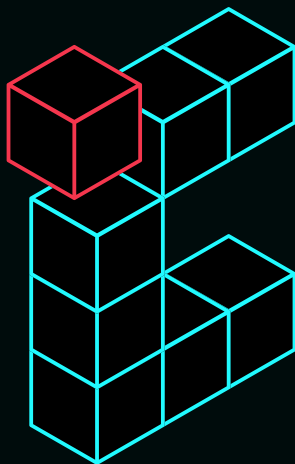


#CyberThreat23



CYBERTHREAT

20 - 21 NOVEMBER 2023
NOVOTEL LONDON WEST, HAMMERSMITH

WELCOME



Paul Chichester
Director of Operations,
National Cyber Security Centre

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

I am very excited to be co-hosting the 4th CyberThreat conference and I fully expect it to be the best so far. With each iteration the quality of submissions, the content and the overall engagement has grown, and this is down to you – our speakers, our delegates, our sponsors and all of those involved in making it a reality. Cyber defence is a team-sport and this is one amazing team – thank you!

Our collective responsibility is exemplified through the ongoing conflict in Ukraine and the unprecedented role which cyber operations are playing, with much of the battle occurring in the information space.

China's rise as a technology super-power poses an epoch-defining challenge for our national security. Throughout 2023, we have continued to see evidence of China state-affiliated cyber actors deploying sophisticated capability to pursue strategic objectives which threaten the security and stability of UK interests.

In parallel, we continue to track wider threats and persistent cyber-crime actors, adversary tactics, techniques and procedures continue to evolve and Artificial Intelligence is starting to add a new level of complexity.

These challenges are global and systemic, and close collaboration with allies, industry and academia will be crucial to further develop our understanding of the cyber capabilities threatening the UK and our ability to defend against them.

At the heart of this is a skilled, motivated and cohesive cyber defence community – this is the purpose and ethos of CyberThreat and it is great to see so many returning delegates and speakers alongside those joining us for the first time – welcome and enjoy!



Stephen M Jones
Managing Director UK and
Nordics, *SANS Institute*

We are back – bigger and better than ever!

It's so great to return to London for the 4th 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 advancement such as AI inevitably leads 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

AGENDA
SPEAKERS
EVENT PARTNERS
SPONSORS

AGENDA

To view the latest Agenda,
[click here](#) or scan the
QR code below:



CONTACTS



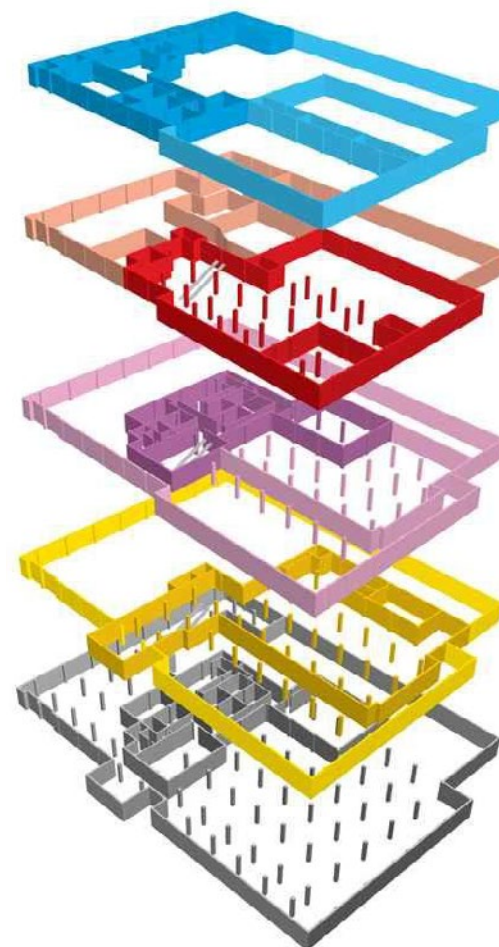
Ollie Stebbings
Head of Summits EMEA,
SANS Institute
ostebbing@sans.org
+44 7799 768 600



Hazel Postma
Summits Content Development Manager,
EMEA, SANS Institute
HPostma@sans.org
+44 7442 509 215

For in-person and live online event
queries please email:
cyberthreat@sans.org
or call:
+44 203 384 3470

VENUE MAP



SECOND FLOOR



FIRST FLOOR CYBERTHREAT CHAMPAGNE SUITE

REGISTRATION
MAIN CONFERENCE AREA
SPONSOR AREA
CATERING
RETRO AND MODERN GAMING
FLIGHT SIMULATOR
SCHOOLS AREA 1
CTF101



MEZZANINE FLOOR



GROUND FLOOR CYBERTHREAT CHABLIS SUITE

LUNCH AREA
SCHOOLS AREA 2




LOWER GROUND FLOOR

CAR PARK

SPEAKERS

James Lyne

Chief Technology
& Innovation Officer,
SANS


 @jameslyne



James Lyne is SANS' Chief Technology and Innovation Officer and has worked with many organizations on security strategy, handled a number of severe incidents and is a frequent industry advisor. He is a certified instructor at the SANS Institute and is often a headline presenter at industry conferences. James has been featured on many TV programs explaining security issues and delivered multiple TED talks. With a rich background in security across disciplines, James today is most enthused about using technology to build amazing ways for people to practice their skills and learn.

Paul Chichester

Director of
Operations, NCSC

 @OxChich



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.

Sophia N


Deputy Head of IM,
NCSC



Sophia is the Head of Incident Management at the National Cyber Security Centre where she coordinates the NCSC and cross government response to nationally significant cyber incidents.

Ollie Whitehouse

Chief Technology
Officer, NCSC

 @ollieatnowhere



Key Note Speaker

Ollie Whitehouse is the CTO of the UK's National Cyber Security Centre where he helps maintain the NCSC's role as the National Technical Authority for cyber security. Ollie's career spans over 27 years in applied cyber attack and defence combined with over a decade of private and public sector executive and advisory positions.

His operational tenures include over ten and half years at NCC Group where he was Group CTO, BlackBerry and Symantec. Ollie has given oral evidence to the UK Parliament Joint Committee on the National Security Strategy twice in 2017 and 2022 on matters related to cyber security.

Juan Andrés Guerrero-Saade

AVP, SentinelLabs at
SentinelOne

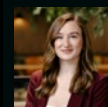


Key Note Speaker

Juan Andrés Guerrero-Saade is AVP of SentinelLabs at SentinelOne and an Adjunct Professor at Johns Hopkins SAIS Alperovitch Institute. 'JAGS' was Chronicle Security's Research Tsar, co-founder of Stairwell, Principal Security Researcher at Kaspersky's GREAT, and worked as a Senior Security Advisor to the Government of Ecuador. His joint work on Moonlight Maze is now featured in the International Spy Museum's permanent exhibit in Washington, DC.

Ellie Watts

Security Consulting
Manager, Accenture



Ellie's Psychology degree, gained in her home country of England, was an unlikely springboard into a career in cyber security.


Despite no traditional technical background, a deep-rooted interest into the weird and wonderful aspects of human behaviour navigated her into her first cyber role in social engineering simulation, training, and awareness. This led to delivering complex security behaviour uplift programs to enterprise organisations across the globe.

Particular professional highlights include a personal record of one million simulated phishing emails sent to one client in a year, and running round a bank in South Africa scattering USB sticks, aiming to see who would plug it in and click the totally legitimate looking file labeled 'EMPLOYEE PERSONAL BONUSES'.

Since then, one move across the pond later, Ellie has worked in the MxDR space in Australia delivering capability and service uplift for clients across the Asia Pacific region. Most recently, Ellie is now truly gaining an insight into the width and breadth of human behaviour, leading client delivery in APAC for cyber incident response, crisis management, and cyber incident readiness and preparedness services at Accenture.

Patrick Staubmann

Threat Researcher,
VMRay


 @sm4sh1t

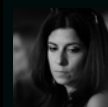


Patrick Staubmann joined VMRay as a threat researcher back in 2019. As part of the Threat Analysis team, he continuously researches the threat landscape and conducts analyses of malware samples in depth. To further improve the companies' product, he also extends its detection capabilities in form of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

Ifigeneia Lella

Cyber Security Officer,
ENISA

 @ifigeneialel



Ifigeneia Lella joined ENISA in 2016 as Cybersecurity Officer. Initially, she has been in charge of EU wide cyber exercises such as Cyber Europe 2018 and is currently engaged in the preparation of the 2022 edition of the event.

SPEAKERS CONTINUED

Thomas Griffith

Senior Threat Intelligence Analyst, Microsoft



Thomas is a senior threat intelligence analyst at Microsoft and primarily focusses on state or state sponsored cyber threat activity targeting Microsoft and Microsoft's customers within the 'MSTIC' team. Prior to Microsoft, Thomas's experience in the public sector included malware reverse engineering, network analysis, incident response and developing strategic relationships.

Daniel W

NCSC



Dan C

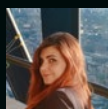
Incident Management Deputy Technical Director, NCSC



Sveva Vittoria Scenarelli

Cyber Threat Intelligence Manager, PwC

@cyberoverdrive



Sveva is a Cyber Threat Intelligence Manager at PwC. Her focus is on tracking advanced persistent threats based in North Korea and China, spanning malware and infrastructure analysis and intrusion clustering. Sveva holds industry-recognised certifications in Threat Intelligence and Malware Reverse Engineering, and has presented her research at several international conferences including BlackHat, VirusBulletin, CONFidence, and CyberThreat. Sveva's passion is to deep-dive into the activity of threat actors over time, to highlight how they change techniques and targeting, and what defenders can do about it.

David Greenwood

Product, EclectIQ



David Greenwood helps early stage cyber-security companies to build products that make users go; "Wow! That's what I need!".

During his career he has worked with great minds at Splunk and Anomali. David currently works at EclectIQ building world-class threat intelligence solutions.

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 co-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.

Stuart Wiggins

Strategic Threat Advisor, CrowdStrike



Stuart has spent over 14 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.

Mathias Frank

Principal Incident Response Consultant, Mandiant, part of Google Cloud



Mathias is a Principal Incident Response Consultant in Mandiant's UK office and delivers emergency response services for clients facing security breaches. He specialised in providing enterprise-scale Incident Response operations for sophisticated network intrusions. Mathias has led organisations and government bodies in responding to breaches by highly-sophisticated adversaries such as nation-state sponsored espionage actors and cybercriminals aiming to extort or ransom victim organisations.

Lior Rochberger

Security Researcher, Palo Alto Networks


@lior_rochberger



Lior Rochberger is a senior threat researcher at Palo Alto Networks, focusing on threat hunting and malware research. Lior began her career as a team leader in the security operations center in the Israeli Air Force, where she mostly focused on incident response and malware analysis.

SPEAKERS CONTINUED

Rowland Corr

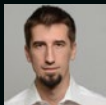
Vice President & Head of Government Relations, Enea AB (formerly AdaptiveMobile Security Limited)
 @RowlandCorr



Rowland Corr is Vice President Government Relations at Enea where he helps cybersecurity agencies, regulators, and other government stakeholders to evolve and execute their national cybersecurity strategies. Rowland participated as an expert in a public hearing of the European Parliament's PEGA Committee of Inquiry to investigate Pegasus and equivalent surveillance spyware in 2023.

Nazar Tymoshyk


Lead Specialist, CERT-UA



Nazar Tymoshyk is a Ph.D. and a seasoned cybersecurity professional with over 22 years of experience in enterprise security. He specializes in cyber defense, particularly in incident response and post-breach recovery, as well as modern security architecture, blue and purple teaming.

As CERT UA member, he specialized in incident response, intrusion research, and threat hunting, tracking adversary behaviors and intrusions by various APTs.

Daniel Frank

Principal Threat Researcher, Palo Alto Networks
 @powdertoastcat



Daniel Frank is a Principal Threat Researcher at Palo Alto Networks, with over a decade of experience. His core roles as a Threat Researcher include researching emerging threats, reverse-engineering malware, threat hunting, and threat intelligence. Frank has a BSc degree in information systems.


Ertugrul Kara

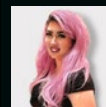
Sr. Product Marketing Manager, VMRay



Ertugrul Kara is the Senior Product Marketing Manager for VMRay. With a career spanning over 10 years in cybersecurity, he has seen the advancement of security products from open-source firewalls to automation-powered threat detection technologies following the evolution of threat landscape. He is currently focused on leading the marketing efforts for VMRay's security automation solutions while enhancing the alignment between the products with enterprise customer needs. Previously, he has held various roles in early-stage security startups, led the product launch and growth strategies, and run his own startup specialized in network security. Ertugrul attended the Middle East Technical University for undergraduate studies where he earned his bachelor's degree in Aerospace Engineering.

Charlotte Hooper

Helpline Manager, The Cyber Helpline
 @_cyberbarbie

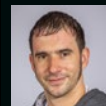


Charlotte is the Helpline Manager at The Cyber Helpline and has supported thousands of victims of cybercrime and online harm, specialising in cyberstalking and technology-facilitated intimate partner violence. On top of her role at The Cyber Helpline, Charlotte has a first-class degree in Policing and Criminal Justice and a masters degree in Cybercrime Investigation. Charlotte delivers cybercrime related training sessions around the world for police forces, victim support charities and private organisations.

Her areas of expertise include: Cybercrime investigations, cybercrime law enforcement & regulation, open-source intelligence, cyberstalking & online harassment, the cybercrime & online harm threat landscape and the impact of cybercrime on victims.


Paul Moon

Senior Manager Technical Analysis Cell, CrowdStrike



Paul Moon is the Senior Manager of the Technical Analysis Cell (TAC) in the CrowdStrike Intelligence team. He manages four teams of malware reverse engineers specialising in targeted intrusion and eCrime threats covering multiple architectures and including adversary use of vulnerabilities, mobile applications and cloud. Previous to managing Paul was a principal security researcher on the team focused on reversing samples from targeted intrusion adversaries.

Saher Naumaan

Principal Threat Intelligence Analyst, BAE Systems Digital Intelligence
 @saffronsec

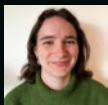


Saher Naumaan is a Principal Threat Intelligence Analyst at BAE Systems Digital Intelligence. She currently researches state-sponsored cyber operations with a focus on threat groups and activity originating from Iran and North Korea. Saher regularly speaks at public and private conferences around the world and is a former European Cyber Conflict Research Initiative (ECCRI) fellow. She is also the creator and organiser of RESET (2018 and 2019), the first cybersecurity conference in Europe with an all female line-up.

SPEAKERS CONTINUED

Molly Elliott

Threat Intelligence Analyst, BAE Systems Digital Intelligence



Molly Elliott is a Threat Intelligence Analyst at BAE Systems Digital Intelligence. She maintains a research focus on Iran-based threat groups, and cyber operations during Russia's invasion of Ukraine. She has a background in international relations, and specialises in analysis covering the intersection of geopolitics and cyber operations.

Marcus Hallberg

Security Engineer, Spotify

@monrava89



Marcus is a security engineer at heart, and works for Spotify in Stockholm, Sweden.

He spends his time with cybersecurity detection and response where he has a passion for finding new ways to automate workflows and cross-cloud incident response and forensics.

When he has time off, he enjoys rock climbing, folk dancing and cross-country skiing.

Jamie Collier

Senior Threat Intelligence Advisor, Mandiant Intelligence, Google Cloud

@TheCollierJam



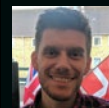
Dr Jamie Collier is a Senior Threat Intelligence Advisor at Mandiant, part of Google Cloud. He works with organisations in the EMEA region to help them understand their threat landscape and build threat intelligence capabilities. He was previously the Cyber Threat Intelligence Team Lead at Digital Shadows. Based in London, Jamie has presented at numerous conferences in Europe and the Middle East, and his commentary is regularly included in media reports (including Bloomberg, The Wall Street Journal, and The Guardian).

Jamie leads on Mandiant's academic engagement within EMEA and he remains active as a researcher. He previously completed a DPhil (PhD) in Cyber Security at the University of Oxford, where he focused on the diffuse nature of cyber security provision and its implications for global politics. Jamie was also previously based at MIT as a Cyber Security Fulbright Scholar and involved in the University of Oxford Centre for Technology and Global Affairs as a Research Affiliate. His research is published in several journals, book chapters, and conference papers.

Jamie has previous experience working with the NATO Cooperative Cyber Defence Centre of Excellence, Oxford Analytica, and PwC India. He remains passionate about improving cyber security career pathways and building better collaboration between operational and strategic communities within the security industry.

Jay Christiansen

Senior Consulting Manager, Mandiant, Google



Jay leads the Mandiant EMEA Red Team and their advanced capability project "APT66". In this role he coordinates, plans and executes the Adversarial Emulation engagements in the region alongside a team of experienced Red Teamers, and develops strategy and milestones for the group developing custom malware and implant capabilities, as well as adopting threat actors TTPs. Recently, the team focus has been on expanding more complex Purple team engagements as well as OT/ICS advancements around the CNI sector.

Magpie Graham

Technical Director of Intelligence, Dragos, Inc.



With over 17 years' experience in cyber security, Magpie has engineered and architected multiple generations of pan-government IDS, reversed sophisticated nation-state malware and tracked state-sponsored actors from around the globe. As Technical Director leading Capability Development in the Dragos Intel Team, he sets strategic requirements for the systems and data acquisition required to fuel a top-tier Threat Intelligence cell, as well as delivering tactical solutions to surface findings through automation and enable Hunters to find threats more efficiently across huge volumes of data.

Prior to joining Dragos he led a team of threat intelligence analysts at Microsoft, focused on tracking groups from Eastern Europe and Russia. Prior to this, Magpie served with the UK NCSC, tracking nation states threat to UK Critical National Infrastructure.

Dagmar Heidecker

Consultant, Microsoft

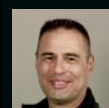


Dagmar Heidecker works as a Principal Consultant for Microsoft's Compromise Recovery team. An essential part of this role is to quickly figure out whether PKI has been actively abused during an attack or has vulnerabilities or misconfigurations which might allow attackers to strike back. Working in this area for many years, she has analyzed many attacks against PKI, Active Directory, Azure and other types of infrastructures.

Dagmar's first point of connection with PKI was during writing her master thesis in the 1990s. Since then, PKI always has been part of her work.

Andreas Luy

Consultant, Microsoft



Andreas Luy is a Principal Consultant for Microsoft's Compromise Recovery team. An essential part of this role is to quickly figure out whether PKI has been actively abused during an attack or has vulnerabilities or misconfigurations which might allow attackers to strike back.

Andy started started his career in Microsoft more than 20 years ago and before moving to Compromise Recovery, he worked in different proactive roles, always having IT security in mind and helping customers in strengthening their IT infrastructure. PKI has been his passion since Active Directory Certificate Services were introduced back in the year 2000.

Thank you to our event partners and sponsors



SPONSORS

VMRay Platinum Sponsor



VMRAY

VMRay's solutions for automated detection and analysis of advanced threats close detection gaps in the organization's existing security stack and help security teams to handle the growing volume of security alerts with far greater speed and precision.

CrowdStrike Platinum Sponsor



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

Mandiant Gold Sponsor



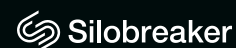
Mandiant's trusted effective security is based on the right combination of expertise, intelligence, and adaptive technology, the Mandiant Advantage SaaS platform scales decades of frontline experience and industry-leading threat intelligence.

Dragos Gold Sponsor



Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The Dragos Platform offers the most effective industrial cybersecurity technology, giving customers visibility into their ICS/OT assets, vulnerabilities, threats, and response actions. The strength behind the Dragos Platform comes from our ability to codify Dragos's industry-leading OT threat intelligence, and insights from the Dragos services team, into the software. Our community-focused approach gives you access to the largest array of industrial organizations participating in collective defense, with the broadest visibility available. The strength behind the Dragos Platform comes from our ability to codify Dragos's industry-leading OT threat intelligence, and insights from the Dragos services team, into the software.

Silobreaker Silver Sponsor



Silobreaker is a SaaS platform that enables threat intelligence teams to produce high-quality and relevant intelligence at a faster pace. It brings all the steps of the intelligence cycle together in one place to cover cyber, physical and geopolitical PIRs and automates all the manual work, so your analysts can focus on finding and prioritising threats faster and producing higher quality intelligence – and stakeholders can make better-informed, intelligence-led, decisions to reduce risk and protect revenue.

River Security Silver Sponsor



Established in Norway in 2020, River Security is reshaping the cybersecurity realm. Leading in technological innovation, we utilize our distinctive Attack Surface Management tech combined with continuous penetration testing to address evolving threats. Renowned for our exceptional service and actionable reporting, we've cultivated lasting bonds with clients who regard us as their premier offensive cybersecurity partner. Our signature service, Active Focus, merges cutting-edge technology with human expertise, providing clients with invaluable insights into their attack surface.

Secure Impact
Silver Sponsor

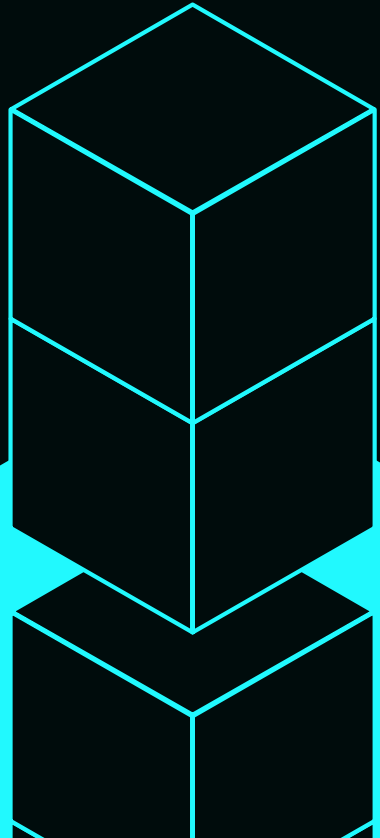
SECURE^{*}
IMPACT

In an industry that's noisy, commoditised and compliance-driven, you need cyber security partners who can add value and create real outcomes for your organisation. Secure Impact (SI) offers world-class penetration testing & security assessment services geared towards your security objectives and bespoke risk profile, and detailed, accessible reports that allow you to make immediate actionable changes to improve your security posture.

SentinelOne
Silver Sponsor



SentinelOne is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. The Singularity Platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.





We take pride in being
a cybersecurity leader.

**When we're #1,
our customers
win.**

#1

**XDR | EDR | MDR
Incident Response**

CrowdStrike is continually recognized as a leader by analysts, evaluators
and customers. Learn more at crowdstrike.com/leader.



VMRAY

➤ The Industry's Most Advanced Technology For **Malware and Phishing Analysis** ◀

- ♦ Accelerate Alert Triage, Investigation, and Validation Gain
- ♦ Comprehensive Understanding of Malware Behaviour
- ♦ Identify Zero-Day Malware and Evasive Threats
- ♦ Generate Actionable Threat Intelligence
- ♦ Accelerate Incident Response and Mitigation

vmray.com

Check out our community portal with over 200,000 malware analysis reports:
threatfeed.vmray.com



MANDIANT[®]

NOW PART OF Google Cloud

www.mandiant.com



Dragos is the Industrial Cybersecurity company on a relentless mission to safeguard civilization!

In a world of rising cybersecurity threats, Dragos protects the most critical infrastructure — those that provide us with the tenets of modern civilization — from increasingly capable adversaries who wish to do it harm. Devoted to codifying and sharing our in-depth industry knowledge of ICS/OT systems, Dragos arms industrial defenders around the world with the knowledge and tools to protect their systems as effectively and efficiently as possible.

visit our stand / contact us
(saleseurope@dragos.com)

SANS

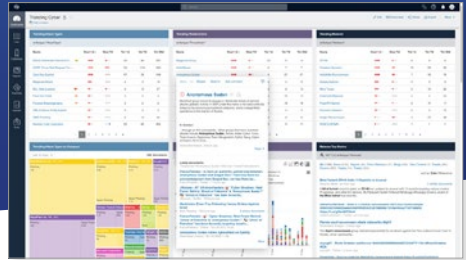


National Cyber
Security Centre

DRAGOS[®]

Make Intelligence-led Decisions. Faster

Deliver relevant, actionable intelligence to mitigate risk and improve cyber resilience.



Uncover relevant intelligence from millions of open and dark web sources, at scale



Connected analysis and reporting, in a click



Unlock cyber, physical and strategic risks, in a single console



Protect your organisation from brand threat abuse

Reduce risk faster and with fewer tools

86%

Faster actionable intelligence

Accelerate the intelligence cycle with a single workflow providing aggregation, contextualisation and dissemination of intelligence tailored to your environment.

27%

Improved analyst productivity

PIR-led AI and automation make it faster and easier for analysts to pinpoint and analyse relevant risks and communicate clear and timely insight.

401%+

Return on investment

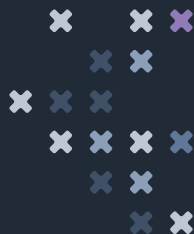
Answer more security use cases with a single tool, streamline operational costs and improve decision-making from more actionable intelligence.

Source: ESG Economic Validation, Analyzing the economic benefits of the Silobreaker security intelligence platform



SECURE IMPACT

Your security team.



Cyber security services which drive real business outcomes.

We don't do commoditised scans, tick box exercises, or generic reports. Instead, our GIAC-certified team will help you to develop your security posture and create real business outcomes through collaborative offensive and defensive engagements.

From penetration testing to consultancy to DFIR, we promise services which are bespoke to your risk profile, and geared to achieving your security objectives. We partner with CISOs and security teams from the FTSE 100 to VC-backed scale-ups, creating shared learning outcomes for our clients, and developing a roadmap to improve their cyber security maturity.



To discuss how we can partner with you, please contact Georgia Cacace:
gcacace@secure-impact.com



SI OFFENSIVE

- Penetration testing
- Red team assessment
- Purple team assessment
- Security assessment
- Cyber due diligence



SI DEFENSIVE

- Digital forensics
- Incident response
- Digital footprint service
- Blue team assessments
- Incident response planning



SI CONSULTING

- CISO for a day
- Cyber range exercises
- Tabletop exercises
- Bespoke consultancy

A man in a dark SANS shirt is pointing his right hand towards a screen. The screen displays technical diagrams, including a stack of layers labeled 'K', 'E', 'R' and 'Applications', and a diagram with '0x0' and '0x1' labels. The background is dark blue with a subtle pattern of binary code and technical terms.

SANS

**The most trusted
resource for
information security
training,
cybersecurity
certifications and
research.**

“

**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

**View the Upcoming SANS Training Events in the UK:
www.sans.org/u/1tn0**

emea@sans.org | +44 203 384 3470 | sans.org/uk

PROACTIVE CYBER SECURITY KNOW YOURSELF



3 STEPS TO PROACTIVE CYBER SECURITY

MAP OUT
DIGITAL
ATTACK
SURFACE

01

DISCOVER
CHANGES TO
ATTACK
SURFACE

02

PENETRATION
TEST ALL
CHANGES

03

ACTIVE[®]

FOCUS



#ProactiveCyberSecurity

#AlwaysOnPentesting

#AttackSurfaceManagement

- Continuously identifies **vulnerabilities** and **threats** to the digital environment
- Provides a **complete** and continuous **overview** of a company's external attack surface
- Supported by "Innovation Norway" and "The Research Council of Norway"
- Aligned with **CIS18 Critical Security Controls**
- Ideal and **unique** combination of automated processes and **expert** assessments
- Utilizes a broad **technological toolbox** and **self-developed** scripts



RIVER

SECURITY

Thank you for attending



CYBERTHREAT

We very much value your feedback and opinion.

Please fill out the evaluation forms provided by [clicking here](#)
or **scanning the QR code** below:

