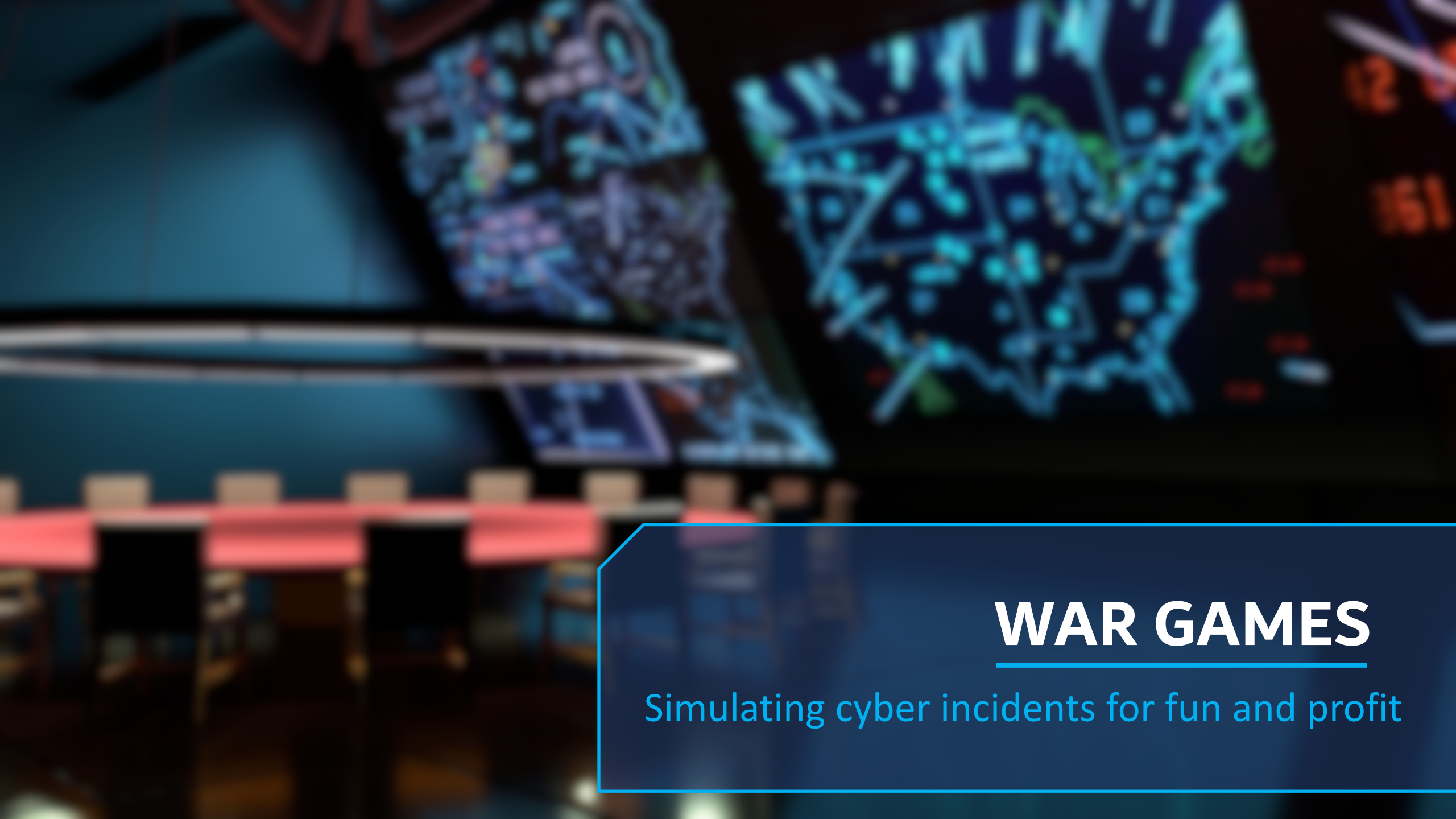


WAR GAMES

Simulating cyber incidents for fun and profit

Who am I?

Steve Davies

@northvein

Consultant at DeltaSec IS

Co-founder of DC151

DC151 DC44114

DC151 is a regular social gathering in Leeds for hackers, makers & people interested in security & tech.

Follow us on Twitter! @_DC151

When: Every 2nd Wednesday

Where: A well known Leeds location

Who: Everybody Welcome

Format: Anything goes

Length: 30 mins max

How: Contact the Organisers

This Talk

Core Concept

What is a War Game?

Purpose

Why you should War Game

Planning I

Designing a war game

Planning II

Running the war game

Execution

How to run your own tests

Game Over

Concluding testing, reporting & next steps

BSides Leeds 2019

Track Two

Time: 14:00

Attendance: ~120

Matt Hall

@pentestmatt

Audience Participation

Lightning Scenario 1

C-Level Phish

Lightning Scenario 2

Supply Chain Compromise

Core Concept

What is a War Game?

Definition

War game (disambiguation)

From Wikipedia, the free encyclopedia

War Game or **War Games** may refer to:

- Military exercise, a training operation
- Military simulation, a live or computer exercise to develop military strategies
- Single combat
- Wargaming, a recreational game simulating a military operation
- Wargaming (company), a videogame developer and publisher
- Wargame (video games), a genre that emphasizes strategic or tactical warfare on a map
- Wargame (hacking), a challenge involving exploiting or defending a computer system vulnerability
- Business war games, a role-playing exercise set in the world of commerce
- Airsoft (sometimes known as "wargames"), a combat sport using non-lethal pellet weapons
- Board wargame, a genre that emphasizes strategic or tactical warfare on a map
- War (card game), a simple card game featuring a series of "battles" between two players

Literature [edit]

- "War Game" (short story), 1959, by Philip K. Dick
- *War Games*, a 1966 novel by James Park Sloan
- *War Game* (novel), a 1993 children's novel about World War I

Film and television [edit]

- *The War Game*, a 1965 BBC television film
- *The War Game* (1962 film), directed by Mai Zetterling

Our Definition

A War Game is a training exercise which allows an organisation to test various components, processes and individuals through the use of a realistic scenario.

Quick Survey

- **Who has done any sort of scenario testing before?**
- **As an organiser?**
- **As a participant?**

Entry Requirements

You don’t have to be an expert

You’ll need buy in & sponsorship

You’ll need to do some planning

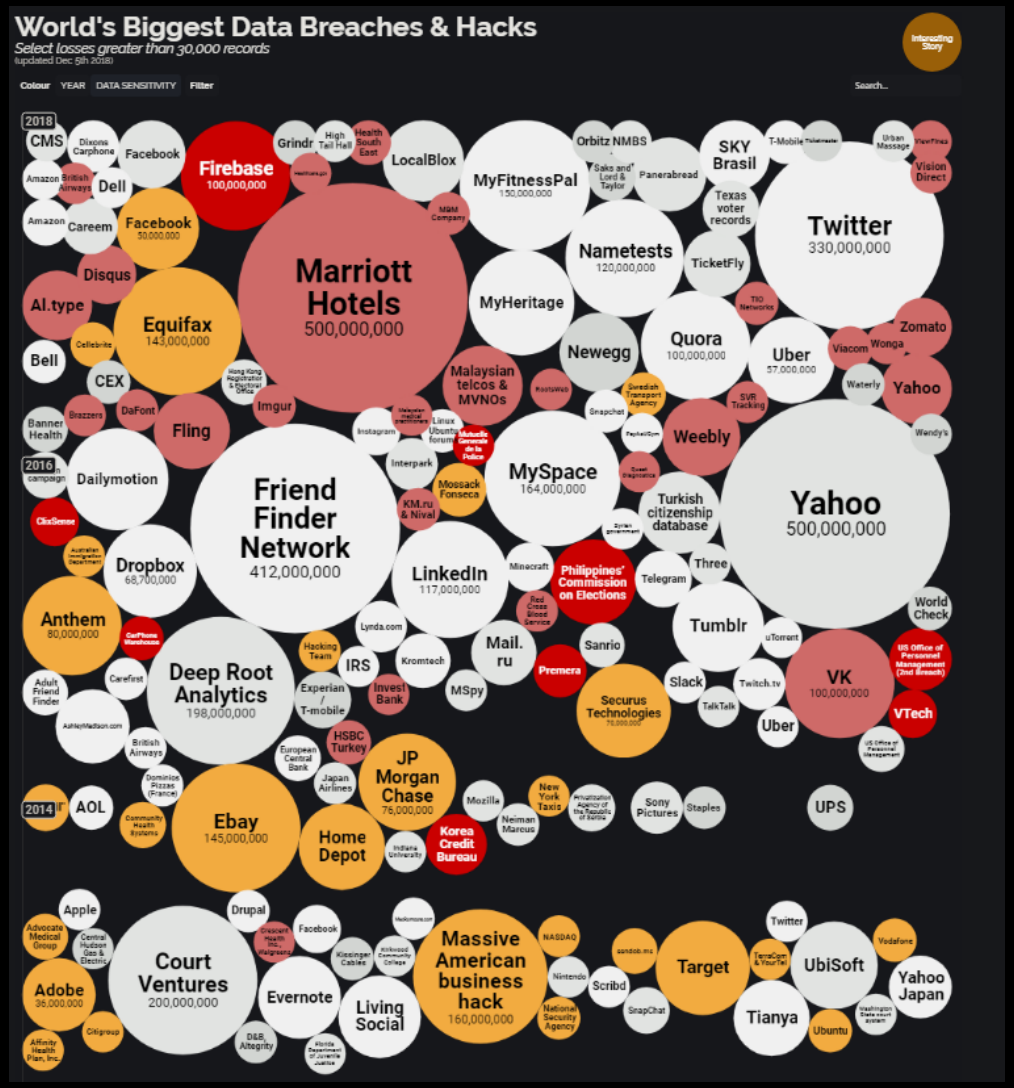
You’ll need to see it through

You’ll need to write a report and present it

Purpose

Why you should war game

The Age of Assume Breach



Ransomware and distributed denial of service attacks (WannaCry/NotPetya/Mirai)

Supply chain compromises (MeDoc/CCleaner)

Massive data breaches (Equifax, Uber, Yahoo)

Fake news and information operations (US Election/Brexit Disinfo Ops)

The Age of Assume Breach

Team Work

Readiness

Strategies

Resilience, Response, Recovery

Why War Game – How to sell it

Exercise Incident Readiness

Leadership, People, Processes, Technology

Demonstrate Investment & Alignment

Internally and externally

Consequences of Not Testing

Internally and externally

Consequences of Testing

Things to consider

Why War Game – How to sell it

Exercise Incident Readiness

Exercise Leadership

Why War Game – How to sell it

Exercise Incident Readiness

Exercise Leadership

Exercise People

Why War Game – How to sell it

Exercise Incident Readiness

Exercise Leadership

Exercise People

Exercise Processes

Why War Game – How to sell it

Exercise Incident Readiness

Exercise Leadership

Exercise People

Exercise Processes

Exercise Technology

Why War Game – How to sell it

Demonstrate Value - Internally

People – headcount, training, retention…

Technology – controls, software, monitoring…

Why War Game – How to sell it

Demonstrate Alignment – Internally

Maintains awareness with key stakeholders and responders

Aligns priorities across the business

Why War Game – How to sell it

Demonstrate Value & Alignment – Externally

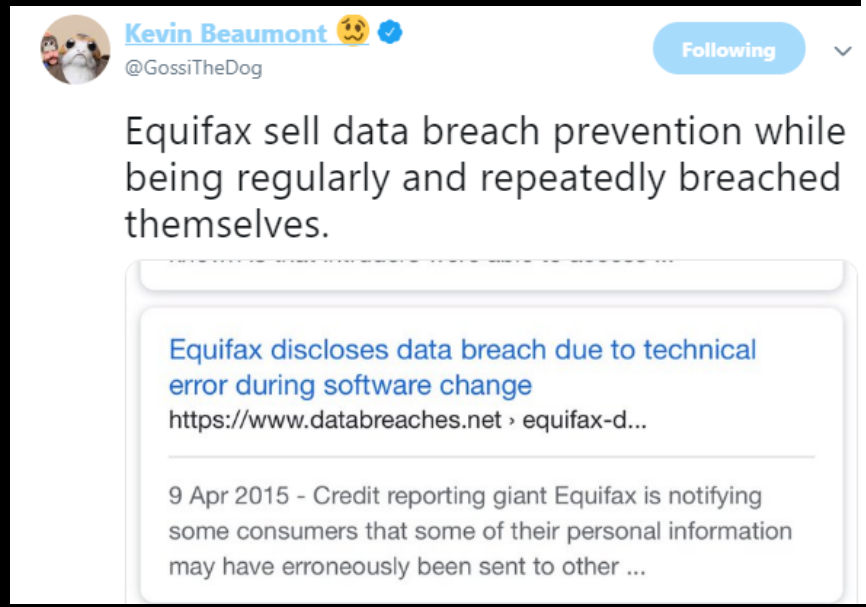
Demonstrates the maturity of your organisation (Insurers, regulators…)

Affects your brand, trust in your org and consumer confidence

Draws attention to competence of leadership team

Consequences of not War Gaming

As word gets out, you'll likely become the target for increased attention…



Consequences of War Gaming

Demonstrates, for better or worse, the maturity of;

The Organisation

The Leadership Team

The Security Team

The *dirty washing* effect

Planning I

Designing a war game

Planning I

1. Define Objectives

Objective

2. Select a realistic scenario

3. Break down the scenario into injects

Inject

4. Draft Guidance for each inject

Guidance

Planning I – Define Objectives

Objective

What do you want to know, test or verify?

Planning I – Select a realistic scenario

What's keeping the sponsor awake at night?

What's in the news?

What are your customers asking you about?

@BadThingsDaily

Planning I – Select a realistic scenario

Start small, start simple

Don’t go all *Bandersnatch* on your first run

Start with non-disruptive scenarios

Objective should be iterative, continuous improvement

Planning I - Example Scenarios

Open S3 Bucket

Reported publicly by a breach hunter, data confirmed by staff

CxO Phished

Forwarding rules put into Outlook 2 week ago, everything copied

Crypto Malware

On the HR server holding all the references, emergency contacts

DNS Hijacked

All TLDs repointed to who knows where, all services impacted

Ransomware Outbreak

All Windows PCs & Servers on the LAN need rebuilding

DDoS Threat

High profile threat actor demands ransom or you're going offline

Twitter Compromised

Official account compromised, defaced and massages accessed

Snr. IT figure arrested

Employee taken into custody, charged with selling stolen data

Secrets Lost

All production secrets exposed via misconfigured replication

Planning I – Break the scenario into Injects

Inject

Consider the scenario and the major plot points

Each should drive the story along

They should provide just enough information

Each response should relate to you objectives

Planning I – Writing Guidance

Guidance

Consider each inject and what questions might arise

Guidance should provide clarity (or deliberately not)

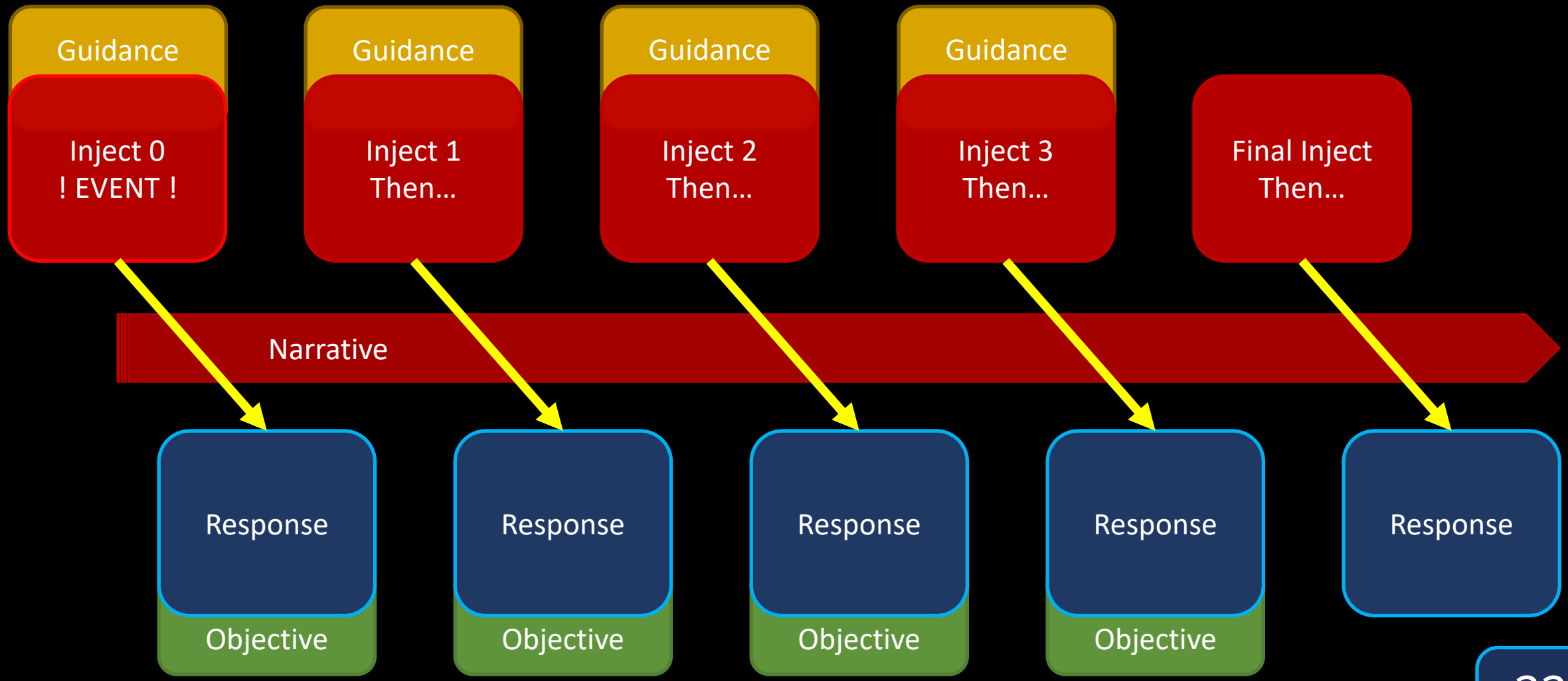
They shouldn’t detract from the testing

They shouldn’t answer questions for the participants

Planning I – Low Level

Inject 0 : Data Breach Report Received Details: A customer reports finding their account details on the internet	Objective(s) Validate use of incident reporting tools and information captured in case notes	Guidance What information has the customer provided? Is there sufficient detail? Is this an isolated issue?
Inject 1 : More Reports Received Details: Growing numbers of customers have reported finding their account details on the internet	Objective(s) Validate escalation of incident. Validate role and responsibilities understood. Validate case linking.	Guidance What are the implications? What is the process for escalating incidents and what are the criteria? Where is this information held?

Planning I – High Level



Planning II

Running a war game

Planning II

1. Secure Sponsorship and Approval
2. Identify Participants (check availability)
3. Identify and appoint overseers
4. Check schedule for major conflicts or distractions

Planning II – Getting Approval

It’s vital

Outline the proposal in terms of benefits

Explain how it will work (mechanics)

Sell it on it’s low risk, high reward potential

Planning II – Selecting Participants

Identify Participants (check availability)

Ask the sponsor for their preferences

The scenario might lend itself to selection

Consider making ‘formation’ you’re first objective

Planning II – Overseers

It’s probably you

Planning II – Conflicts & Distractions

Probably don’t schedule your first one during…

Major Events: The World Cup

Major Distractions: An Office Move

Major Upheaval: Redundancies

Planning II – Logistics 101

Reserve venue, AV equipment, parking spaces...

Prepare resources (slides, packs, props, etc)

Buy snacks, order pizza

Planning II – Final Steps

Send out invitations

Expect resistance

Expect complaints

Planning II – Handling Resistance

As soon as word gets out you're going to receive complaints

You're probably expecting issues with certain people

Try and be sympathetic but stand firm

Influence over Instruction

Planning II – Handling Resistance

Offer the *‘reality check’:*

“I know you’re busy BUT this is important too”

“There is never a GOOD time for something bad to happen”

“We need to be sure we’re ready and we need YOU”

“Leadership asked you were involved specifically“

Planning II – Handling Resistance

Resist the urge to tell people to:

“Suck it up"

“JFDI”

“Dial whine-whine-whine for a Wambulance”

Execution

How to run your own tests

Execution

Roll call

Explain what’s going to happen

Encourage participation

Set some ground rules

Have Fun

Execution – Ground Rules

Don’t fight the scenario

Game Over

Concluding testing, reporting & next steps

Game Over

Formerly conclude the exercise

Send out thank you notes, cards, flowers...

Request feedback

Highs, lows, near-misses…

Game Over

Write up (yes, a report)

Critical observations

Objectives

Performance review

Recommendations

Game Over

Share any risks identified with the sponsors ASAP

Schedule a presentation of the findings

Secure support for the next test

Wash. Rinse. Repeat…

Conclusions

Conclusions

- Nothing brings people together like a shared experience
- Experience doesn’t have to be perfect to add value
- Technology provides an illusion of readiness

Conclusions

- There will only ever be more breaches
- We need to challenge the perimeter mindset
- We need to preach resilience whilst promoting readiness and recovery

Lighting Scenario

C-Level Phish

Lightning Scenario 1

- Widespread phishing campaign… CEO falls for it and reports sharing their credentials…

Lightning Scenario 1

- Widespread phishing campaign… CEO falls for it and reports sharing their credentials…
- Analysis of the your logs shows no suspicious use of the credentials…

Lightning Scenario 1

- Subsequent analysis of forwarding rules shows there has been one in place for their inbox for over a year…
- The CEO doesn’t recognise the destination and cannot explain it…

Lighting Scenario

Supply Chain Compromise

Lightning Scenario 2

- You read in the press that your anti-virus vendor has been compromised and access to their internal network and data stores sold on the *dark web*…
- The vendor doesn't deny the claim but provides no information around the extent of the intrusion…

Lightning Scenario 2

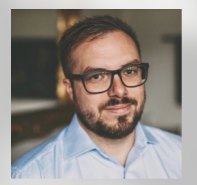
- Microsoft release an emergency patch to address a wormable RDP exploit…
- Your anti-virus vendor reveals they have a working exploit for the RDP exploit…

Thank You

DC151

@_dc151

www.dc151.org



Steve Davies

@northvein

www.deltasecis.com

@deltasecis