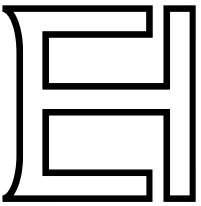

PROGRAMME
SECURI-TAY 2022

SECURI-TAY 2022

PRESENTED BY



Abertay Ethical Hacking Society

team@hacksoc.co.uk

@AbertayHackers

WELCOME

Welcome to Securi-Tay 2022!

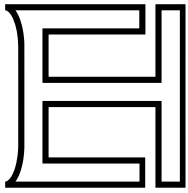
Securi-Tay is organised each year by Abertay's Ethical Hacking Society. We would like to thank all of our members for their support in organising Securi-Tay, allowing it to run every year (COVID aside!) for a decade. We would also like to thank the staff at Abertay's Student Association for their guidance throughout the year. Additionally, we would like to extend our thanks to Abertay University for providing us a space with which to hold the conference.

This year there are going to be a total of twenty talks running across three simultaneous tracks, alongside the workshop village hosting two separate workshops. We would like to thank all speakers and workshop leaders for giving up their time to present their research and experiences at this year's conference.

As Europe's largest student-run information security conference, Securi-Tay would not be possible without the generosity of our sponsors, and we would like to extend our thanks for supporting this year's event.

Have a brilliant day and please tag your posts throughout the event using **#SecuriTayX**

Rory, Peter, Allan, and Sophie
Abertay's Ethical Hacking Society Committee



	TRACK 1	TRACK 2	
09:45	Keynote - The A		
11:00	No more alert(1)	Building A Security Program From The Ground Up	
11:30			
12:00	Open Source Reverse Engineering - 60 things in 60 minutes	Accidental Insider Threat Identification	
12:30			
13:00	L		
14:00	I'm in your pipes, stealing your secrets	Practicing Safe Sex(t) - with xxxtra content	
14:30			
15:00	Microsoft Azure Sentinel, Log Analytics and Kusto Query Language - what a Security Analyst does on a daily basis	Social Scoring; Stealing all your information in a digital age (OSINT)	
15:30			
16:00	Delusions of Operational Security	Hacking 9 to 5; A Day in the Life Of...	
16:30			
17:00	E		
17:15	Keynote - Grok the problem		
18:30	F-Secu		

	TRACK 3	WORKSHOPS
e Art of Fighting Bullies		
	Social Engineering: How to hack the humans	
	Docker? I hardly know her! - Container security 101	
	A brief overview of video game anti-cheat	Can you Save the Power Plant? *Waterstons*
	Changing Career: From Teaching Students to Cybersecurity Student	
LUNCH		
	How we're developing the next generation of vulnerability researchers, and how the lessons learnt can be applied to your own training	Can you Save the Power Plant? *Waterstons*
	The Continued Evolution of Userland Linux Rootkits.	
	Finding novel forensic artifacts	Mapping and Attacking Active Directory *Derek Price*
	An Exploration into QR codes and their prevalence as an unexpected Phishing Vector	
	Defensive Coding Reloaded - A Guide to Active Web Application Defence	
	Responding to the ever evolving threat landscape	
BREAK		
em, don't let security be the problem		
ecure Afterparty		

KEYNOTE

09:45 The art of fighting bullies

(or why we choose to build a company in an industry that was too used to terrifying people into buying things they didn't need, at prices they couldn't afford, for problems they didn't have)

This talk is about our history, about the things we got right, and the things we got wrong, to get to here, and what we believe people can do to have a long-lasting positive impact in a problem that – sometimes – feels too big to tackle.

FEDERICO CHAROSKY

Federico is the founder and Chief Executive of Quorum Cyber, a UK cyber security firm enabling customers globally and across industries to confidently operate in a hostile digital landscape.

Federico has 20 years' experience providing cyber security services across Americas, Europe, and Middle East. He was previously VP Group Head of Security at a Middle East bank; Company Director and Head of Consulting for a cyber security firm in UK; Senior Advisor for several blue chip and FTSE100 companies.

TRACK 1

11:00 No more alert(1)

No more alert(1) aims to get pentesters and blue-team security professionals on the same page. After listening to blue-team and non technical staff (everyone from seasoned security professionals to non technical project managers), this talk aims to bridge the gap between the two arms of security by showing the different ways proof of concepts can be gathered. A deep dive into exploiting XSS and a light touch on some of the other vulnerabilities, combined with all the best ways to demonstrate how to show exploitability to clients, means that whether you're a hardened CTL, a new product manager without technical knowledge, or entry level in any discipline, you should walk away having learned something new.

LIAM FOLLIN

Professionally, I look after the Service Desk and Service Development at Pentest People (pentestpeople.com), am the volunteer IT Director at Trust Leeds (trustleeds.org.uk) and develop the various service offerings at DarkInvader (darkinvader.io). Personally, I love coding tools to make pentesters lives easier, with a little bit of martial arts on the side!

12:00 Open Source Reverse Engineering - 60 things in 60 minutes

This talk revolves around the open source reverse engineering toolkit Radare2 (r2) - which is written in C and has been in development since 2006. Radare2 is an advanced suite of tools & features for working with binaries on many platforms and architectures. The tools also come with language bindings for many popular languages allowing for easy plugin/tool development. During this talk, we'll blitz over 60 interesting features or Easter eggs available in Radare2, in 60 minutes. The aim is to pique your interest in r2 by showing you features that you can use to make your life easier, whether you're doing DevSecOps, reversing code, or mobile app pentesting. Hold tight, we're going for a bit of a 0x72 0x69 0x64 0x65.

GRANT DOUGLAS

Grant is an Abertay Ethical Hacking alumni and has been in the industry for over 8 years. Grant is currently a Principal Consultant at Synopsys and specialises in mobile security - holding strong skills in reverse engineering, threat modelling, pentesting, code review, and more.
Grant has contributed to common open source tooling such as Frida & Radare2 and has presented frequently at conferences on various AppSec topics.

14:00 I'm in your pipes, stealing your secrets

Supply chain attacks are higher profile than ever, and Continuous Integration and Continuous Development (CI/CD) pipelines are rapidly forming the basis of modern software development and DevSecOps workflows. These pipelines grant developers flexibility to perform automated testing regularly during development, and can aid in reducing the number of steps required to get code from a keyboard to a development environment. While this is convenient for developers, with great convenience comes great attack surface. This presentation will provide an introduction into CI/CD pipelines, then discuss some of the ways we have compromised customer environments using a pipeline or code repository as a starting point. The presentation will draw common attack paths and escalation vectors, and hopefully provide some useful guidance on how to lock down your own environments and reduce the blast radius of a compromised pipeline.

IAIN SMART

Iain is the containerisation and orchestration practice lead at NCC Group. He enjoys playing with new technologies, and if he's not hacking a Kubernetes cluster or attacking a build pipeline he can probably be found writing new home automations to annoy his family.

15:00 Microsoft Azure Sentinel, Log Analytics and Kusto Query Language - what a Security Analyst does on a daily basis.

This talk will be based around my experience as a Security Analyst. My focus will be around Microsoft products: Azure Sentinel and Log Analytics and how investigations can be performed with the use of Kusto Query Language (KQL). The talk will give a bit of an insight into what the role of a security analyst means and what are the benefits of this path.

ELIZABETH MOMOLA

I am a graduate apprentice studying GA Cyber Security at Edinburgh Napier University. I also work as a Security Analyst at Quorum Cyber. My journey with Cybersec started over 2 years ago when I joined the graduate apprentice program coming from an administration/ customer service background. As part of my job I mainly work with Microsoft products like Azure Sentinel and Defender platforms to investigate security alerts. I'm also involved in security engineering, incident response and customer engagement, which allows me to gain a better understanding of cybersecurity industry as a whole. In my 'free' time between work and uni, I'm a mum of two and strive to engage with the infosec community by attending conferences and mentoring.

16:00 Delusions of Operational Security

A look at how attempted Operational Security (OPSEC) failed in practice for a group of alleged January 6th Capitol attackers.

This talk analyses the steps taken by the group to organise, protect their identities and communications.

MICHAEL JACK

Former AbertayHackers Vice Gaffer.
Purveyor of macOS security & rum.
War Studies postgrad Terrorism, Radicalisation & British intelligence.
Security Engineer.

TRACK 2

11:00 Building A Security Program From The Ground Up

Whether you're a company's first security hire or you're on your first steps to becoming a security manager, it can be tough to know what to do first.

This talk covers everything you need to get started, from technical skills and tools you can deploy through to the do's and don'ts of dealing with other teams within the business to make sure you make progress and can build a valuable security program.

JAMIE MACDONALD

Jamie is Head of Security at Rasa and has previously worked as a security engineering lead at Fortinet and ZoneFox. He works on bringing usable security to businesses and making sure that security isn't seen as The Team Who Says No.

12:00 HoneyPoC Analysis Part 2: Accidental Insider Threat

Not all talks are Red/Blue/Purple, some are learning opportunities for all. HoneyPoC opened the eyes of many folks and why is it important to be careful about the Proof Of Concepts(POC) that you download/ review. What started off as a minor troll turned into an integrated research project, the talk will embark on knowledge about steps taken to uncover insider threats via passive analysis and identification of internal hosts.
This was a particularly "amusing" troll because the sort of people who keep up with CVEs and look for proof-of-concept exploits should really know better than to run random code they just got off GitHub without checking what it does.

ANDY GILL

Andy is a seasoned offensive security professional who specialises in red and purple teaming with a focus on obscure insider threat attacks. He is a hacker at heart and a keen supporter of the wider community with blog posts, talks and podcasts. Most known for his book LTR101 and HoneyPoC, a troll that became a research project.

14:00 Practicing Safe Sex(t) - with xxxtra content

18+

CONTENT WARNING

There will be sensitive content discussed in this talk such as sexual violence, domestic abuse and suicide.

Nudes, Dirties, Pics, whatever you call them, you've probably sent them or know someone who has. But how can we protect ourselves and our opsec when we're sexting, producing sexual content of ourselves or even watching and buying sexual content online? This talk will discuss how we can protect our physical bits online, how to practice safe sexting properly, how we can learn opsec from sex workers and looking into the weird, wonderful and sometimes scary world of sex online. This talk has been delivered before, but has been updated to include new content about sex toys, porn consumption and how it's changed over the years, as well as how the pandemic affected sex online.

TIA C[redacted]

Tia is a fourth year ethical hacking student at Abertay University. She has delivered various workshops and talks at conferences and societies around the country. These talks and workshops vary from social engineering, offensive security and most recently discussing how to practice safe sex online.

15:00 Social Scoring; Stealing all your information in a digital age (OSINT)

Over the past year I have been doing research into OSINT as part of a research proposal. I will present an in-depth view on how I am building a social scoring system by compiling detailed profiles on people existing in the UK (Specifically England). This talk focusses on the social aspect of having an online presence, and the dangers associated. It presents ethical questions regarding data governance and the right to privacy. By the end of this talk you should have a detailed idea on how Governments, Adversaries and other organisations are able to build up an entire profile of your personal life, and how to best defend against it.

DYLAN WHEELER

Dylan Wheeler is an ex-blackhat hacker known for his involvement in the Xbox Underground hacking group (featured by WIRED US and Darknet Diaries). Dylan currently resides in London and has been a major advocate for responsible disclosure in recent years, working largely within both the financial and entertainment sectors. Dylan takes an unusual and often eccentric approach towards the information security field and in 2019 was rumoured to be assaulted at the ICE London conference by a vendor for a security disclosure gone awry.

16:00 Hacking 9 to 5; A Day in the Life Of...

Talk will cover entry-level industry certifications, ways to demonstrate an active interest in offensive security and what to expect daily as a penetration tester in the 9 to 5 job. Additionally, coverage of the most common types of testing engagements experienced as an offensive security professional.

MARK ROSE

Mark is an experienced Penetration Tester who graduated from Abertay in 2016. Since then, Mark has went on to engage with clients worldwide to help them improve their security maturity and improve their defences against attackers. Outside of work, Mark hacks his way around the golf course.

SYNOPSYS®

*In the Synopsys Software Integrity Group (**SIG**), we work to help customers build security in to all areas of the development lifecycle: **secure design** & **architecture review**, **code review**, **penetration testing**, **threat modelling**, and more. We work in many domains: **automotive**, **IoT**, **mobile applications**, **web**, **thick client software (and games), and more** - so come say hello if you're interested! We are always on the look out for interns, graduates and other senior roles too.*

We are presenting two talks today:

Closing keynote: Grok the problem, don't let security be the problem
You've found an issue. What should be done about it? Sometimes finding the issue is the precursor to the hard part - fixing the defect. Oftentimes, as security professionals, we don't think twice about the true scale and impact of what appears to be a slam dunk fix. We'll use examples to illustrate how fixes go wrong, usually due to a chain reaction of unanticipated consequences or because the design tradeoffs were not considered. This talk aims to motivate attendees to think more deeply about a problem space before pitching security solutions

Open Source Reverse Engineering - 60 things in 60 minutes
During this talk, we'll blitz over 60 interesting features or Easter eggs available in Radare2, in 60 minutes. The aim is to pique your interest in r2 by showing you features that you can use to make your life easier, whether you're doing DevSecOps, reversing malware, or mobile app pentesting.

Additionally, at our booth, we are running some fun challenges suitable for any level of skill so come introduce yourself and prove your 1337-ness. There's some giveaways for attempting the challenges too so crack the extra-terrestrial code or step in to the shoes of Neo and solve our Matrix challenge.

SCAN ME

TRACK 3

11:00 Social Engineering: How to hack the humans

Social engineers use several techniques to bluff, charm threaten or deceive their way into getting someone to commit an act that may or may not be in their best interests. Over the past year I have been doing research into social engineering, the psychology behind influence and how malicious actors combine the two to manipulate and influence people into undertaking actions that are not in their best interests. This presentation will show the six pillars of influence and how they can transpire to trick people like you or me.

CONNOR DUNCAN

Connor currently works as an Analyst at Pa Consulting, working on various cloud security projects. He graduated from Abertay University in 2020, and has a particular interest in Social Engineering and the psychology behind people.

11:30 Docker? I hardly know her! - Container security 101

Containers are only increasing in popularity, with Docker being almost synonymous with the term but one thing a lot of us don't consider is the security. Just because they are inside a container does not mean they are fully isolated or invulnerable to attack. My talk is going to discuss a brief history of containers, how they work and why do we use them. Then going to talk about some common vulnerabilities, famous CVEs and a hacker group or two you may want to look out for! Finally what are some ways to secure your container from super simple solutions like namespacing to more complicated and involved methods such as creating custom AppArmor profiles for your container applications.

MAIRI MACLEOD

An Abertay alumni who is currently working as a cyber security analyst, Mairi has a love/hate relationship with containers. Where she loves breaking out of them and hates having to spell Kubernetes. Hobbies wise Mairi spends her free time taking photos of her cat, watching anime and waiting in Final Fantasy raid queues.

12:00 A brief overview of video game anti-cheat

Video game cheating is an interesting dilemma faced by game development companies. With cheats being originally built into games, being unlocked with a code. To China arresting cheat makers for games. The current solution is software used to detect the presence of cheating done by the user of the device, known as "Anti-Cheat". Which is like running anti-virus on a malware creators' computer. This talk will discuss about what is anti-cheat, its history, the present, the good, the bad and the silly.

FRASER.A

I'm a Abertay ethical hacking year 3 student, and I like computers (Big surprise). I've done a talk before at the Abertay Ethical hacking society (And at the time of writing am preparing to do another talk).

12:30 Changing Career: From Teaching Students to Cybersecurity Student

1 - Brief Overview of Talk Structure

2 - Career Change to Cyber - My reasons behind leaving and teaching and why I am pursuing Cybersecurity.

3 - Why teachers should consider retraining to cyber and why cyber should consider training teachers (many skillet crossovers I will expand on)

4 - Reflection on experiences of first year so far and challenges other career shifter may face if retraining to cyber.

5 - Questions/Suggestions/Advice from audience

EWAN TAYLOR

Ewan Taylor is a 1st year Cybersecurity student, former teacher and music graduate, now seeking to build a new career in the exciting world of Cybersecurity.

14:00 How we're developing the next generation of vulnerability researchers, and how the lessons learnt can be applied to your own training

This talk is designed for people looking to break into computer security, and specifically the vulnerability research field. During this talk we'll break down training techniques, principles, and approaches that we've used to help develop the next generation of vulnerability researchers and how those same techniques can be applied to your own training.

JAMES STEVENSON

James Stevenson is a vulnerability researcher, public speaker, and published author. James has been in the computer security field for around 5 years and currently works for the vulnerability research company Interrupt Labs. At IL James, with others, have developed a training platform from the ground up - designed to bring those new to computer security to the level of specialised vulnerability researchers.

14:30 The Continued Evolution of Userland Linux Rootkits

From libncom.so to Jynx, Azazel to "libcurl", userland Linux rootkits have been a growing, but often ignored, part of the Linux malware ecosystem for over a decade now. Despite crippling architectural flaws, this evolutionary dead-end of sorts in Linux malware continues somehow to thrive due to the relative ease of development, deployment, and reliability when compared to kernel based rootkits. Somehow, they even evade modern, expensive EDR products. This talk will be a brief primer on this category of rootkits. Where it began, where it is, and where you can take it next.

DARREN MARTYN

Darren is a security researcher/consultant based on a small, damp rock in the Atlantic with a special fondness for Linux malware.

15:00 Finding novel forensic artifacts

During an IR case, there are many well-known sources of evidence which can be used for triage or in-depth investigation. Because these artifacts are familiar to investigators, mature tooling and analysis capabilities are available. However, adversaries have the same level of understanding and can use it to cover their tracks. While many e-crime groups just don't care, other more advanced actors have created tooling to automate anti forensics. For example, the uncategorised threat group, tracked by FireEye as UNC1945, utilizes an ELF executable called LOGBLEACH which deletes log entries in a selection of log files such as syslog and auth.log. In lieu of the usual sources, investigators must rely on more obscure artifacts to fill in the blanks and solve the case.
This talk will outline the threat landscape and drill down into the process of identifying novel forensic artifacts using the example of the wget-hsts file.

JOE DANIEL

Joe is a Security Researcher and Incident Responder, currently studying Cybersecurity & Forensics. He has previously worked as a Site Reliability Engineer and enjoys programming in his spare time. AFK, Joe is into fitness, travel and photography.

15:30 An Exploration into QR codes and their prevalence as an unexpected Phishing Vector

This talk will explore the understudied technology of QR codes. Most people will know what a QR code is, and have likely scanned many throughout their life. Very few people know how the technology works, nor have considered the use of QR codes for alternative uses. With the newly increased usage and acceptance of QR codes caused by covid track and trace, more people will be willing to and expecting to scan a QR code on their way into a building. This increased prevalence further escalates the probability of QR codes being used for a more modern version of phishing.

JOSH HILL

4th-year ethical hacker, I've attended 3 Securi-Tays so far and many other conferences. I want to be able to speak at our home conference to give back for all the good conferences that have been run in past years.

16:00 Defensive Coding Reloaded - A Guide to Active Web Application Defence

When considering defending and protecting web applications, rarely do we speak about what the web applications themselves can actively do when under attack. Built-in detection and response capabilities can be a highly effective and underutilized method to mitigate attacks and to act as a canary for malicious activity.
In this talk, I'm going to introduce the concept of application intrusion detection and highlight the techniques available to make web applications attack-aware. Furthermore, I will also illustrate ongoing research on how developers can take advantage of their frameworks and language-level mechanisms to get started.

TOLGA ÜNLÜ

Hey there! My name is Tolga and I'm one of the PhD candidates in Cybersecurity here at the Abertay University. In my research, I'm investigating the integration of attack-awareness capabilities in web applications, a topic where also two of my favourite interests come together - development & security.
Before I re-joined Abertay for my academic journey, I have worked as a web application engineer for a Startup in the lovely region of Allgäu (Germany), where I'm currently based.

@tolgauedev
https://tolgadevsec.github.io

16:30 Responding to the ever evolving threat landscape

The Secureworks Counter Threat Unit constantly analyses threat data across our worldwide customer base and actively monitors the cyber threat landscape to provide a globalised view of emerging threats, zero-day vulnerabilities, and the evolving tactics and techniques of advanced threat actors. This session will provide the latest intelligence on the threat landscape, considering the criminal threat from ransomware as well as trends from hostile state actors. We will also cover practical measures your security team can use to keep you protected and how Secureworks can help your organisation accelerate threat detection and response.

DON SMITH

Don Smith leads the Secureworks Counter Threat Unit's™ Cyber Intelligence Cell (CTU-CIC), a global team of experienced threat analysts who deliver actionable and timely intelligence products on the threats most relevant to Secureworks clients. Based in the UK, Don also leads the Secureworks CTU research team in EMEA. Don joined Secureworks in 2005 and his enthusiasm and threat expertise means that he regularly represents the company and their more than 20 years of industry-leading threat intelligence at industry events. With more than two decades of experience in the IT industry, he was previously responsible for security architecture and operations for a multi-billion enterprise and took a lead role in successfully integrating 14 acquisitions. Don is a recognized subject-matter expert in many areas of cybersecurity and advises threat intelligence partners and Secureworks customers around the world.

OUR BRONZE SPONSOR

CROWDSTRIKE

CLOSING KEYNOTE

17:15 Grok the problem, don't let security be the problem

You've found an issue. What should be done about it? Sometimes finding the issue is the precursor to the hard part - fixing the defect. Oftentimes, as security professionals, we don't think twice about the true scale and impact of what appears to be a slam dunk fix. We use some examples to illustrate how fixes go wrong - usually due to a chain reaction of unanticipated and unintended consequences, or because the design tradeoffs were not considered. The goal of the talk is to motivate attendees to think more deeply about the problem space before proposing a (security) solution.

ANDREW LEE-THORP

Andrew Lee-Thorp is an occasional speaker, trainer and security jack of all trades who currently works as a Principal Consultant for Synopsys Software Integrity Group where he engages in teaching, threat modelling, pen-testing and bug hunting. Andrew has been in the security trade long enough to experience deja vu every time a new bug comes out. He has lived two previous lives as a software developer and as a research scientist which means he has six lives still to go.

THE COURIER BUSINESS AWARDS 2021
in association with Henderson Loggie
WINNER

NCR

NCR Corporation is a leading software and services-led enterprise provider. We help our customers run their store, self-directed banking or restaurant. NCR Dundee is the home of banking where we focus on Security, Saas, Software Architecture and apply scaled Agile practices.

Working with McAfee™ and Fintech Scotland™ we continue to innovate and bring new technologies to our global markets.

McAfee

FinTech Scotland

Software Product Management

Software Development

600 Employees

Banking

Software & Technology

Professional Services

Software Support

Security Engineering

Scan me for more information

N-ABLE™

Do you have a passion for possibility?

N-RICH LIVES
We use our talents and find meaning and purpose in all that we do.

N-SPIRE OTHERS
We unlock potential and help bring out the best in others.

N-JOY THE JOURNEY
We are passionate about what we do and have fun along the way.

Find your next career with us

n-able.com

careers.n-able.com

WORKSHOPS

12:00 & 14:00

Can you Save the Power Plant?

In this Lego cyber resilience tabletop exercise, your team has been tasked with the mission of managing the security of a newly acquired power plant. You will be given a small budget to implement a range of different defensive cyber options.

Your team of up to 8 players will be given 60 minutes to use your decision-making skills to determine the best course of action for the organisation.

Will you keep the plant running?

NOTE: You must sign up for the session beforehand. Visit the Waterstons sponsor stand to sign up. Either create your own team (max 8 players) or individually sign up and we will assign you a team.

WATERSTONS

Waterstons are an NCSC approved Cyber Consultancy with over 25 years of helping our clients to protect their critical data and reputation. Our mission is to become a trusted security partner to our clients, continually protecting their organisation from the evolving cyber threat landscape. Waterstons contain a range of experts in all areas of information security, from the Cyber Resilience Team to our 24 x 7 Security Operation Centre (SOC).

S

15:00

Mapping and Attacking Active Directory

A workshop to show people how to map out there active directory and what attacks can be used to compromise AD. Workshop will include a vulnerable AD to run tooling against and demos of how to attack these findings and how to fix them.

This workshop will be for up to 25 people and slots will be on a first come first serve basis. It is preferable for students to use their own machine.

DEREK PRICE

My name is Derek and have been in security for 10 years now and got the opportunity to key note a few years ago at this event. My interests are Active Directory and cloud

Scottish Business Resilience Centre

The vision of SBRC is to become the catalyst that makes Scotland one of the safest and most resilient places to live, work, and do business, both on and offline, especially during these times of economic recovery

It is our intention that every Scottish organisation have the skills and knowledge to protect themselves against online attacks. We achieve this through the delivery of education and preventative training, as well as actively raising awareness of threats throughout the business community.

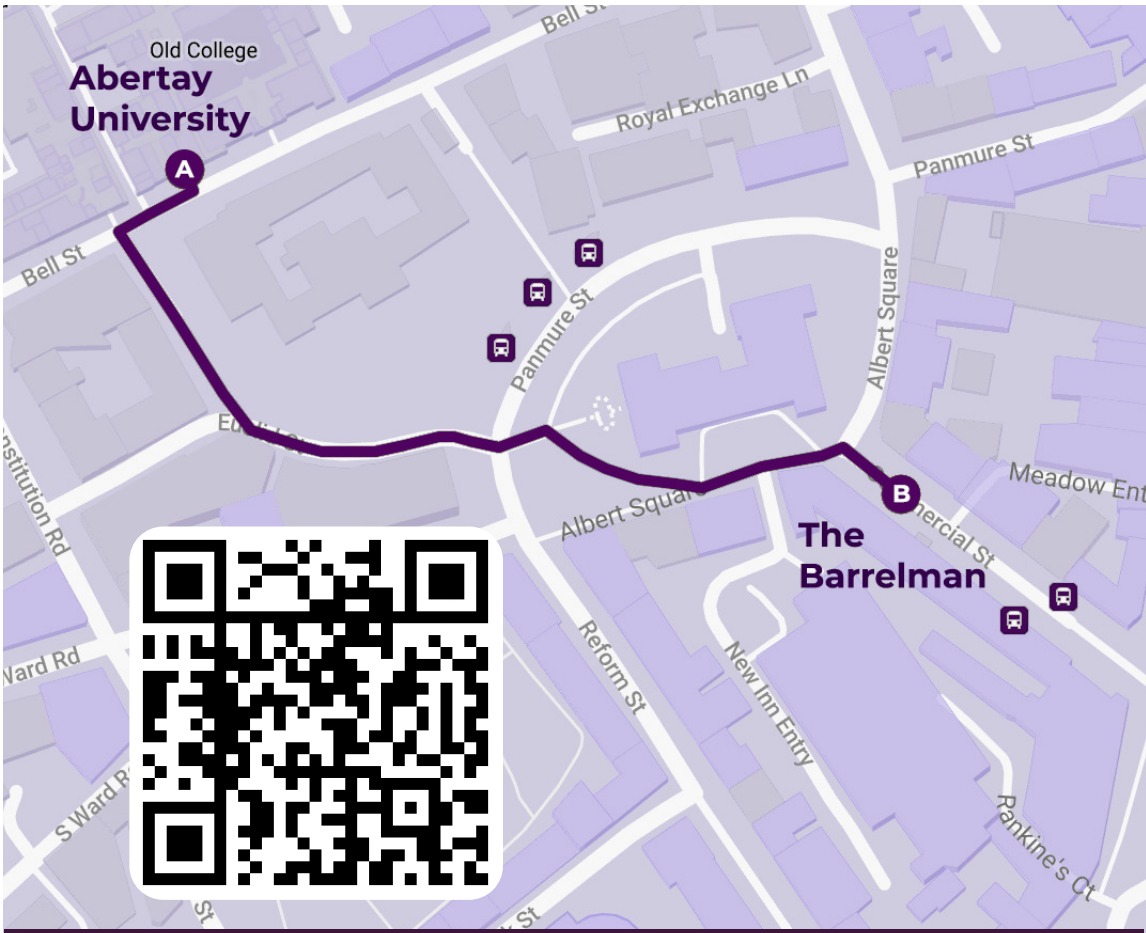
Follow us:

@SBRC_Scotland

Scottish Business Resilience Centre

www.sbrcentre.co.uk

AFTERPARTY



Our Afterparty is being held at The Barrelman Dundee (location B on the above map)

Use this map, or scan the QR code for a Google Maps Location.

F-Secure

Proud sponsors of the Securi-Tay 2022

AFTER PARTY

F-Secure

JOIN US THERE 6:30PM

The Barrelman, Dundee

AT OUR STAND

Puzzles | Lock picking | CTF challenge | Giveaways

IN THE EVENT

Top Incident Responder Alan Melia,
presenting on a real-life APT investigation.

Join the next generation of cyber security specialists at F-Secure Consulting

- Feel welcome, whatever your background
- Satisfy your intellectual curiosity
- Develop creative solutions to complex challenges
- Research, investigate, share globally
- Work with recognized figures from the infosec community

FIND OUT MORE

https://www.f-secure.com/en/consulting/our-people

CAPTURE THE FLAG

The Securi-Tay CTF is back!

We have been working hard to build challenges designed exclusively for Securi-Tay 2022 by Abertay students and alumni. With hundreds of pounds in prizes on offer, be sure to give this year's CTF a go!

Go to **https://ctf.securi-tay.co.uk/** for full information and to sign up.

1st Prize:
An exam voucher for INE eJPT or a CompTIA certification of your choice.

2nd Prize:
O.MG Cable

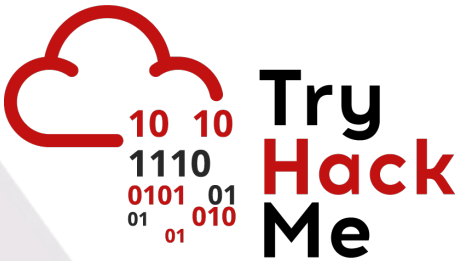
3rd Prize:
Books from No Starch Press

Most of the challenges
are hosted at
https://ctf.securi-tay.co.uk/

with full-pwn challenges
kindly hosted by
https://tryhackme.com/

Challenges will open at the start of the day. **Scores will freeze at the start of the closing keynote.**

Winners will be announced at the end of the closing keynote, and the challenges will be left up for a few days after if anyone wants to keep at them.



Quorum Cyber

www.helpfightbullies.com

Starting up in Edinburgh in 2016, we have now grown to be a major force in cyber security worldwide, a Microsoft Gold Partner and member of Microsoft Intelligent Security Association.

We're growing fast, building our customer base through exceptional products and services delivered by exceptional people. Join us and you'll join a community of passionate, likeminded individuals providing cyber security services to organisations worldwide. We are powered by Microsoft technology, delivered entirely from the UK, and connected by a simple cause that we all believe in.

Graduate Development Programme

In Cyber security, there is no substitute for an in-depth knowledge and understanding of all the moving parts. You need to know and recognise the cyber security landscape in the forensic detail that sets Quorum Cyber apart as a place to learn and build your career. On our new graduate development programme, we will equip you for success in your chosen area of expertise. It's a comprehensive programme that offers external and internal learning and development opportunities that will stretch and expand your horizons.

> "One of the reasons I stayed working within Quorum Cyber after the Internship programme is the opportunity to move Teams within the company – I think it is a great way to learn something new and expand your knowledge."

Scott, from Internship to Cyber Security Analyst

- Challenging & rewarding work
- Private Medical Cover
- Unlimited Holidays
- Active Learning & Development
- Flexible working
- Access to the latest technology
- Contributory Pension

Sign up to hear more about the Quorum Cyber Graduate Programme.

Follow us on social & get in touch!


Quorum Cyber
JOIN THE TEAM
#HelpFightBullies
quorum-cyber
recruitment@quorumcyber.com
@QuorumCyber

ADARMA
TOGETHER WE'VE GOT THIS

PROTECTING THE PROMISE OF CYBER RESILIENCE.

ADARMA.COM

Thank you

We'd like to say a huge thank you to the Abertay Students Association. Without their hard work and effort, Securi-Tay wouldn't be the success that it is.

ABERTAY SA

Waterstons

we're with you

Waterstons has been around for over 25 years and have offices in London, Glasgow, Durham and Sydney. Our mission is to become a trusted security partner to our clients to continually protect their organisation from the evolving cyber threat landscape.

The Waterstons Cyber Resilience team has expertise in assisting clients to develop holistic and pragmatic cyber strategies and gain certification with best practice standards (such as Cyber Essentials & ISO27001). We implement effective security controls and technologies, whilst providing ongoing support via our Security Manager service and 24 x 7 Security Operations Centre (SOC).

When you choose to join Waterstons, you're choosing more than a job. You're choosing to become part of a like-minded community of ambitious people. We're brimming with inspiring colleagues in the UK and beyond, delivering work for industry-leading clients.

Find Out More

careers@waterstons.com

Waterstons

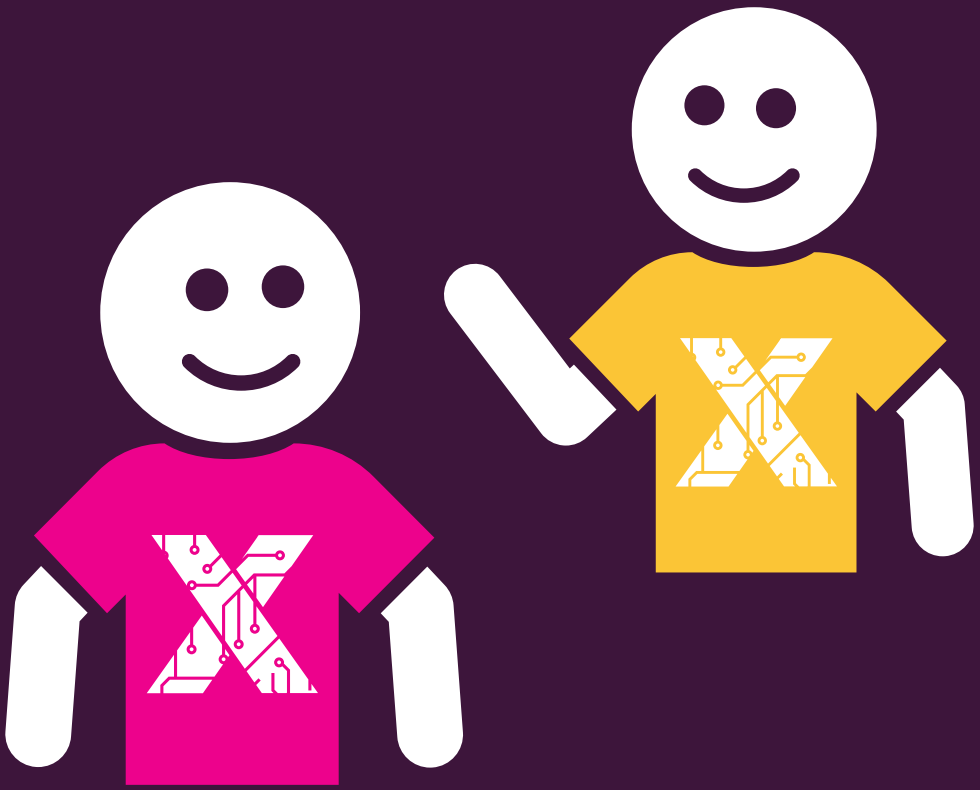
@WaterstonsLtd

@WaterstonsLtd

FEEDBACK
SECURI-TAY 2022

Scan here to let us know what you thought of the conference and how we can improve!

NEED HELP?



If you have a serious issue during the event (e.g. a Code of Conduct violation), please speak to one of our volunteers **(wearing yellow t-shirts)**, or a member of the committee **(in pink t-shirts)**.

Abertay Ethical Hacking Society