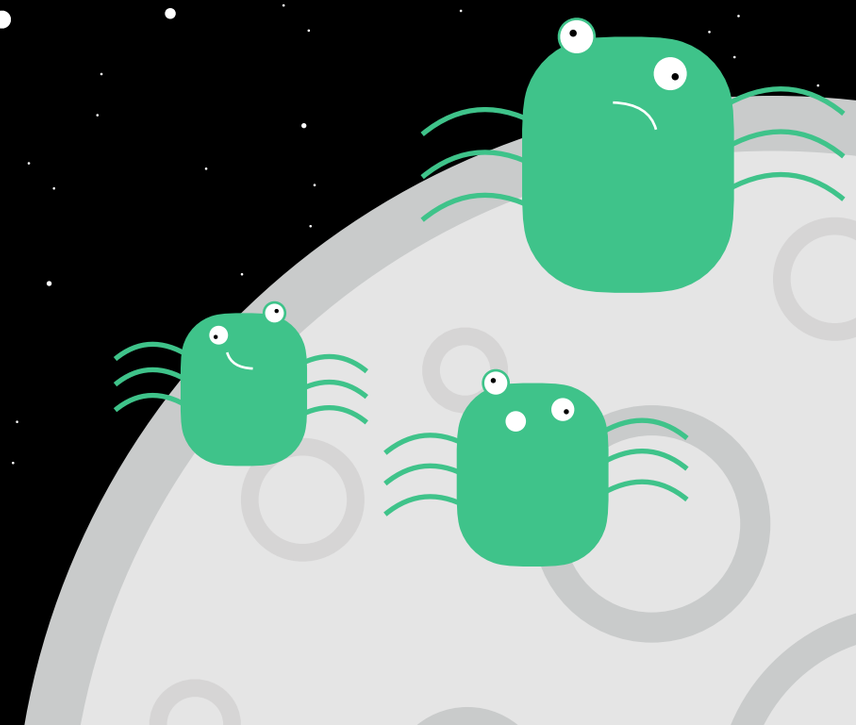
The Internet is Broken and so are We

Saskia Coplans and Alastair O'Neill



Digita|nterruption.

Who are we

Alastair O'Neill - Head of Defensive Security

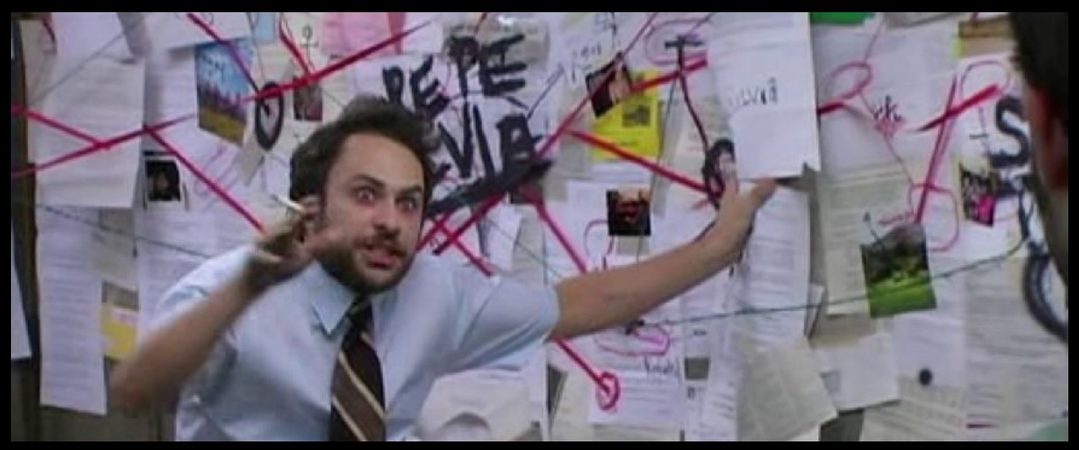
10 years experience in penetration testing

Saskia Coplans - Head of Security Risk & Compliance

10 years experience in information governance

Really in to weird and obscure InfoSec stuff not related to this talk

Really in to weird InfoSec conspiracy theories also not related to this talk



Digita|nterruption.

What is information governance

- The management of information at an organisation level
- It balances the use and security of information
- Helps with legal compliance, operational transparency, and reducing expenditures associated with this
- An organisation can establish a consistent and logical framework for employees to handle data through IG policies and procedures
- These policies guide proper behaviour for how organisations and their employees handle electronically and physically stored information

What does information governance encompass

- information security and protection
- compliance
- data governance
- electronic discovery
- risk management
- privacy
- data storage and archiving
- audit
- analytics
- business operations and management
- knowledge management
- IT management
- master data management
- enterprise architecture
- business intelligence
- big data
- data science
- finance

Digital Interruption.

www.digitalinterruption.com
@DI_Security

What is information security

- Information Security is a subset of information governance
- Providing organisations with appropriate controls over their data to create the CIA triad
- Its not just creating March's favourites unhackable black boxes, or Saskia’s favoured inaccessible vaults
- In the real world people need to be able to actually access data so a balance has to be struck between risk and availability

Integrity

Confidentially

Availability

Digital|nterruption.

www.digitalinterruption.com
@DI_Security

What does that mean in practice

- Information security is a continuous process, there is no end to it
- As long as the business, or the need to process data continues so does the need to secure it
- This means the need for security is not constrained
- However our solutions to insecurity often are constrained

The Jeff Goldblum Theory

Digital Interruption.

www.digitalinterruption.com
@DI_Security

A constrained solution to a continuous problem puts a strain on the mechanisms and people responsible for it

Stress leads to burnout
Burnout leads to quitting
Quitting leads to skills shortages

Understanding the skills shortage

- Penetration Tester
- Security Researcher
- Red Team Member
- Compliance Manager
- Incident Responder
- Threat Intelligence
- Firewall Engineer
- Security Architect
- SOC Team Members
- *Privacy / Data Protection Specialist
- *Risk Manager

Digital Interruption.

www.digitalinterruption.com
@DI_Security

Skills Vs Competencies

- No real formal pathways into InfoSec roles
- Every other skilled profession that deals with high risk has competencies that are:
  - clearly formerly defined
  - universal
  - scalable
  - transferable
  - regulated
  - accountable
  - assessable

Fear leads to anger
Anger leads hatred
Hatred leads to the dark-side

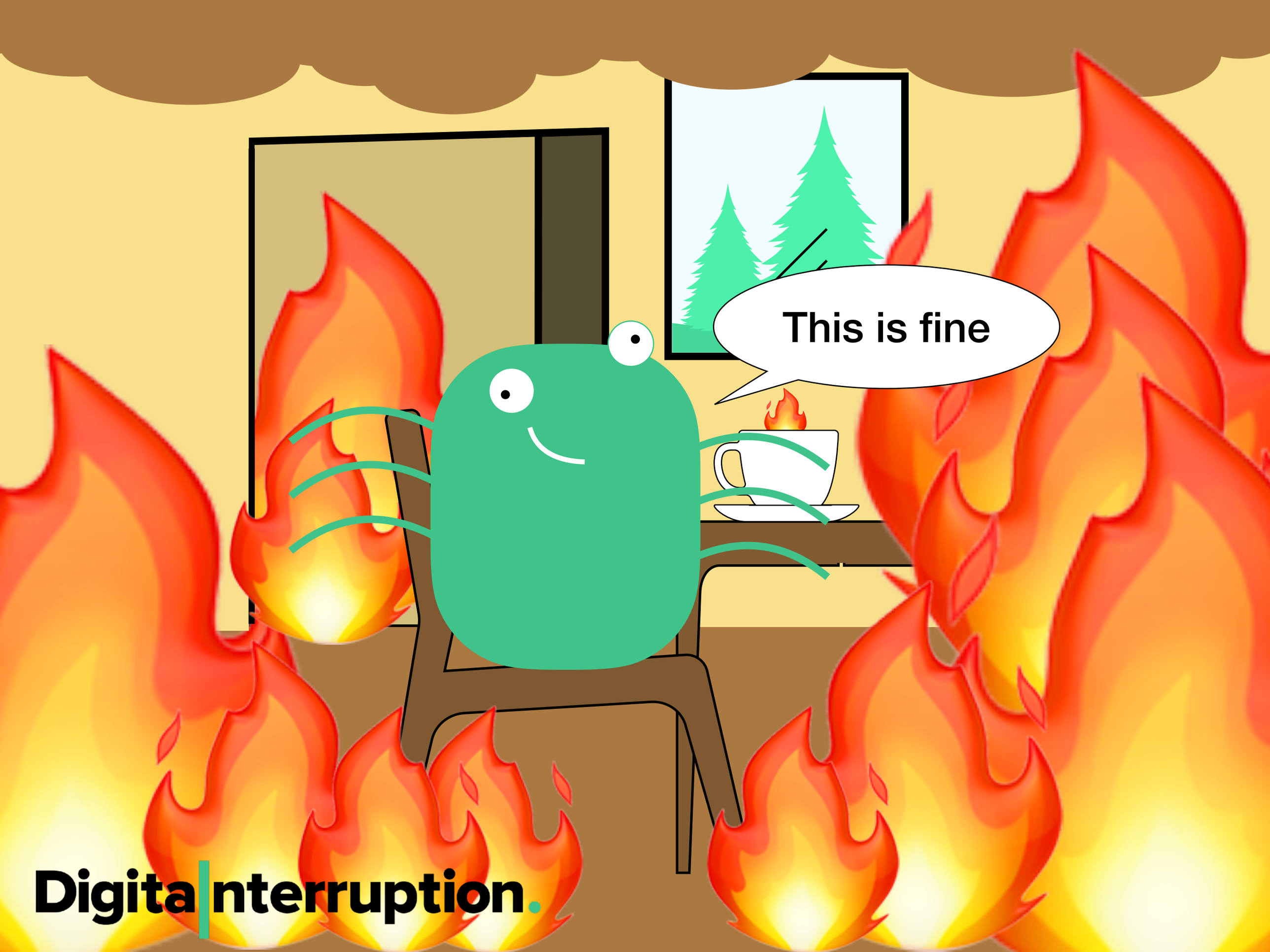
www.digitalinterruption.com
@DI_Security

	DEVELOPERS	DESIGNERS	PROJECT MANAGERS	QA	SYSADMINS	SECURITY
SEEN BY **DEVELOPERS**						
SEEN BY **DESIGNERS**						
SEEN BY **PROJECT MANAGERS**						
SEEN BY **QA**						
SEEN BY **SYSADMINS**						
SEEN BY **SECURITY**						

How does this impact consumers

- Businesses and developers feel judged
- When we attack and are inconsistent we are seen as bullies
- When we prevent software from going live we are seen as blockers
- People stop listening to us and because of this software is still released in an insecure state and people still use it insecurely

Stress leads to burnout
Burnout leads to quitting
Quitting leads to skills shortages


This is fine
Digital Interruption.

How can we do this differently?

Left shifting security and DevSecOps

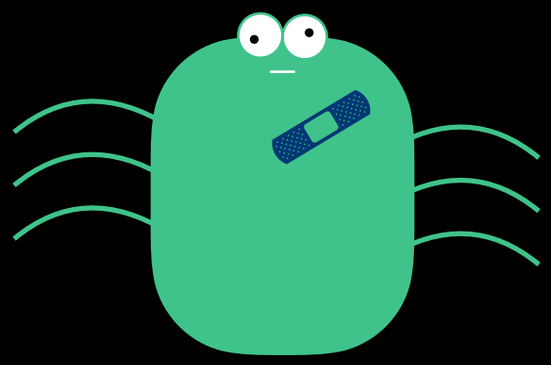
- Integrating security in to the development pipeline
- This works for software, hardware, networks, in short anything that has a build pipeline
- The responsibility for security is distributed reducing technical debt
- A space in created for non technical security to add value
- As security people we take on the role of Yoda, using and imparting our security knowledge to guide and architect a solution from the start

Creating the right tools

- Instead of tools for hackers, tools for everyone
- Intuitive design and interfaces
- Continuous feedback
- Instead of teaching people how to hack, we give them the tools to develop securely
- Tools aren’t just software in this context

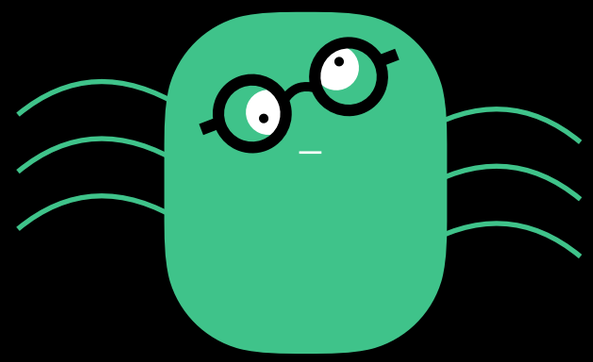
Building security in to existing personas

Product Owner



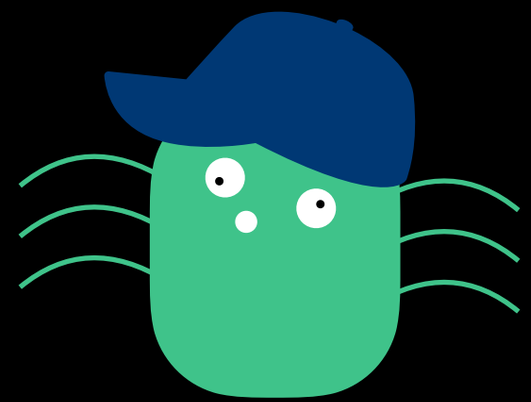
- Creates the correct requirements
- Initial security considerations
- Defines risk & response

Developer



- Creates secure code & builds
- Implements technology
- Interprets vulnerabilities and solutions

Tester



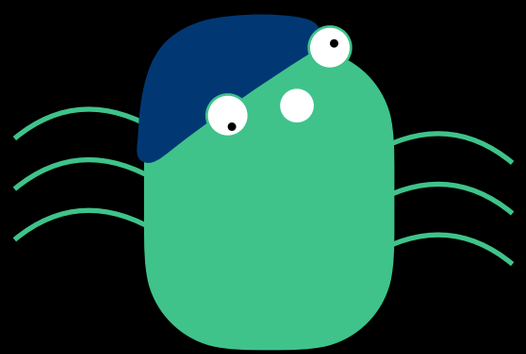
- Investigate & Influence
- Initial due diligence
  - Requirements
  - Technology
  - Vulnerabilities

Digita|nterruption.

www.digitalinterruption.com
@DI_Security

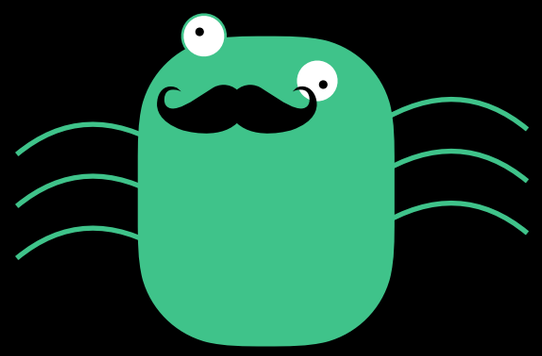
Building security in to existing personas

Designer



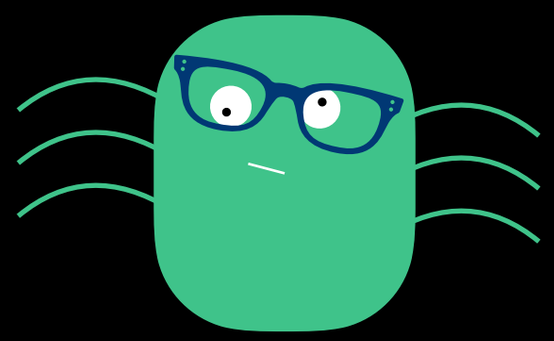
- User Interaction
- Scalability
- Usability
- Guiding & Monitoring

Deployment



- Correct pipeline configuration
- Security considerations designed in the pipeline
- Final due diligence

Security



- Investigate & Influence
- Threat Modelling
- Advanced Techniques
- Verification

Digitalinterruption.

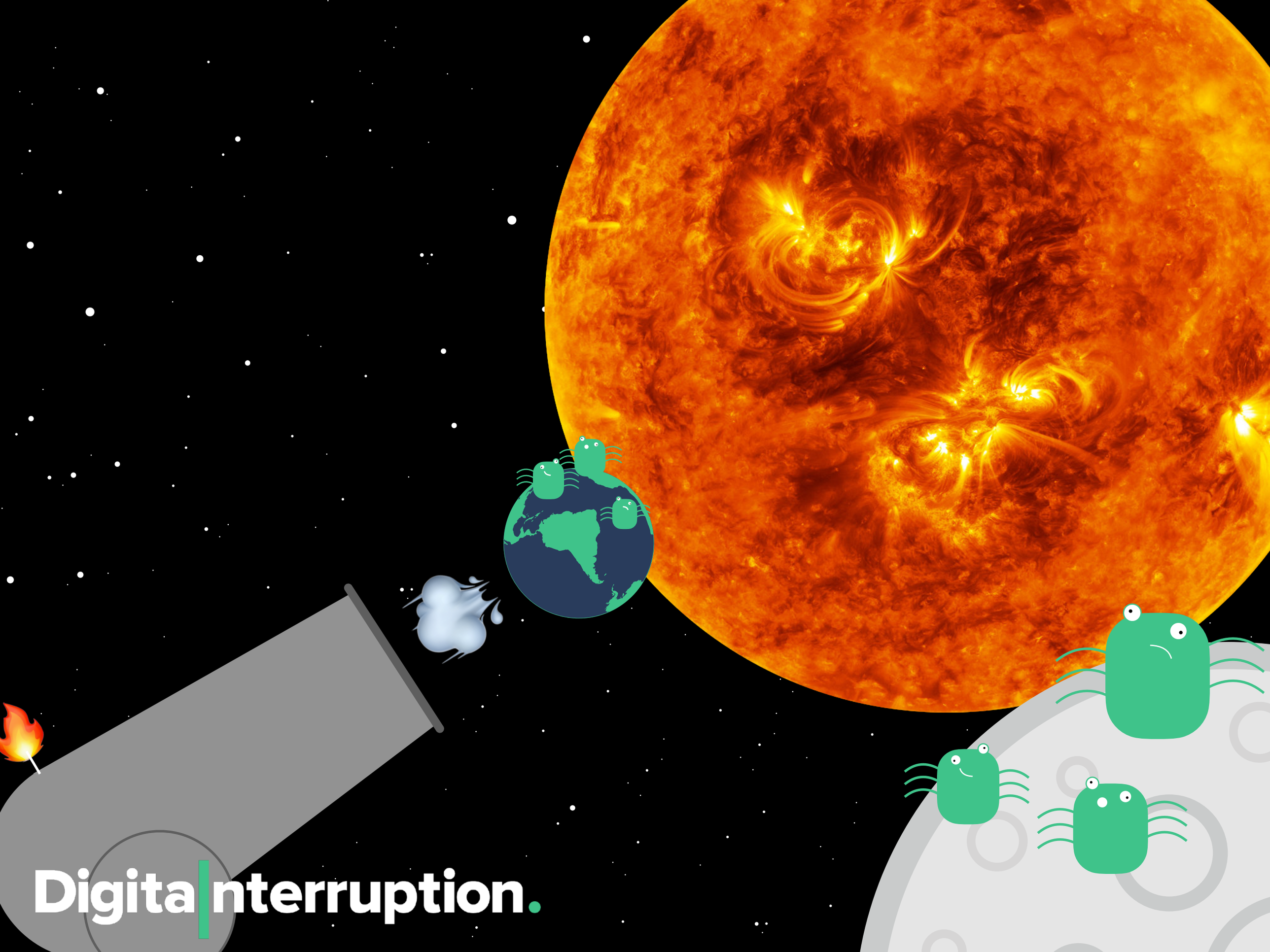
www.digitalinterruption.com
@DI_Security

How does this impact us

- If security is embedded when **we** test it is more interesting, more welcome and has greater positive impact
- Our tests are performed in smaller bursts, in stages as the dev teams require (instead of one massive test at the end that knocks everything over)
- These smaller tests can be performed in shorter timescales with the results being communicated via discussion, raising tickets, presentations and other collaborative means, rather than PDF reports
- This is something Digital Interruption is already doing

Why did we decide to do this?

www.digitalinterruption.com
@DI_Security


Digita nterruption.

But resources are also people

5 pledges

we made to

Protect Mental Wellbeing

in our business

1. Unlimited personal days
2. No forced on site work
3. Realistic utility
4. Flexible working
5. No bosses

Digital Interruption.

www.digitalinterruption.com
@DI_Security

5 pledges

you can make

Protect Mental Wellbeing

in your business

1. Don’t promote bad managers
2. Enforce good policies
3. Ask your staff
4. Trust, not toys
5. Don’t buy in bad practices

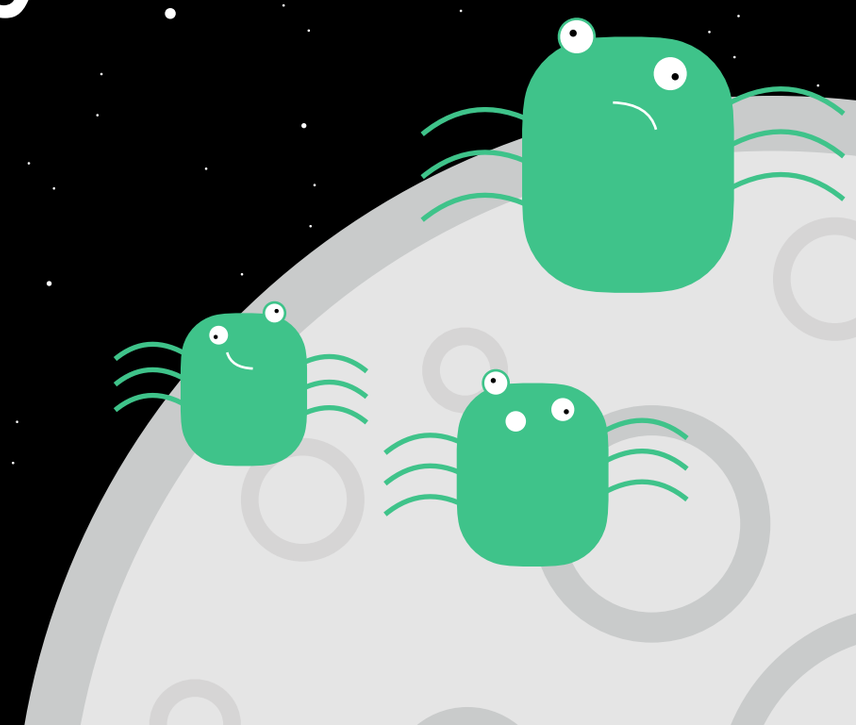
Digital|nterruption.

www.digitalinterruption.com
@DI_Security

www.digitalinterruption.com

contact@digitalinterruption.com

@DI_Security



Digita|nterruption.