Digitalnterruption.

digitalinterruption.com

Manchester Technology Centre
Oxford Road, Manchester
M1 7ED

+44(0)161-820-3056

contact@digitalinterruption.com

CYBER ESSENTIALS

ICO Registration Number: ZA446620

Digital Interruption

Digital Interruption is a cyber security agency. We provide penetration testing, managed vulnerability scanning, defensive security with compliance services and security training.

Founded by Jahmel Harris and Saskia Coplans in 2017 our growing team is based at the Manchester Technology Centre in the heart of the city's innovation district.

Our Ethos

Digital Interruption is passionate about data security. As part of our disruptive business model we offer more than the usual services you'd expect from a security consultancy. Along with penetration testing we provide defensive security integrated with compliance services. We support this with our managed vulnerability scanning and security training.

We describe ourselves as ethical, not just because of our team of experienced ethical hackers, but also because of our business practices. We are smaller and more dynamic than traditional consultancies. This means we can work more closely with our clients to recommend bespoke services and solutions where needed.

Ultimately our clients have more control over how they use our services. We have streamlined the scoping process and use transparent pricing models, offering fixed price packages and online booking to reduce cost and increase quality.

We believe that consistent and sustainable relationships facilitate the best for both us and our clients. We protect the wellbeing of our team to ensure this, enforcing strong mental health policies and giving agency to team members.

Our Services

Vulnerability Scanning

We recommend regular scanning of applications and infrastructure between penetration testing as a proactive means of assessing your security posture.

Automated scans can cover a wider area than a manual test in a far shorter time. By performing regular scans, our clients gain insight into their patching processes, data hygiene and exposed attack surface. This provides our clients with peace of mind between penetration tests and can highlight any issues that require further exploration via manual testing.

Our experienced testers will configure automated scans for you, interpreting the results in a clear report to give you assurance about the robustness of your networks and applications.

We offer monthly subscriptions for this service, with prices starting from £100 for a basic scan.

Find out more about our services, prices and packages on our website.

Our full package includes the following service:

1. **Initial configuration**. This is to configuring the tools to work with the systems they are scanning to achieve the right level of coverage. This is a fixed one-off charge.
2. **A monthly report detailing current vulnerabilities.** These are classified as either critical, high, medium or low risk along with recommendations for remediation.
3. **False positive removal.** Findings are analysed and verified by our consultants to assure that the vulnerability exists in the system.
4. **Monthly report comparison.** Vulnerabilities are compared against previous scans to build a complete picture of security improvements over time.
5. **Assurance document.** Provided on request, this gives assurance that the application and network is free from high or critical vulnerabilities, as per the scan results.

Our Services

Penetration Testing

We recommend Application and Infrastructure Penetration Tests every 12 months or after any significant change.

Just like it's important to test software for bugs that could cause applications to not work as expected, penetration testing is used to find security weaknesses that could be used by attackers to find confidential data or take control of your company.

The time required for a Penetration Test differs depending on the size of the application or infrastructure. A good average is 5 days per application.

We offer testing packages for both application and infrastructure penetration testing, starting from £2,000 for a targeted micro test.

Find out more about our services, prices and packages on our website.

There are a number of different tests you can choose from:

1 **Application testing.** We follow industry standards specific to **mobile** and **web** application testing including the OWASP top 10, testing your applications against common attack scenarios.

2 **Infrastructure & network testing.** With experience in network testing for big banks and governments, our Offensive Security certified consultants test networks to identify vulnerabilities and weaknesses that may put your business at risk.

3 **Red teaming.** Using phishing, social engineering, infrastructure and web attacks, our experts simulate a real world attack on your business to help you understand your organisations security and how quickly you can detect a real cyber threat.

4 **Code review.** As former developers, our technical consultants have many years experience in reviewing source code and uncovering security vulnerabilities. This helps ensure your code is secure from the very beginning.

Our Services

Defensive Security with Compliance

We believe just following the regulations isn't enough. Your business needs to be proactive to make sure it stays secure.

As registered DPOs, our full range of services enable us to support our clients in all aspects of data security. We focus not just on the various privacy and data protection regulations and compliance requirements, but we unpick what those regulations mean specifically to you. As virtual CISOs we work with you to develop and implement successful action plans that provide tangible security solutions to help your business stay safe.

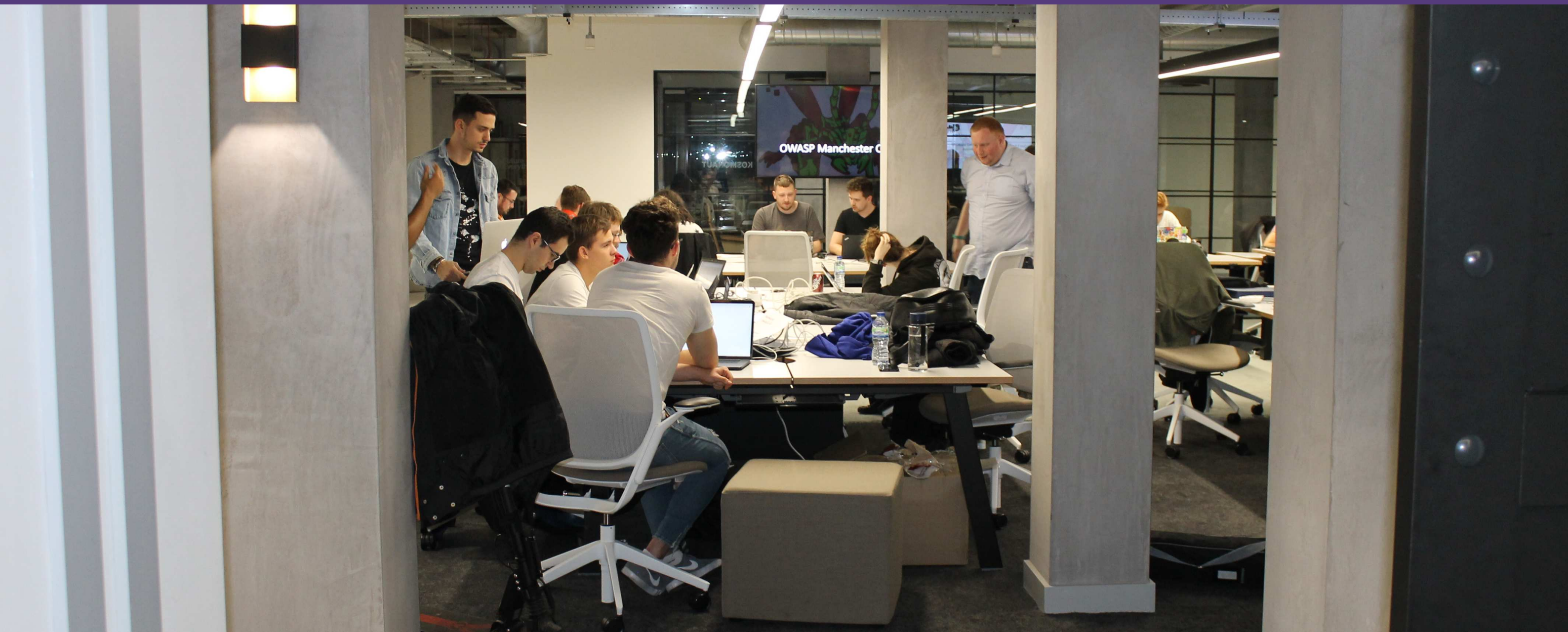
We also help our clients prepare for Cyber Essentials and ISO accreditations, and are specialists in sensitive and special category data.

Security Training

Training is a key a part of keeping data secure. We train on a number of security topics ranging from secure coding to ethical hacking, defensive security and compliance. Training can be delivered either as bespoke e-learning or class room training sessions, whichever works best for you.

We train both small and large organisations including the financial and public sector and host training workshops at conferences worldwide.

As part of our ethical business model, we provide free introductory training workshops to community groups across the UK and internationally.



Who are Digital Interruption?

Jahmel Harris - Head of Penetration Testing

Jahmel, also known as Jay, is a security consultant, researcher and ethical hacker. Supported by his background not just in security but also in software development, his work focuses both on the offensive "ethical hacking" side and also in integrating secure coding practices into organisations and their project lifecycles.

Jahmel has a proven record of finding and providing recommendations on high and critical risk issues for FTSE 250 companies. He pushes industry knowledge forward with published security research and regularly presents to hackers and software developers in security both in the UK and internationally.

Saskia Coplans - Head of Security Risk and Compliance

Saskia is a registered Data Protection Officer (DPO) and a privacy specialist. She has over ten years experience in information security and governance along with standards and policy development. She has worked across Europe and Central Asia for Governments, NGO's, Regulators and the Private Sector.

As well as representing a number of our clients as their registered DPO she develops risk based defensive security strategies and presents at events and conferences on security standards, compliance and ethical business practices.

Who are Digital Interruption?

Robert Carr - Head of Research and Development

Robert is an experienced software developer who has been active within the security community for a number of years. He has contributed to a number of open-source projects and community efforts, with the aim of helping to improve security and make it more accessible to the general public.

Robert is experienced in web security; with a focus on WordPress. He has contributed a number of modules to the Metasploit Framework project to aid in the penetration testing of WordPress powered systems and created a dedicated framework for WordPress exploit development and testing.

Alastair O'Neill - Head of Defensive Security

Alastair has more than a decade of experience in information security, both as a security consultant and as a researcher. His skills range from embedded device exploitation to mainframe hacking, along with a significant grounding in all shapes of UNIX.

He regularly presents in the UK and abroad on topics ranging from cutting-edge malware research to innovative offensive techniques, and has a strong passion for offensive and defensive hacking.

Why Digital Interruption?

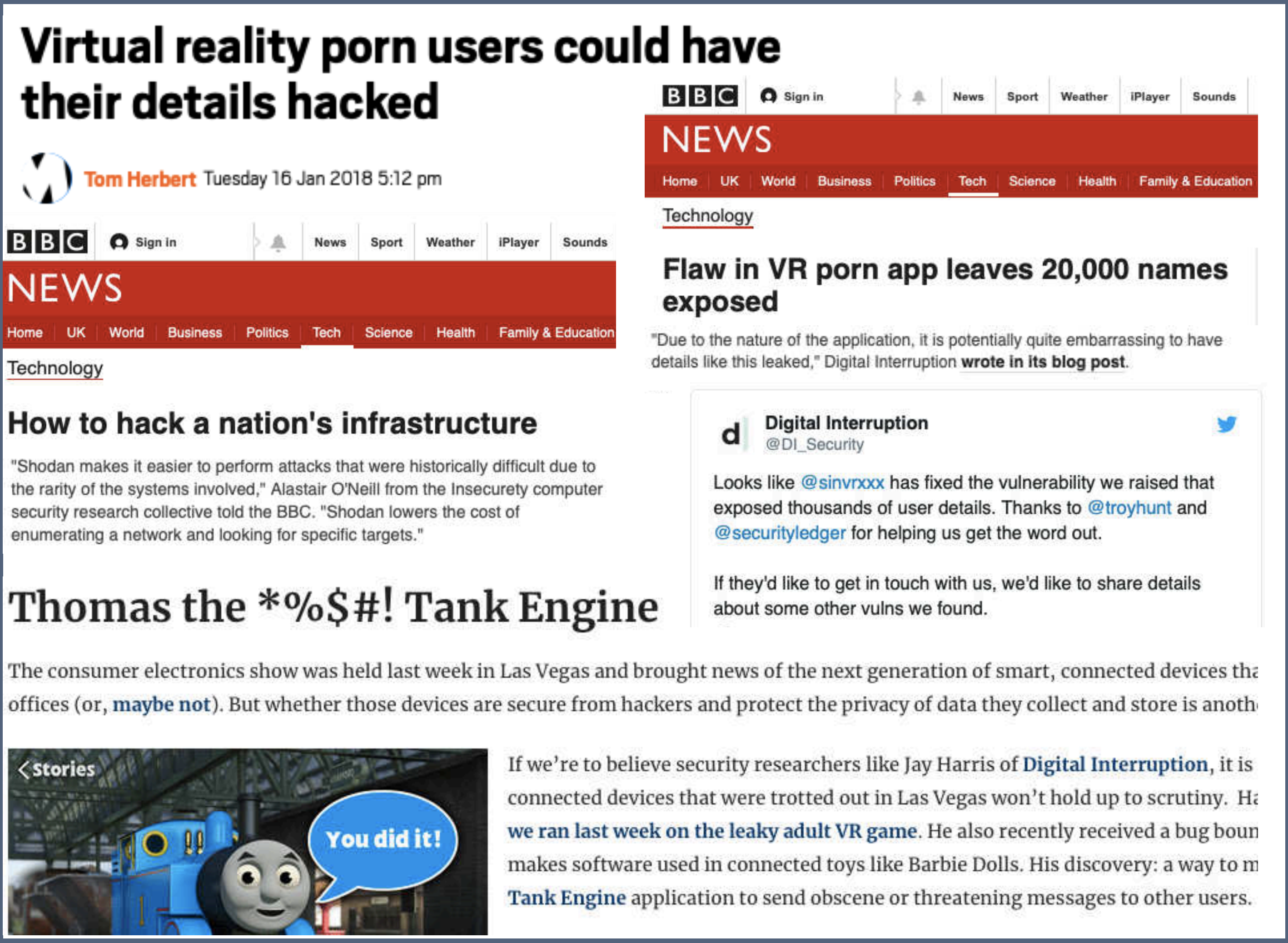
Our Research

Alongside the services we provide we also dedicate time to foster our research and development practice.

We believe that research is critical to remaining current and relevant in the security market. We have won a number of bug bounties, and our research on Virtual Reality Applications Vulnerabilities and Infrastructure Hacking have made national and international headlines, including the front page of BBC Technology.

We release regular blogs and have written white papers on secure application development, hardware hacking, how to embed security and compliance and have numerous CVEs attributed to our staff.

We present our research at conferences and events wold wide.



Virtual reality porn users could have their details hacked

Tom Herbert Tuesday 16 Jan 2018 5:12 pm

Technology

How to hack a nation's infrastructure

"Shodan makes it easier to perform attacks that were historically difficult due to the rarity of the systems involved," Alastair O'Neill from the Insecurety computer security research collective told the BBC. "Shodan lowers the cost of enumerating a network and looking for specific targets."

Technology

Flaw in VR porn app leaves 20,000 names exposed

"Due to the nature of the application, it is potentially quite embarrassing to have details like this leaked," Digital Interruption **wrote in its blog post**.

Digital Interruption
@DI_Security

Looks like @sinvrxxx has fixed the vulnerability we raised that exposed thousands of user details. Thanks to @troyhunt and @securityledger for helping us get the word out.

If they'd like to get in touch with us, we'd like to share details about some other vulns we found.

Thomas the *%$#! Tank Engine

The consumer electronics show was held last week in Las Vegas and brought news of the next generation of smart, connected devices tha offices (or, maybe not). But whether those devices are secure from hackers and protect the privacy of data they collect and store is anoth

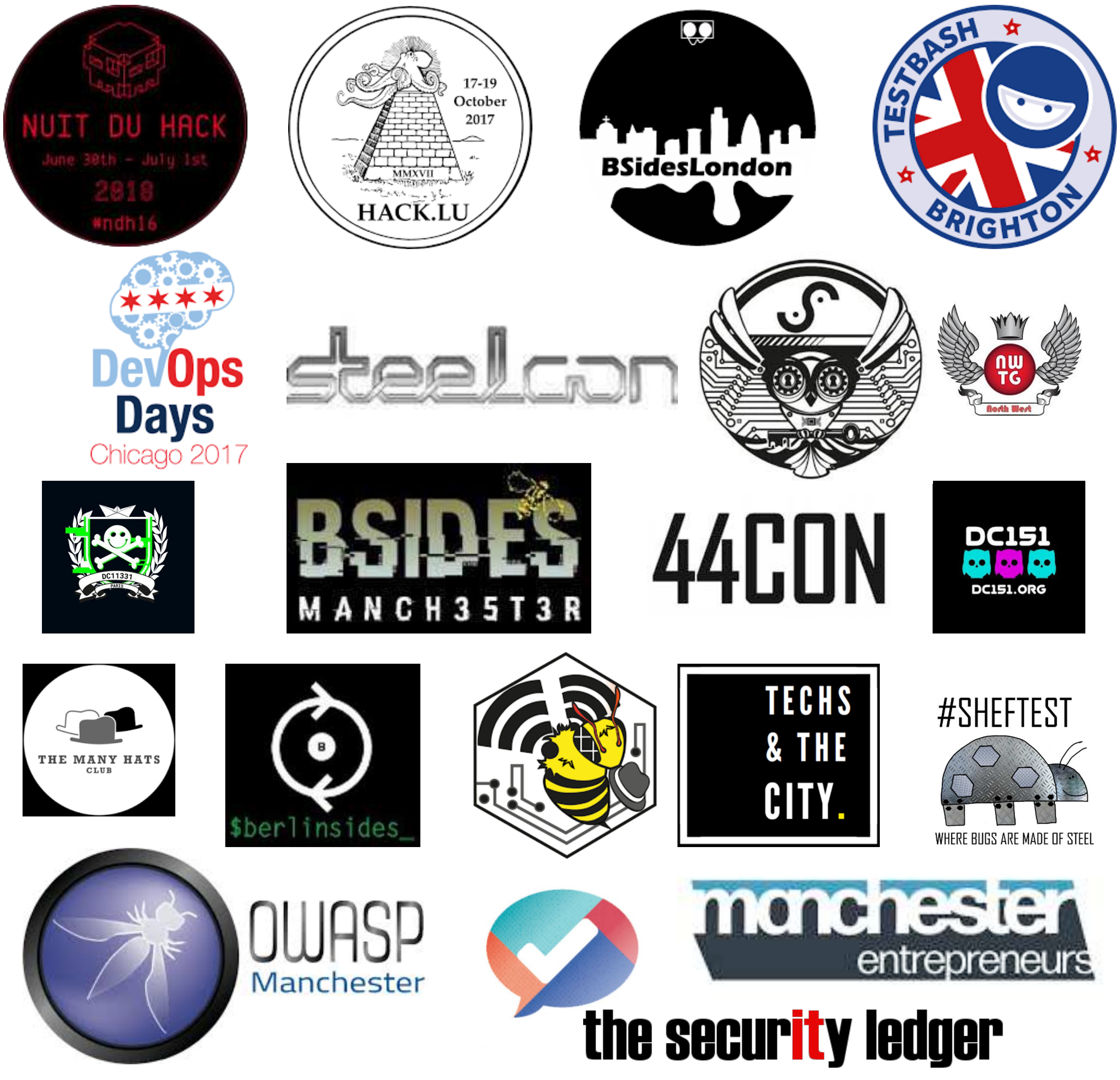
If we're to believe security researchers like Jay Harris of Digital Interruption, it is connected devices that were trotted out in Las Vegas won't hold up to scrutiny. Ha we ran last week on the leaky adult VR game. He also recently received a bug boun makes software used in connected toys like Barbie Dolls. His discovery: a way to m Tank Engine application to send obscene or threatening messages to other users.

Why Digital Interruption?

The Infosec and Cybersec Community

Infosec moves at an incredible speed so engagement with the wider infosec community is key to understanding our business. We do this through a combination of research, community groups and conferences.

Since incorporation in 2017 we have spoken at the following conferences , groups and podcasts:



digitalinterruption.com

Manchester Technology Centre
Oxford Road, Manchester
M1 7ED

+44(0)161-820-3056

contact@digitalinterruption.com

CYBER
ESSENTIALS

ICO Registration Number: ZA446620