LE TOUR DU HACK

22nd – 23rd April 2023

The largest student-run 2-day conference and CTF in the UK!

ENUSEC>_

Welcome!

Hello all, and welcome to Le Tour Du Hack 2023!

From our oldest friends who have been diligently supporting us since the start as well as every new face to our 6th Le Tour Du Hack, we extend a warm welcome. We are delighted to have you with us to participate and share in this fantastic weekend. The fact that so many of you travelled long distances to be here serves as a reminder to us all just how awesome the Cyber-Security community is!

First and foremost, the LTDH23 team wish to sincerely thank and acknowledge every one of you who extended help to us for making this event a grand success. Trust us, all of this would not have been possible without the tremendous support received.

Our mission with Le Tour Du Hack 2023 is to improve upon previous years, while continuing the educational and community ethos which has underlined previous years. To do so, we decided to bring back the format of a technical conference and a capture the flag weekend. We believe this will encourage an excellent atmosphere for the exchanging of ideas and the making of friends along the way.

From the three-track technical conference allowing the exchange of novel ideas as well as the opportunity for new up and coming individuals to share the spotlight, to the exhibition area allowing enthusiastic Cyber-Security students to network with passionate Cyber-Security organisations, to the capture the flag event where competitors' skills will be honed and put to the test!

With the outstanding line-up of speakers and master crafted CTF challenges we have assembled; we are confident there is something for everyone!

We wish you an awesome weekend, and hope you enjoy your time in Edinburgh and Le Tour Du Hack 2023.

The LTDH23 Team




RULES & ETIQUETTE

Le Tour Du Hack 2023, as with any ENUSEC event, abides by the Berlin Code of Conduct to ensure we are doing our part to make our events inclusive to the largest number of contributors, with the most varied and diverse backgrounds possible.

The Berlin Code of Conduct outlines the following unacceptable behaviours:

- Intimidating, Harassing, Abusive, Discriminatory, Derogatory or Demeaning speech or actions.
- Harassment includes harmful or prejudicial verbal or written comments related to gender, sexual orientation, race, religion, disability, inappropriate use of nudity and/or sexual images; inappropriate depictions of violence; deliberate intimidation, stalking or following; harassing photography or recording; sustained disruption of talks or other events; inappropriate physical contact, and unwelcome sexual attention.

The full Berlin Code of Conduct can be found online at berlincodeofconduct.org

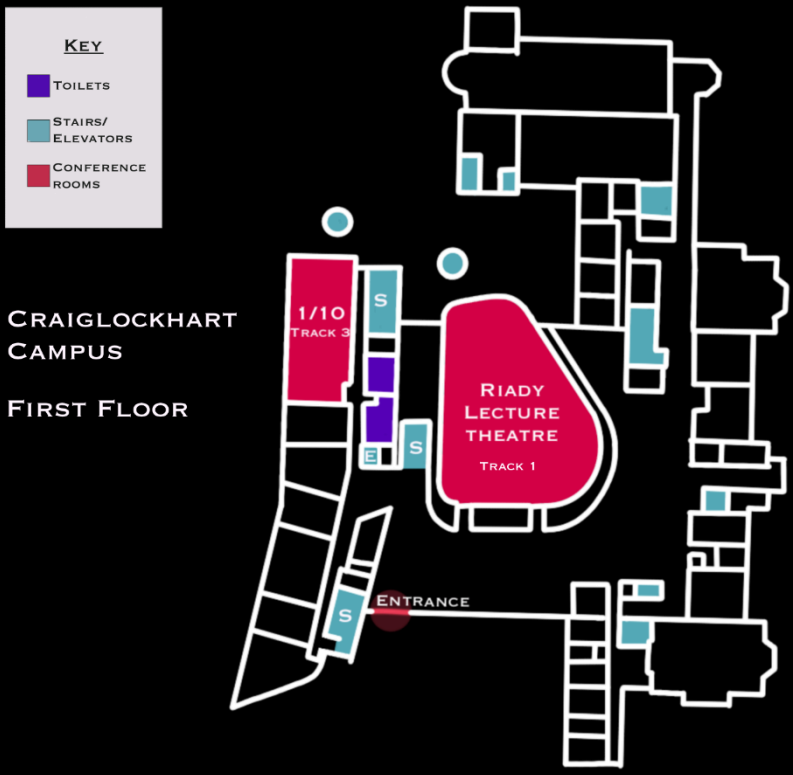
The Berlin Code of Conduct applies to all activities taking place during the Le Tour Du Hack 2023 weekend.

Unacceptable behaviours from any attendee, including sponsors and those with decision-making authority, will not be tolerated. Anyone asked to stop unacceptable behaviour is expected to stop immediately. Le Tour Du Hack 2023 team may take any action they deem appropriate, up to and including expulsion from the event without warning and refund.

Alert a member of the Le Tour Du Hack 2023 team if you notice a dangerous situation, someone in distress, or violations of this Code of Conduct, even if they seem inconsequential.

The Le Tour Du Hack 2023 team can be identified as those wearing the blue event t-shirts with “Committee” and “Volunteer” on the back.

MAP


Key
Toilets
Stairs/ Elevators
Conference rooms
Craiglockhart Campus
First Floor
1/10
Track 3
S
Riady Lecture Theatre
Track 1
S
S
Entrance

Craiglockhart Campus

Second Floor

LE TOUR DU HACK

CONFERENCE DAY AGENDA

22nd APRIL 2023

	TRACK 1	TRACK 2	TRACK 3
09:00-09:30	REGISTRATION		
0930-10:00	OPENING REMARKS The ENUSEC Committee		
10:00-11:00	OPENING KEYNOTE Scott McGready		
11:00-11:45	Hack the Planet: Building a Home Lab Sean Wright	Bitweighting for perceptual hash similarity comparisons Karen Taljard	Litigating for Naruto - A Ramble through Tech Law David Alexander
11:45-12:15	Coffee Break - 30m		
12:15-13:00	Smartphones and their permissions - A dreaded nightmare waiting to happen Dónnan Mallon	Breaking In: The Physical Frontline of Information Security Ben Jacob	Anti-Virus Evasion through BadUSB Cristian Cornea
13:00-14:00	LUNCH		
14:00-15:00	A Day In the Life - A Memoir Miguel Marques	Over-Clocking Sunflowers Eliot Bolster	They're listening but is it you that's talking, attacks on voice recognition systems Fraser Wilson
15:00-15:30	Have You Been Zucked? Probably, here's how you can find out! Charlie Hosier & Lloyd Davies	Are the UK's data laws still fit for purpose? George Brightman	How to fix a bigoted AI Dominik Hanlon
15:30-16:30	CLOSING KEYNOTE Zibby		
16:30-17:00	CLOSING REMARKS The ENUSEC Committee		
19:00-LATE	AFTER PARTY @ CASK SMUGGLERS		

Edinburgh Napier UNIVERSITY | School of Computing

School of Computing

Edinburgh Napier University

1. We pride ourselves on our one-year work placements and study abroad options
2. Our specialists labs produce cutting-edge research outputs
3. Practical classes prepare you for the world of work

Contact
ugadmissions@napier.ac.uk
pgadmissions@napier.ac.uk

Quorum Cyber

How would you like to put your skills to the test to help good people win?

At Quorum Cyber we do this every day. Our teams work with the latest Microsoft Security technologies to protect over 150 organisations around the world and safeguard their data, their customers and their reputations.

Founded in Edinburgh in 2016, we're one of the fastest growing cyber security companies in the UK. We defend government departments, charities and businesses in every industry. Our mission is to reduce their cyber security risk and enable them to thrive in a hostile and unpredictable digital environment. We're proud to be a Microsoft Solutions Partner for Security (formerly called a Gold Partner), a member of the Microsoft Intelligent Security Association (MISA) and CREST approved.

Help our customers win

Our customers depend on our creativity, innovation and clear communication, not to mention our world-class technical skills, every day of the year. We've doubled the size of our business in the last 12 months, helping customers in the UK, North America, Asia and Australasia. We won't stop there – we have huge ambitions to defend as many organisations in every region of the world as we can. So we're constantly looking to add talented, energetic and enthusiastic graduates who share our passion for learning to join our expanding team.

Graduate Roles

Every year we recruit a number of enthusiastic and talented graduates into our graduate programme. This is a unique rotational two-year programme where the successful candidates get the opportunity to experience working in several of our Cyber Security teams, including our SOC, Incident Response, Offensive, and Advisory teams. They will gain meaningful experiences in each area and have an insight into what direction they wish to take their careers, collecting industry-recognised certifications along the way. We start the annual process early, and applications for 2024 will open this November, so don't miss the opportunity to apply!

However, our graduate programme is just one route to joining the team at Quorum Cyber. We also recruit graduates directly into our teams, particularly into the SOC, so if you can't wait until 2024 to join, keep your eyes peeled!

If successful, you'll be rewarded with an excellent salary, world-class benefits including private healthcare, plus flexible working and unlimited holidays.

Come and meet us today

We have a stand here at Le Tour Du Hack, so why not come over to meet us to find out what it's like to work at Quorum Cyber?

Visit **www.helpfightbullies.com/** to learn more and take the first step in your journey in cyber security.

KEYNOTE

10:00 – 11:00

Scott McGready

@ScottMcGready

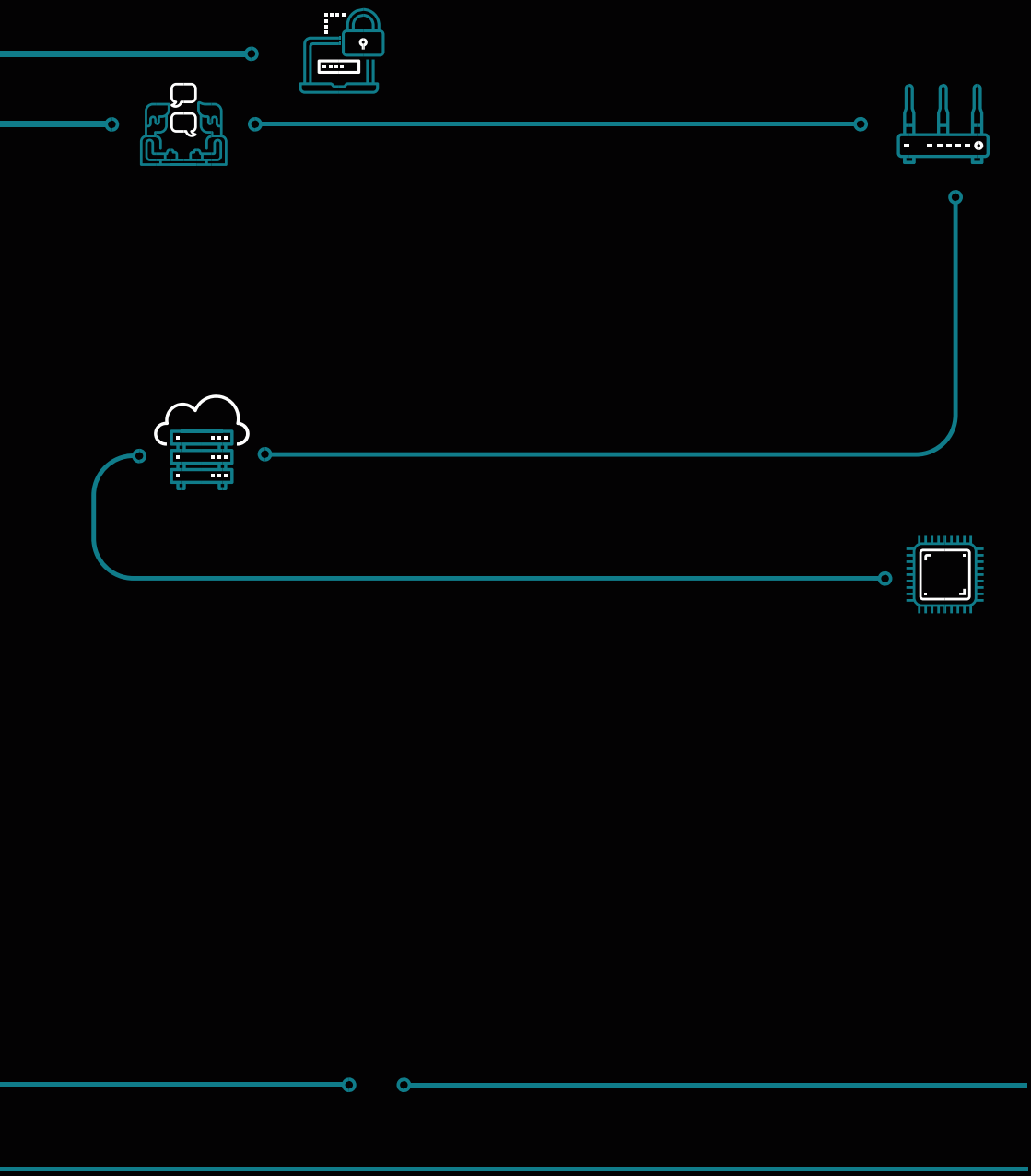
Bio

Maker, breaker, fixer, faker. Hacker trying to make the world a safer place. Mediocre engineer. As seen on TV & heard on radio.

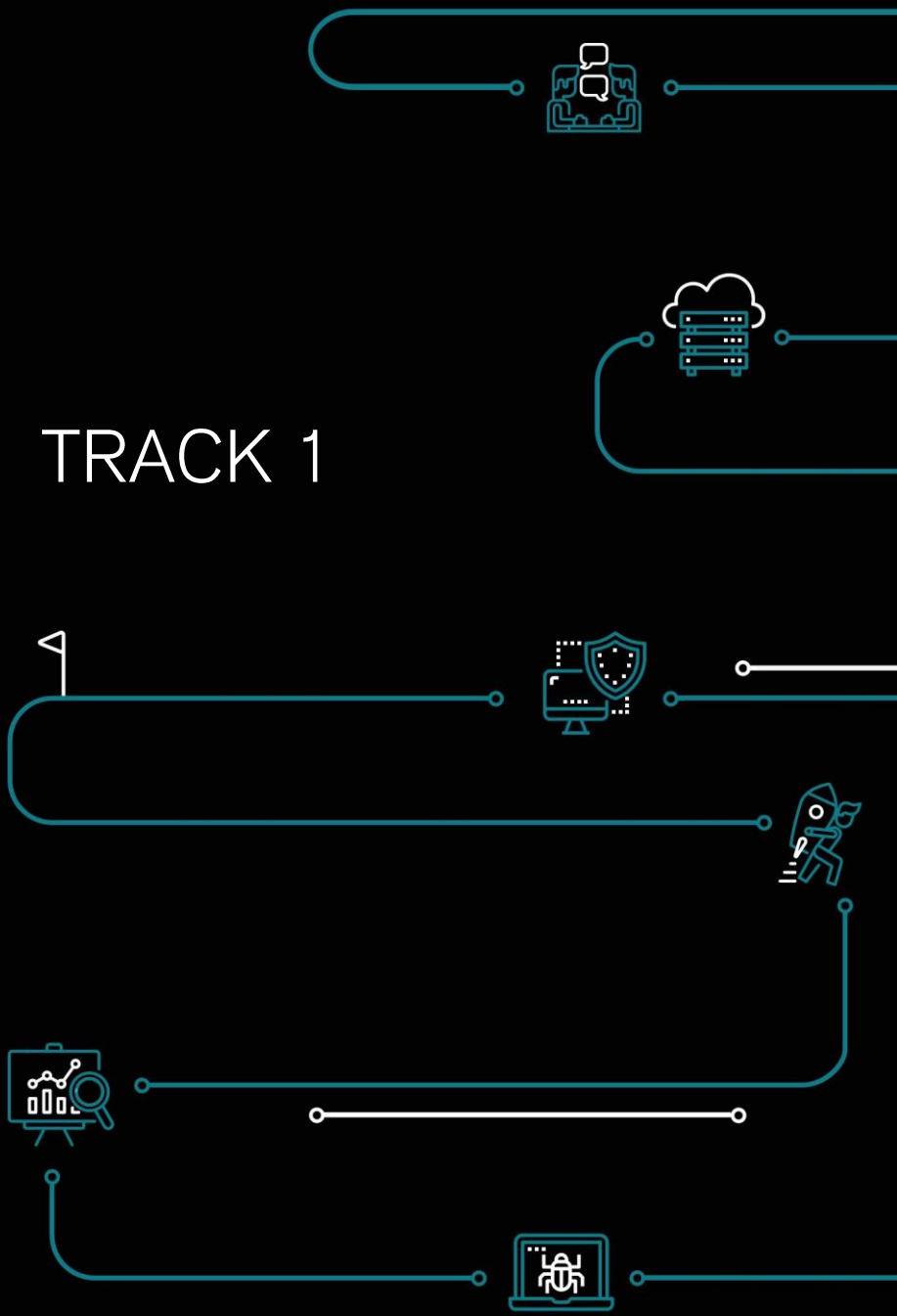
Talk Outline - Fatima’s next job best friends could be in cyber - she just doesn't know it yet.

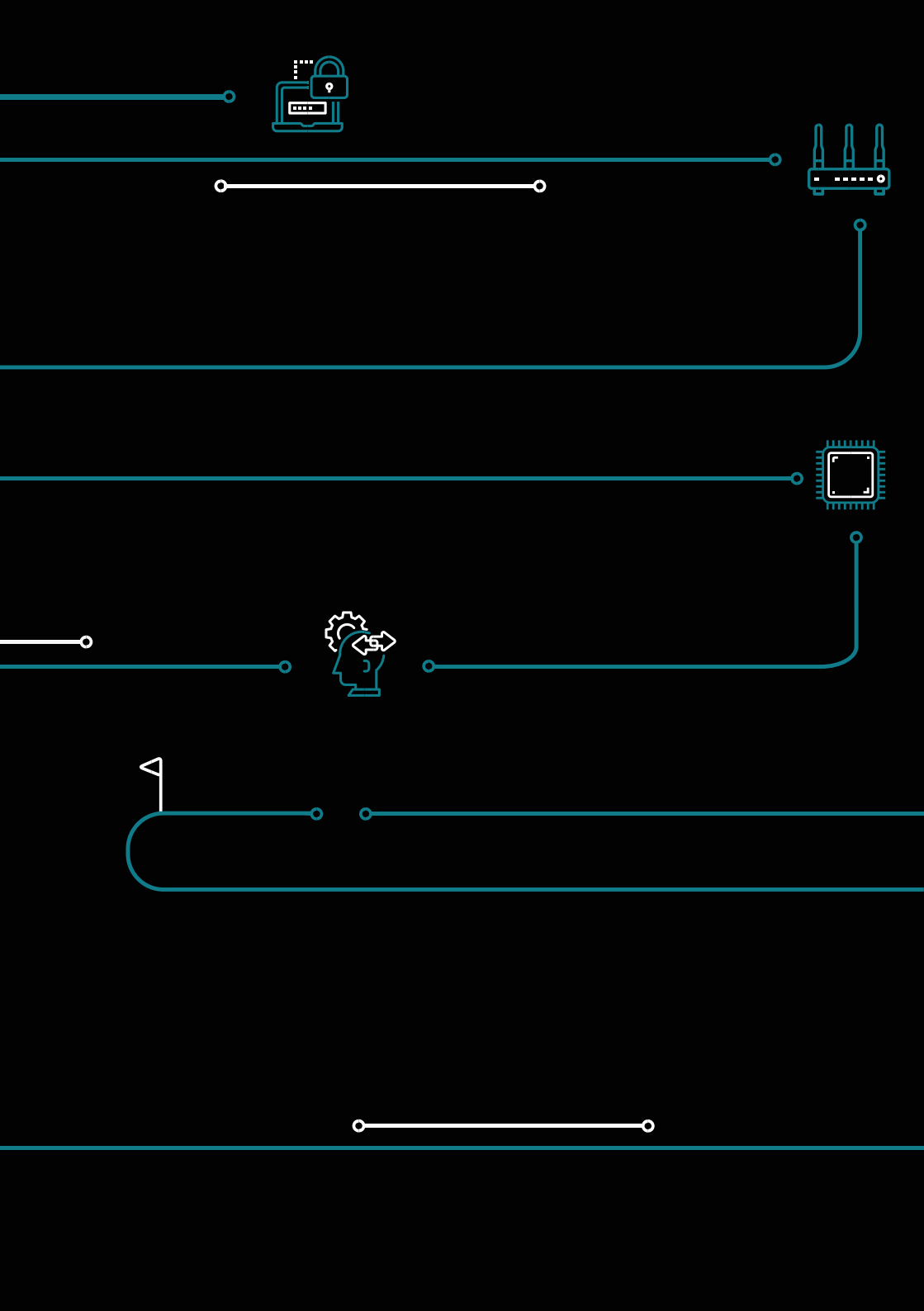
Relegated beneath the certs, hidden away behind the HR barriers, there's an aspect of cyber that's often overlooked, but is equally - if not more - important. "Breaking into cyber" isn't just about learning how to attack, or defend, systems – it's also about community.

Join me to hear why you should make friends, attend conferences, and be brave enough to send that DM.



TRACK 1





Hack the Planet: Building a Home Lab

11:00 – 11:45

Sean Wright

Talk Outline

A home lab is a really useful and fun way to learn new security related topics and skills. It is also a great tool to allow one to carry out their own security research. This talk will cover how one can go about building their own home lab. This talk will give advice on the things to do and not to do when attempting to do so. Best of all, it doesn't have to cost the earth to set one up.

Smartphones and their permissions - A dreaded nightmare waiting to happen

12:15 – 13:00

Dónnan Mallon

@ Cyb34_DO

Talk Outline

Applications have used permissions on Smart Phones as a way of providing function towards the user. But what happens when these permissions get abused? We'll take a deep dive into the function/importance of mobile permissions and how they can be leveraged by adversaries to carry out malicious actions. This will cover an array of smart phone providers such as Android and IOS and how they differ when being targeted by Threat Actors.

A Day In the Life - A Memoir

14:00 – 15:00

Miguel Marques

@ z0mbi3

Talk Outline

In this talk, I will share what I do as a pentester and what I think pentesting is, desirable traits I tend to look for when trying to hire for my team, tips and tips if you're thinking about joining the offensive security side of things, keeping current and sharing some war stories! I've done a similar talk like this to Napier students some years ago (and there is even a recording!)... But since then, I've moved companies (twice!), got promoted into management roles while still being kept technical (and hopefully relevant!). This is the pep-talk I'd like to have had before I chose to embark into this pentesting role... but would still be valid for multiple aspects of the cyber industry! It know it started out as "A Day in the life of a pentester"... but it is now a Memoir!

Have You Been Zucked? Probably, here's how you can find out!

15:00 – 15:30

Charlie Hosier & Lloyd Davies

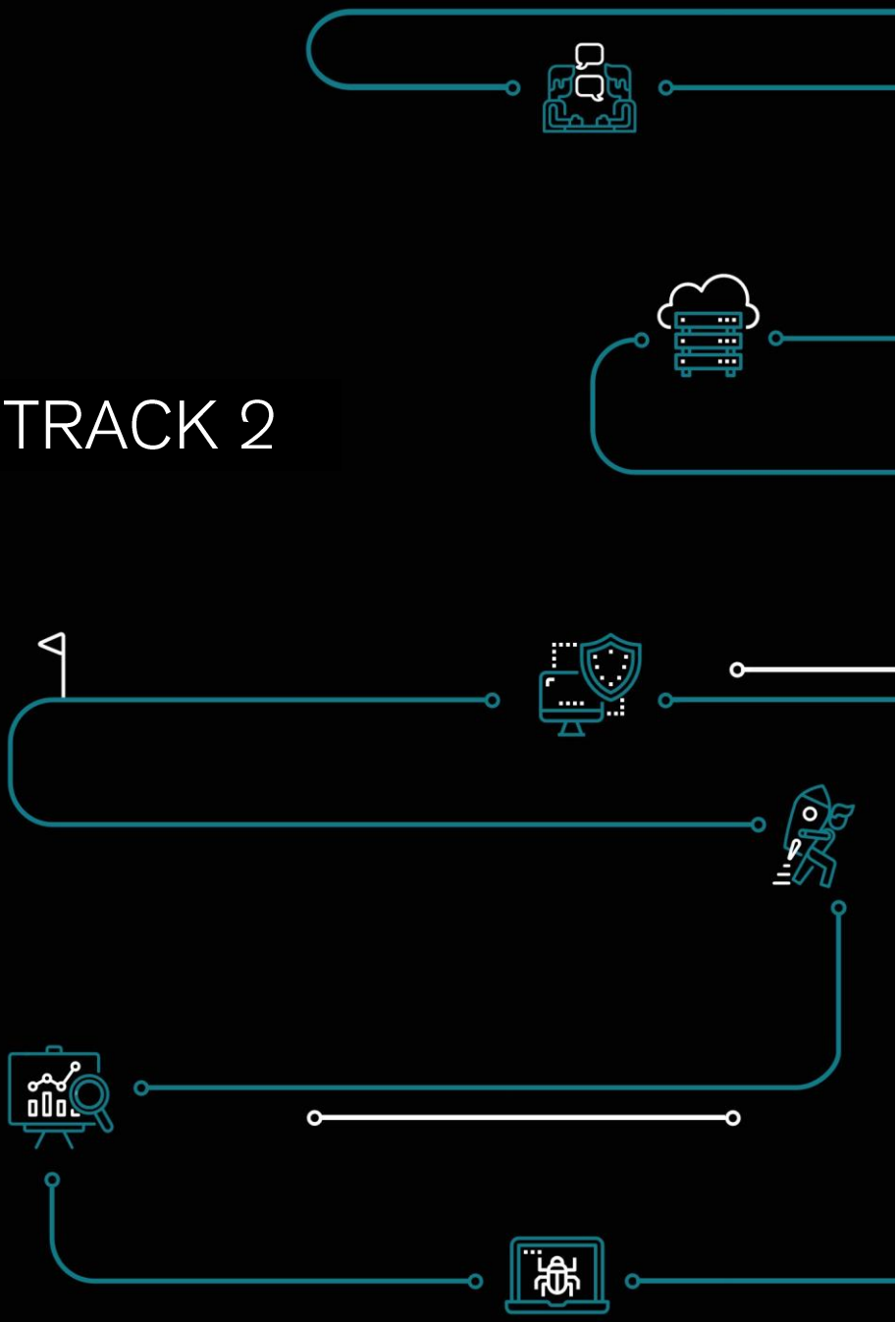
@su__charlie

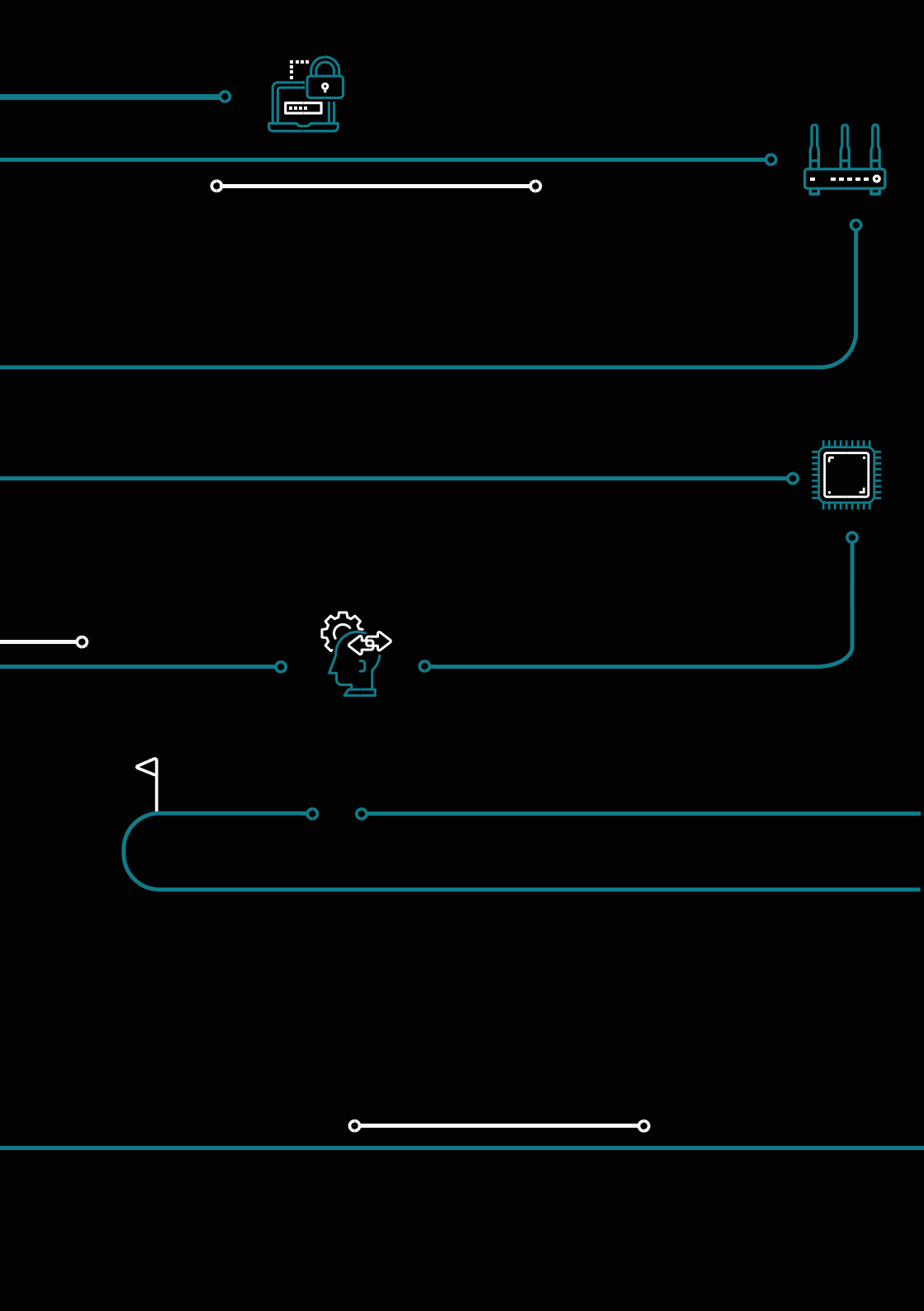
@LloydLabs

Talk Outline

On the 3rd April 2021 we awoke to the news that 533 million Facebook users' information was released in a colossal breach of user security. As panic spread across the security community, 2 University students began a discussion. What could they do to help? They responded rapidly and over a single evening these students created the website HaveIBeenZucked.com. A haveibeenpwned clone dedicated to querying the contents of the Facebook breach by phone number, email, name or facebook identifier. What started as a jokeful website project written in the early hours and a frontend hosted on a 5$ digital ocean droplet quickly escalated and became the goto search tool to check if you had been compromised and with this our 5 minutes of fame began. In this presentation we will outline the entertaining rise in popularity of the HaveIBeenZucked website going from a small personal project to having millions of hits, being endorsed by some of the top security professionals, oscar-award winning Netflix series representatives and across international media outlets. We will speak in detail about breach-detection and finally, we will address the backlash from the privacy community and what we would do differently when Facebook is inevitably breached again.

TRACK 2





Bitweighting for perceptual hash similarity comparisons

11:00 – 11:45

Karen Taljard

@kit_codes

Talk Outline

Discussing the math and decision to explore a bit weighting model used by Natural Language Processing models into comparing image hashes (particularly perceptual hashes) and their positives and negatives.

Breaking In: The Physical Frontline of Information Security

12:00 – 13:00

Ben Jacob

Talk Outline

In today's digital world, organisations heavily invest in enhancing the security posture of their digital assets. However, using social-engineering techniques and simple DIY tools, organisations can often be vulnerable to physical attacks, allowing an adversary to walk-in and compromise an organisation's crown-jewels. This talk will explore various physical breach techniques, review recent war-stories and overall raise awareness about how physical threats can affect the integrity of digital assets.

Over clocking sunflowers

14:00 – 15:00

Eliot Bolster

@_davewm_

Talk Outline

The idea of using electricity to control devices is almost as old as evolution itself with every plant and animal using this method, how can we use this to help us become more connected to our planet rather than further removed how have we used it in the past, is my play also a password and of course is gene editing the future of plants.

Are the UK's data laws still fit for purpose?

15:00 – 15:30

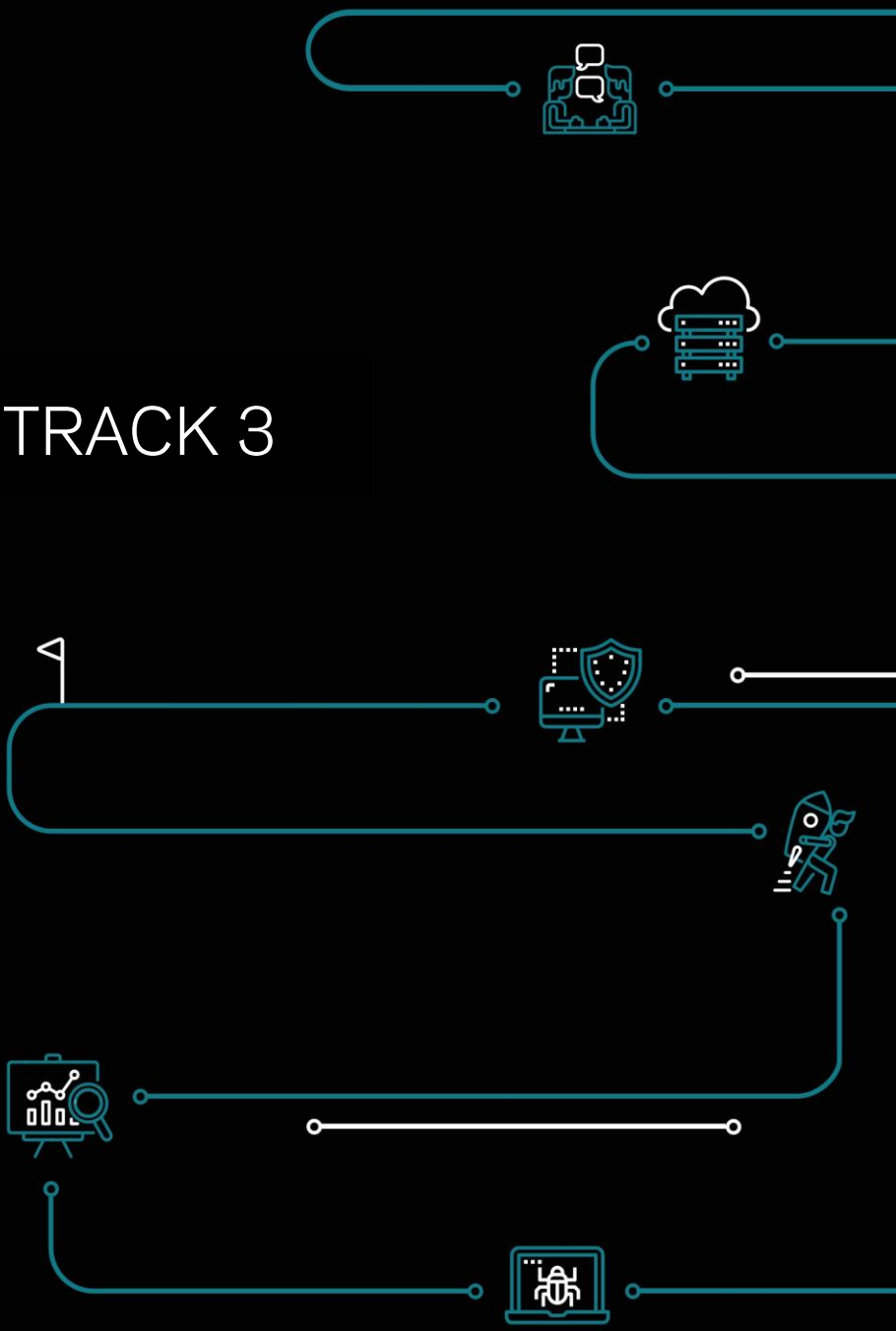
George Brightman

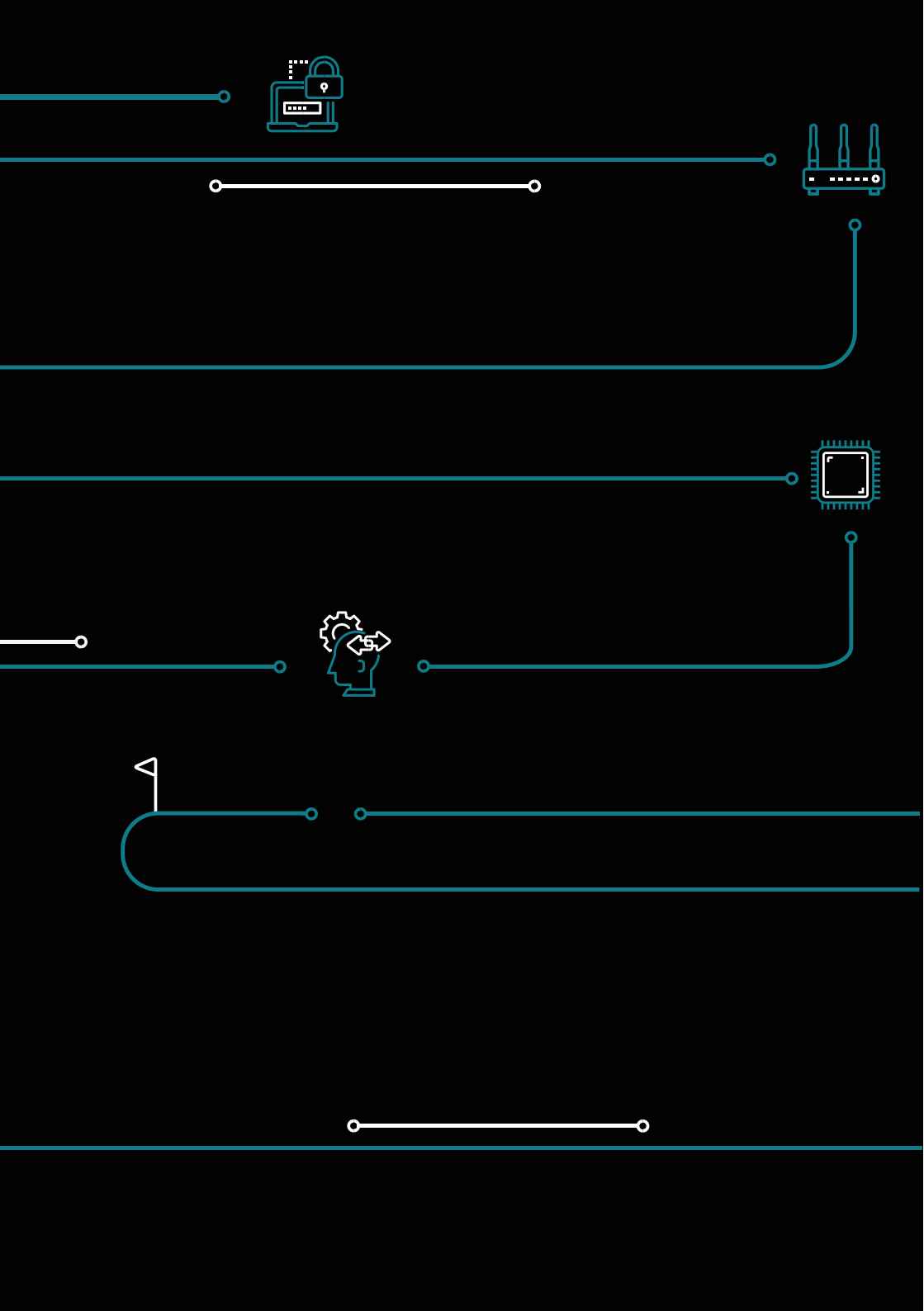
@gbrightman01

Talk Outline

The talk will explore simple issues with the UK's data laws and will allow the audience to make up their own minds on the issue. The talk will also discuss how we can change the laws so they are better for everyone.

TRACK 3





Litigating for Naruto - A Ramble through Tech Law

11:00 – 11:45

David Alexander

@David_Ulph

Talk Outline

A short dive into how the law struggles its way to comprehending the modern advancements of society into technology, the internet, and AI, with (hopefully) entertaining anecdotes from a AI courts to robot redundancy packages

Anti-Virus Evasion through BadUSB

12:15 – 13:00

Cristian Cornea

Talk Outline

During this presentation, we will take a look over how we can bypass most Anti-Virus detection using a payload embedded on a BadUSB device, resulting in a silver bullet for gaining initial access inside a victim network. Demo will be also included during the presentation.

They're listening but is it you that's talking, attacks on voice recognition systems

14:00 – 15:00

Fraser Wilson

@ItWasNae_Me

Talk Outline

With the ever-increasing proliferation of voice controlled smart devices with access to confidential data come new threats which must be addressed. What are these threats? What are the solutions? What limitations do we face? I hope to at least start to help you answer those questions in this talk. We will explore a range of attacks that can be used to trick voice recognition systems into thinking you are talking to them, from high to low tech, including playback attacks, deepfake audio attacks, and other voice spoofing and conversion attacks. Then we will look at what possible countermeasures there are and what the pros and cons of these solutions are, and whether they are worth it or practical.

How to fix a bigoted AI

15:00 – 15:30

Dominik Hanlon

@dominikhanlon

Talk Outline

How the idea of the left and right have eroded politics and led to people supporting bad ideas on both sides and how we can use technology to fix systemic issues.

KEYNOTE

15:30 – 16:30

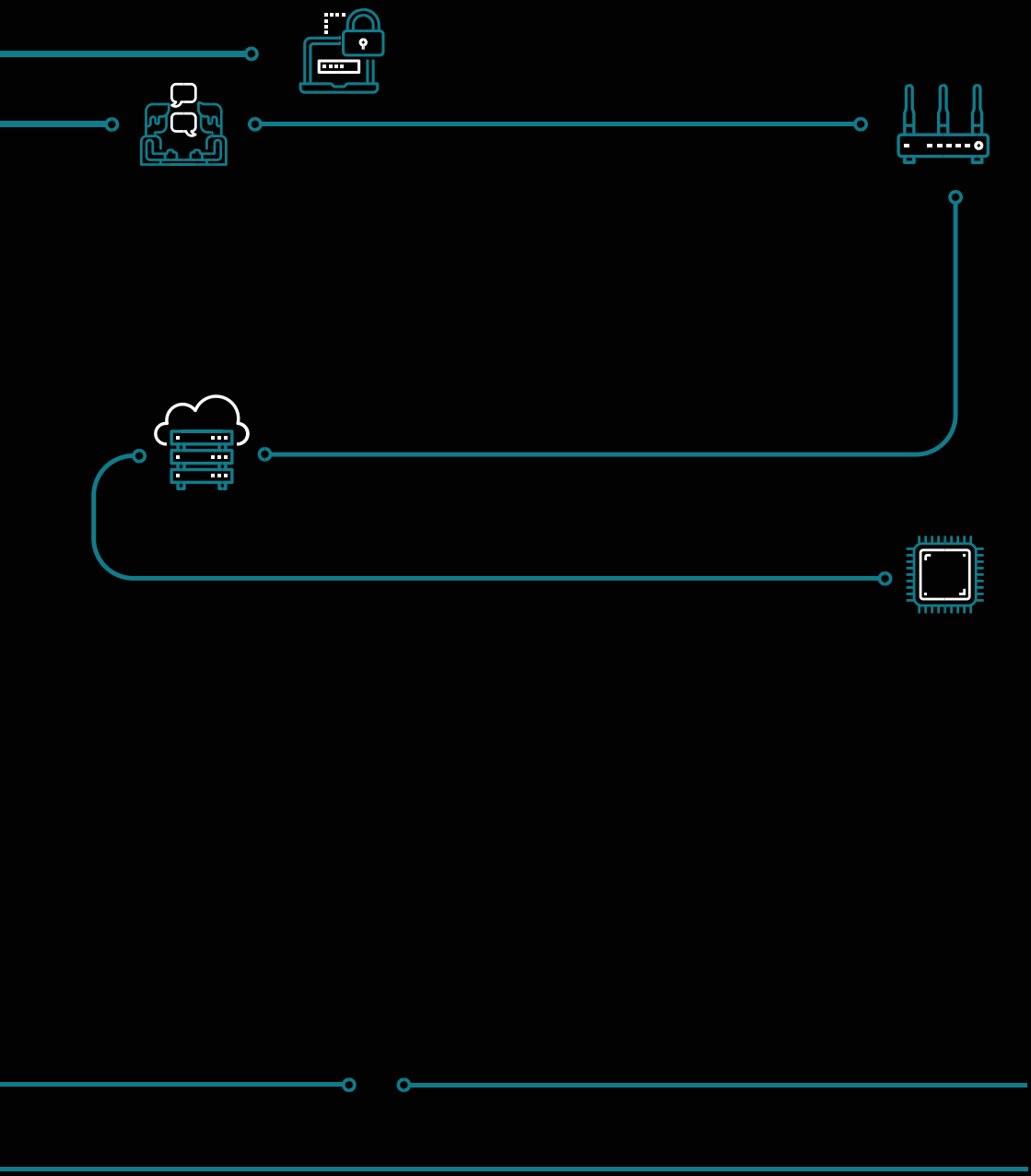
Zibby Kewcka
Quorum Cyber
@DrKwecka

Bio

Zibby progressed from electronics, through advanced networking, and research in privacy-preserving cryptographic techniques, to helping some of the biggest organisations secure by design and defend their assets. On this journey he has inspired further development of covert-channel analysis and crypto solutions, assisted in forming one of the first CSOCs in UK, designed card data tokenisation solutions, and played cameo role in securing a banking grade distributed ledger system. Recently UK Head of Information Security at Heineken, and now, vCISO Lead at a rapidly scaling-up cybersecurity firm, Zibby continues to collaborate with CISOs, the cyber security industry and academia.

Talk Outline - Hack you life, before it is hacked for you

This talk is your compass to Hack the World. Whether you are just starting the journey with paid work, or you have been doing it for the while, this geek guide to Hitchhiking the Galaxy is for you.



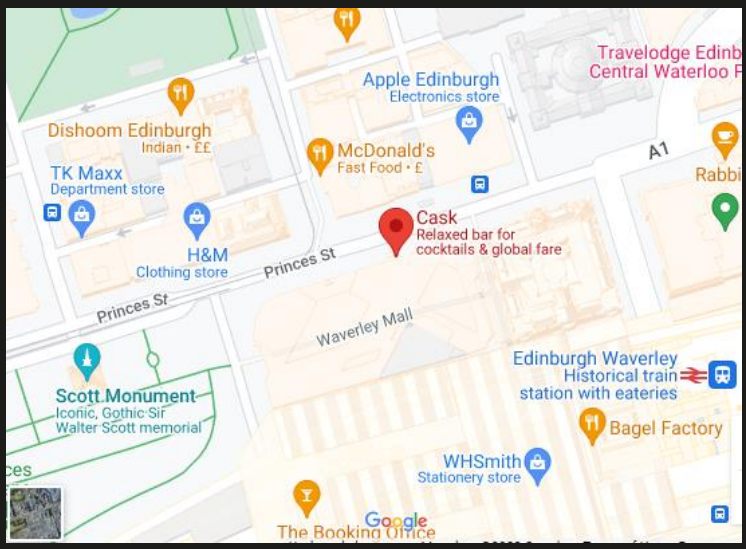
AFTERPARTY!

We are thrilled to announce that this year's afterparty will be held at Cask Smugglers!

Be sure to be wearing your LTDH Afterparty wristbands found in your swag bags, else you won't get served without one.

Lothian Busses which go near the Afterparty Venue:

- 10
- 27
- 45



CAPTURE THE FLAG

The CTF competition is tomorrow!

With competitors coming together to test and develop their problem-solving skills, competing in numerous varied & intense challenges. The Jeopardy-style CTF will take place in the rooms marked on the map, with puzzles aimed at both beginners and pros will be released throughout the day, touring you through a variety of topics in the Cyber Security realm. You may find yourself trying to exploit a vulnerability in a website and using it to gain remote access, or perhaps you will have to crack a code by exploiting a weakness in the encryption algorithm used.

Team up with four other friends to compete for the prizes!

Remember! Make sure you bring your laptop with a Kali VM and a charger.

09:00	REGISTRATION
10:00	CTF BEGINS
13:00	LUNCH
17:00	End of CTF

ADARMA

TOGETHER WE'VE GOT THIS

BECOME A CYBER DEFENDER

ADARMA.COM/CAREERS

Feedback

We need your help!

By completing the feedback form accessible by scanning the QR code, you have the opportunity to shape the future of Le Tour Du Hacks to come.

THANKS

The first Le Tour Du Hack took place in 2017, attended by 70 enthusiastic cybersecurity students located in the Scottish central belt. Since then, Le Tour Du Hack 2018, 2019, 2021 and 2022 grew exponentially with students coming from further afield and developed to include our first conference day!

After a tough couple of years, we're thrilled to be back in person, and to see Le Tour Du Hack continue to grow!

An event of this size and calibre was uncertain when we started organising, however, thanks to the support and generosity of certain individuals and organisations. With a lot of work and some luck, the dream came true. If not for the hard work of all involved, Le Tour Du Hack 2023 wouldn't have been here.

Therefore, the LTDH23 team would like to thank the following people

Abertay Ethical Hackers · All our awesome speakers · Cask Smugglers Wonderful Staff · Edinburgh Napier University · Our CTF Challenge Creators Team · Stickermule · Vistaprint · Edinburgh Napier University Printing Services · Total Merchandise · All Our Conference Day Volunteers · Quorum Cyber · Adarma · Edinbrugh Napier School of Computing · Rich Macfarlane · Cooper (@Ministraitor)

LTDH23 SPONSORS

Quorum Cyber

ADARMA

Edinburgh Napier UNIVERSITY

School of Computing

ENUSEC>_

TEAM & CONTACT

Kit
PRESIDENT

[redacted]
VICE-PRESIDENT

Colin McDaid
SECRETARY

Jon
TREASURER

Lewis Watson
MEDIA OFFICER

Fraser Wilson
SOCIAL EVENTS OFFICER

GET ONLINE!

Here are the essential WIFI details!

Students can make use of EDUROAM with their student credentials.

Non-Students can access the Public University WIFI.

SOCIALS

Get Involved!

Make sure to keep up to date on the weekend's activities using the **#LTDH23** hashtag!

Tweeting using **#LTDH23** will enter you into a draw for the chance to win a free ticket to the next Le Tour Du Hack!

NOTES

NOTES

Quorum Cyber

ADARMA

Edinburgh Napier UNIVERSITY

School of Computing

ENUSEC>_