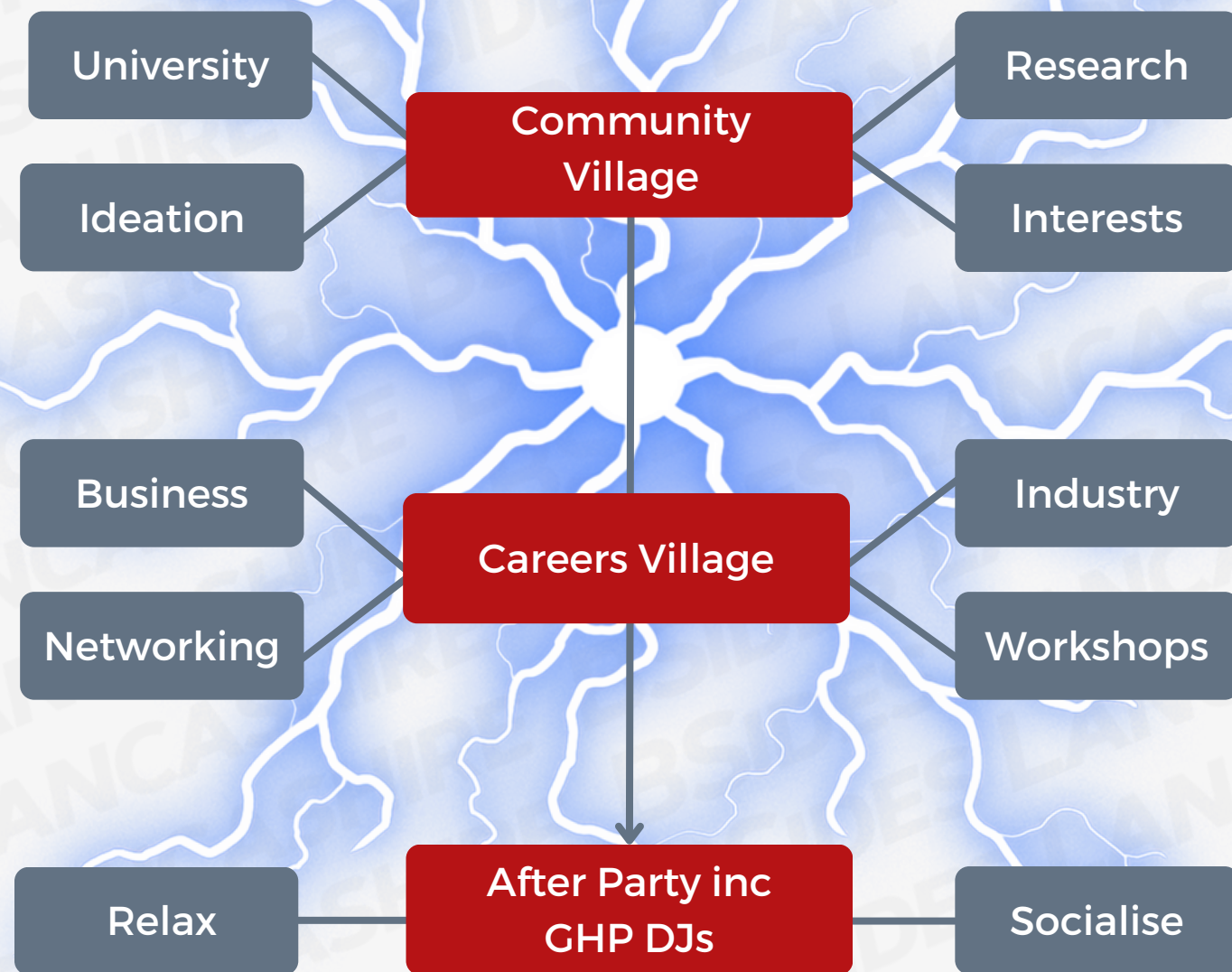


BO LANCASTHIRE
SIDES



About BSides 2024

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.





Mike Somers
Co-Founder



Jen McCulloch
Co-Founder



Dr. Dan Prince
Co-Founder



Gabbi Burley
Lancaster Support



Josh Talleyman
Lancaster Support



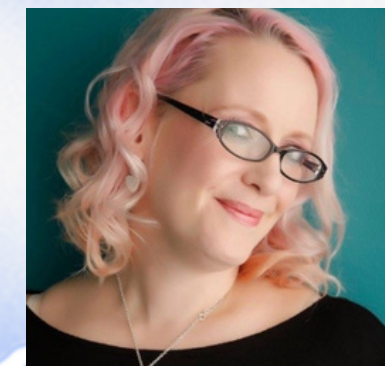
Holly-Grace Williams
Co-Founder



Sean Atkinson
Co-Founder



Rosie Anderson
Co-Founder



Sam Humphries
Strategic Advisor

Our Leadership Team

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 continue with a BSides back to the North West.

52,000

Number of
businesses in
Lancashire

500

UK's largest
Aerospace
cluster

£5bn

National
Cyber Force

**North West
Cyber
Corridor**





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

 **exabeam** **BARCLAYS**  **Citation Cyber**

 **PlexTrac**[®]

 **netskope**

Lancaster University 

 **BOSS SIDES**
LANCASHIRE

CAPSLOCK[™]

 **CYBER HOUSE PARTY**

th4ts3cur1ty.com >

 **AKIMBOCORE**
UNRIVALLED PENETRATION TESTING

 **The SecOps Group**

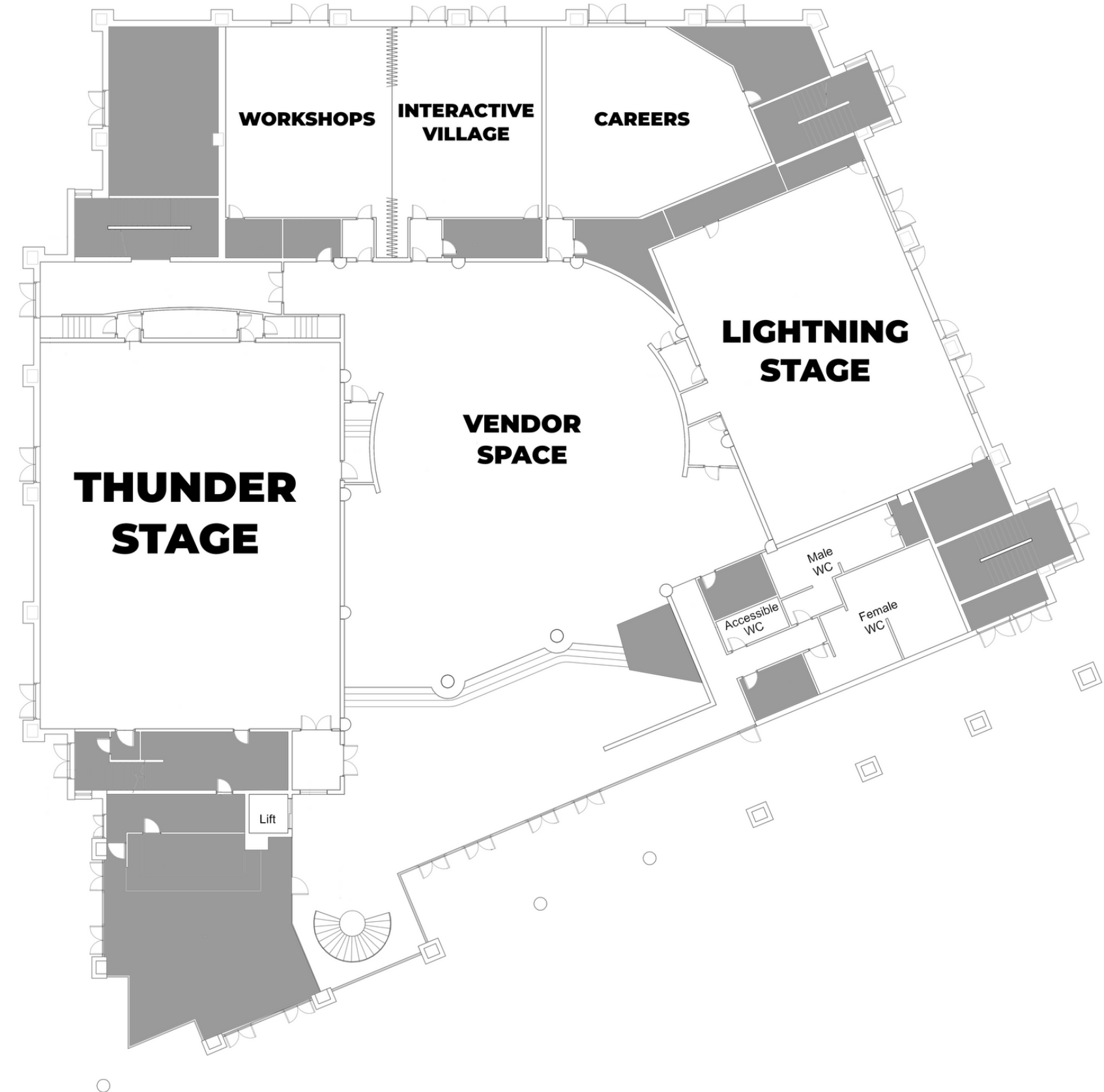
 **Sandinista Consulting**
CYBER SECURITY:
WE KNOW THE WAY

Our Venue

On March 27th, 2024, the second BSides Lancashire will take place at the George Fox Lecture Theatre, Lancaster University. The venue has a capacity of up to 450 people.



Scan the QR Code to explore the Lancaster University campus. The venue is automatically highlighted for you!



Our Venue

Prayer Room Directions

رمضان كريم

RAMADAN KAREEM



MazeMap

Cyber Security, Simplified

Who are we?




Founded by a team of specialists in cyber security, consultancy, and information security, we're a trusted cyber security provider with a passion for quality service.

Our mission is to provide dynamic security services, covering your testing, training, and certification needs, that extends beyond technology to encompass people, culture, processes, and even the physical environment; to make businesses resilient in our ever-evolving digital world.



Citation Cyber HQ

What we do

-  **Test Your Systems**
Ensure your devices and systems are operating as they should be with testing solutions designed to strengthen your infrastructure.
-  **Train Your Workforce**
Build company resilience and empower your human firewall with training solutions designed with your team in mind.
-  **Certify Your Business**
Remain compliant and demonstrate you take the protection of your devices and data seriously with cyber certifications.

Join us in making cyber space a safer place

Don't worry, these QR codes are secure!



Secure your business!



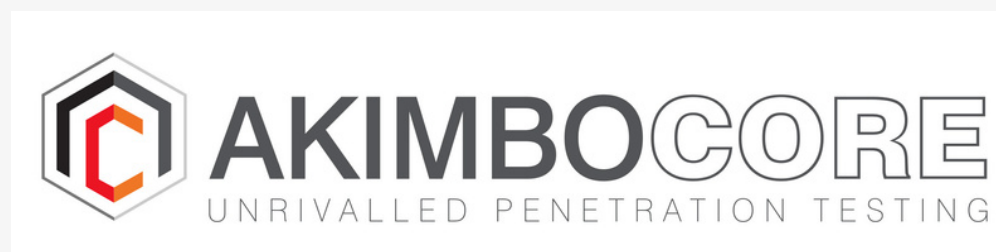
Partner with us!



Join our team!



Thunder Stage Talks





Opening Keynote



Operating at the forefront of the cybersecurity industry, Sarah Armstrong-Smith is the Chief Security Advisor at Microsoft. She has led a long and impactful career, guiding businesses through digital attacks and teaching organisations how to protect their people and data.

Sarah's previous positions include Group Head Business Resilience & Crisis Management at The London Stock Exchange Group and Head Continuity & Resilience, Enterprise & Cyber Security at Fujitsu. Such high-profile roles earned Sarah a place in the Most Influential Women in UK Tech and Most Influential Women in Cybersecurity.

In 2022, Sarah released her first book 'Effective Crisis Management' which quickly became the publisher's best-selling book. With a new way to share her expertise with a large audience, her leading insight into technology and security is respected by many throughout the industry.

Sarah's latest book 'Understand the Cyber Attacker Mindset' explores the psychology of cyber warfare and how organisations can defend themselves from attack. The human aspects of cybersecurity have never been more critical.

Follow the link here to purchase Sarah's new book: [Understand the Cyber Attacker Mindset](#)

Sarah Armstrong-Smith

Microsoft
CSA

 [Sarah Armstrong-Smith](#)

 [SarahASmith75](#)



Andy Barratt

Coalfire
Vice President

 [Andy Barratt](#)



Save the Chicken, Save the world.



The year is 2020 - the world is in the midst of a global pandemic. You know who isn't slowing down? The Fin7 Criminal organisation. This is the story of a major fried chicken chain in the US that suffered a huge card data compromise across multiple states and how the investigation became a global effort, with the event becoming public knowledge due to Brian Krebs getting a tip off.

I'm here to tell the tale, as the lead investigator on the case. The case was technically interesting, logistically challenging, had locations that were dripping with malware, owner operators who were completely unaware of what their tech was doing, or who bought it, or what it did, or where it was, or where it was from in some cases. May be thats the correlation?



Leum Dunn

DAZN Bet
Head of
Information &
Cyber Security

 [Leum Dunn](#)



AI AIEEEEEEE! (the end of the trilogy)



AI is a racist, sexist, ableist tool of the oppressor and we should all be ashamed of ourselves. A humorous look at amplified bias in the current crop of machine learning tools.

A non-technical tech talk. The last one I plan to do before everyone gets bored of me banging on about this stuff!



Paul Smith

Lancaster University
Professor in the
School of Computing
and Communications



Securing Critical Infrastructure: Navigating Technology Risks and Benefits



This talk will give an overview of recent research that has explored the benefits and challenges of the application of emerging digital technologies for critical infrastructures and, more specifically, industrial control systems. In general, our critical infrastructures are being digitized in increasingly sophisticated ways, which introduces cyber security risks; we will look at some case studies, examining challenges and opportunities for cyber security and resilience.



[Professor Paul Smith](#)



Holly-Grace Williams

AkimboCore
Managing Director

 [HollyGraceful](#)

 [Holly-Grace Williams](#)



Keynote - Money Laundering is Hard



Holly Grace has seventeen years of experience working within cybersecurity, with a focus on penetration testing and cybersecurity consultancy. Holly Grace has been a CREST Certified Application Tester since 2015 and has professional software development experience in Python and Rust, including taking software products to market.

She has strong experience in building and securing cloud environments, with a focus on AWS and Azure. She has performed a significant number of penetration testing engagements for a wide range of companies from innovative start-ups to multinational corporations, in fields ranging from e-commerce to banking.



Alsa Tibbit



Unearthing Digital Fossils From Raptor to Troodon

Advancing APT Detection with Explainable AI



This talk navigates the dynamic realm of cybersecurity, tracing the journey from the groundbreaking RAPTOR project to the ongoing Troodon initiative. RAPTOR, supported by Innovate UK, leveraged data mining and unsupervised learning to categorise Advanced Persistent Threats (APTs), laying the groundwork for understanding these intricate threats and paving the way for Troodon.

Troodon, a collaborative endeavour between Sheffield Hallam University and La Trobe University in Australia, delves into Explainable Artificial Intelligence (XAI) to enhance Intrusion Prevention Systems (IPS). It promises increased interpretability and transparency for cybersecurity effectiveness and accountability.

Sheffield Hallam
University & Manchester
University
Cyber Security & AI
Researcher

 Alsa Tibbit

 Alsa_dat



James Bore

Bores Group Ltd
Managing Director



I Was Threatened With A Defamation Lawsuit and All I Got Was This Lousy T-shirt!!



Being publicly active in any field comes with risks, especially in an industry where fake it until you break it influencers are a fact of life. Calling out bad behaviour can come with consequences and in the UK SLAPP (Strategic Lawsuit Against Public Participation) aren't uncommon.

This talk does not constitute legal advice, but does cover the process of being threatened with one of these lawsuits, responding to it, why you want insurance, and what you can, can't, and shouldn't do afterwards.





Those who can't do...



James Starnes

Altrincham Grammar
School for Girls
Teacher - Computer
Science

 [James Starnes](#)

In this engaging talk, James Starnes takes you on a journey through the unconventional paths that led him to become a Computer Science teacher at the top-ranked state secondary school in the Northwest. The narrative unfolds with unexpected twists, including experiences such as answering 999 calls and contemplating a career in nursing.

The discussion extends beyond James's personal journey to offer valuable insights into how businesses can effectively engage with the education sector, whether they are seeking to recruit the next generation of talent or considering a strategic partnership. James sheds light on the various routes individuals can take to transition into teaching, highlighting the allure of government incentive packages and the inherent satisfaction of giving back.

Diving into his own unique experiences, James shares the challenges, triumphs, and pivotal moments that have shaped his career in teaching Computer Science. The narrative is interwoven with anecdotes from the classroom, offering a glimpse into the dynamic world of education.

As the talk unfolds, James emphasizes the significance of fostering diversity in STEM, with a particular focus on encouraging women to pursue careers in InfoSec. He details his efforts in driving his school to achieve recognition as the first CyberFirst Silver School in Greater Manchester, showcasing a commitment to inclusivity and breaking down barriers for students with dyslexia and neurodivergent traits.

In conclusion, James invites the audience to reflect on the impactful ways they can contribute to education. Whether considering a career change or seeking opportunities to support schools and educators, the talk inspires individuals to recognize the fulfilling aspects of shaping the future generation.



Introduction to the Hacking Games

“All kids seem to do these days is play games”




Fergus Hay

Hacking Games
CEO & Co-Founder

 [Fergus Hay](#)

Sam Humphries

Hacking Games
Board Advisor

 [Sam Humphries](#)

All kids seem to do these days is play games



We're entering the era of natural-born coders. 61% of NYC kids have hacked by the age of 16.

Our mission is to create a generation of ethical hackers to make the world safer.

Through captivating entertainment, comprehensive education, and clear career pathways, we're nurturing a new age of defenders and researchers.

Please visit www.thehackinggames.com to find out more and join us to build a safer digital world.

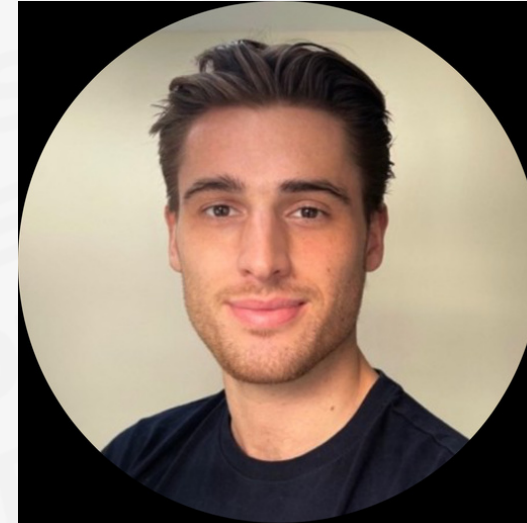
Closing Panel



Sam Humphries
Exabeam &
Hacking Games



Zain Javed
Citation Cyber



Seb Hyde
Netskope



Dr Andrea Cullen
Capslock



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.





Lightning Stage



Talks





From Alert to APT The Evolution of WildCard



Embark on a riveting journey that began with a modest alert, unveiling a labyrinth leading to the discovery of the elusive multi-platform backdoor, "SysJoker," with its eyes set at infiltrating Windows, Mac, and Linux.

Ryan Robinson

Intezer
Security Researcher

The actor behind the malware immediately made changes to respond to our public announcement, which birthed a revised iteration in the formidable fortress of Rust, named "RustDown". This eventually unfolds into announcing a new and shadowy APT group, "WildCard", emerging two years post-alert.

Join us as we talk about the intriguing saga of incident response, bespoke malware, action, reaction, intrigue, deception, ethics, and a hint of cyberwar. As we observe WildCard, WildCard observes us.



MhicRoibin



Daniel Basher

Digital Transit Limited
Product Engineer

 [Daniel Basher](#)



Operational Technology Cyber Security in Railways



Digital Transit have secured funding from Innovate UK for a 500K project involving the creation of an OTCS tool which utilises Natural Language processing (NLP), a form of AI, to ensure the cyber security of operational technology (OT) environments. The system will guide a user, who is unfamiliar with cyber security requirements, through rules and regulations to create a system that is both compliant and secure.

No real body of knowledge currently exists in this area. It is daunting for manufacturers and operators of transit systems to reach compliance with mandatory regulation, and high costs can be incurred if cyber security is not properly addressed.

DTL has developed novel NLP tools to assess systems engineering artefacts and will be applying this knowledge in the new OTCS tool.

No integrated process currently exists to guide companies through systems definition, operational context, risk assessment, and system and architectural requirements -- effectively a "cyber readiness" assessment.

The potential benefits from enhanced OT cyber security cannot be overstated and bear repeating. If it is not secure, it is not safe!

This paper will discuss our progress and how we will carry out this 3 year long research project.



Write your damn report!



Paul Johnston

Pentest Limited
Security Consultant

Reporting is not the most glamorous part of pen testing, but doing it effectively is vital for a good outcome.

Over the years I've worked with a number of reporting systems - manual, automated, bespoke and commercial.

The talk covers what works in a report - effective structure, language and information. It also covers specifics of building a bespoke report writing system with tool integration.

Finishes with some speculative ideas of ways we could make reporting even better.



Thomas Win

University of
Sunderland
Associate Head of
School (Computer
Science)



[Dr Thomas Win](#)



Adversarial AI Attacks in Cyber Security (A3CS)



Artificial intelligence-based cybersecurity solutions have been widely adopted in recent times to detect a wide variety of cyber attacks, ranging from network-based attacks to more sophisticated Advanced Persistent Threats (APTs).

To counter this, cyberattackers are targeting the AI models to negatively impact the latter's ability to detect cyber threats.

This talk will look into the various model and data poisoning attacks against AI models, as well as various countermeasures in existing cyber security research.



Carlos Gonçalves

Banco do Brasil

CTI Leader

 [Carlos Goncalves](#)



Intel-Driven Red Teaming: Bridging the Gap Between Security Teams



In this talk, we will explore how a threat intelligence-based red teaming process can integrate security teams and guide an organization's defense strategies. This approach enables the red team to prioritize security testing more effectively, focusing on the organization's critical threats. By adopting the Mitre ATT&CK framework as the foundation for a continuous purple teaming process, we will demonstrate how detected technical vulnerabilities can be aligned with the NIST SP 800-53 security controls, assessing their potential impacts.

This methodology allows for the translation of technical information to the executive level, with the potential to directly influence the security program, policy formulation, and the acquisition of new security solutions. Consequently, the organization will be able to make well-informed decisions and manage risks more effectively, promoting a proactive and resilient security posture.



Cherry Colby

Acorn Insurance
Head of Information
Security

 [Cherry Colby](#)



Doing the Basics Brilliantly

Key focus areas for security leaders.



The aim of my talk is for security leaders, particularly in small to medium businesses (SMBs) to walk away with some helpful key areas of focus to improve how they lead and develop their team, and improve their organisation's security strategy and ISMS, sometimes on a small budget with a limited team.

Focus areas are:

1. Security Strategy - write one, a simple one is better than none.
2. Industry Frameworks - choose one, structure gives a starting point, clear set of requirements, clear way to show improvement and impact you're having.
3. Say No to No culture - think about security in terms of risk and advise your business that way.
4. Build your team and beyond - focus on early development of your immediate team.

Set disciplines, behaviours and expectations. No team?

Leverage others who can help strategically, use cyber champions.



Mark Goodwin

Causaly
Senior Staff Security
Engineer



What your Browser can teach you about Secure Design



We take browsers for granted; they're ubiquitous and they've been around for ages... But have you ever stopped to think about what they `_do_`? They execute arbitrary code, from untrusted sources on the Internet. By design.

And were supposed to be OK with that?

Unsurprisingly, how they do this provides some useful lessons in how we can build secure systems.



[Mark Goodwin](#)



Wayne May

ScamSurvivors.com
Site owner




Anything online can be faked. Here's how.



A demonstration on how anything can be faked online, from simply stealing images to using AI to generate realistic voice or video.

The talk focuses on the ways scammers are using these methods, but shows how anyone can use them via cheap/free software and websites.

It features practical demonstrations including ways to create a virtual webcam, create AI text to speech using 30 seconds of sampled audio and swap the face of a person in a video among others.

 [Wayne May](#)



Building my ultimate home detection lab



Oliver Creed

Cyber Security
Engineer

Hi my talk, which isn't get finished will be about building my ultimate home lab for detection, not super original but i still feel it provide good content for new comers in getting started. I want to cover acuring and what hardware, software and design considerations such as limited space and what goals and the usefulness of having a home lab



[Oliver Creed](#)



Detect the Undetectable™

Eliminate blindspots and respond to threats faster and more accurately

Learn more > www.exabeam.com



Cloud-scale Security Log Management



Powerful Behavioral Analytics



Automated Investigation Experience

The Next Evolution of SASE and Zero Trust

The Power of One

- One engine, one client, one gateway, and one network

Ultimate Visibility and Protection

- Use the precision of the Zero Trust Engine to stop data loss and threats

A Phenomenal User Experience

- Accelerate your enterprise and manage the experience from end-to-end



Netskope One

One platform.

Protect and accelerate.

Everything to everywhere.

For more information visit [Netskope.com](https://www.netskope.com)

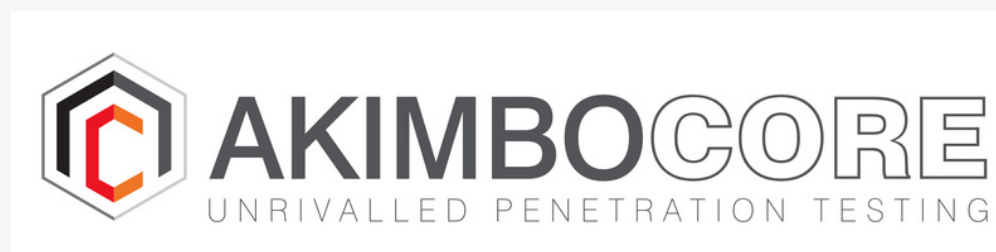
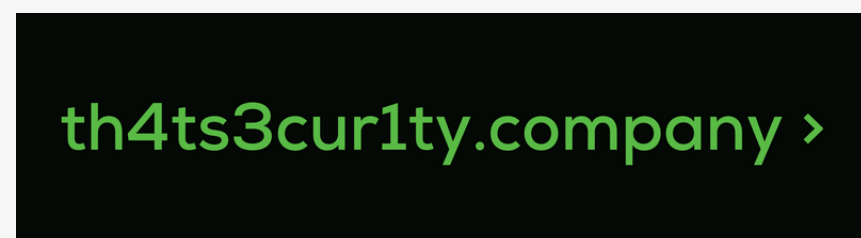




Career Stage



Talks





Tim Ogle

Founder

Toggle Switch Consulting



Removing the fear of Sales and Business Development (EEEEK!) for all technical consultants.



Are you a deeply technical person, who loves delivery and problem solving but hates anything to do with sales and BD? As you progress in your career you are likely to be asked to get involved in sales / BD work and this session will provide some helpful tools and tactics for you to help breakdown fears and build confidence in sales. Having helped transform how a number of cyber security businesses went to market, the secret tool in all cases was always the technical consultants. The complication was that most technical people don't like sales. Therefore I will be exploring what the barriers were and how you can start to overcome them. This session will break down sales so that you can figure out how this can work for you in a non-sales role.

- I will be covering the fundamentals of:
- The barriers to BD for non-sales people
- Why and how people buy
- How to build trust

How to be the authentic you so you perform at your best (even in sales situations) As a result of this session everyone will view sales as something that is actually more about problem-solving and a lot less about being "salesy". The tools and ideas will help everyone take a fresh look at BD and consider how it can help their cyber security career advance.



[Tim Ogle](#)



Rosie Anderson

Head of Strategic
Solutions

th4ts3cur1ty.com




Cyber Relevance - The Titanic Effect



Just like the Titanic didn't prepare for icebergs, thinking it was unsinkable, many businesses fail to prepare for the relevant cyber security threats they could face.

This talk will focus on Cyber relevance, ensuring that when you are buying services and tools from vendors, they are relevant for your business, and how to communicate to the board to ensure you secure the budget you need, to ensure you have the lifeboats in the event of cyber icebergs.

 [Rosie Anderson](#)



Ian Thornton-Trump
aka Phat Hobbit

Cyjax Ltd
CISO



Data Breach Loss P**n



I've come across a strange new trend in the discussion of data breach costs. Not only are the numbers being reported by the UK firm Capita and USA firm Rackspace alarming for what - on the surface looks to be a very basic failure of security best practices.

I'm adapting the phrase "loss porn" defined as "Screenshots of stock or cryptocurrency trades that show extreme losses shared in online forums." Into "cyber loss porn"

I'm not sure why we need an update on how much firms are spending on cyber security event clean up's. is it newsworthy? I mean other than the "shock and awe" cost for reasons which are upon analysis, both elusive and obfuscated.

Join Phat Hobbit as he picks apart the numbers and concludes "it's a con-job".



Ste Wright

Lead Developer
th4ts3cur1ty.company



The Origin of DracoEye



DracoEye is a free tool for security analysts created by myself and the team at th4ts3cur1ty.company

This talk will cover

- What DracoEye is
- What's coming next?
- Why we built it?
- Why we need community input
- Examples of how it helps a security engineer or a SOC analyst day-to-day



Careers Panel



Dr Andrea Cullen
Capslock

Glenn Pegden
Flutter

Graeme Moss
University of Leeds

James Riley
Immersive Labs

Natasha Harley
Cyber Chain Alliance

CAPSLOCK[•]

**Award-winning
cyber security bootcamps**

capslock.ac

th4ts3cur1ty.company >

No nonsense,
just defence.

✉ info@th4ts3cur1ty.company

🌐 th4ts3cur1ty.company

☎ 020 8133 0660

🐦 @th4ts3cur1ty

🌐 th4ts3cur1ty.company

📷 thatsecuritycompany



AKIMBOCORE

UNRIVALED PENETRATION TESTING

PENETRATION TESTING
CYBER SECURITY TRAINING
SYSTEM HARDENING

UK Based Cybersecurity Experts

Akimbo Core are a cybersecurity company with a strong focus on Penetration Testing. We work with organisations all around the world to improve their security maturity through testing, training, and consultancy.

info@akimbo.com

0161 327 1941





Workshops





How to build Robots (for complete beginners)



Everyone wants to learn to build robots, right?

Well here's your chance!

Come over to our workshop!!

Mark Goodwin

Causaly
Senior Staff Security
Engineer



[Mark Goodwin](#)



Taming the supply chain



As software is increasingly integrated with many third party components, particularly open-source components, it is essential to have a clear understanding of all of the software that is deployed regardless of where it is used. With an increasing focus on improving the Cybersecurity of the many different parts of the supply chain, there is a growing expectation that a Software Bill of Materials (SBOM) will become a key artefact of any software asset to help capture all of the software components being used.

But just generating an SBOM doesn't add any value; where the value comes is when they are integrated and used as part of a proactive security programme which is looking at mitigating the security risk to threats in the operational environment. And this applies throughout the life cycle from the identification of components, procurement of components, integration and management of deployed products as new vulnerabilities are continually identified.

This workshop will take participants through an SBOM lifecycle including the creation and analysis of various SBOMs. Participants will be introduced to various tools during the workshop which can be used to create and analyse SBOMs.

Participants should bring a laptop with a Python environment installed (version 3.10 or later) and will need to be able to install software during the workshop.

Anthony Harrison

APH10

Founder and Director

 [Anthony Harrison](#)

[APH10 - LinkedIn Page](#)



Daniel Oates-Lee

FireDuck
Founder



Terraform Titans: Navigating the CI Pipeline without Tripping the Security Alarms



In an era where infrastructure as code (IaC) has become a cornerstone of modern IT operations, mastering tools like Terraform is no longer just an advantage; it's a necessity. However, the real challenge lies not just in utilising these tools, but in doing so securely, especially when integrated into Continuous Integration (CI) pipelines. This workshop, "Terraform Titans: Navigating the CI Pipeline without Tripping the Security Alarms," is designed to turn you into a master of secure Terraform scripting within the CI environment.

Our journey will commence with an overview of Terraform and its pivotal role in defining, provisioning, and managing infrastructure with IaC principles. We'll explore Terraform's syntax, modules, and state management to ensure a solid foundation. This is where our focus shifts to the heart of our workshop: implementing Terraform within CI pipelines securely.

We live in a world where cyber threats are not just rampant but are also constantly evolving. In response, we must be agile and vigilant. This workshop will guide you through the best practices for securing your Terraform scripts. You'll learn about common vulnerabilities and how to avoid them, ensuring that your infrastructure remains robust against potential threats.

Next, we dive into the world of Continuous Integration pipelines. CI is a crucial part of DevOps, enabling developers to integrate code into a shared repository early and often. However, integrating Terraform into CI pipelines demands a nuanced approach to maintain both efficiency and security. We'll dissect real-world scenarios, demonstrating how to integrate Terraform into CI pipelines effectively while ensuring that security is not compromised. This includes managing secrets, using policy as code, and automated compliance checks.

But what's theory without practice? Our interactive sessions will have you getting your hands dirty, applying what you've learned in real-time scenarios. You'll experience first hand the thrill of deploying secure infrastructure through Terraform in a CI pipeline, all under the guidance of seasoned professionals.

Furthermore, we'll navigate the emerging trends and future outlook of Terraform in CI environments. The landscape of technology is ever-changing, and staying ahead means being aware of what's on the horizon. We'll discuss potential future developments and how to prepare for them.

To add a bit of fun to our serious subject, we'll intersperse our workshop with cybersecurity-themed games and challenges. These activities are designed not only to entertain but also to reinforce your learning experience in a memorable way.

By the end of this workshop, you'll not only be proficient in using Terraform within CI pipelines, but you'll also be a champion of securing them. You'll leave equipped with the knowledge, skills, and confidence to implement Terraform in your CI pipelines securely, ensuring that your infrastructure is both powerful and protected. Join us in this adventure to become a true Titan of Terraform and CI pipelines, where securing the digital realm is our quest and excellence our path.



[Daniel Oates-Lee](#)



Tom Blue

University of Lancaster
Student



Intro to the code compilation process



We'll delve into the process of how code is converted into machine code - delving into compilers, linkers, lexers, parsers etc. There will be a focus on C but the process for higher level languages would also be touched upon. After this talk you'll come away with an understanding of what happens between writing code and compiling it, and how to leverage that knowledge to write better and more efficient code.

Whilst this talk isn't purely security it'll explain a lot of concepts important for low level binary exploitation as well as compiler optimisations etc. I aim for it to be beginner friendly with as little pre requisite knowledge as possible, everyone who attends should come away knowing something new and things will be explained from the very basics.

I don't plan a demo per se, but I'll likely use things like godbolt (an interactive browser based C compiler) to demonstrate how certain bits of code compile.

Basically I want to teach people what happens between hitting compile and getting an executable binary



[Tom Blue](#)



[tom_bluu](#)



Our After Party.



Our After Party will be at Barker House Farm.

Join us for a Fireside Chat with Chris Roberts, a Lancashire Pub Quiz (with prizes) followed by Cyber House Party from 9pm.

Drinks and food provided by our wonderful sponsors.

Scan the maze map for directions from George Fox



After Party Evening Speaker



Chris works as an advisor for several entities and organisations around the globe. His most recent projects are focused within the aerospace, deception, identity, cryptography, Artificial Intelligence, and services sectors. Over the years, he's founded or worked with several folks specializing in OSINT/SIGINT/HUMINT research, intelligence gathering, cryptography, and deception technologies. These days he's working on spreading the risk, maturity, collaboration, and communication word across the industry. (Likely while coding his EEG-driven digital clone that's monitoring his tea and biscuit consumption!)

Since the late 90s Chris has been deeply involved with security R&D, consulting, and advisory services in his quest to protect and defend businesses and individuals against various types of attack. Prior to that, he jumped out of planes for a living, visiting all sorts of interesting countries and cultures while doing his best to avoid getting shot at too often. (Before that, he managed to get various computers confiscated by several European entities.)

He's considered one of the world's foremost experts on counter-threat intelligence and vulnerability research within the Information Security industry. He's also gotten a name for himself in the transportation arena, basically, anything with wings, wheels, tracks, tyres, fins, props, or paddles has been the target of research for the last 15 years. (To interesting effect.) Chris has led or been involved in information security assessments and engagements for the better part of 25 years and has a wealth of experience with regulations such as GLBA, GDPR, HIPAA, HITECH, FISMA, and NERC/FERC. He has also worked with government, state, and federal authorities on standards such as CMS, ISO, CMMC, and NIST.

Chris has been credentialed in many of the top IT and information security disciplines and as a CyberSecurity advocate and passionate industry voice, he is regularly featured in national newspapers, television news, industry publications and several documentaries. He can typically be found waving arms on a stage somewhere on this planet...or hacking into whatever's taken his fancy... (Cows and camels being two of the more bizarre things, we'll ignore things in space for now.) As one of the well-known hackers and researchers, Chris is routinely invited to speak at industry conferences. CNN, The Washington Post, WIRED, Business Insider, USA Today, Forbes, Newsweek, BBC News, Wall Street Journal, and numerous others have covered him in the media.

And the worst case, to jog the memory, Chris was the researcher who gained global attention in 2015 for demonstrating the linkage between various aviation systems, both on the ground and while in the air that allowed the exploitation of attacks against flight control system.



Chris Roberts

CISO



[Chris Roberts](#)



“We are back again for the Hot Pot, Butter Pie and the incredible atmosphere at BSides Lancaster to raise much needed funds for the NSPCC. Please donate what you can every £1 makes all the difference. Join us for a fun filled evening of dancing and laughter. A room where everyone is welcome “

**WE ARE
BACK AT
BSIDES
LANCS
27TH
MARCH
9PM TIL
LATE**



NSPCC



Hackademia



Get a ticket • Submit a talk • Sponsor us

hackademia.ac • info@hackademia.ac

Lancaster University's first
student-run cyber-security
conference

For professionals and students

1st June • Lancaster University



BO LANCASTHIRE
SIDES

