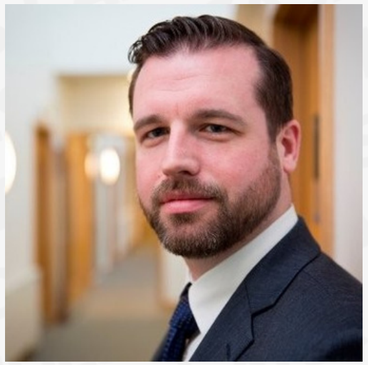

LANCASHIRE
SIDES

Our Leadership Team

Mike Somers
Co-Founder

Jen McCulloch
Co-Founder



Dr. Dan Prince
Co-Founder

Sam Swift
Head of Commercial

Holly-Grace Williams
Co- Founder

Sean Atkinson
Co-Founder

Rosie Anderson
Co-Founder

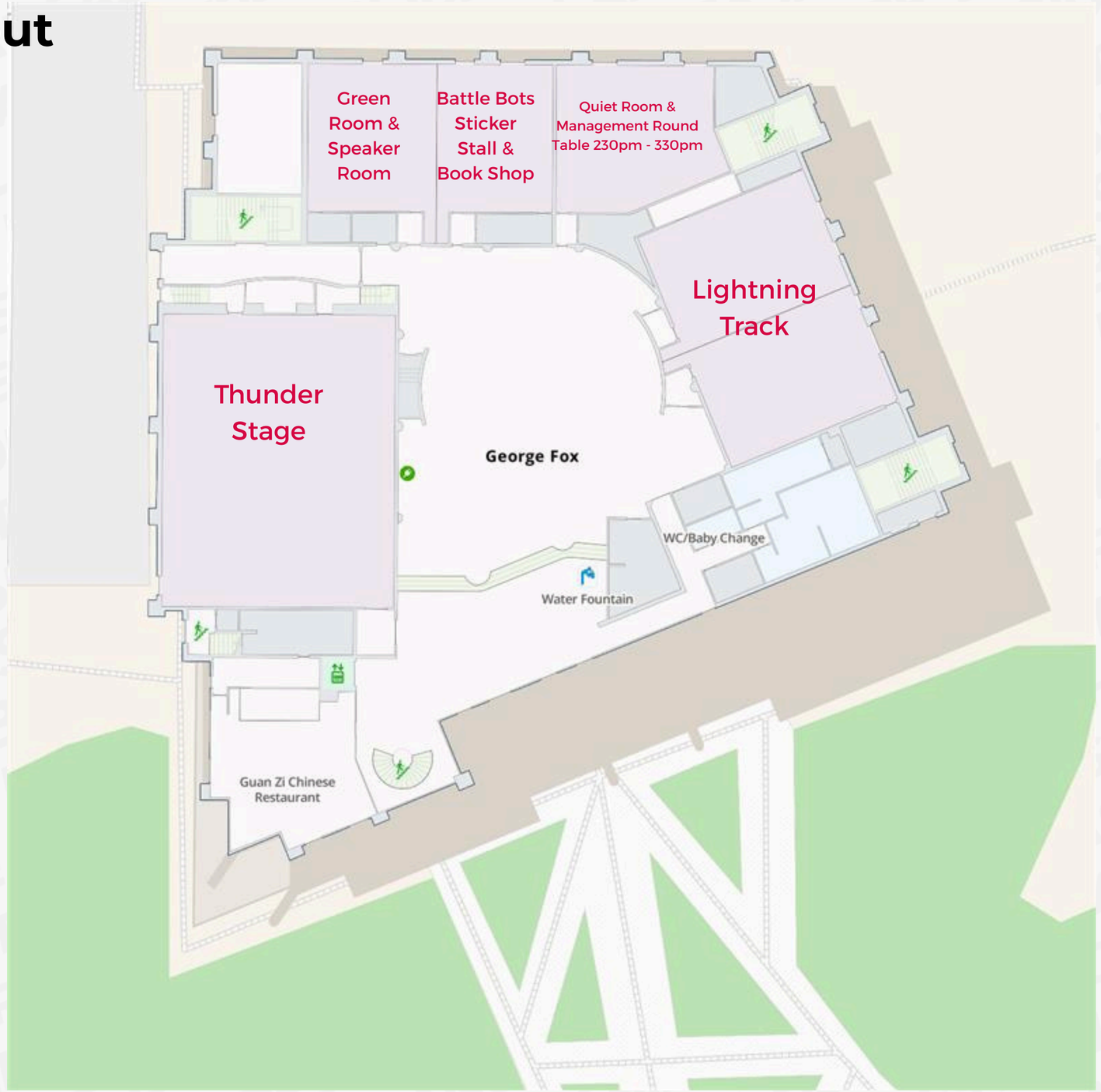
BSIDES LANCASHIRE

About BSides 2025

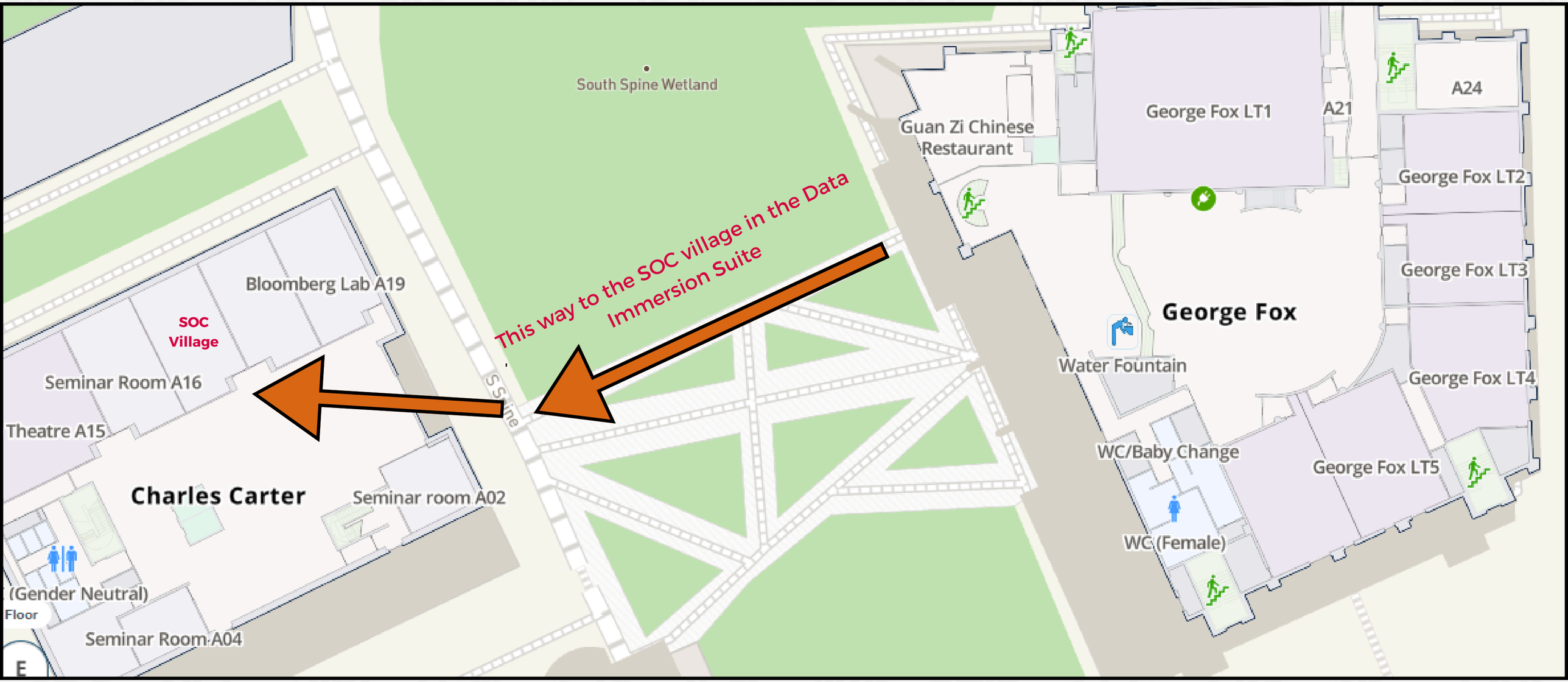
The event will be focused on valuable technical research, inclusion, diversity, and career progression. There will be insights from various disciplines and roles within the industry and will cater to anyone from the more seasoned professionals, to anyone with an initial interest in cyber.

Our BSides Lancashire event is proud to be partnered with Lancaster University and will be held in the prestigious George Fox Hall on the Lancaster University Campus, with career workshops and drop-ins with industry leading experts.

Conference Layout



How to get to the SOC Village



Why Lancashire?

Lancashire has a strong and established security community and an ever-growing complement of businesses and consultancies working in the security space.

**The North West Cyber Corridor is well-established,
so it makes sense to have a BSides community in the North West.**

2019
Last North West BSides

350
Target Attendance

£5bn
National Cyber Force

GCHQ
Based in Manchester

Why Lancaster University?

Lancaster University has been recognised as an Academic Centre of Excellence in Cyber Security Education (ACE-CSE) and in Cyber Security Research (ACE-CSR) by the UK's National Cyber Security Centre. It is one of only seven in the UK with both recognitions and the only one in the North West.

Over the next five years, the University will grow the diversity of talent entering into cyber security careers, through the new Cyber Security Executive MBA programme, a new BSc/MSci degrees in Cyber Security and our already existing NCSC-certified MSc in Cyber Security.

MBA
New Exec. Cyber Degree

BSc
New BSc Degree

InfoLab
Centre of Excellence

500+
Computing Students

£20m
Data Cyber Quarter

NCSC
Accredited inc. EPSRC

SentinelOne

cytix

Citation Cyber

blackfoot cybersecurity

We would like to say a huge thank you to our event sponsors!

CAPSLOCK

DAINTTA
Finding intelligence in data

FIRE DUCK

Scan the QR code to see the schedule

Security Lancaster | Lancaster University

AKIMBOCORE
UNRIVALLED PENETRATION TESTING

th4ts3cur1ty.company ›

Sandinista Consulting
CYBER SECURITY: WE KNOW THE WAY

Our Chosen Charity

Bowland Pennine Mountain Rescue Team

Bowland Pennine Mountain Rescue Team (BPMRT) is a registered charity providing an essential, life-saving emergency service to the people of Lancashire and beyond.

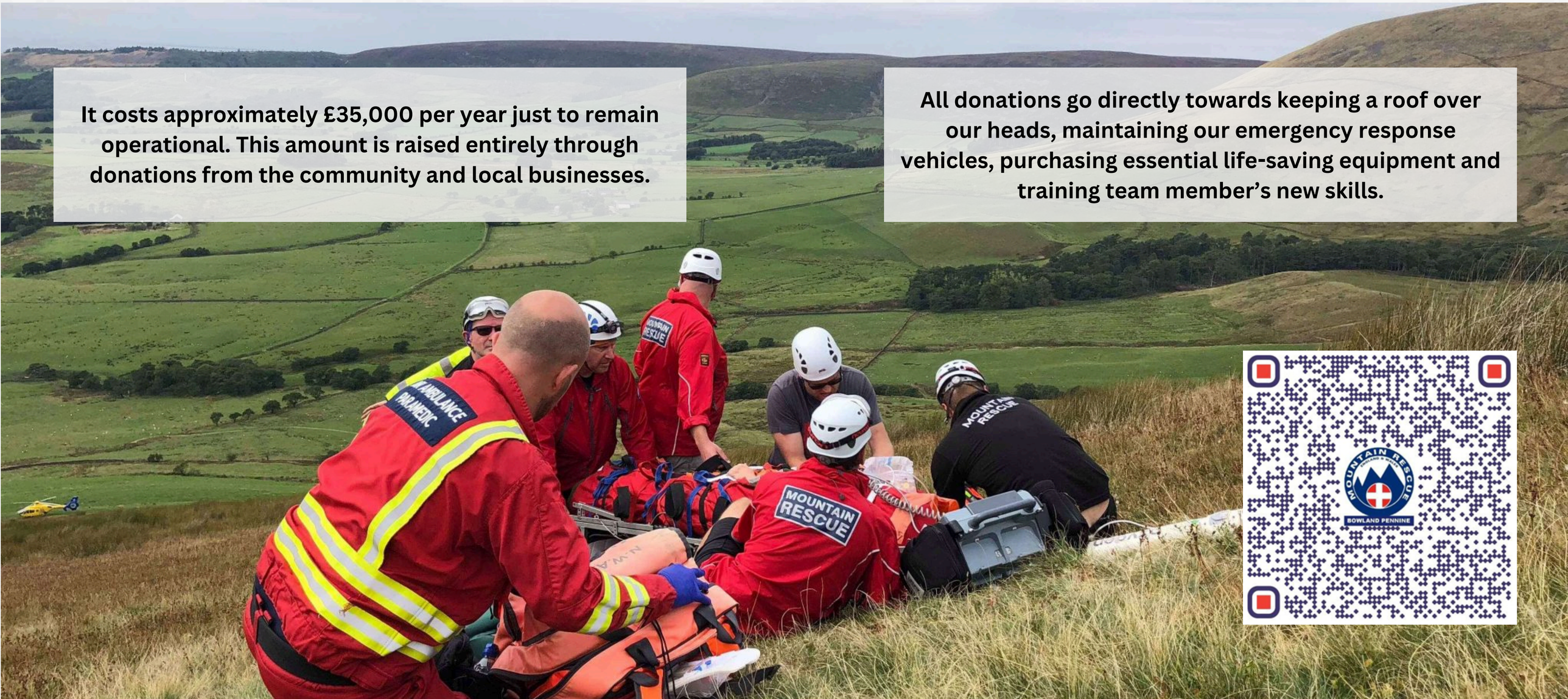
The Team attends an average of 70+ callouts each year and is staffed entirely by unpaid volunteers

Our Chosen Charity_

Bowland Pennine Mountain Rescue Team

It costs approximately £35,000 per year just to remain operational. This amount is raised entirely through donations from the community and local businesses.

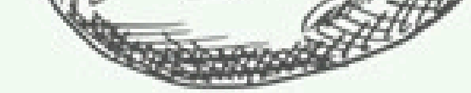
All donations go directly towards keeping a roof over our heads, maintaining our emergency response vehicles, purchasing essential life-saving equipment and training team member's new skills.

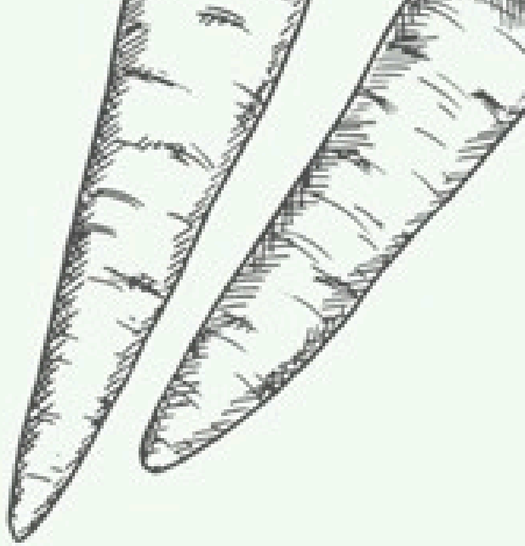


Prayer Space	Building	Room / Comments
Furness Muslim Prayer Room	Adjacent to Pizzetta	Laundry / Has nearby ablution facilities and prayer mats in the room
Hindu Prayer Room	Bowland	SR16
Jewish Synagogue	Chaplaincy Centre	A19
Christian chapels	Chaplaincy Centre	Foyer A10/A13
Buddhist Meditation Room	Chaplaincy Centre	B1

Some of these rooms require a code to enter. The BSides staff will be able to help you with this on the day. Please ask a volunteer in the red T-shirts for assistance.

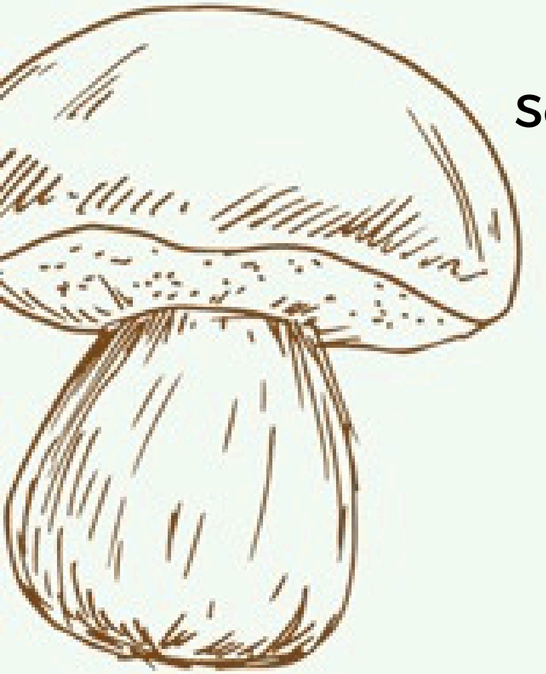

cytix





Hot Fork Lunch Menu

served from our hotplate



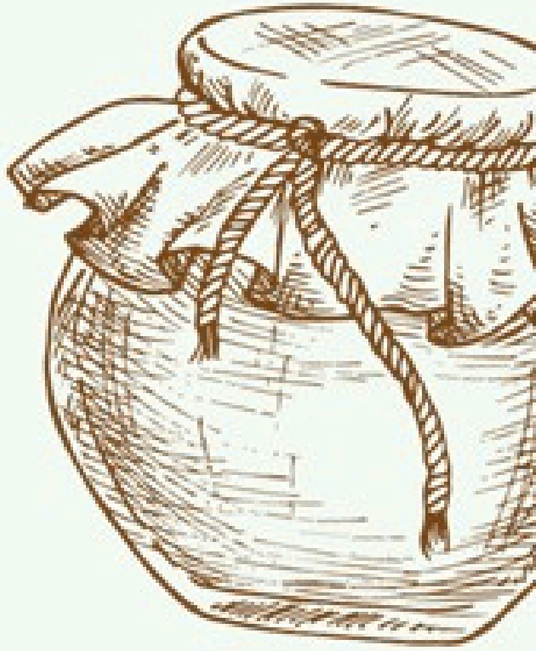
Vegetarian hotpot (V)(VG)(GF)(DF) Lamb hotpot (GF)(DF)

Served with crusty bread, mushy peas, red cabbage and pickled onions

Mixture of sandwiches

A selection of mini cakes

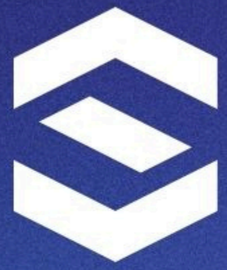
Tea, Coffee and Orange juice



(V) Vegetarian, (VG) Vegan, (GF) Made with Gluten-free ingredients, (DF) Dairy Free

Please note our kitchens handle all major allergens.

If you have an allergy or food intolerance,
please speak to a member of our team.



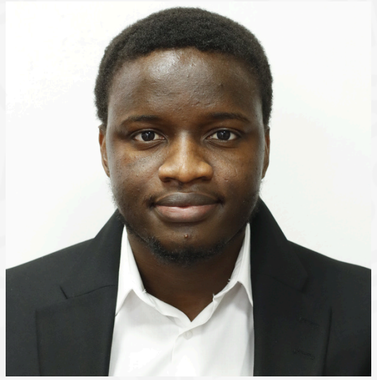
SentinelOne®

World-Leading Cybersecurity. Powered by AI.

One Enterprise Platform Protecting Endpoint, Cloud, and Data.

THUNDER STAGE SCHEDULE

Kat Fitzgerald
10:00 Keynote



Victor Onyenagubom
10:30

Ric Derbyshire
12:05

Helen Oluyemi
12:40

Wayne May
14:30

Pete Neve
15:05

Simon Chapman
13:40

David Lodge
16:30

LIGHTNING STAGE SCHEDULE

Anuska Kundhu
10:30

Natalie Takpah
10:50

Rob McLellan
11:10

Andrew Lucas
12:00

Katie Paxton Fear
12:20

Phat Hobbit
12:45

Gerald Benischke
14:30

Victor Oriakhi
14:55

Greta Caikinaite
15:15

Joe Burton 15:35

BSIDES LANCASHIRE

Security Lancaster | Lancaster University

SentinelOne

cytix

Thunder Talk Synopsis & Bios

AKIMBOCORE
UNRIVALLED PENETRATION TEST NG

th4ts3cur1ty.company ›

Citation Cyber

CAPSLOCK

blackfoot cybersecurity

Sandinista Consulting
CYBER SECURITY: WE KNOW THE WAY

FIRE DUCK

DAINTTA
Finding intelligence in data

10:00 Keynote Kat Fitzgerald

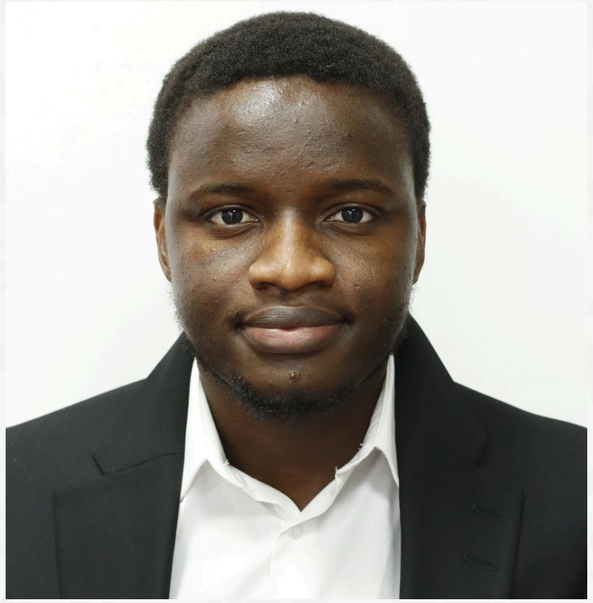
[Kat Fitzgerald]

Just your average rnbwkat blending cybersecurity expertise with a dash of chaos and whimsy.

Based in Chicago and unapologetically a natural creature of winter, I thrive on snow/cold, open-source tools, homelabs and the occasional delightful disruption. My security journey began in the era of magnetic tapes and armed guards, where parking lot security was as crucial as system passwords. With over 40 years in the cybersecurity world, I've spent my career demystifying complex security topics, whether navigating 3rd party risk at massive scales or guiding engineers who've forgotten the finer points of infosec fundamentals.

When I'm not sipping Grand Mayan Extra Añejo or conjuring defenses with honeypots, magic spells, and the legendary Sasha the Dancing Flamingo (the official mascot of BSidesChicago.org), you'll find me creating playful yet practical solutions to modern security challenges. My network of honeypots scattered across the globe keeps me informed on emerging threats, though my neighbors' networked refrigerators & dishwashers provide equally fascinating research opportunities.

Honeypots and those same "smart devices" rank among my favorite things—though my neighbors might have a different opinion. And yes, if it involves curiosity, creativity, and a touch of mischief, I'm all in.



10:30 Talk Synopsis & Bio

Victor Onyenagubom

Victor Onyenagubom is a Lecturer in Cybersecurity at Teesside University and a global speaker at high-profile tech conferences, Victor shares insights on AI-driven and cloud-powered cybersecurity solutions, as well as other emerging technologies. His expertise in cloud engineering, cybersecurity, research, and community service underscores his dedication to helping others navigate and secure the digital world, positioning him as a respected voice in both academia and the tech community. As a Lead IT Trainer with CodeYourFuture, he empowers refugees and asylum seekers by teaching essential digital and cybersecurity skills. In addition, he serves as an industry reviewer for the Centre for Finance, Technology, and Entrepreneurship (CFTE) in London, providing expert feedback on cutting-edge programs in cybersecurity. Victor is also a cybersecurity consultant with CybAid, where he volunteers to help charities strengthen their cybersecurity defenses, showcasing his dedication to making a difference in both the tech industry and underrepresented communities.

The talk "Virtual Assistants, Real Threats: The Cyber Risks of Corporate AI Chatbots" explores the growing reliance on AI-powered virtual assistants in corporate environments and the associated cybersecurity risks.

As businesses increasingly adopt AI chatbots to streamline operations, enhance customer service, and improve efficiency, these systems become attractive targets for cybercriminals. I explore how AI chatbots, while beneficial, can introduce vulnerabilities such as data breaches, phishing attacks, and unauthorized access to sensitive information.

I highlight the technical and human factors that make AI chatbots susceptible to exploitation, including weak encryption, poor authentication protocols, and the potential for malicious actors to manipulate AI responses. I examine real-world examples of chatbot-related security incidents to illustrate the potential consequences of inadequate safeguards. I also address the ethical implications of AI chatbots, such as privacy concerns and the risk of biased or harmful outputs.

To mitigate these risks, I emphasize the importance of robust cybersecurity measures, including regular vulnerability assessments, employee training, and the implementation of advanced threat detection systems. I advocate for a proactive approach to AI security, urging organizations to balance innovation with risk management. Ultimately, my talk serves as a call to action for businesses to recognize the dual nature of AI chatbots—as both powerful tools and potential liabilities—and to prioritize cybersecurity in their AI strategies.

12:05 Talk Synopsis & Bio

Ric Derbyshire

Ric is a Principal Security Researcher at Orange Cyberdefense, an Honorary Researcher at Imperial College London, and a Fellow at the Research Institute in Trustworthy Inter-connected Cyber-physical Systems. He has a PhD in computer science from Lancaster University. His research involves a pragmatic and practically applicable approach to both offensive and defensive elements of cyber security, with a focus on operational technology, critical national infrastructure, novel attack techniques, and quantitative risk assessment.

Dead Man's PLC: Ransoming the Physical World via Operational Technology

Cybercrime is currently the most pervasive threat to organisations who use operational technology (OT), but it isn't the most significant threat to OT itself. That's because cybercrime models like ransomware and double extortion are aimed at IT and simply don't translate well to OT. However, as cybercriminals diversify and specifically target OT, the development of a viable modus operandi for extortion would be a watershed. In this talk we will introduce Dead Man's Programmable Logic Controller (PLC), an entirely novel technique for holding OT environments to ransom.

Current ransomware attacks depend on data encryption, a tactic ill-suited to OT devices such as PLCs due to its cost, ineffectiveness, and limited scalability. For cybercriminals to successfully target OT assets, they would need exploits for vulnerabilities in each unique device—a considerable challenge given the technological diversity within a single plant, not to mention across organisations or sectors. Even if such an approach were technically feasible, standard engineering response and recovery practices typically involve replacing compromised devices, diminishing the impact of the threat.

Rather than rely on exploits and encryption, Dead Man's PLC utilises legitimate functionality of the victim's OT against them. Moreover, it circumvents traditional engineering response and recovery practices by considering the entire OT environment as the entity under ransom, meaning that affected assets cannot be managed or replaced without triggering the attack's consequences. Ultimately, Dead Man's PLC is a robust, universal method of extortion, which fundamentally redraws the OT threat landscape.

12:40 Talk Synopsis & Bio

Helen Oluyemi

This talk will explore how new advancements in artificial intelligence, especially in machine learning and computer vision, are making it easier to bypass reCAPTCHA and other CAPTCHA systems.

We will explore the growing AI techniques that allow for this bypassing, show examples of how it works, and suggest better ways to authenticate users that go beyond traditional CAPTCHA methods.

Will reCAPTCHA be enough: Securing Websites in an AI-Driven World

Helen is an accomplished cybersecurity professional with over eight years of experience in the field. She specializes in Vulnerability and Threat Management, Cloud Security, Incident Response, Risk Assessment and Impact Analysis, and the implementation of security standards such as ISO 27001 and PCI-DSS.

With a first-class degree in Computer Engineering and multiple industry-recognized certifications including CISSP, CCSP, CISM, CRISC, ISO 27001 Lead Implementer/Lead Auditor, and CEH. Helen brings both deep technical knowledge and strategic insight to her work. Beyond her technical skills, she is a dedicated mentor, committed to inspiring and guiding the next generation of cybersecurity professionals.

Helen excels at helping organizations understand and mitigate risk, safeguarding their information assets and ensuring robust protection against cyber threats. Her strong communication, problem-solving, and collaboration skills enable her to work effectively with cross-functional teams to create a culture of security and resilience.

14:30 Talk Synopsis & Bio

Wayne May

So you want to be a baiter?

If you've ever seen a video of scambaiting and wanted to give it a go yourself, then this talk is for you.

We're going to discuss how to get scammer emails, how to write to them and how to bait both ethically and safely, and we'll even show you how to call up scammers on the phone to mess with their minds.

The talk features a number of “trophies” obtained from scammers over the years, and even has a talking hamster called Houdini talking to "The Pope" over the phone.

Wayne has been a scambaiter/antiscam advocate for almost 20 years, running www.scamsurvivors for the past 13 alongside a group of likeminded individuals.

He has appeared in the media around the world discussing scams, being cited as an “expert”, has published several books on the subject and has given talks at previous BSides events, to the dating site industry and to law enforcement.

15:05 Talk Synopsis & Bio

Pete Neve

CASE0001: The Inside Man

This the real story of an international incident response to a serious and prolific insider threat. We'll walk through the challenges of uncovering evidence whilst dealing with internal interference, and look at investigative techniques and evidence that is often overlooked.

Highlighting the forensic analysis and intelligence-gathering techniques used, we'll share practical strategies for identifying and addressing insider risks. Expect real insights, useful takeaways, and lessons learned from tackling insider threats firsthand.

Pete Neve is the Director of Information Security at Synamedia. He has decades of experience in offensive security, physical pentesting and protecting critical national infrastructure both in the UK and around the world. He has led hundreds of serious investigations in both the public and private sector, and runs training courses on using investigative interview techniques for DFIR.

Simon Chapman

15:40 Talk Synopsis & Bio

Counterintuitive Outcomes in OffSec Consulting

Ever thought the toughest part of pentesting was picking complex application logic apart? Well, guess again. Sometimes the real challenge is fending off perfectly "reasonable" client requests without ending up in an ethical quagmire.
I've had clients ask me to fudge vulnerability severities to support security budget requests, or to remove a reported finding because they've supposedly already fixed it in record time. Or worse, instructions to cease testing an app where serious vulnerabilities were about to be disclosed.

In this session, I'll also share why defending your work is a rite of passage every pentester must experience first-hand. No amount of theory can truly prepare you for a meeting where someone pokes holes in your findings - or tries to refashion your words to suit their agenda. It's a crash course in people skills that you simply cannot learn from a textbook.
We'll also tackle the top three misconceptions about life in OffSec (spoiler alert: not everybody loves you). Along the way, you'll pick up strategies to say "no" without burning bridges, draft bulletproof caveats, and sniff out when a client might be gearing up to throw you under the bus.

Sound intriguing? Join me to hear the uncensored truths of OffSec consulting – and it might just save your reputation (and your sanity).
Talk content suitable for all attendees. Some swearing likely.

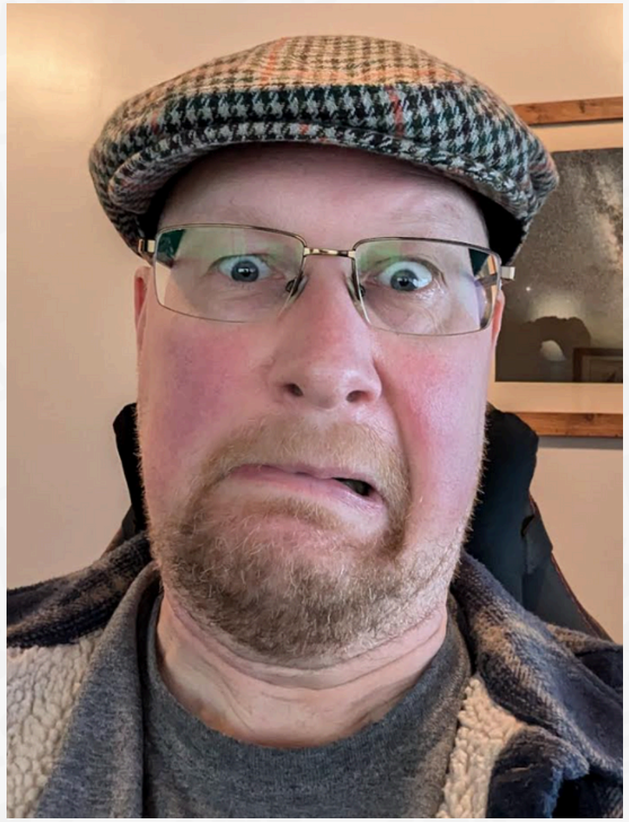
I've spent over 25 years in offensive security, building and leading teams across banking, retail, tech, and government. My hands-on roles have included everything from coding and penetration testing to network engineering and technical architecture, as well as advising boards on strategic decisions. This blend of experiences has shown me one simple truth: bridging the gap between business objectives and deep technical detail is absolutely key.

While I'm a firm believer in solid technical capability, I've found that strong communication skills really set top consultants apart. It's why I founded Conversec, a small consultancy focused on helping pentesters sharpen how they share complex ideas, whether they're talking to senior leadership or a wider audience. Over the years, I've seen firsthand how better communication fosters trust, smooths out projects, and leads to far better outcomes.

Even with all that time in the field, I'm still learning every day – cybersecurity moves too fast for anyone to stand still. It's not just about finding the latest exploit; it's about making sure everyone truly understands why it matters.

16:30 Talk Synopsis & Bio

Siri, Are You Spying on Me?



[David Lodge]

"Something that is often said is that phones are sneakily listening to people and serving up adverts. Can this happen? Does it actually happen? Are there other explanations?

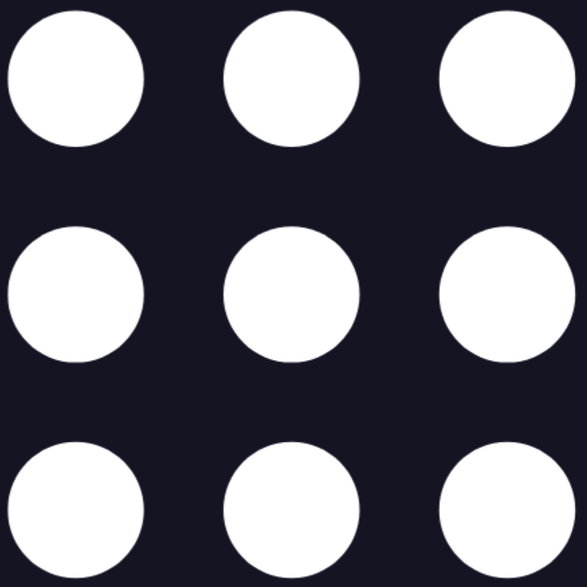
This is a meandering talk about whether this and other devices actually listen to you. Including Furbies, a left-wing German militant organisation and TV detector vans.

It will also include the results of subjecting some gullible people ^W^W friends (and maybe even the audience) to some basic experiments."

Dave is an old school pen tester, who sort of fell into it because it was interesting.

He talks a lot about things he doesn't know much about. He's also terrible at writing bios about himself.

Currently he's a pen tester and head of R&D at Pen Test Partners.



blackfoot
cybersecurity

BSIDES LANCASHIRE

Security Lancaster | Lancaster University

SentinelOne

cytix

Lightning Talk Synopsis & Bios

Citation Cyber

th4ts3cur1ty.company ›

AKIMBOCORE
UNRIVALLED PENETRATION TEST NG

CAPSLOCK

blackfoot cybersecurity

Sandinista Consulting
CYBER SECURITY: WE KNOW THE WAY

FIRE DUCK

DAINTTA
Finding intelligence in data

10:30 Talk Synopsis & Bio

Anuska Kundu

Hailing from India, Anuska works as a software engineer with the Scottish government. She's passionate about cryptography, formal mathematics and the impact of geopolitics on cybercrimes. Strengthened with a masters degree from the University of Manchester, she stays motivated to design and develop resilient and secure solutions and spread awareness on cyber safety. She's a fun, social techie, keen on networking and would love to walk away with meaningful connections today.

Weaponisation of Misinformation in Democratic Nations

My talk will explore how digital technology reshapes the political landscape and influences public opinion by weaponising misinformation. I'll briefly address the structural and social aspects that make misinformation a powerful tool, focus on case studies of its use during elections, riots, and foreign relations, examine the motivations and strategies behind these campaigns, and discuss how they were countered. Reflections from these incidents will guide recommendations for tackling such campaigns.

Since social media is a primary information source, weaponised misinformation poses a serious challenge to democracy. Misinformation,false or inaccurate information shared unintentionally can escalate into disinformation when deliberately crafted to deceive. This distinction is critical: while misinformation stems from misunderstanding, disinformation is intentional manipulation. Both spread rapidly, driven by algorithms that prioritise engagement over accuracy.

Social media encourages emotive, controversial content, making sensational posts more shareable. Skilfully designed misinformation targeting socio-political groups spreads easily without verification. Traditional media faces declining revenues and tighter budgets, often leading to less rigorous fact-checking. These factors create ideal conditions for disinformation agents-rival states, social groups, or profit-driven individuals-to inject misleading narratives to influence perceptions and votes.

Structural and social factors worsen the issue. Online echo chambers deepen confirmation bias by exposing users only to information that aligns with their beliefs. This makes false information more credible. Marginalised communities, with limited access to diverse news sources, are particularly vulnerable. Poverty, low digital literacy, and restrictive internet policies hinder source verification. Older adults, individuals in conflict-ridden or censored regions, and those with limited exposure to unbiased reporting are also at high risk. Campaigns often exploit language barriers, cultural tensions, and religious divisions, spreading fear during elections or stoking division about immigrants and minorities.

Disinformation can incite violence, erode trust, and polarise societies. During COVID-19, conspiracy theories disrupted vaccination campaigns, undermining public health. Disinformation has sabotaged diplomatic relations, enabled foreign interference, and fragmented civic discourse. Campaigns during the 2016 U.S. presidential election and Brexit flooded social media with inflammatory, misleading narratives. Countermeasures like fact-checking websites and tighter regulations were introduced but lacked speed or scale to match viral falsehoods.

Collaboration between tech companies, governments, and journalists is essential to curtail disinformation. Policies informed by psychology and sociology can promote accuracy and community values. Investments in transparency and digital-literacy are crucial.

10:50 Talk Synopsis & Bio

Nathalie Takpah

Fortifying Modern Supply Chains: Strategic Cybersecurity Imperatives for the Digital Era

Fortifying Modern Supply Chains: Strategic Cybersecurity Imperatives for the Digital Era examines the evolving cybersecurity challenges in procurement, logistics, and supply chain management. Drawing on over a decade of experience across construction, telecom, and healthcare, I aim to provide a data-driven approach to securing global supply chains against emerging cyber threats.

As supply chains become increasingly digitized, organizations face rising risks, from data breaches to operational disruptions. This section explores securing ERP systems, mitigating supplier vulnerabilities, and ensuring compliance with industry standards such as ISO 28000 for supply chain security and ISO 31000 for risk management. Through real world case studies, it highlights how cybersecurity frameworks enhance resilience, protect procurement platforms, and safeguard critical infrastructure.

By bridging supply chain management with advanced cybersecurity strategies, this presentation offers practical insights for industry leaders and policymakers. It presents a comprehensive roadmap to fortify supply chains against cyber threats, ensuring operational continuity in an interconnected, data-driven world.

Experienced in cybersecurity, data analysis, and machine learning, I focus on securing supply chain operations across industries.

I have applied predictive analytics, robotics, and AI to optimize procurement, mitigate risks, and enhance efficiency. With expertise in contract negotiation, supplier management, and logistics, I integrate cybersecurity protocols to safeguard ERP systems and procurement platforms from threats.

11:10 Talk Synopsis & Bio

Rob McLellan

Gateway to IoT

IoT Gateway devices are used to add connectivity to devices that lack network support or for remote connections to OT hardware. They are also used to access Out Of Band management interfaces for hardware not generally connected to end user networks. As such they present an interesting target for attackers.

Many of these devices are low powered and do not respond well to standard network scanning tools. This talk will walk through the process of identifying common IoT Gateways on the network and reverse engineering their traffic flows to uncover security weaknesses. Finally we will spoof a device on the network in order send malicious traffic and compromise an engineer workstation used to manage gateway devices.

Rob has worked in the security industry for over ten years. Originally a sysadmin before making the jump to the dark side of penetration testing he is now a Senior Penetration Tester at Trustmarque and has delivered security assessments and advice to client across sectors such as retail, finance and government.

A chronically short attention span and perpetual desire to chase new shiny things has made Rob a jack of all trades and master of none. He lives by the belief that any desk not littered with the elements of at least three unfinished projects is a wasted space.

12:00 Talk Synopsis & Bio

[Andrew Lucas]

The Magical Science of Cyber

The science is clear. If we keeping setting our bar at “Awareness” we are destined to remain short on our aspirations to strengthen security. This fun, light-hearted 15 minute demonstration explores how we can think “differently” when seeking to communicate and engage people about cyber security.

In the summer of 1973, over eight days, the CIA conducted a series of scientific experiments, in carefully-controlled conditions, to test the ability of an individual use paranormal perception to replicate drawings unseen to them. The CIA’s intention was to explore possible new avenues with which to exfiltrate key intelligence from the Soviet Union.

As a result of the success of the experiment, they concluded that the individual had demonstrated paranormal perceptual ability in a convincing and unambiguous manner. The individual being tested was Uri Geller. Over 50 years on from these experiments, and using declassified original CIA documents available on their website, we seek to recreate that original drawing replication experiment at BSides Lancashire.
Of course, the moral of our story is not that our Information Security systems need urgently updating to accommodate protection from psychic powers. But the presentation does demonstrate that even when tight controls are applied, individuals can be misled through deception and deceit.

Andrew’s path into cyber security is far from traditional. A burning curiosity in multiple diverse subjects led to a combined honours degree and first Masters that was an exercise in procrastination about which path he wanted to follow when he grew up. After 25 years in media and the arts, Andrew subsequently worked in environmental science, politics and the Civil Service. Throughout his career, he led digital transformation, security and culture change projects. Following a second Masters in Cyber Security at Lancaster University,
Andrew worked as a consultant and was subsequently appointed Director of CentriVault. He is also founder and Director of NaturallySecure.Net, a startup which is driving action research into strengthening cyber security behaviours and cultures. Andrew is a qualified teacher and has lectured at colleges and universities. He has always been passionate about seeking creative ways to engage audiences in new learning and experiences. Magic has been a love since childhood. As a teenager, he performed regularly and had a trick published in an international magic magazine. As real life took over, the magic was retained as a hobby and occasionally brought out for, family, friends and colleagues. On working in cyber security, Andrew realised the possibilities of using magic to demonstrate cyber security concepts. It may have also have provided an excuse to spend rather too much money going to magic conventions and buying tricks. He is still intensely curious.

12:20 Talk Synopsis & Bio

Besties and Bastards: So your developers hate you, what next?

Conflict in cyber security is something we are all familiar with, red team vs blue team, attackers vs defenders the age old story of good guys vs bad guys, but what happens when you're the baddie? When heroic security teams swoop down to save the poor helpless developers we should be thanked. In reality though in developer circles security teams are, well, disliked, and can you blame them? Changing the way they work, adding extra jira tickets to already overloaded sprints, constantly interrupting progress with results of automated scans, forcing extra steps in build pipelines and generally getting in the way of them producing code. Even when they know it's the right thing to do, the added pressure of managing security on top of high workloads, builds resentment. This talk is for those whose development team groans seeing a slack notification from you and will discuss approaches to help repair these relationships and move away from security-as-a-chore to security-as-a-choice. This is not an easy process, reducing expectations, handing control back to development teams, and changing security culture, however it will present actionable steps and milestones for a developer recovery plan and how to not burn out your security team in the process.

Katie Paxton-Fear

Dr Katie Paxton-Fear is an API security expert and Principal API security researcher at Traceable, in her words: she used to make APIs and now she breaks them. A former API developer turned API hacker. She has found vulnerabilities in organizations ranging from the Department of Defense to Verizon, with simple API vulnerabilities. Dr Katie has been a featured expert in the Wall Street Journal, BBC News, ZDNet,

The Daily Swig and more. As she shares some of the easy way hackers can exploit APIs and how they get away without a security alert! Dr Katie regularly delivers API security training, security research, to some of the largest brands worldwide. She combines easy-to-understand explanations with key technical details that turn API security into something everyone can get.

12:45 Talk Synopsis & Bio

[Phat Hobbit. Cyber Security Ombudsman.]

Et Tu CISO?

We all know by now how to do cybersecurity but is there a way to do cyber security at an organisational level without lying on the ground from trying? From heart attacks to indictments Phat Hobbit explores - with humour and jaded cynicism - why and how some CISOs fail to make situations better and often times make situations worse. From personal experience, infosec media reporting and some infamous CISOs - where the C stands for celebrity - Phat Hobbit takes a look at the protections cyber security leaders don't have, may have and likely need.

“You’ve never heard of the Phat Hobbit? It’s the ship that made the Kessel run in less than 11 parsecs beating the Millenium Falcon’s record! It’s the fastest hunk of junk in cyber security.”

14:30 Talk Synopsis & Bio

Gerald Benischke

Love Letter to Legacy

"This tech stack is outdated, it's a legacy system and oh my goodness just look at metaphorical gaffer tape that's being used in code" - sound familiar? How about "We can't recruit for this position, because nobody wants this legacy tech anymore"?

Why? So-called legacy code is the backbone of so much software engineering. How many banks, insurances or government departments would just stop working if the mainframes were switched off?

Far from something to outsource to the lowest bidder, looking after legacy is a job for experienced engineers. Far from being the short straw, brown field development is just as exciting - if not more - than working in a feature factory knocking out microservices with the latest shiny patterns.

The talk will introduce the takeaways:
*** Legacy code is then one that makes the money**
*** How can we make maintenance "sexy" again?**
*** How does the You Build It, You Run It approach fit in with software maintenance**
*** Why is it so important that the engineers looking after your legacy software are not a revolving door of burnt out engineers**
*** The importance of autonomy and sticking with the agile mantra of "people over processes and tools"**
*** What are the AppSec implications**

14:55 Talk Synopsis & Bio

[Victor Oriakhi]

Securing the Future: Hardware Engineering for Resilient IoT Systems

Securing the Future: Hardware Engineering for Resilient IoT Systems
As the Internet of Things (IoT) expands across industries, hardware security is becoming a critical concern. While software-based protections are essential, insecure hardware can expose entire networks to cyber and physical threats. How can we design IoT devices that are resilient, secure, and scalable?

In this talk, Victor Oriakhi will explore the role of hardware engineering in IoT security, covering key principles such as:

- **Secure microcontroller architectures to prevent unauthorized access.**
- **Hardware-based encryption to safeguard sensitive data.**
- **Trusted Platform Modules (TPMs) and Physically Unclonable Functions (PUFs) for authentication and integrity.**

Victor will discuss real-world applications of secure IoT hardware across industries like healthcare, energy, and smart infrastructure. He will also highlight the importance of preparing the next generation of engineers to tackle emerging security challenges. This session offers practical strategies for embedding security-first principles into IoT hardware design. Whether you're an engineer, researcher, or cybersecurity professional, you'll gain valuable insights into building resilient IoT systems that can withstand the threats of tomorrow.

Victor Oriakhi, MIET, is a Design Engineer specializing in hardware systems, IoT, and embedded electronics. His expertise lies in developing secure and resilient hardware solutions, particularly for connected devices and smart technologies. With a strong background in Robotics and Automation, Victor has contributed to research and innovation in hardware security, focusing on integrating cybersecurity into IoT architectures.

Beyond his technical work, Victor is a Project Manager at BeScience STEM, a nonprofit organization dedicated to STEM education and innovation. He has led various STEM outreach initiatives and has been instrumental in mentoring the next generation of engineers. Additionally, he is a mentor at the University of East London, where he supports students in building technical expertise, industry knowledge, and career development.

Victor is also an active speaker in the tech industry and has presented at multiple technology events and conferences on topics ranging from IoT security and hardware engineering to AI and emerging digital technologies. As a peer reviewer for esteemed journals, he continues to contribute to the advancement of knowledge in AI, cybersecurity, and electronics engineering.

15:15 Talk Synopsis & Bio

Greta Caikinaite

"Know Thyself: Delving into Personal Risk Appetite Through OSINT" is a beginner-friendly exploration of open-source intelligence (OSINT) and its relevance to personal security and privacy. This 15-minute talk will guide individuals through assessing their digital footprint, understanding their personal risk appetite, and taking actionable steps to regain control over their online exposure.

This talk is ideal for anyone looking to better understand their digital privacy, offering tools and knowledge to make proactive changes to protect their online presence. Whether you're new to cybersecurity or simply curious about your own digital footprint, this session will empower you to take control of your online exposure.

Greta is a Cyber Security Consultant at Pentest People, specialising in penetration testing for network infrastructures and web applications. With a strong interest in social engineering and physical intrusion testing, she is expanding her skill set to better understand various aspects of cyber security.

Growing up during the rise of the internet and social media, she, like many, shared personal information online without recognising the risks. At the time, posting personal details was the norm, and the dangers of digital footprints were not widely recognised. Over time, as she became more aware of these risks, her interest in cyber security grew.

She pursued an undergraduate degree in Mathematics and Philosophy, driven by her love for problem-solving and interest in exploring the meanings of things and societal structures. After completing her degree, she realised cyber security combined her analytical thinking with a passion for complex systems, prompting her to pursue a Master's in Cyber Security Management.

At work, Greta focuses on network and web application testing to identify vulnerabilities that could be exploited by attackers. She is eager to deepen her knowledge in social engineering and OSINT, areas essential to understanding the full scope of security challenges. As she grows in the field, she is exploring what a truly comprehensive security approach looks like and how to bridge gaps across different security disciplines. Her mission is not only to defend systems but to raise awareness about the risks of digital footprints and the importance of controlling personal data. With many organisations still underestimating privacy risks, Greta is dedicated to empowering individuals to safeguard their digital presence and navigate the evolving threat landscape.

Joe Burton

15:35 Talk Synopsis & Bio

Data Poisoning and the Security of Artificial Intelligence (AI)

This research paper seeks to contribute to the literature on sociotechnical cybersecurity by considering some fundamental but unanswered questions about the practice of 'data poisoning' in the context of AI. The paper builds three core arguments. The first is that data poisoning has mainly been approached from a technical point of view in the existing scholarship – that is to say that some work has emerged on how data present in AI systems can be poisoned, the methods that are available, and the technical effects of the targeting of AI systems, but that wider questions as to why and with what effect malicious actors might seek to poison AI related data have not been addressed head on.

The second contribution of this paper is to place data poisoning in a geopolitical security context; how data poisoning might be used by state actors as part of the strategic interactions with other countries and to link data poisoning to broader efforts to subvert states, political systems and their techno-industrial bases. The third argument of the paper develops an argument based on adversarial transferability of data poisoning attacks. The literature on data poisoning is beginning to reveal how data poisoning techniques can be transferred from one different type of AI model/system to another – from a deep learning system to a Generative AI system, for example – but the transferability between threat actors has been underexamined in the literature. The paper seeks to illuminate conceptually how attempts to poison data might spread between state actors and between the state and non-state actors.

Dr Joe Burton is Professor of International Security in the Department of Politics, Philosophy and Religion (PPR) at Lancaster University. He joined the university in July 2023 as part of the Security and Protection Science initiative. Prior to that he held permanent positions at the University of Nottingham and the University of St Andrews and was a Marie Curie (MSCA-IF) fellow at Université libre de Bruxelles (ULB), working on the two-year European Commission-funded project Strategic Cultures of Cyber Warfare (CYBERCULT). Joe is the author of NATO's Durability in a Post-Cold War World (SUNY Press, 2018), editor of Emerging Technologies and International Security: Machines the State and War (Routledge, 2020), and his work on Artificial Intelligence and Cyber Security has been published in a range of leading scientific journals, including International Affairs, Journal of Global Security Studies, Technology in Society, Asian Security, Defence Studies, the Cyber Defence Review, the RUSI Journal and Political Science.

Dr Burton has served as a ministerial advisor in New Zealand and the UK. He is the coordinator of the CYDIPLO Jean Monnet Network on Cyber Diplomacy and a recipient of the US Department of State (DoS) SUSI Fellowship (New York, Washington D.C.), the Taiwan Fellowship (Ministry of Foreign Affairs, Taipei), and has been a visiting researcher and lecturer at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Joe has implemented projects and received funding from the US Department of State, the Taiwan Ministry of Foreign Affairs (MOFA), the NATO Science for Peace and Security Programme (NATO SPS), NATO CCDCOE, the European Commission (Marie Curie program and Jean Monnet Network lead), the National Cyber Security Centre (NCSC), the Alan Turing Institute and the New Zealand Department for Prime Minister and Cabinet (DPMC).

BSIDES LANCASHIRE

Security Lancaster | Lancaster University

SentinelOne

cytix

Village Info

Citation Cyber

th4ts3cur1ty.company ›

AKIMBOCORE
UNRIVALLED PENETRATION TEST NG

CAPSLOCK

blackfoot cybersecurity

Sandinista Consulting
CYBER SECURITY: WE KNOW THE WAY

DAINTTA
Finding intelligence in data

Management Round Table

14:30 - 15:30 - Workshop Room

Led by th4ts3cur1ty.company, our roundtable event will explore the qualities of effective leadership, focusing on what drives success in cyber leadership roles and board-level negotiations. Additionally, we will explore insights based on our industry observations, and examine scenarios where leadership efforts falter, identifying common pitfalls that can undermine authority and damage internal credibility.

Chatham House Rules will apply to foster open and honest dialogue, and a highly-interactive, collaborative environment. The roundtable is designed for individuals in leadership positions, and is limited to just 10 spots!

SOC Village - Decision Theatre

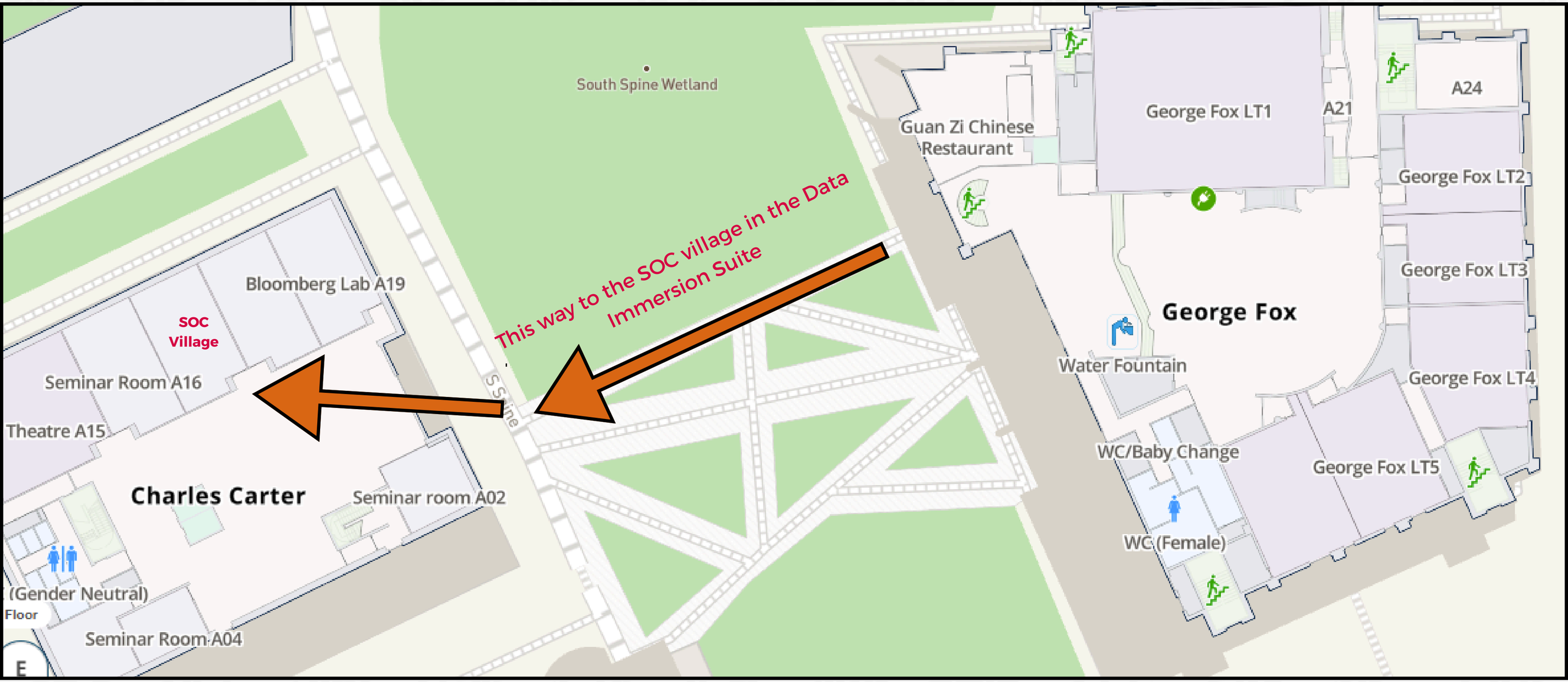
th4ts3cur1ty.company ›

Join us at the SOC Village for an interactive dive into the world of security operations! We'll guide participants through a hands-on experience, featuring:

- A simple lab environment preloaded with real-world data.
- Curated alerts to demonstrate triage and hunting techniques.
- In-depth discussions and workshops on crafting and optimizing detection rules using Sigma and Suricata.

Whether you're new to SOC workflows or looking to sharpen your skills, our village is the perfect place to explore detection engineering, learn practical techniques, and enhance your security expertise in a supportive setting.

How to get to the SOC Village



Merch Available to Purchase
Vendor Hall

B-SIDES EVENT - STUDENT T-SHIRT V1

B-SIDES EVENT - STUDENT PULL OVER HOODIE

Come and get hands on with the Infosec Battle Bots, where creativity combat and engineering come together to create an unforgettable experience.

In the Workshop Room

Merch Available to Purchase Villages Room

After Party at Barker House Farm

Evening Buffet Menu Options

Carvery (served from the hotplate)

Portabella mushroom red pepper and melting mozzarella (V)(GF)

Carrot wellington with spiced marmalade (V)(VG)(DF)

Honey roast ham (DF) Roast turkey with cranberry sauce with chipolata sausages (DF)(GF)

Served with

Gravy, seasonal vegetables, potatoes and a selection of homemade deli salads
Baked rolls (Gluten free available)

Followed by

A dessert table to include a choice of local Dewlay cheese and biscuits

Tea and Coffee

CODE OF CONDUCT

RESPECT
IN SECURITY

BSides Lancashire supports inclusion, collaboration, and diversity, especially the diversity of thought and opinion.

As an organization that cares about everyone that attends this event, we will not tolerate any form of harassment, and we expect a level of respect for all attendees, sponsors or speakers at this event.

We support the Respect in Security pledge.


LANCASHIRE
SIDES