Thank You to Our Sponsors and Hosts!

OWASP
NEW
ZEALAND
owasp.org.nz

DATACOM

QUANTUM
SECURITY

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

myob

Pulse Security
www.pulsesecurity.co.nz

VOCUS

security initiative

SEQA
Information Security

Without them, this Conference couldn't happen

What We Said (35 mins)

ABSTRACT

Wherever you find yourself, we often find ourselves looking at the other "side" of security and wondering what it's like. In this session, we'll share some lessons from both sides of the fence. Is the grass really greener? Is that fake grass, carpet painted green, or…really impressive mould?

DESCRIPTION

There are many different parts to be played in security. It's easy to find yourself thinking someone else has it "easier" when they've really got their own set of challenges. The two of us went from the outside as Pen Tester and Auditor, to the inside as Head of Security and Assurance Lead – securing one of New Zealand's biggest online companies. We learned a whole lot along the way, about communication, motivation, technology, business, and ourselves.

We'll have stories from the outside, lessons from after, and tips for success. We'll pass some of what we've learned, and hopefully make you understand, and empathise with, those you interact with just a little bit better.

False Dichotomy (n):

~~*“[A] fallacy in which a statement falsely claims or assumes an "either/or" situation, when in fact there is at least one additional logically valid option.”*~~ – *Wikipedia*

*“A handy narrative device for storytelling”** – *Kate*

*We have references for the full “rainbow” of colors in the appendix

Outline

Opening (1 min)
Quick Discussion on intersectional security and false dichotomy (1 min)
Background and Terminology (5 mins)
- History of Red and Blue (1 Min)
- Introducing Red & Blue (2 mins)
- Introducing Kate, Chloe, and Trade Me Security (1 min)
- How this talk is going to work (1 min)

Match 1 - Motivation (Bubbles vs Experts)
- (B) Security isn't a bubble. Unless you're selling bubble blowers.
- (R) The expert's dilemma (experts love completeness, edge cases, and spherical cows)

Match 2 - Communication (When/Why vs How)
- Process - Talk after analysis (R), or during (B)? - To make a decision (B) vs when a decision is made (R)
- How - Language - Talk in the way the other side does, not your own dialect, and NOT a pidgin. (B @ R)

Match 3 - Technology (Exploitation vs backwards engineering)
- Exploitation - Proof of vulnerability is not proof of failure (R)
- Backwards Engineering - Reverse engineering is not merely engineering in reverse - Poc is MUCh easier than a scalable solution (B)

Match 4 - Business (Appetite Vs Ideology)
- Appetite - Business is about taking sensible risks (B)
- Ideology - Security is a continuum, don't treat is as a religion (R)

Match 5 - Ourselves (Stretches vs priorities)
- Stretches - It's HARD to adjust from breaker to colleague (R)
- Priorities - Finding what's wrong is different to finding what matters (B)

Scoreboard - Summary
- Easy problems on one side are impossible on the other
- Good business on one side is destructive on the other
- Some "Simple" things aren't so simple
- Some "good ideas" are terrible

Podium - Conclusions
- Context makes the difference
- Motivation matters
- Communication matters
- Empathy Matters

Afterparty
- K thnx, Bai
- Appendices

Presenting

Kate Pearce (@secvalve)

and

Chloe Ashford

From

Trade Me

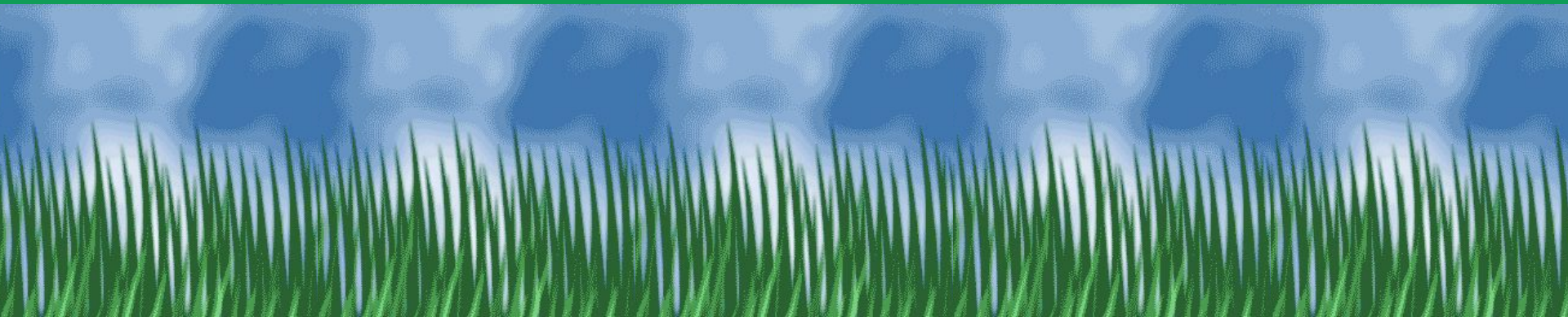
at

Appsec NZ 2021

entitled:

Red vs Blue

Which Grass is Greener?



Introducing....

The Trade Me Security Team as:

In the Red corner ... Kate

The away team

Outside

Attacker

Rattling the doors

In the Blue Corner... Chloe

The home team

Inside

Defender

~~Shaking in their Boots~~

Kate will argue for the hacker view

Chloe will defend the home turf

Matches

- **Motivation** – Who is living in a bubble?
- **Communication** – How do you get things done?
- **Technology** – Which technical challenges are better?
- **[Y]ourselves** – Jumping over the fence is easy, right?

Match 1: Motivation

Motivation

Experts

I'm right in theory, wrong in practice

Experts give guidance that aligns to industry best practice and standards

I give great advice.

Other consultants agree!

Practitioners

I'm wrong in theory, right in practice

Practitioners actually make stuff happen

I decide and take action.

Match 2: Communication

Communication

Precise

I have a bunch of carefully chosen words to convey a specific meaning

I search for gaps to fill to meet a standard

I am most concerned with the things you're doing wrong

Persuasive

I choose my words appropriately to drive a specific outcome

I translate the gaps in the standard into tasks

I make sure we do things more right

Match 3: Technology

Technology

“Engineering” Backwards

I show what’s broken so you can fix it

I tell you what looks bad, and how bad it can be

I show you remediation options you can do

Risk Aversion

“Backwards” Engineering

I decide what’s worth fixing

I decide if it matters, and how much I care

I work out which fixes are actually achievable

Risk Appetite

Match 3:
[Y]ourselves

[Y]ourselves

Stretches

Jumping the fence requires more flexibility than you think

Know your biases, adapt for them

Priorities

Finding what's wrong is different to finding what matters

Know your oversights, adapt for them

Summary of Results

Which Grass is Greener?

The “other” one*

*Neither - It’s concrete as far as the eye can see

Summary Item 1/2:

Some “simple” things aren’t simple

Easy problems in one part of security are impossible in another

Summary Item 2/2:

Some “good” ideas are terrible

Good business in one type of security business can be destructive in another

Post-Event Analysis

Working across the Red/Blue Divide:

1. **Empathy** – Put yourself in their shoes
2. **Motivation** – Yours is not theirs
3. **Communication** – Persuade, don't preach

Remember: Context makes the difference

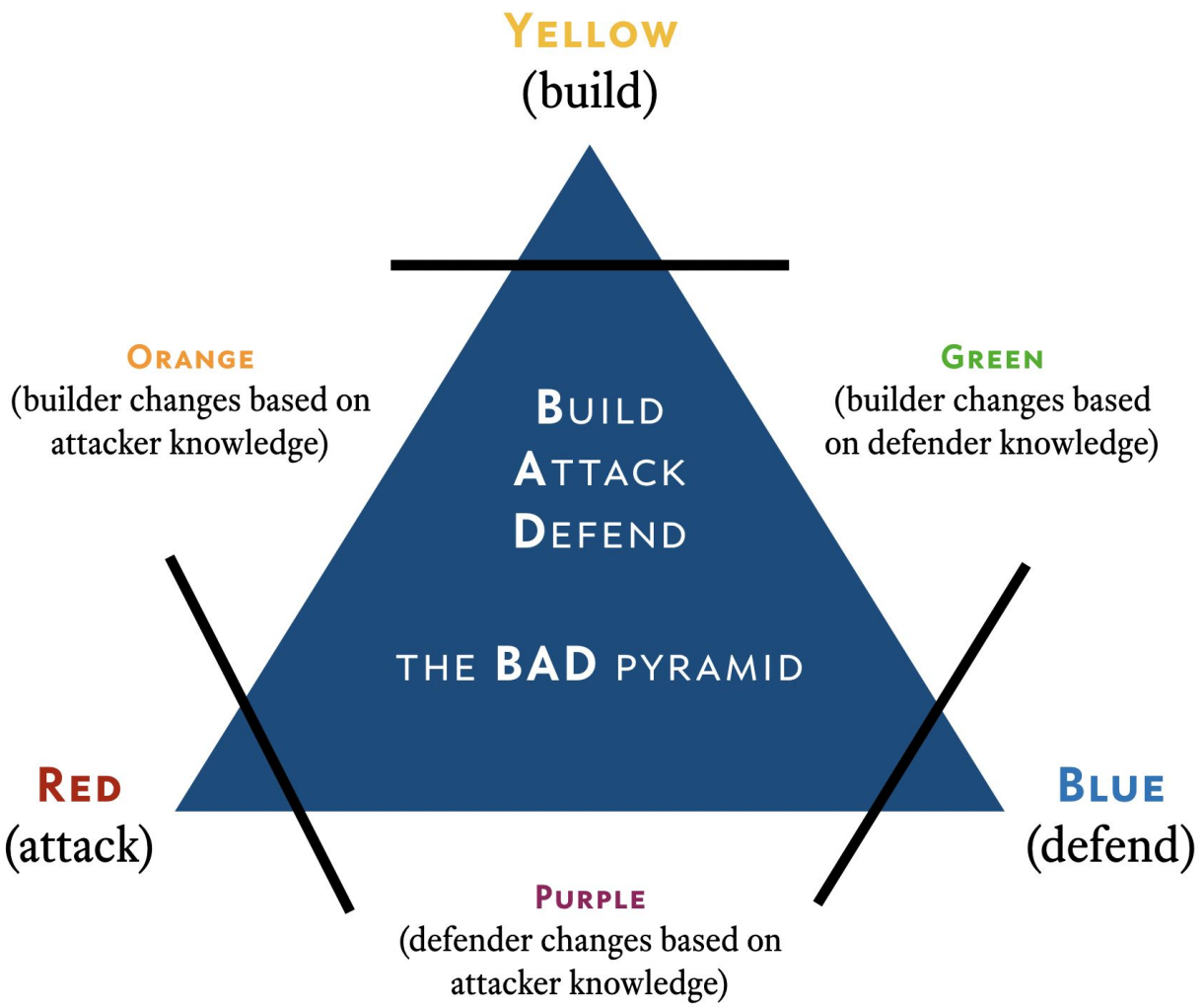
Questions?

Kate: @secvalve
Chloe: ...TikTok?

Afterparty(?)

The Full Infosec Colour Rainbow

(Not printer cartridges)



See

- April Wright, BH USA 2017 Orange is the New Purple
- Daniel Messler - The Difference Between Red, Blue, and Purple Teams