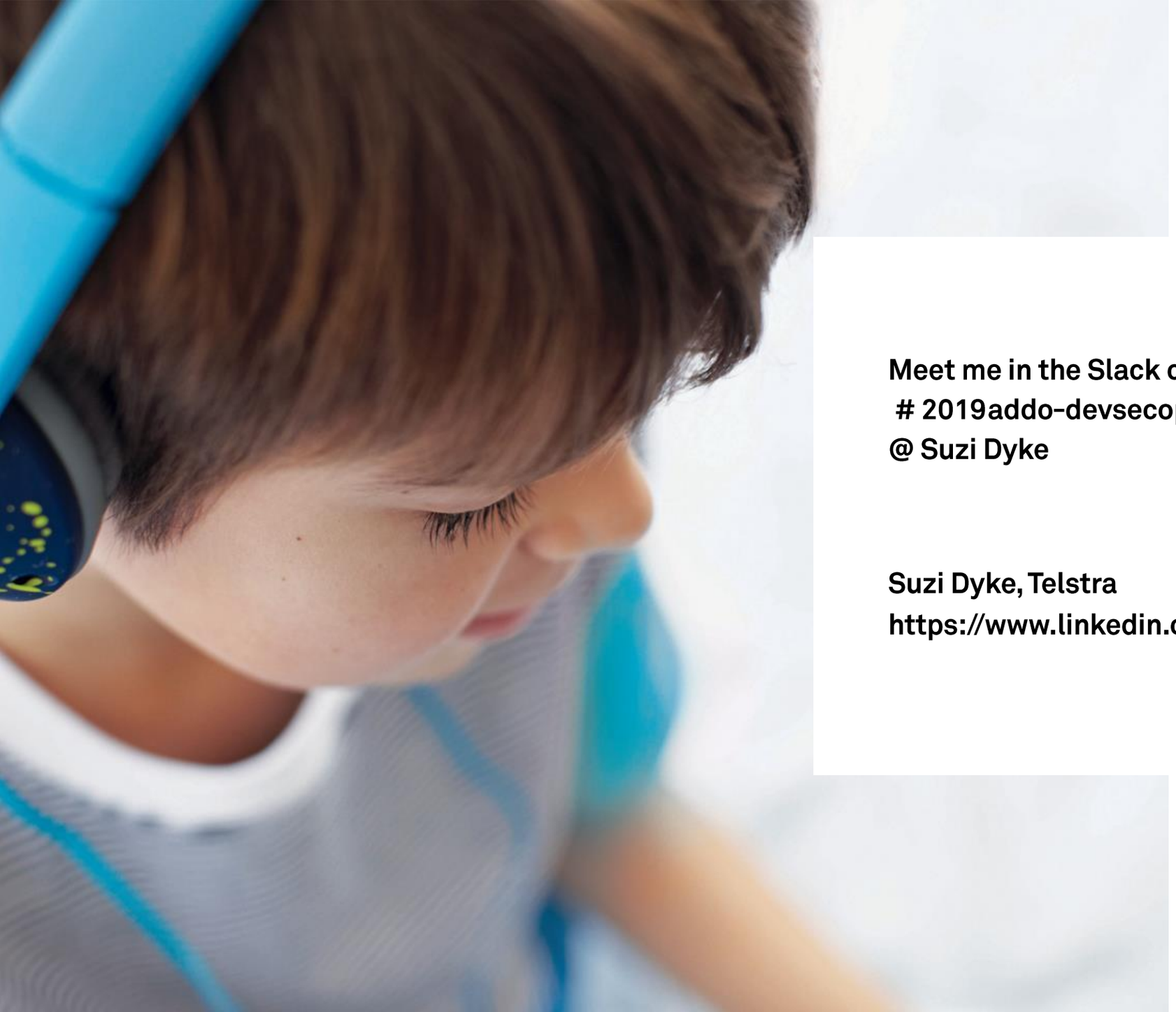
TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire



Meet me in the Slack channel for Q&A
2019addo-devsecops
@ Suzi Dyke

Suzi Dyke, Telstra
https://www.linkedin.com/in/suzanne-dyke/