CYBERTHREAT

LONDON_2024

9-10 December

Novotel London West, Hammersmith

National Cyber
Security Centre
a part of GCHQ

SANS | GIAC
CERTIFICATIONS

WELCOME

Paul Chichester
Director of Operations,
National Cyber Security Centre

Here we go again, it's great to see you!

It's my privilege to welcome you to CyberThreat24, as we gather at a time when the stakes for global security, technological advancement, and collaboration have never been higher.

We find ourselves in an era defined by unprecedented change and complexity. Geopolitical landscapes are shifting with greater speed and uncertainty than we have seen in decades, and in parallel, technological innovation - while transformative - presents its own paradox. Artificial intelligence, quantum computing, and autonomous systems promise solutions that can propel humanity forward. But these same advancements, if misused, can exacerbate vulnerabilities and amplify the scale of cyber threats. The very tools we create to safeguard our future can, in the wrong hands, undermine it.

Amid this uncertainty, one thing remains clear - we cannot face these challenges alone. The intricate web of threats we confront know no borders, and neither should our resolve to counter them.

Effective operational cyber defence demands more than cutting-edge tools or isolated expertise; it requires a cohesive, resilient, and informed community.

That is precisely why conferences like CyberThreat24 exist. Here, we not only exchange experience and insights but also build trust, forge alliances, and remind ourselves that behind every system and protocol is a network of dedicated individuals united by a shared mission.

Today, I'd like to take a moment to express my deepest gratitude to those who have made this gathering possible. To the experts, researchers, and policymakers who have dedicated their time to share knowledge, thank you for your invaluable contributions. To the organisations who support and sponsor this event, we appreciate your commitment to advancing the state of cyber defence. And to those of you joining us for the first time - Welcome! Your presence here represents a vital infusion of fresh ideas.

Over the next 2 days, I encourage you all to embrace the opportunity to connect, challenge assumptions, and collaborate. Let us leverage the strength of our community to meet the challenges ahead with both determination and hope.

John Davis
Director of UK and Ireland,
SANS Institute

We are back – bigger and better than ever!

It's so great to return to London for the 5th instalment of CyberThreat, bringing hundreds of cyber security professionals together from around the world once again.

This cyber security community has perhaps never been more challenged to change and adapt over the years. As the cyber security landscape is continuously evolving, this presents us with challenges that demand innovation and adaptability. We have the important job of keeping pace with ever evolving technology and the opportunities or threats these may bring.

We continue to see even greater advancements in technology and increasing reliance on systems and networks in every part of our lives. New technologies and advancements such as AI inevitably lead to new threats, new challenges and an ever-increasing need for defence and resilience in our technology and in the implementation of that technology.

SANS knows this and, whilst the past years seemed daunting, they have also allowed us to implement innovation, to experiment, to challenge the status quo and ultimately to grow as an organisation in the most challenging of times. In recent years, we launched an entirely new virtual training method in Live Online and we released an unprecedented number of new training courses and certifications. Many of our curricula grew exponentially to help counter the new threats and challenges our society has to face today.

Our mission is always at the front of our minds, to help educate and to train not just governments, but all organisations, all of our special community and to do our bit to help make the world a safer and better place. I am proud of the SANS team who have again worked tirelessly to create and deliver this unique event alongside our partners at NCSC.

I hope that you leave here inspired with new ideas, a better understanding of the latest threats and developments and that you are motivated to join us in our mission and to fight the good fight.

CONTENTS

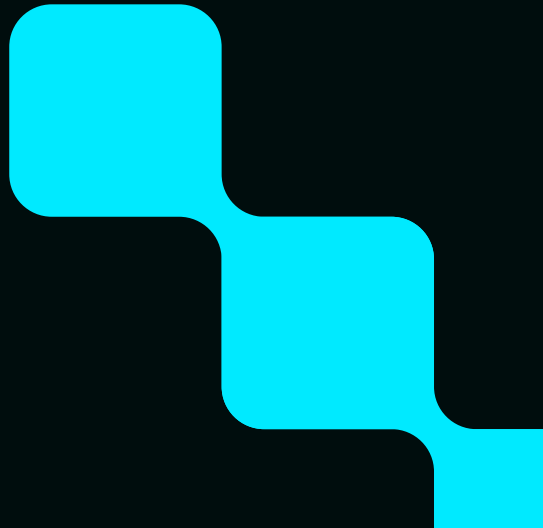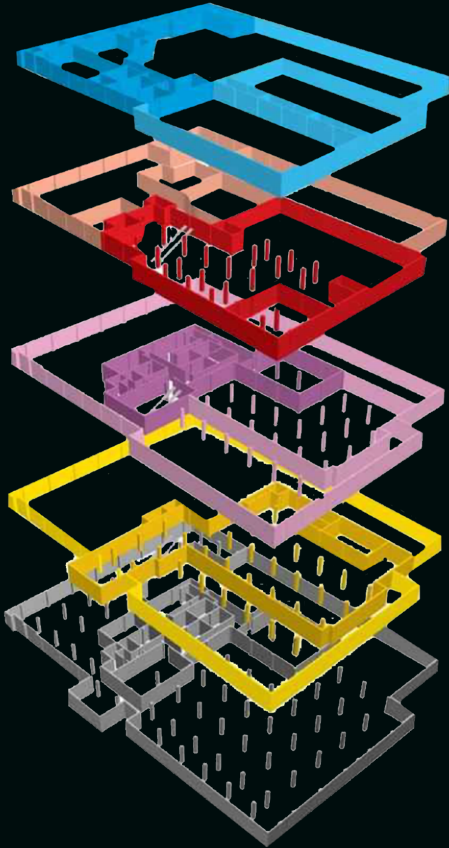# CONTACT

Email: **summitemea@sans.org**

Tel: **+44 203 384 3470**

AGENDA

To view the latest Agenda, click here or scan the QR code below:

VENUE

SECOND FLOOR

FIRST FLOOR
CYBERTHREAT
CHAMPAGNE SUITE

REGISTRATION

MAIN CONFERENCE AREA

SPONSOR AREA

CATERING

RETRO AND MODERN GAMING

CAR SIMULATOR

SCHOOLS AREA 1

CTF

MEZZANINE FLOOR

GROUND FLOOR
CYBERTHREAT
CHABLIS SUITE

LUNCH AREA

LOWER GROUND FLOOR

CAR PARK

EVENT CHAIRS & KEYNOTE SPEAKERS

Paul Chichester
Director of Operations, NCSC

@0xChich

Event Chair

Keynote Speaker

Paul is currently the Director of Operations at the UK's National Cyber Security Centre where he is responsible for managing nationally significant cyber incidents (such as WannaCry) and ensuring UK Government understands and can counter a wide range of state and non-state threats.

Rob Lee
Chief of Research and Head of Faculty, SANS Institute

@robtlee

Event Chair

Rob Lee is the Chief of Research and Head of Faculty at SANS Institute and runs his own consulting business specializing in information security, incident response, threat hunting, and digital forensics. With more than 20 years of experience in digital forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response, he is known as "The Godfather of DFIR". Rob co-authored the book Know Your Enemy, 2nd Edition, and is course co-author of FOR500: Windows Forensic Analysis and FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics.

Allison Wikoff
Director, Global Threat Intelligence, Americas Lead, PwC

Event Chair

Allison Wikoff is a director at PricewaterhouseCoopers (PwC) leading the Americas region of the firm's Global Threat Intelligence practice. She has over 20 years of experience working as a network defender, incident responder, intelligence analyst and threat researcher in organizations including the US Federal Reserve System and prior to joining PwC, IBM.

The focus of the latter half of Allison's career has been researching Iran-based threats. She holds numerous industry certifications and an advanced degree from Columbia University where she guest lectures for several information security-focused graduate courses.

Ciaran Martin

Professor, Director of SANS CISO Network, SANS Institute

@ciaranmartinoxf

Keynote Speaker

Professor Ciaran Martin, CB, joined SANS Institute in January 2023 as Director of SANS CISO Network and Summits EMEA. Respected as a world leader among public authorities for cybersecurity, he is the UK's National Cyber Security Centre's (NCSC) founder and former head.

Ciaran's belief in the collaboration of government and industry to enhance cybersecurity makes him as an ideal lead for today's Chief Information Security Officers (CISOs).

Thomas Rid

Professor of Strategic Studies, Founding Director of Alperovitch Institute

@RidT

Keynote Speaker

Thomas Rid is Professor of Strategic Studies and founding director of the Alperovitch Institute for Cybersecurity Studies at Johns Hopkins University's School of Advanced International Studies. Rid is the author of the acclaimed Active Measures, a sweeping history of disinformation (Farrar, Straus and Giroux, 2020).

Rid's commentary has appeared in The New York Times and the Washington Post, and he has testified in front of the U.S. Senate Select Committee on Intelligence as well as in the German Bundestag and the UK Parliament. His books are widely translated.

SPEAKERS

Richard Horne

CEO,
NCSC

Richard Horne has been CEO of the NCSC since October 2024. Before joining the NCSC, Richard was a Cyber Security Partner and chair of the Cyber Security Practice at PwC UK, where he helped global boards and executives shape their cyber risk strategies and led the response to critical cyber incidents. He oversaw the post incident review for the Irish Health Service after the ransomware attack that disrupted healthcare services across Ireland in 2021.

Before his time at PwC, Richard was Managing Director of Cyber Security for Barclays PLC, where he was responsible for cyber security risk management across the Barclays Group. In 2011 he was seconded to the Cabinet Office to help develop and implement the first national plan for cyber security, impacting both government operations and the wider economy.

Richard holds a PhD in Mathematics from Royal Holloway, University of London. He has represented the UK on security matters at international organisations such as the Organisation for Economic Cooperation and Development, the European Commission and the International Standards Organisation. Richard has also served on advisory boards for academic institutions and technology startups in the field of cyber security.

Sebastian Demmer

Senior Incident Response Consultant,
Mandiant

Sebastian is a Senior Incident Response Consultant at Mandiant's UK office. He has eight years of experience responding to security incidents, and protecting against nation state and financially motivated threat actors.

When not responding to incidents, Sebastian is working on automation and tooling to support incident response, both internally at Google, and externally, contributing to open source projects.

Chris Eastwood

Senior Incident Response Consultant,
Mandiant

Chris is a Senior Incident Response Consultant in Mandiant's UK office. As part of the Incident Response team, Chris provides emergency services to clients experiencing a security breach, through conducting forensic investigation and analysis. Chris has led organizations in responding to breaches by highly-sophisticated adversaries such as nation-state sponsored espionage actors and cybercriminals aiming to extort or ransom victim organizations. Chris has also led Compromise Assessments for Critical National Infrastructure (CNI) and high-profile organizations.

www.cyberthreat24.com
#CyberThreat24

Roey Shua
Security Researcher, Check Point Software Technologies Ltd

Roey is a Security Researcher with five years of experience in diverse roles in the Israeli Public Sector and Silicon Valley. Currently, he's leading the field of Forensic Incident Response in Check Point's Research (CPR) Group, Investigating the activities of sophisticated threat actors.

Diana Selck-Paulsson
Lead Security Researcher, Orange Cyberdefense

@DianaSelck

Diana is a Lead Security Researcher for Orange Cyberdefense, where among other projects she heads the companies efforts to track, analyze and report on current ransomware trends. Her primary interests and focus are on data analysis, researching cybercrime trends, victimology and the human element in cyber security.

Simone Kraus
Senior CSIRT, Orange Cyberdefense

Simone Kraus, a seasoned IT-Security professional, has navigated the industry since 2001. After an apprenticeship, she pursued computer science studies and excelled as a specialized SAP consultant. In 2013, she temporarily left IT, exploring roles as a triathlete, fitness coach, and "Civilian on the Battlefield" (COB) for the US Army and Bundeswehr. Her passion for IT security led her back, starting as a DFIR Consultant and transitioning to a Security Analyst with Orange Cyberdefense in June 2022. Simone's role encompasses Incident Response in both OT and IT environments, with a versatile skill set covering "MITRE Detection Engineering" and threat modeling. With over two decades of experience, Simone Kraus is a valuable asset in the ever-evolving field of cybersecurity, continuously adapting to its challenges and complexities.

Joel Snape
Security Researcher, Crowdstrike

Joel Snape is a security researcher at CrowdStrike, working on all things involving security, computers, and unusual challenges. I'm interested in how stuff works, and using that knowledge to disrupt adversaries. Previously, I have worked for a major UK telecom company working to protect key networks, and carried out security testing, research and consulting for clients with a focus on embedded systems.

Hanno Heinrichs
Security Researcher, Crowdstrike

Hanno Heinrichs is a security researcher at CrowdStrike. His main task is to collect information on APT and eCrime activities. Previously, he has worked in the pentesting and adversary simulation industry

SPEAKERS CONTINUED

Will Thomas
Co-author and Instructor,
SANS Institute

@BushidoToken

Will Thomas is currently working as a Cyber Threat Intelligence (CTI) Researcher for the Equinix Threat Analysis Center. In addition to his work at Equinix, he is a SANS instructor and c-author of the SANS FOR589 course: Cybercrime Intelligence. He holds a Bachelor of Science (BSc) degree (Hons) in Computer and Information Security from the University of Plymouth. William chose cybersecurity not only because he enjoys puzzles, challenges, and investigations, but also because it is a crucial part of modern technology that continues to be overlooked despite the severe consequences and precedence of doing so. In addition to being a SANS instructor and working in the field, he also works in the professional community as the co-founder of the Curated Intelligence community and volunteered as an OSINT analyst for the National Child Protection Task Force.

Thomas Willkan
Lead Analyst,
Dark-web Reconnaissance Team, Accenture

Thomas "Mannie" Willkan is a senior Cyber Threat Intelligence (CTI) Dark Web Analyst based in Europe. Originally from Denmark but currently resides in London. Mannie focusses on dark web intelligence, OSINT and threats emanating from emerging technologies. Mannie is an accomplished threat-analysts whose analysis and work has been featured in outlets like Wall Street Journal, CyberScoop, Venture Beat and The Register. Mannie has previously presented at BlackHat US 2023 and 2024 as well as Black Hat Europe 2023 and various ISACs.

Daniel Frank
Threat Research Team Lead,
Palo Alto Networks

@powdertoastcat

Daniel Frank is the Threat Research Team Leader at Palo Alto Networks, with over a decade of experience. Frank previously worked in RSA Security, F5 Networks, and Cybereason. His core roles include researching emerging threats, reverse-engineering malware, threat hunting, and threat intelligence. Frank has a BSc degree in information systems.

Or Chechik
Principal Security Researcher,
Palo Alto Networks

@orchechik

Or Chechik is a Principal Security Researcher at Palo Alto Networks, with almost a decade of experience and a BSc in Computer Science. He is passionate about low level research, threat research and vulnerability research.

Patrick Staubmann
Team Lead Threat Research, VMRay

@sm4sh1t

Patrick Staubmann joined VMRay as a threat researcher back in 2019 and took over the lead position of the threat analysis team in 2023. As part of the Threat Analysis team, he continuously researches the threat landscape and conducts analyses of malware samples in depth. To further improve the companies' product, he also extends its detection capabilities in form of behaviour-based rules, YARA rules, and configuration extractors. He is especially interested in reverse-engineering, low-level system security and exploitation.

Pol Thill
Cyber Threat Investigator

@tr3gleos

Pol Thill lives for the hunt! Be it nation-state adversary or eCrime actor, he will explore any means to expose their operations and unmask the individuals hiding behind the digital veil. Drawing upon this expertise, Pol has held different Threat Intelligence positions as well as lead the Luxembourgish cybersecurity team. Cybercriminal investigations are what he thrives for.

Stuart Wiggins
Strategic Threat Advisor, Crowdstrike

Stuart has spent over 15 years working in cyber intelligence and is a champion for using threat intelligence to improve cyber defences and reduce the impact of malicious cyber activity. His role as a Strategic Threat Advisor at CrowdStrike to be an intelligence evangelist, helping to guide customers through all aspects of threat intelligence. Prior to CrowdStrike, Stuart started his career as an intelligence analyst in the UK Intelligence Community and has worked in a number of operational, tactical and strategic roles covering a variety of national security and cyber security related topics, including a three-year posting the to the United States where he worked with several U.S. Federal Government agencies.

Alemdar Islamoglu
Senior Staff Security Intelligence Researcher, Lookout

Alemdar Islamoglu is a security intelligence engineer at Lookout who focuses on mobile threats and related threat actors. He has prior experience in reverse engineering, pentesting, and security software development. He also enjoys organizing and participating in capture the flag competitions when he can find the time.

SPEAKERS CONTINUED

Tom McElroy
Principal Threat Intelligence Analyst, Microsoft

Tom is a Principal Threat Intelligence Analyst with the Microsoft Threat Intelligence Center (MSTIC) where he leads a team of Europe based analysts working to counter nation-state threats. Tom has over a decade of experience tracking and disrupting nation-state threat actors and has also worked in security research roles, with a particular focus on securing cloud environments. Prior to joining Microsoft Tom work in the UK NCSC.

Anders Nielsen
Senior Threat Intelligence Analyst, Microsoft

Anders is a Senior Threat Intelligence Analyst with the Microsoft Threat Intelligence Center (MSTIC). Anders has over a decade of experience tracking and disrupting nation-state threat actors. Prior to working at Microsoft, Anders worked in various threat intelligence roles within the Danish Government, NATO and the private sector.

Stephen Begley
UKI Red Team Lead, Mandiant

Dr. Begley is the Head of UK and Ireland Red teaming at Mandiant. He specialises in delivering engagements simulating threat actors breaking into and achieving their objectives in real-world environments. Prior to his two and a half years at Mandiant, Stephen spent six years as a consultant and then team leader in the Cyber Attack team at one of the Big 4 Consultancy firms. Before starting his career in cyber, Stephen completed a Masters and a PhD in experimental quantum computing, using trapped ions and photons of light to store and transmit quantum information.

Joseph Rooke
Director, Recorded Future

@JosephRooke

Joseph is Director of Advisory Services at Recorded Future. The team helps clients build intelligence driven security programmes as well as help clients monitor emerging threats.

Prior to joining Recorded Future he worked at BAE Systems on defence programmes and then transitioned to being a Threat Intelligence Analyst tracking nation state cyber threat actors, linking their activity to geopolitical developments. He also spent time working in the Middle East.

In his spare time he also serves as a Reservist with the British Military.

Rebecca Taylor

Threat Intelligence Knowledge Manager,
Secureworks

@RTaylorCyber

Rebecca joined Secureworks in 2014, where she developed an immediate passion for cybersecurity. Rebecca quickly expanded her cyber acumen, working across a variety of roles including Business Operations and Incident Command, finally moving into Secureworks first Threat Intelligence Knowledge Manager role in 2022 within the Counter Threat Unit.

Rebecca is primarily focused on the implementation of knowledge management processes and procedures for the Counter Threat Unit, the ingestion and management of Secureworks Threat Intelligence knowledge, and its associated quality, storage and maintenance.

Rebecca is also an advocate for all things Diversity, Equity and Inclusion, building inclusive best practices not only into the way she works, but also speaking frequently at events, supporting podcasts, offering mentoring and STEM talks, and creating content with a view to showing how Cybersecurity can be an inclusive space for underrepresented groups. Rebecca has been acknowledged in industry for her contributions, most recently winning 'Security Woman of the Year' at the Computing' Security Excellence Awards 2024.

THANK YOU TO OUR EVENT PARTNERS AND SPONSORS

SECURE IMPACT

SPINNING FOX

LUX
TECHNICAL

NOVOTEL
HOTELS & RESORTS

SPONSORS
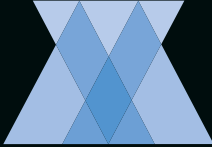
Led by pioneers of advanced threat dtection, VMRay develops best-of-breed technologies to detect and analyze malware and phishing threats that others miss. VMRay empowers organizations to accelerate analysis and response, automate security tasks, and build their own threat intelligence by providing the world's best detection and analysis platform for challenging security threats.

At VMRay, our purpose is to liberate the world from undetectable digital threats. Led by reputable cyber security pioneers, we develop best-of-breed technologies to detect and analyze unknown, evasive, and sophisticated threats that others miss.

We empower organizations to accelerate analysis and response, automate security tasks, and build their own threat intelligence by providing the world's best detection and analysis platform for malware and phishing threats.

VMRAY

PLATINUM SPONSOR

Google Cloud Security

Transform your cybersecurity with frontline intelligence, expertise and AI-powered cloud innovation. With Google Cloud, you can prevent, detect, investigate and respond to security incidents before they impact your business, and build on the most trusted, secure cloud to drive your organisation's digital transformation.

PLATINUM SPONSOR

SPONSORS

CROWDSTRIKE

GOLD SPONSOR

CrowdStrike, a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

SECURE IMPACT

SILVER SPONSOR

Secure Impact is a boutique cyber security consultancy offering bespoke services to a range of organisations, from national security to fintech. We bring to each client, globally renowned experts, including SANS instructors, to ensure they achieve greater success and resilience within their security programmes through pioneering expertise. Our services are wide ranging based on client needs, and include Executive and Technical Tabletops, intelligent penetration testing, SOC maturity assessments and cloud security assessments.

SPONSORS

SILVER SPONSOR

eShard is a leader in chip security testing and binary analysis, offering advanced software for security testing, lab upgrades, and security evaluations. With esDynamic for side-channel analysis, fault injection, and failure analysis, and esReverse for vulnerability research and malware analysis, we go beyond delivering tools. Our turnkey solutions transfer expertise, empowering teams to build internal knowledge, make informed decisions, and proactively manage cyber risks.

SILVER SPONSOR

Inzpire is a dynamic UK-based company specialising in innovative training, technology solutions and consultancy for defence, aerospace, and security sectors. Focussing on enhancing operational effectiveness, Inzpire offers a range of cyber security services aimed at protecting organisations from digital threats, including risk assessments, immersive exercising, incident response planning, and training programmes.

BRONZE SPONSOR

New UK company CIA provide premium advisory services, delivering outcomes and strategy for C-Suite to Operations teams. +17yrs SecOps subject matter experts globally.

Sandboxing reinvented
for the threats of today -
and tomorrow.

VMRAY

The world's most advanced technology
to analyze unknown, evasive & targeted
malware & phishing threats.
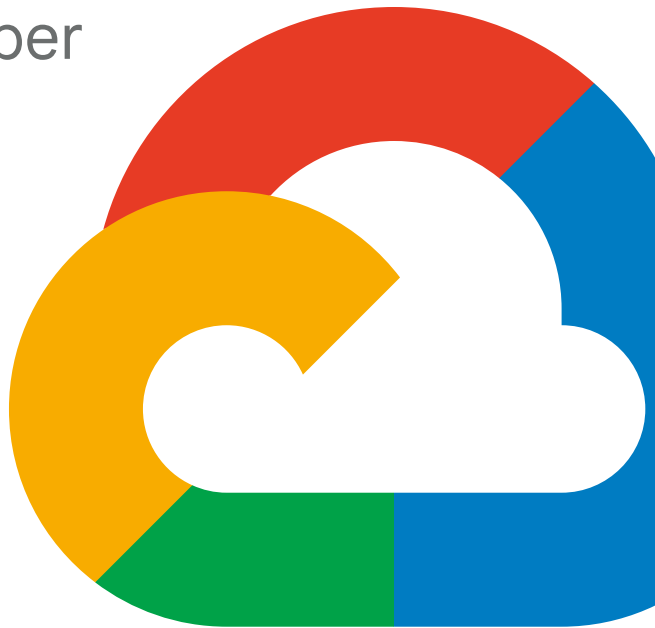
CROWDSTRIKE

2024 THREAT HUNTING REPORT

KNOW THEM. FIND THEM. **STOP THEM.**

245+
adversaries tracked
globally by CrowdStrike

70%
YoY increase in adversary
exploitation of RMM tools

86%
of hands-on-keyboard attacks
were executed by eCrime actors

2024 THREAT HUNTING REPORT

Read the Report now

Redefining cyber security consultancy for *real results*

High-impact services, delivered by globally renowned experts and tailored to your risk profile

How we help organisations

// **Intelligent Penetration Testing**
Go beyond automated scans with rigorous, manual testing that uncovers vulnerabilities others miss and provides actionable insights to strengthen your defences.

// **Red Teaming**
Bespoke adversarial simulations tailored to real-world threats pertinent to your organisation, uncovering blind spots and testing your full attack surface – physical, digital, and human.

// **Executive and Technical Tabletops**
Scenario-driven tabletops led by global experts including SANS instructors. Designed to enhance decision-making, coordination, and resilience, we deliver actionable insights to strengthen preparedness and response.

// **And more**
From cloud security services to SOC maturity assessments and architecture reviews, we will work with you to deliver improvements across your security program.

Curious to see what truly *impactful* security consultancy looks like?

Offensive security services:
secure-impact.com/pentest

Wider consultancy services:
secure-impact.com

Contact Giorgia Cacace, General Manager to discuss your requirements:
gcacace@secure-impact.com

CIA

CYBER INTELLIGENCE & ADVISORY LTD

CIA: Trusted by leaders around the world

Who are CIA?

Cyber advisory services for all of your needs, by industry experts.
Security transformation with real outcomes is our business.
A British owned & run company.

Why CIA?

- SecOps Subject Matter Experts
- Business People Process Technology veterans
- Government and commercial expertise
- Outcomes of value defined by a client, on budget and on time

Example Services

- Virtual CISO, Board Advisor
- Threat model & Use Case workshops
- Metrics with meaning of value

Address

124 City Road
London
EC1V 2NX

Contact

+44 (0)20 3026 4626

www.ciauk.ltd

sales@ciauk.ltd

Company: 15898804
VAT: 475 8724 43

UK BUSINESS

SANS

35 Years of defining cybersecurity excellence

150+
Countries & Governments

400k+
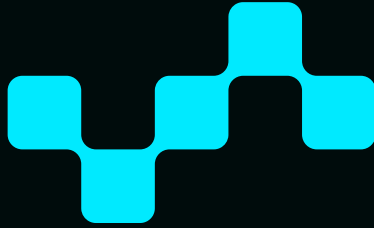Cybersecurity Practitioners

492
Fortune 500 Companies

230k+
Certifications granted by GIAC

*"SANS training, if not the best, is **one of the best in the industry**. I love everything about this class, labs and materials. I hope to take other SANS classes after this."*

- Rafael Mation, EY

Find out more
about SANS Institute

CYBERTHREAT

LONDON_2024

We very much value your feedback and opinion.

Please fill out the evaluation forms provided by
[clicking here] or scanning the QR code below.

National Cyber
Security Centre
a part of GCHQ

SANS | GIAC
CERTIFICATIONS