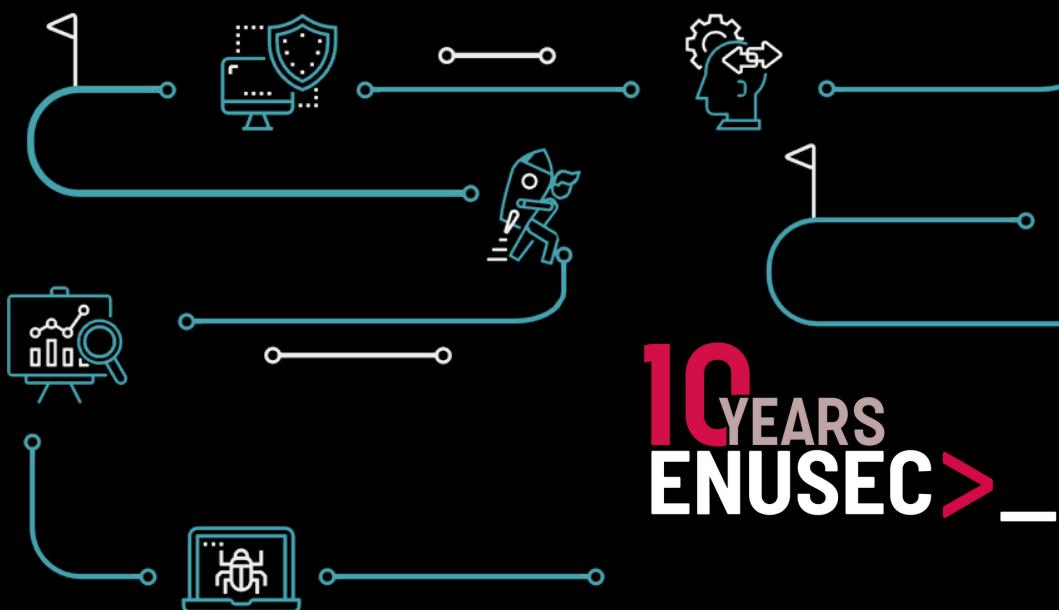




Le Tour Du Hack 2025

Conference: 10th May 2025

Capture the Flag: 11th May 2025



**10 YEARS
ENUSEC >_**

Welcome!



Whether you're a long-time friend of ENUSEC or stepping into one of our events for the very first time: Welcome! We're absolutely thrilled to have you join us for what promises to be another fantastic weekend of community, curiosity, and collaboration.

This year is a special one: 2025 marks ten years of ENUSEC. A whole decade of students, professionals, and passionate hackers coming together to build something bigger than themselves. It's a milestone that wouldn't have been possible without the relentless energy, creativity, and time poured in by countless individuals over the years. To everyone who's helped shape ENUSEC into what it is today - **Thank you**. We are here because of you!

And to those just starting your journey with us: this is your community too. The next ten years start now, and we're excited to see what you'll bring to the table. Whether you're here to compete, learn, connect, or just hang out - we're all better off because you're here.



10 YEARS
ENUSEC >_

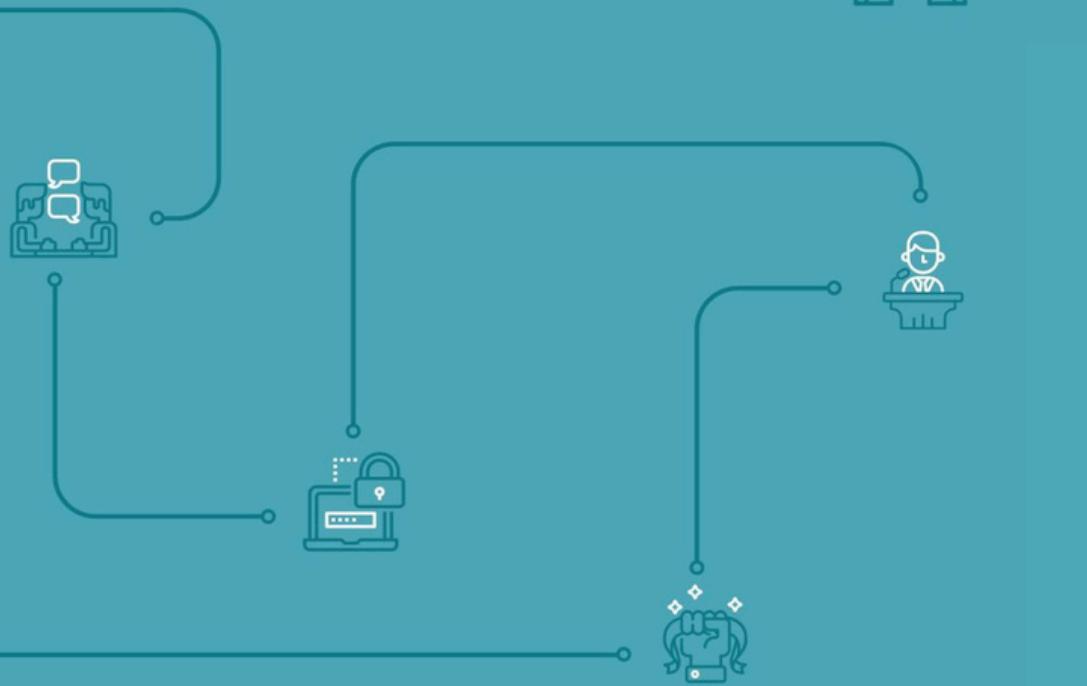




Our mission for Le Tour Du Hack remains as true as ever; to create a space where people come together over a shared passion for security, technology, and just figuring stuff out. In a world that keeps changing, be it through the rise of AI, industry shifts, or new challenges - we stand stronger together. This event is proof of that.

The three-track technical conference, the talks, the challenges, the conversations - all of it is here to spark curiosity and connection. This weekend is about sharing knowledge, meeting like-minded people, and celebrating the creativity that drives this community forward. So dive in, make new friends, ask questions, share stories, and most of all...enjoy yourself!

Without further ado... let the Le Tour Du Havin' Fun begin! 🙌



Rules & Etiquette

Le Tour Du Hack 2025, just like any other ENUSEC event, abides by the Berlin Code of Conduct. This is to ensure we are doing our part to make our events inclusive to the largest possible 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.



10 YEARS
ENUSEC > _

Code of Conduct

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 2025 weekend.

Unacceptable behaviours from any attendee, including sponsors, speakers, volunteers and/or those with decision-making authority, will not be tolerated. Anyone asked to stop unacceptable behaviour is expected to stop immediately. Le Tour Du Hack 2025 team reserves the right to take any action they deem appropriate, up to and including expulsion from the event without warning nor refund.

Alert a member of the Le Tour Du Hack 2025 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 2025 team can be identified as those wearing a red or light blue shirt marked "Committee" or "Volunteer" on the back.



10 YEARS
ENUSEC > _

bugcrowd



Quorum
Cyber



Verkada



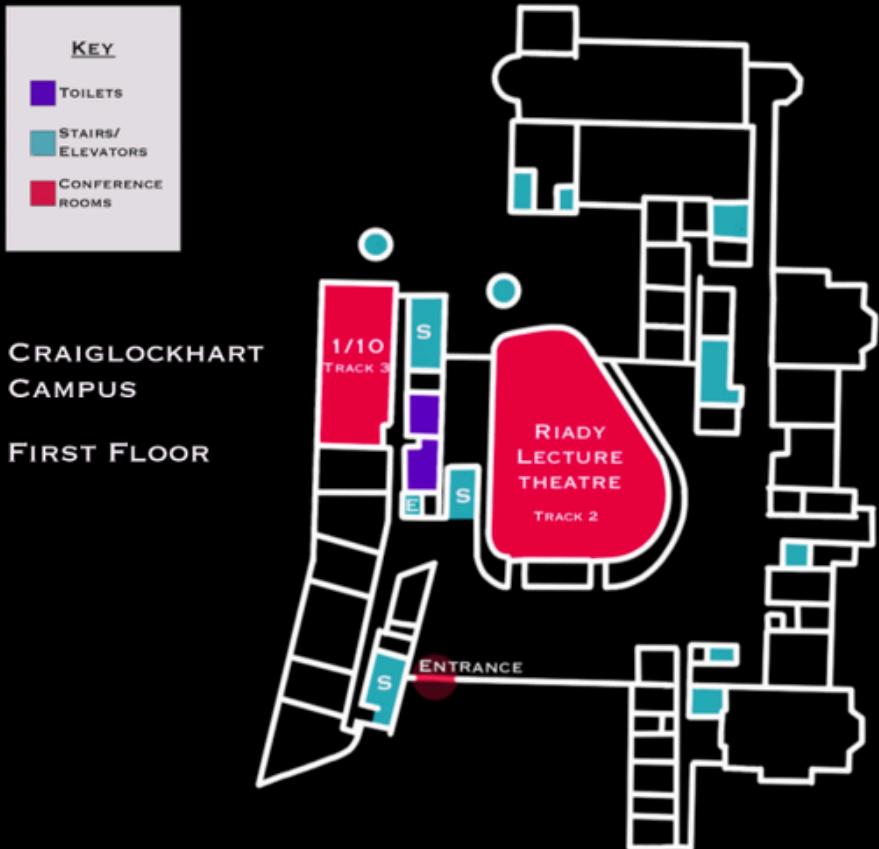
Zero Days

Edinburgh Napier
UNIVERSITY

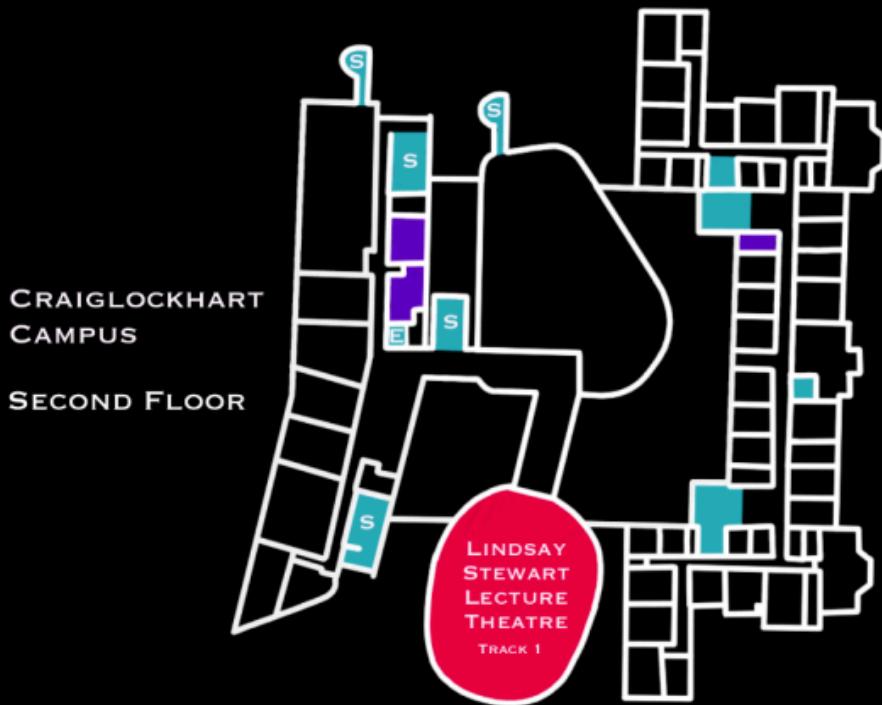
10 YEARS
ENUSEC >_



Map - Ground Floor



Map - First Floor



LE TOUR
DU HACK

10 YEARS
ENUSEC >_

Common Locations

Toilets

Located on the ground floor on the way to Track 3

Track 1

Up the stairs to the left of Riady (Track 2),

Head towards the Egg from there

Track 2

Riady Lecture Theatre (the big one in the Craiglockhart Foyer)

Track 3

Head towards the stairs up to T1, Take a left, then a right,

Walk down the corridor to room 1/10 past the toilets

Quiet Room

To Be Confirmed but will be notified on the conference day

Prayer Room

Room 4/32 upstairs via the lift, or

Room 4.03 for Muslim Prayer Room (directions at

<https://ltdh.enusec.org/prayer>)

Refreshments + Lunch

Served in main Craiglockhart Foyer,

All sofas, chairs etc. in there can be used



Conference Timetable

Track 1 Lindsay Stewart Lecture Theatre	Track 2 Riady Lecture Theatre	Track 3 Room 1/10
Registration 09:00 - 09:30		
Opening Remarks - Track 2 09:30 - 10:00		
Opening Keynote - Track 2 Bill Buchanan 10:00 - 10:45		
Adrian Smales - Health, IoT, Robotics & Digital Evidence 10:45 - 11:15	James Kwaan - 10 Years on, What is new on the threat landscape? 10:45 - 11:15	Karen Taljard - Burning the candle at all ends 10:45 - 11:30
Break 11:15 - 11:20		Break 11:30 - 11:35
Michael Varley - Ransomware Diaries: Hackers, Hostages and the Price of Panic 11:20 - 12:20	Basil Manoussos - Digital Evidence in the times of Artificial Intelligence. A glimpse into the future 11:20 - 12:20	Fraser Wilson - They're Listening, But is it You That's Talking! 11:35 - 12:20
Lunch 12:30 - 13:30		



10 YEARS
ENUSEC > _

Panel Discussion - Track 2

Neurodiversity in Cyber - Superpower vs. Kryptonite?

13:30 - 14:15

Break

14:15 - 14:20

David Brown - Cyber War Chronicles: My Path to Becoming a DFIR Consultant
14:20 - 14:50

Eliot Bolster - Is my OT becoming Rusty?
14:20 - 14:50

Del Delgianoudis - The Absolute State of Nvidia
14:20 - 14:50

Break

14:50 - 14:55

Dónnan Mallon - InfoStealerz - The Phantom Menace
14:55 - 15:55

Harry McLaren - Modern Cybersecurity Operations: Responsibilities, Knowledge & Skills
14:55 - 15:55

Cameron Cottam - CAPTCHA Clicked, System Compromised: Understanding the ClickFix Phishing Technique
14:55 - 15:55

Afternoon Refreshments

15:55 - 16:15

Kirils Solovjovs - A Big Bad App: Welcome to Corporatocracy
16:15 - 17:00

Thomas Xuan Meng - The Evolution of Syscalls: A Winding Path to Untraceable Execution
16:15 - 17:00

Kat Fitzgerald - Confound and Delay: Honeypot Chronicles from the Digital Battlefield
16:15 - 17:00

Closing Keynote - Track 2

Cary Hendricks

17:00 - 17:45

Closing Remarks

17:45 - 18:00



10 YEARS
ENUSEC > _

Opening Keynote

10:00-10:45

Prof. Bill Buchanan

Edinburgh Napier University

X @BillAtNapier

Professor at Edinburgh

Napier University

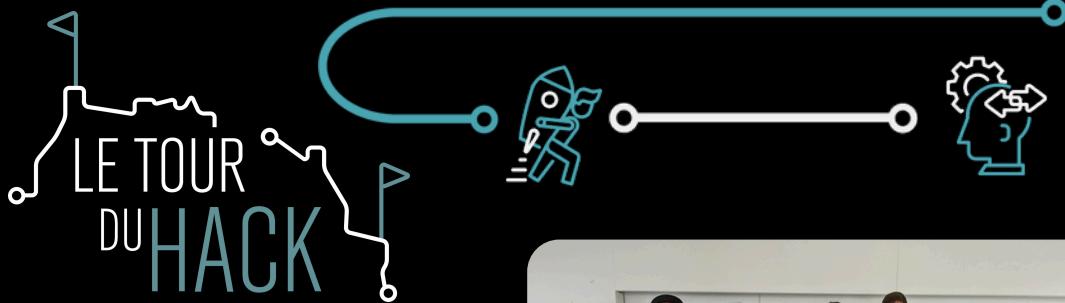


Bill Buchanan is a Professor of Applied Cryptography in SCEBE at ENU, a Fellow of the BCS, a Principal Fellow of the HEA, and a Fellow of the Royal Society of Edinburgh. He was appointed an Officer of the Order of the British Empire (OBE) in 2017 for services to cybersecurity and has received multiple student-voted teaching awards in 2011, 2014, 2015, 2019, 2020, and 2023. He is the founder of the Blockpass Identity Lab and Director of the Scottish Centre of Excellence in Digital Trust and DLT. Bill has published over 30 academic books and over 450 research papers, alongside one of the most extensive cryptography sites in the World (asecuritysite.com).

The Cybersecurity Horizon: Post Quantum Cryptography (PQC), Quantum Computers, and the rise of GenAI

This presentation will look to the major disruptors in the world of cybersecurity, including for the integration of PQC and in the usage of quantum computers, along with outlining the risks around the rise of GenAI.





#ENUSEC_X



10 YEARS
ENUSEC >_





Track 1



10:45 - 11:15

Adrian Smales

X @asmalestech



Bio

Adrian Smales is what happens when a digital visionary collides with real-world chaos—and wins. He's wrangled £700k in innovation cash, built award-winning health tech, and advised the NHS through a system meltdown (without breaking a sweat). Part CIO, part cyber wizard, part data whisperer, he's led transformations across Europe, merged humans and machines (ethically), and still finds time to teach Python to neurodiverse students. Armed with a PhD and a killer instinct for strategy, Adrian doesn't just talk change—he makes it happen, brilliantly and boldly - Written by ChatGPT 4o!

Talk Overview

Pacemakers, insulin pumps and autonomous gadgets now chat over 5G, but every heartbeat they broadcast is an open invitation to hackers. The warning is clear: when code meets flesh, failures aren't blue screens—they're funerals. Regulators finally demand cybersecurity, yet current standards ignore digital evidence. Without immutable, cryptographically signed logs, exploited devices can erase their own fingerprints, leaving victims defenceless. Developers must bake in blockchain-backed audit trails, tamper-proof clocks and sensor-decision-command logging that survives courtroom scrutiny and legal recourse. Build it lean so life-saving timing isn't sacrificed. Log everything, lock it down, or risk turning lifesaving tech into lethal weapons for humans.



Ransomware Diaries: Hackers, Hostages and the Price of Panic



11:20 - 12:20

Michael Varley

X @ltasme92

Bio

Mike has been chasing cybercriminals for over a decade and still hasn't caught a break. From building SOCs to battling ransomware gangs, they now spend most days knee-deep in digital crime scenes. If it's encrypted, exfiltrated, or just plain broken, they've probably dealt with it. Today, they're here to share war stories and help you dodge the ransomware bullet (or at least know where it's coming from).

Talk Overview

Step into the high-stakes world of ransomware incidents, where companies face impossible choices and criminals sometimes show unexpected mercy.

Through real-world case studies, we'll unravel how attackers break in, how they steal data, how they cripple organisations and what happens when victims negotiate. Expect war stories featuring creative exploits, bizarre negotiations and the occasional ethical dilemma.

We'll cap it off with actionable takeaways to avoid starring in the next episode of Ransomware Diaries.



Cyber War Chronicles: My Path to Becoming a DFIR Consultant

14:20 - 14:50

David Brown

X @davidbrown1982



Bio

Napier Alumni, Police Officer 18 years and Lead DFIR Consultant at NCC Group. Now manages the UK, Iberia and North America team whilst still delivering and managing large technical breaches, predominantly ransomware.

Talk Overview

Navigating your way through life can be a challenge. Having done Computer Science at Uni in the very early 00's then joining the Police I now find myself as a Principal DFIR Consultant for one of the world's leading Cyber companies. This talk will take you through my experiences, including my time at Napier, and provide some real world insight into the life of an IR Consultant battling with Scattered Spiders...



InfoStealerz: The Phantom Menace

14:55 - 15:55

Dónnan Mallon

X @Cyb34_DO



Bio

I'm a CTI analyst with a fondness for travel and exploration. Like photography and building bricks for that extra serotonin. I enjoy the odd type of music here and there as well as an alumni of Edinburgh Napier. Books are also cool too.

Talk Overview

Welcome to the wacky world of Information Stealers! They come in all shapes and sizes. We'll be discussing the rise and impact these infostealers have had globally throughout various industries and how some have met their downfall through Law Enforcement. The talk further looks into how infostealers can disguise themselves and abuse legitimate applications at the cost of the victims information.



A Big Bad App: Welcome to Corporatocracy

16:15 - 17:00

Kirils Solovjovs

@k@chaos.social



Bio

Kirils Solovjovs is Latvia's leading white-hat hacker and IT policy activist, renowned for uncovering and responsibly disclosing critical security vulnerabilities in both national and international systems. Kirils started programming at age 7 and by grade 9 was spending his lunch breaks writing machine code directly in a hex editor. With deep expertise in network flow analysis, reverse engineering, social engineering, and penetration testing, he has significantly contributed to cybersecurity advancements. Notably, Kirils developed the jailbreak tool for MikroTik RouterOS. He currently serves as the lead researcher at Possible Security and as a research assistant at the Institute of Electronics and Computer Science.

Talk Overview

We live in a world where corporations decide how we interact with digital systems, and they are not on our side. If something goes wrong and you're not the 1,000th person to report it, it's your problem. Customer service? That's just a chatbot pretending to care.

This talk is about what happens when the system isn't built for you – because it never was. A mobile operator refused to sign a contract with me because they couldn't remove "I agree to receive ads." My orders get randomly canceled because I refuse to have a phone number. My industry certifications? Gone. Because I stood up for my privacy rights.

We'll go through these experiences and dissect why things are this way. Why must we adapt to their systems, but they won't adapt to ours? Why does a company's "official support channel" usually mean "no support at all"? Why do startups optimize for growth at the cost of basic usability?

This isn't just a rant (though there will be rants). It's a call to stop playing by their rules. We'll discuss examples of where people have pushed back and won, and where we've completely failed. If you've building an app or website, and intend to respect your users, this talk is for you.



Hack. With. Bugcrowd

A Place
Where You
Succeed

TOP REASONS TO HACK WITH BUGCROWD

01 Rewards

Earning serious cash hacking on our programs

02 Bragging Rights

Jump our leaderboard & impress your friends

03 Experience

Join our welcoming community & build crowd experience

04 Career Opportunities

Learn about becoming a cybersecurity professional

05 Passion

Build your passion with industry friends

JOIN THE COMMUNITY

https://bugcrowd.com/user/sign_up

Twitter: @Bugcrowd

Discord: Bugcrowd Community

ABOUT US

A crowdsourced security platform where we match the talents of the crowd with the growing security needs of our customers. We have no shortage of targets including Web, API, iOS, Android, Automotive, and Binary Apps. Come work with us to make the world a more secure place to work, live, and do business.



Cybersecurity is a fast growing space and it needs you. Whether you're a beginner or experienced. Driven by passion or rewards. Curious about APIs or hardware; there's a place for you at Bugcrowd. #ItTakesACrowd



Track 2

ENUSEC>_



Le Tour du Hack: What has changed in cyber disruption in 10 years and what skills do you need to be successful now?

10:45 - 11:15

James Kwaan

X @jaykaywan



Bio

James Kwaan's leadership roles and recognition reflect his dedication to advancing cybersecurity as a profession and addressing challenges such as workforce shortages and evolving cyber threats. He has actively championed diversity as a strategy to address the shortage of skilled professionals in cybersecurity.

Talk Overview

In the last 10 years there have been significant changes, I will cover the key factors affecting the threat landscape to help us understand who is likely to attack us and why?

I will explore the disruptive geopolitical context and current threats and trends and the new frontiers which cyber is now breaking into.

Summing up what skills and things do you need to learn to position yourself for a successful career in the dynamic wave of change we are all facing with the advent of technological change!



Ransomware Diaries: Hackers, Hostages and the Price of Panic

11:20 - 12:20

Basil Manoussos

X @BasilonCyber



Talk Overview

Digital Forensics and Digital Evidence have long been viewed as the "poor relation" of Cybersecurity—often overlooked by both academia and industry. However, the tide is turning. With the growing sophistication of cybercrime, these fields are gaining the attention they deserve. Artificial Intelligence is now being leveraged for everything from orchestrating complex cyberattacks to crafting phishing emails and generating realistic fake imagery. But as AI advances, so do the threats.

- What do these developments mean for cybercrime and the global effort to combat it?
- Are law enforcement agencies and practitioners prepared for what's coming?
- Can AI be used in counter-forensics—and if so, how do we respond?

In this thought-provoking presentation, Basil Manoussos will share his insights, predictions and concerns about the rapid, largely unregulated deployment of AI tools such as Large Language Models (LLMs) and Generative Pre-trained Transformers (GPTs), particularly in the hands of criminals. Drawing on years of fieldwork and recent academic research, his talk will offer a compelling look at the intersection of AI, cybersecurity, and the future of digital evidence.



11:20 - 12:20

Basil Manoussos

X @BasilonCyber



Bio

Basil Manoussos is a seasoned expert witness in digital evidence, with over 15 years of practical experience handling hundreds of cases—including several high-profile investigations. He has collaborated with INTERPOL on major initiatives such as Project LEADER I and CPX SIRIUS, and has been a keynote speaker at three INTERPOL Digital Forensics Expert Group (DFEG) events. In 2025, Basil successfully hosted DFEG2025 at Edinburgh Napier University, following more than two years of dedicated planning and coordination. He has also developed and delivered the highly regarded Cybersecurity Certification for Lawyers programme for the Law Society of Scotland, running for over five years.



From 2017 to 2025, Basil led the Cyber Academy at Edinburgh Napier University, further cementing his influence in public cybersecurity awareness across Scotland, the UK, and internationally. He frequently speaks at global conferences (United Kingdom, The Netherlands, Romania, Greece, Poland) and academic institutions including UCL, Sheffield Hallam, Strathclyde University, American College of Greece, SAN, Glasgow University, ENU, Kadir Has University, UWS. He has held visiting lecturer roles at the Catholic University of Lyon (Faculty of Law) and Sheffield Hallam University.

Basil is currently pursuing a doctorate focusing on the use of Artificial Intelligence in cybersecurity research. He has also completed the Artificial Intelligence Programme at the University of Oxford and the Ethics & AI programme at the London School of Economics (LSE) as well as the Oxford Cyber Security for Business Leaders Programme. He was the first expert witness to achieve the prestigious University of Aberdeen / Bond Solon certification for Expert Witnesses under the Scottish legal system. Since 2025, Basil is running the first ever Cyber Marathon, a 24-hour cyber event, that attracts some of the greatest names in cybersecurity. Basil has won the Best Educator Award at the PICCASO Privacy Awards (Europe) and has been shortlisted five times at the Scottish Cyber Awards.



10 YEARS
ENUSEC >_



Is my OT becoming Rusty?

14:20 - 14:50



Eliot Bolster

X @eliotbolster

Bio

Eliot is an OT engineer, who has been working with National Grid for the past 2 years after graduation from Napier. He has been a member of ENUSEC, they have always been interested in IOT and OT and has followed that passion through uni and beyond something something cyber security something something great to be back

Talk Overview

Could Rust be a viable option for coding our critical OT systems, adding another language to the IEC 61131-3 standard?



Despite IT loving a trend it has always been harder for these trends to get adopted within industrial systems, fads are often sold as OT solutions but do not get the same mainstream acceptance as the IT counterparts, making the industry look like its moving at a pace that would only impress glaciers.

In this talk I will go over Rust, fads and OT to look at what the future may hold and what exactly might make Rust the next C when it comes to our operational tech.

Modern Cybersecurity Operations: Responsibilities, Knowledge & Skills

14:55 - 15:55

Harry McLaren

N/A

Bio

Established technology leader with 17 years of experience in IT and cybersecurity. Currently focused on solving complex cyber-related problems at Tesco as the Head of Cybersecurity Engineering. Security Operations subject matter expert and "Blue Team" obsessed! Active member (and founder) of the Scottish cyber community Cyber Scotland Connect.

Talk Overview

Overview of why cyber is an interesting place to work, what 'cybersecurity operations' is, the main focuses of the blue team (preparation, detection, response and recovery), adversary knowledge frameworks (ATT&CK), and finally an overview of important technical and behavioural skills needed in 2025 and beyond!



The Evolution of Syscalls: A Winding Path to Untraceable Execution

16:15 - 17:00

Thomas Xuan Meng

N/A

Bio

I am a cybersecurity enthusiast and a former Edinburgh Napier student.

Talk Overview

This presentation provides a step-by-step, technical exploration of the evolution of syscalls. It begins with the fundamental role of NT Windows APIs in executing syscalls within kernel space. The introduction of the talk clarifies what constitutes a legitimate call stack and explains syscall stubs and System Service Numbers (SSNs), grounding the audience in the core concepts required to understand detection and evasion strategies.



It then progresses to modern process injection primitives, covering the memory allocation, writing, and execution phases of shellcode in both local and remote address spaces. A comparison is drawn between Win32 API-based injection and their native API equivalents. These implementations are evaluated from a detection standpoint, focusing on stack trace inspection and two widely deployed detection mechanisms in AV/EDR systems: syscall stub hooking in ntdll.dll and IAT hooking in other System32 modules. These mechanisms provide critical telemetry to heuristic detection engines.

Two major development paths can be taken: using undocumented APIs or exploits, and using syscalls. This talk focuses on the latter. Direct and indirect syscall implementations are examined in detail, with specific attention to detection surfaces observable through call stack anomalies.

The final session introduces an advanced "proxy indirect syscall" technique, which merges indirect syscalls with proxy callback functions to generate legitimate looking call stacks while bypassing EDR hooks without altering memory. This approach is presented as a highly evasive execution primitive.

"proxy functions" are legitimate, system-defined function pointers or callback handlers that are invoked by the Windows kernel or userland subsystems. These functions can be hijacked or intentionally used to indirectly invoke syscalls, allowing the red team to preserve a legitimate call stack. Notably, some proxy functions reside within function blocks that are not retrievable via conventional GetProcAddress. There are many proxy function stubs available, which can be identified using a pattern scanning tool wrote by the author. This tool will be published on GitHub soon.



**10 YEARS
ENUSEC >_**



Panel Discussion:

13:30-14:15

Sharon Moore

 /in/sharonannemoore

Sharon serves as IBM Technology's Global CTO for Government with over 20 years of experience across outsourcing, consulting, and sales. Awarded an MBE in 2018, she's a passionate advocate for inclusion in tech through her work with BCSWomen and other organizations. Sharon is a Trustee of BCS, the Chartered Institute for IT, and was inducted into the Computer Weekly Most Influential Women in UK Tech Hall of Fame. Her mission focuses on transforming public services with technology and driving positive change in the tech industry.

Sarah Williamson

 /in/sarahspeaksmh

Sarah is a Social Work Operational Manager for mental health services in Renfrewshire. A social worker since 2011, Sarah has specialised in mental health since 2016. An accredited trainer in suicide intervention through LivingWorks, Sarah has been in management positions for 5 years and works with a diverse range of staff including those who need additional support or adapted working arrangements to reach their full potential at work.

Jonathan Marnoch

 /in/the-nd-cyberguy

A season IT professional with 25 years of experience. Jonathan (Jonty) Marnoch has worked with some of the largest companies in the UK and globally.

Currently Principle Cyber Security Architect at JLR their expertise spans various sectors, including Defence, Banking, Utilities, Retail and currently automotive. Diagnosed in the last few years with AuDHD, Jonathan champions Neurodiversity in the workplace wants to have more open and frank discussions about Mental Health especially in the Cyber community where Cyber Burnout is on the increase. - Offering open and frank guidance, support and communications allowing us to be OK with not being OK.



Panel Discussion:

13:30-14:15



Ruby Richardson

/in/ruby-richardson-821388228

Ruby is a 4th year BEng student in Cybersecurity and Forensics at Edinburgh Napier University. During her third year, she completed a year long industrial placement at Gymshark, where she gained hands on experience across a range of cybersecurity roles.

Diagnosed with dyslexia in primary school, Ruby has had to continually adapt to overcome challenges, both academically and professionally.



Stephanie Golstov

/in/steph-g-77b67219b

Steph is a creative and strategic consultant specialising in digital transformation. She co-founded the digital consultancy Osta Labs Ltd which, for the past seven years has supported clients with digital strategy, machine learning and AI-readiness. Steph is proudly and (mostly) comfortably neurodivergent and has a particular interest in how technology can support inclusive and exciting workplaces of the future.



Panel Discussion

We're so glad to be bringing back the Panel event again this year, as it's been very well received over the years it has ran; always bringing insightful questions and industry experience to the forefront. This year, we believe the panel topic of '**Neurodiversity in Cyber: Superpower vs. Kryptonite?**' is more relevant than ever, especially as neurodivergent individuals become recognised within the industry.

"About 15% to 20% of the world's population shows signs of neurodivergence" - Northwestern Medicine, 2025

In an industry that thrives on unconventional thinking, this is not just a statistic. It's a reminder of the incredible diversity of minds shaping cybersecurity. Whether you personally identify as neurodivergent or not, these conversations impact all of us. From recruitment and workplace culture to problem-solving approaches, understanding and embracing neurodiversity makes our community stronger.

So make sure to come along to hear what our brilliant panelists have to say, challenge your assumptions, and ask your questions - this space is for you too!



10 YEARS
ENUSEC >_



Quorum
Cyber

Quorum-Cyber

helpfightbullies.com

@QuorumCyber

Microsoft Security

Excellence Awards 2025

Microsoft Intelligent
Security Association

WINNER

Quorum Cyber

Security MSSP of the Year



#ENUSEC_X



10 YEARS
ENUSEC_X

A graphic element consisting of a blue line-art icon of a line graph with three data points, positioned above the text "10 YEARS ENUSEC_X".



Track 3

10 YEARS
ENUSEC >_



LE TOUR
DU HACK



#ENUSEC_X



10 YEARS
ENUSEC >_

Burning the Candle at all Ends



10:45 - 11:30

Karen Taljard

X @Kit_Codes

Bio

I am a threat hunter and ex Napier student who loves to help people where I can.

Talk Overview

Life sucks. Between the chaos of work life and personal life, it can be hard to make time for some R&R. Today we will discuss what you can do to better manage the chaos as well as activities you can do to unwind and disconnect from the world for a bit.



The Absolute State of Nvidia

14:20 - 15:50

Del Delgianoudis

🦋 @netrunnervt.bsky.social



Bio

Last year's ENUSEC president, general tech tinkerer and more recently known for becoming a vtuber, trying to stuff an LLM into a Pi Zero 2 W and being mad at Intel, AMD and Nvidia at the same time.

Talk Overview

Since 2018, Nvidia's consumer graphics division has been developing a severe case of we-don't-care-about-you-itis. This talk aims to be a historical deep-dive and recap of the past ten years of Nvidia - 2016 to 2025 - with a focus on their desktop hardware business and how they sometimes go out of their way to make your life less fun.



They're Listening, But is it You That's Talking!



11:35 - 12:20

Fraser Wilson

X @ItWasNae_Me

Bio

Graduate of Napier, and former ENUSEC, now working at Quorum Cyber. In my free time I enjoy breaking things, trying to fix things (especially cameras), sailing, and taking photos on one of my (far too many) cameras

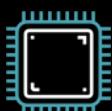
Talk Overview

Smart voice assistants are everywhere and have so much access to our lives and data and rely upon tools like Automatic Speaker Verification to secure their access, but how good are they really at telling whether it is you. Let's look at audio based attacks and see how secure (or unsecure) they really are, and then lets talk all things audio weirdness.

LE TOUR
DU HACK



10 YEARS
ENUSEC >_



From Verification to Infection: A Deep Dive into ClickFix Techniques and Fake CAPTCHA Exploits

14:55 - 15:55

Cameron Cottam

 /in/cameron-cottam



Bio

I am a Senior SOC Analyst at Adarma, specialising in incident response and threat detection. I work with clients across multiple industries, helping them investigate high-priority alerts and strengthen their defensive cyber capabilities. I hold a degree from the University of Abertay Dundee, where I developed my passion for cybersecurity. In my spare time, I focus on certification studies and try to get into some personal projects; other than that, I like to play games and go to the gym.

Talk Overview

CAPTCHAs are widely used as a security measure to distinguish humans from bots. However, threat actors have been exploiting this tool into a technique known as ClickFix. By presenting fake "Verify You Are a Human" CAPTCHA pages, attackers aim to trick users into executing malicious PowerShell commands that establish a connection to an attacker's network, delivering malware and compromising the system.

This talk will examine how CAPTCHA has grown from a protective measure to being exploited by Threat Actors tool into social engineering technique by exploring the real-world cases of ClickFix techniques, break down the technical structure behind these attacks, discuss post-compromise tactics, and outline a company's defensive strategies to mitigate this threat.

10 YEARS
ENUSEC >

LE TOUR
DU HACK



Confound and Delay: Honeypot Chronicles from the Digital Battlefield

16:15 - 17:00

Kat Fitzgerald

  @rnbwkat



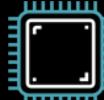
Bio

Chicago-based and proudly a natural creature of winter, I thrive on snow, OSS, and just the right amount of chaos. Whether sipping Grand Mayan Extra Añejo or warding off cyber threats with a mix of honeypots, magic spells, and a very opinionated flamingo named Sasha (the BSidesChicago.org mascot), I keep things interesting. Honeypots and refrigerators rank among my favorite things—though my neighbors would likely disagree.

Talk Overview

Embark on a whirlwind tour of global cyber deception with a seasoned(?) security engineer who's been running honeypots in some of the world's most intriguing locales, including the bustling digital battleground of Ukraine. This talk will blend humor and hard-won wisdom to reveal the lessons learned from deploying, customizing, and maintaining honeypots across diverse environments. Participants will enjoy a lively narrative filled with tales of cyber trickery, cultural quirks, and the occasional mishap, all while gaining actionable insights into enhancing their own security strategies.

Imagine being a digital beekeeper, setting up traps for cyber threats in some of the most unexpected places around the globe—from the frosty landscapes of Ukraine to the bustling tech hubs of Tokyo. Over the years, I've had the peculiar pleasure of watching bad actors stumble into these traps, often with the same grace as a bull in a china shop. This talk is less about the "how" and more about the "what-the-heck-just-happened" moments that have made this journey unforgettable. Buckle up for a rollercoaster ride through the wild world of global honeypots, where every server tells a story, and sometimes, that story is downright hilarious.


**10 YEARS
ENUSEC >_ LE TOUR
DU HACK**





#ENUSEC_X



10 YEARS
ENUSEC >_



Closing Keynote

17:00-17:45

Cary Hendricks

ID Cyber Solutions

 @figjam.sogeek.org

*Global Operations Director
at ID Cyber Solutions*



Cary is an accomplished security technical investigator, advisor and trainer with several decades of experience working with various agencies across the world. He often talks about stuff and things. He is the lead instructor for ID Cyber Solutions and ID Cyber Training UK, which delivers training on Incident Handling, Digital Forensics and Ethical Hacking.

He sits on various boards in the UK coordinating cyber security practices in education, the space industry, supply chains and various cyber security frameworks supported by the NCSC. He is always willing to help wherever he can to make other people's lives easier* (*some effort required)

Hacking Things with AI stuff: How does it fit in security?

Frameworks grew from previous breaches. Leveraging AI in security frameworks will certainly accelerate security. Where are we going to fit in?

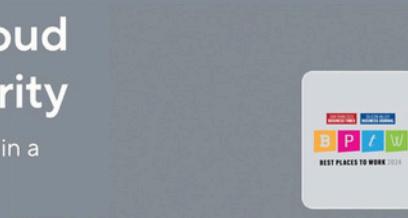


10 YEARS
ENUSEC>



Leading in Cloud Physical Security

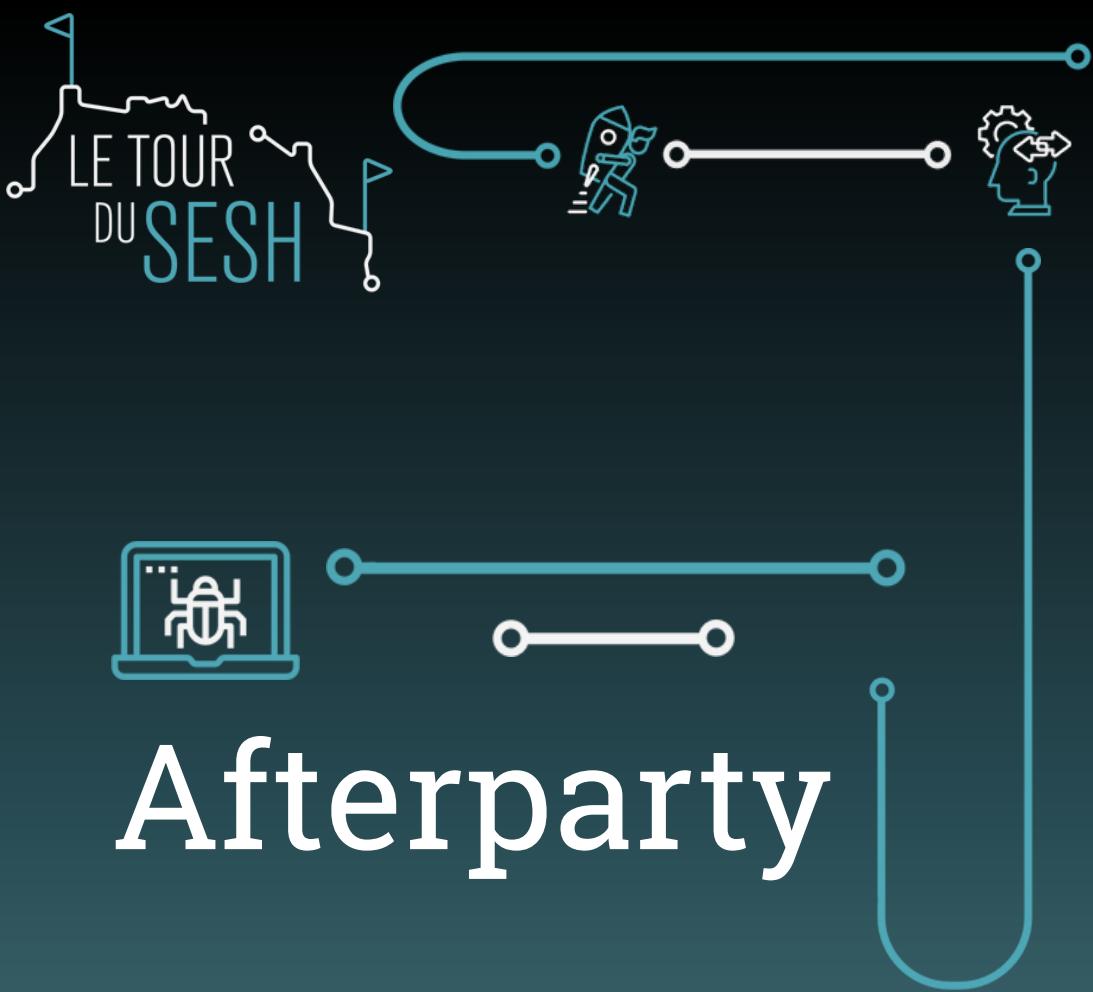
Protect people and places in a privacy-sensitive way.



Join Verkada's rapidly expanding EMEA team in London.
Gain full-stack troubleshooting experience
across hardware, software, and networks.

Scan the QR code to enter
your information!
or email carly.fong@verkada.com





10 YEARS
ENUSEC >_

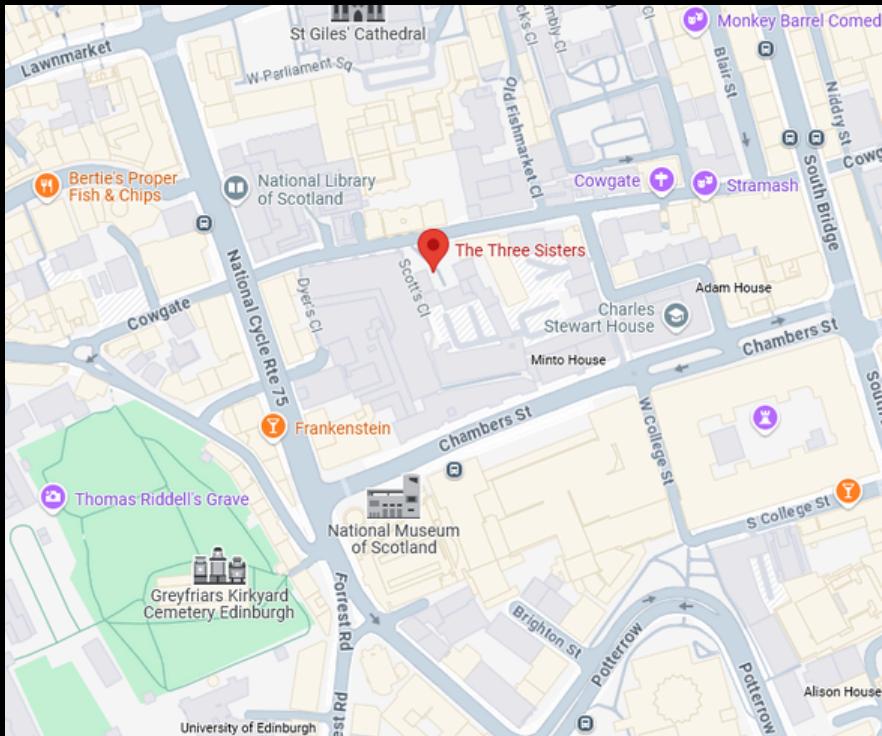


After Party Details

This year our afterparty will be held at The Three Sisters in Maggie's Chamber (upstairs) from 18:30 onwards.

We've got a lovely cocktail/mocktail menu for you for a discounted £5.50 each - plus you get a free drinks tokens on the door so don't forget to collect them and use them at the bar before 8pm! (after 8pm the bar tab can be used on any drinks)

Address: 139 Cowgate, Edinburgh EH1 1JS





Cocktail



Darknet Daiquiri
Malibu, Cream, Pineapple, Citrus

£5.50

OverClocktail
Aperol, Prosecco

£5.50

Mocktail

Error 404

Whitley Neal Raspberry 0%,
Raspberry, Cherry Syrup, Lime &
Cranberry

£5.50

Zero Proof Exploit
Atopia, Lime, Agave, Lemonade

£5.50



LE TOUR
DU HACK



Le Tour Du Hack CTF

Powered by

Zero Days





www.ZeroDays.ie

Capture the Flag

The Competition Starts Tomorrow!

Ready to put your hacking skills to the test? Join us for an adrenaline-pumping Jeopardy-style CTF where competitors unite to crack codes, exploit vulnerabilities, and outsmart security systems!

Whether you're infiltrating websites, breaking encryption algorithms, or hunting for hidden flags, our challenges are crafted for both newcomers and seasoned pros. New puzzles drop throughout the day, taking you on a thrilling tour across the Cyber Security landscape!

- 🔑 Compete solo or form a dream team of up to 4 hackers
- 🏆 Top team wins exclusive invites to next year's ZeroDays CTF
- 🌐 Register now at ctf.enusec.org

The battle happens in track three marked on the map. Don't forget your essentials: laptop loaded with a Kali VM and your charger!

9:00	Registration
10:00	CTF Starts
13:00	Pizza Lunch - CTF Paused
16:00	CTF End



10 YEARS
ENUSEC > _

Feedback

We need your help!

By completing the feedback form, found at ldth.enusec.org/feedback, or scanning the QR code, you have the opportunity to shape the future of Le Tour Du Hacks to come!



Cyber Security at Edinburgh Napier University

NCSC-certified Hon's and MSc degrees, world-leading research, expert staff, industry integration, ENUSEC, NCSC ACE-CSE



Thank you!

The first Le Tour Du Hack took place in 2017, as a CTF attended by 70 enthusiastic cyber security students located in the Scottish central belt. Since then Le Tour Du Hack 2018 and 2019 grew exponentially with students coming from further afield and developed to include our first conference day! We're thrilled to bring LTDH back to you and see it 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 - plus a lot of work and some luck - the dream came true once more. If not for the hard work of all involved, Le Tour Du Hack 2025 wouldn't have been here.

Therefore, the LTDH25 team would like to thank the following people and organisations:

All of our awesome speakers

Bugcrowd

ZeroDays CTF

Edinburgh Napier University

The Three Sisters Staff

Our CTF Challenge Creators Team

Curries Print Centre

Sneddon Signs

Quorum Cyber

Verkada

Edinburgh Napier University Alumni Team

All of our awesome volunteers

Our Community Sponsors

Rich MacFarlane

Superlogo

And YOU!



10 YEARS
ENUSEC >_

LTDH25 Sponsors



Verkada

bugcrowd



Quorum
Cyber

10 YEARS
ENUSEC > _

Edinburgh Napier
UNIVERSITY



Team & Contact



Joyee Bashir
PRESIDENT



Lewis Watson
VICE-PRESIDENT



Benjamin Lang
SECRETARY



Ian Wright
TREASURER



Lewis Morrison
SOCIAL MEDIA OFFICER



Sean Cameron
SOCIAL SECRETARY



10 YEARS
ENUSEC >_

Get Online!

Here are the essential Wi-Fi details:

- Students can make use of Eduroam with their student credentials.
- Non-students can use the University's Guest Wi-Fi.

Socials!

Get involved!

Make sure to keep up to date on the weekend's activities using the hashtag #LTDH25 or #ENUSEC_X to make or revisit some ENUSEC memories!

We'll be active as much as we can so stay connected!



@enusec

10 YEARS
ENUSEC >_

NOTES

NOTES

NOTES



bugcrowd



**10 YEARS
ENUSEC > _**

Edinburgh Napier
UNIVERSITY

