AGENDA

CYBERTHREAT 2022

DAY 1 - MONDAY 16 JANUARY 2023 (GMT)

08:00 - 10:00	**Registration and Networking**	LIVE IN LONDON
10:00 - 10:15	**Opening Remarks** **James Lyne**, Chief Technology Officer, SANS Institute **Paul Chichester**, Director of Operations, NCSC **Katie Nickels**, Certified Instructor, SANS Institute	LIVE IN LONDON LIVE ONLINE
10:15 - 10:55	**Keynote - An overview of the current attacks on Ukrainian infrastructure in 2022 and incident responses carried out by CERT-UA.** **Yevhen Bryksin**, Deputy Chief of the Computer Emergency Response Team of Ukraine (CERT-UA), The State Cyber Protection Centre of the State Service of Special Communication and Information Protection of Ukraine **Viktor Zhora**, Deputy Chairman and Chief Digital Transformation Officer, The State Service of Special Communication and Information Protection of Ukraine **Yevheniia Volivnyk**, Chief of the Computer Emergency Response Team of Ukraine (CERT-UA), The State Service of Special Communication and Information Protection of Ukraine **This talk will be dedicated to the overview of the current attacks on Ukrainian infrastructure in 2022 and incident responses carried out by CERT-UA. We will share tactics and instruments used by the attackers when targeting governmental institutions and infrastructure as well as challenges when conducting cyber investigations and interacting with affected organizations.**	LIVE IN LONDON LIVE ONLINE
11:00 - 11:25	**Emerging threats against cloud application identities and what you should do about it!** **Yochana Henderson**, Identity Program Manager, Microsoft	LIVE IN LONDON
11:30 - 12:30	**CTF & CTF 101** **All registered teams to assemble in the designated pods.** **CTF 101 - A chance for attendees new to Capture The Flag challenges to hear from the technical team that develop our challenges and to learn about the tools and approaches commonly used to solve them. A great preparation for tackling this year's CTF.**	LIVE IN LONDON
11:40 - 12:00	**A case for data-driven cybersecurity orchestration and automation: what it is, what challenges it addresses, and how it handles them?** **Leon Ward**, VP of Product Management, ThreatQuotient **One major use case for SOAR, and orchestration in general, is to ease the burden of rote manual tasks that are required to investigate and respond to a threat. ThreatQuotient recently undertook market research in the UK around security automation yielding interesting results and some actionable information. In this talk, Leon Ward, VP of Product Management at ThreatQuotient will introduce those survey highlights, and the importance of moving from an orchestration-based reactive posture to an automation-based anticipatory posture. What is the difference between a sequential playbook vs. a continuous security operations activity. He will develop the following:** • **Data automation to best anticipate risks according to your maturity** • **How to protect yourself from future threats through automated retrospective analysis** • **How to improve the efficiency, time savings and coordination of CTI teams**	LIVE IN LONDON LIVE ONLINE

National Cyber Security Centre
a part of GCHQ

SANS

12:00 - 12:10	**Think Like an Attacker: The Importance of ASM in Cloud Security** **Nick Miles,** Director Channel Partners, EMEA, Censys Cyber attackers are crawling the Internet constantly, looking for any vulnerabilities to exploit within organizations' Internet-facing and cloud assets. Organizations and their security teams implement cloud data protection solutions, but unknown — and unsecured — assets remain. How can companies prevent and protect from attacks in a comprehensive way? They need to think like an attacker.	LIVE IN LONDON LIVE ONLINE
12:10 - 12:20	**Intelligence Requirements on the Fly** **Jamie Collier**, Senior Threat Intelligence Advisor, Mandiant Intelligence, Google Cloud **Shanyn Ronis**, Senior Manager, Mandiant Intelligence, Google Cloud Standing intelligence requirements are crucial for any organisation looking to adopt a forward-leaning security posture. However many organisations either haven't developed requirements, or their existing requirements are so broad that security teams struggle to operationalise them. This talk outlines a few tactical steps organisations can take in order to develop requirements quickly and impactfully as a first step toward building a more robust intelligence apparatus.	LIVE IN LONDON LIVE ONLINE
12:30 - 13:00	**Leveraging Campaigns to Untangle the Threat Group Ship of Theseus** **Adam Pennington**, ATT&CK Lead, MITRE We have a wealth of intelligence on some of our adversaries, but what happens when we've combined so much into the same threat group that it's become unrecognizable? Many of us follow APT groups that have now been around for years or even decades, but like the Ship of Theseus a group might use no behaviors today in common with their activity a decade ago. We have a different but parallel problem with ransomware, affiliates of a group often act independently with few behaviors in common with each other. In both cases it's typical to pull everything we know together and track it under a single threat group, but we're losing information along the way that we could use for our defense. In this session, Adam will cover how we often combine wildly disparate intelligence related to threat groups and how that may be impacting defensive teams' ability to leverage that intelligence. He'll work though specific examples of threat groups that have undergone large changes over time and have many facets that have been commonly combined. Finally, Adam will share experiences from the MITRE ATT&CK team's efforts to improve our publicly available threat group profiles through the introduction of "campaigns" and restore some of the context that's been lost combining intelligence.	LIVE IN LONDON LIVE ONLINE
13:00 - 14:00	**Networking Lunch - Sponsored by Capital One** **Women and Allies in Cybersecurity** **Randi Kieffer,** Managing Vice President, Deputy Chief Information Security Officer Cyber, Operations & Intelligence, Capital One	LIVE IN LONDON LIVE ONLINE
14:00 - 14:25	**Information operations: Dispatches from the frontlines** **Martin Innes,** Professor, Security, Crime and Intelligence Innovation Institute, Cardiff University **Jack Stubbs,** Vice President of Intelligence, Graphika Researchers from Cardiff University and threat intelligence firm Graphika will present some of their latest findings on information operations conducted by suspected Russian threat actors in 2022. This will cover extensive activity related to the war in Ukraine and a coordinated effort to influence U.S. domestic audiences ahead of the midterm elections.	LIVE IN LONDON
14:30 - 15:30	**CTF** All registered teams to assemble in the designated pods.	LIVE IN LONDON

14:40 - 15:00	**Panel Discussion: Hoaxers and Hax0rs - Disinformation as a cyber threat** **James Lyne,** Chief Technology Officer **Martin Innes,** Professor, Security, Crime and Intelligence Innovation Institute, Cardiff University **Jack Stubbs,** Vice President of Intelligence, Graphika	LIVE IN LONDON
15:05 -15:25	**Why wait for zero days: Vuln4Cast** **Eireann Leverett**, Chief Technology Officer, Concinnity Risks Vulnerabilities will continue to appear, but we don't just have to react to them. We can predict their volume up to a year in advance +/8%. That's bound to get better, but we might be able to predict even more...how many will come from a specific vendor? How many will be CVSS > 7? How many will be network facing? Using these techniques we could make the blue team less reactive and more strategic. We could plan team sizes and simulate patching schedules. We can talk about how many vulnerabilities really matter, and how to get ahead of the problem.	LIVE IN LONDON LIVE ONLINE
15:30 - 15:50	**Networking Break**	LIVE IN LONDON
15:50 - 16:15	**Enterprise IR: live free, live large** **Erik Schamper,** Senior Security Researcher, Fox-IT (part of NCC Group) **Lennart Haagsma,** Senior Incident Handler, Fox-IT (part of NCC Group) At Fox-IT and NCC Group, we are always looking to push our incident response capabilities to the next level. Because no adversary, no matter how high-end, should be beyond our reach. This led to the development of "dissect", a proprietary enterprise investigation framework that we will now open source and share with the world. Dissect supports us, the analysts, from the moment of acquisition of artifacts, to normalisation and processing. Dissect frees us from limitations by data formats and platforms and takes away concerns about how to access investigation data. We can now focus on performing analysis, developing complex analysis plugins or performing research. You know, the cool stuff that we brag about on birthday parties. With dissect, we can go from intake call to patient zero in a matter of hours, even in infrastructures with thousands of systems. For example: we created a method to plug directly into a hypervisor and can now collect forensic data from virtual systems with zero downtime and effort, eliminating traditional software deployment bottlenecks. We're quite proud of that. Attendees will learn about dissect, its capabilities and our methodology. And afterwards they can dive right in, because everything is now open source!	LIVE IN LONDON
16:20 - 17:00	**Navigating the Tradeoffs of Cyber Attribution** **Jamie Collier,** Senior Threat Intelligence Advisor, Mandiant Intelligence, Google Cloud **Shanyn Ronis,** Senior Manager, Mandiant Intelligence, Google Cloud Attribution matters, but to what extent? The game of cyber whodunit is often perceived as a clean and binary question, where threat activity is either attributed or it is not. Yet, it is typically a more complex process that regularly involves difficult tradeoffs. Different forms of attribution — ranging from simply linking threat clusters together to identifying the names and faces of an adversary — present vastly different challenges and resource requirements. Analysts making attribution judgements must also weigh up several competing priorities, including the speed in coming to a conclusion, the completeness of data, and the confidence level behind their assessments. This talk lifts the lid on the messy realities behind attribution. We will provide a framework that outlines the different tradeoffs involved in the process and provide practical advice for network defenders and policymakers navigating the topic.	LIVE IN LONDON LIVE ONLINE
18:00 - 22:00	**Social Networking - Sponsored by ThreatQuotient**	LIVE IN LONDON

DAY 2 - TUESDAY 17 JANUARY 2023 (GMT)

08:00 - 09:00	**Networking**	LIVE IN LONDON
09:00 - 09:05	**Opening Remarks** **James Lyne**, Chief Technology Officer, SANS Institute **Paul Chichester,** Director of Operations, NCSC **Katie Nickels**, Certified Instructor, SANS Institute	LIVE IN LONDON LIVE ONLINE
09:05 - 09:45	**Keynote - What happened to cyberwar in Ukraine - a journalist's perspective** **Gordon Corera**, Security Correspondent, BBC News	LIVE IN LONDON LIVE ONLINE
09:45 - 10:10	**The Clustering Conundrum: A Behind-The-Scenes Look at Creating Threat Groups** **Katie Nickels,** Certified Instructor, SANS Institute The security industry is awash with an overwhelming volume of threat reporting—both public and private. We commonly bemoan the confusing opaque proliferation of named threat groups, but we rarely take the time to think about how and why they're created. In this talk, Katie will shine a light on the often-confusing world of threat groups, presenting real-life examples of how and why different teams classify and create threat groups. Katie will examine the inherent challenges of group creation, including how teams structure data, decide what constitutes "similar enough" activity, and evolve group definitions over time. Attendees will learn several strategies for classifying threats and creating groups so they can choose the methodology that works best for their team—and embrace the fun of clustering new threats!	LIVE IN LONDON LIVE ONLINE
10:15 - 10:40	**ENISA CYBERSECURITY Threat landscape Methodology and Ransomware Threat Landscape** **Ifigeneia Lella,** Cyber Security Officer, ENISA The cyber threat landscape is constantly evolving. The need for up to date and accurate information on the current cyber threat landscape is growing and is becoming key for assessing risks. To respond to this need, the European Union Agency for Cybersecurity (ENISA) introduces an open and transparent methodological framework to develop targeted as well as general reports, recommendations, analyses and other actions on future cybersecurity scenarios and threat landscapes. While increasing confidence in the services offered to attendees, with the present methodology the Agency aims to make available to all interested parties a method for generating their own cyber threat landscape by applying six principal steps. By adopting and adapting the proposed CTL approach, attendees can enhance their ability to build situational awareness, monitor and tackle existing and potential threats. A practical example of how the methodology is applied is the Ransomware threat landscape. The Ransomware report aims at mapping and studying the ransowmare that were discovered from May 2021 and April 2022 it will present trends and patterns observed since ransomware attacks have shown an increase for Q4 of 2020 and Q1 of 2021.	LIVE IN LONDON
10:40 - 11:00	**Networking Break**	LIVE IN LONDON
11:00 - 12:00	**CTF** All registered teams to assemble in the designated pods.	LIVE IN LONDON

11:10 - 11:30	**Deriving Insight from Upstream Threat Actor Infrastructure and Victimology** **Josh Hopkins,** Senior Cyber Analyst, Team Cymru From proactively hunting for attacker infrastructure, to placing the exploitation of vulnerabilities on a timeline often obscured by large spikes in activity. This talk will explore ways in which we can enrich our understanding of the threat landscape beyond that which is shared in threat feeds and reports.	LIVE IN LONDON LIVE ONLINE
11:30 - 11:40	**Initial Access Methods for Edge Devices** **Stuart Wiggins,** Strategic Threat Advisor, CrowdStrike Edge devices range from email servers to firewalls to collaboration tools and all have one thing in common: they are frequently exploited as an initial access point for adversaries to gain a foothold into a network. Due to their deliberate internet exposure edge devices area high risk area for enterprise networks. Understanding adversary TTPs and more importantly, how to proactively defend against them is increasingly important. This talk will review adversary tradecraft as observed by CrowdStrike in exploiting edge devices.	LIVE IN LONDON LIVE ONLINE
11:40 - 11:50	**What's beyond a hash? - Data Science Techniques for Analysing TLS Signatures** **Josh Cowling**, Solutions Architect, Splunk	LIVE IN LONDON LIVE ONLINE
12:00 - 12:30	**Operation CuckooBees: Exploring Winnti's Adventures in Windows CLFS** **Niv Yona,** Incident Response Director, Cybereason **Ofir Ozer**, Security Researcher, Palo Alto Networks Nation-state threat actors are often notorious for their evasive techniques and illusive trails that they leave behind. Among them, China stands out with innumerable successful operations, showcasing broad capabilities and novel approaches. In this talk, we will go over the Chinese-linked Winnti Group, AKA APT41, in their recent operation, abusing Windows' Common Log File System (CLFS) mechanism in a unique way, to hide their malicious payloads. We will start by walking down the history of this group, describing their motivation and evolution. Then, we will present our most recent tackle with the group; beginning with an innocent alert and progressing to a full Incident Response engagement, leading us to months of research. This research uncovered a multi-staged Cyber-espionage campaign that has stayed in the dark for years by leveraging the Windows CLFS mechanism as its hiding place. The presentation offers a unique glimpse into the Winnti intrusion playbook, covering the techniques that were used by the group from initial compromise to data exfiltration, including their latest undocumented and newly discovered payloads. Throughout this talk, we shall familiarize our audience with Winnti's TTPs, and present relevant ways to prevent such attacks in the future. We hope that by uncovering this story, blue teams will get more intimate with the group, to detect more operations like this in the future.	LIVE IN LONDON
12:30 - 13:30	**Networking Lunch**	LIVE IN LONDON

13:30 - 13:55	**Scaling Incident Response through Collaboration and Automation** **Dan C,** Incident Management Deputy Technical Director, NCSC **Matt H,** Principal Technical Lead for Industry, NCSC How the NCSC works with partners to proactively warn organisations targeted by threat groups and how you can help take this to the next level.	LIVE IN LONDON
14:00 - 15:00	**CTF** All registered teams to assemble in the designated pods.	LIVE IN LONDON
14:10 - 14:20	**Rethinking the bad Narrative (419 Prevention): a Nigerian experience** **Sadiq Nasir,** Project Manager, Netswitch limited There is a problem of Nigerian youth increasing getting involved in social engineering attacks for financial gain. The victims of this problems loose millions of dollars, also of the victims are in the global north. The presentation cover the depth of the problem, and the effects, it also seek to present alternative means of curbing the problem by getting various stakeholders involved in the process this cybersecurity mitigation.	LIVE IN LONDON LIVE ONLINE
14:20 - 14:30	**Overwhelmed By Malware and Phishing Alerts? Struggling to Identify Unknown Malware? Here is How to Speed Up Investigation and Response.** **Michael Bourton**, Senior Security Solutions Engineer, VMRay One of the greatest challenges for SOC and Incident Response teams is identifying advanced, unknown, highly evasive malware and targeted phishing quickly. Security teams are flooded daily with alerts from different sources and are expected to rapidly spot the "needles in a haystack" – the alerts that signal a real threat. Successful intervention depends on how fast an Analyst can determine which alerts are valid, and which alerts are time-wasting False Positives, only causing a drain on team resources. With the right tools in place, advanced threats and alert fatigue don't have to overwhelm your security teams.	LIVE IN LONDON LIVE ONLINE
14:30 - 14:40	**Tampering with airplane performance apps** **Alex Lomas,** Managing Security Consultant, Pilot Electronic Flight bags (EFBs) are typically tablet computers that the pilots use to work out how much power to use in order to safely and efficiently take off and land. We'll demonstrate vulnerabilities in several popular EFBs, then show how these security flaws can be exploited to jeopardise the safety of a flight. Numerous incidents, some involving hull losses, have occurred over recent years as a result of mistakes or misinterpretation of EFB data. Real incidents involving miscalculation of weight and balance, runway 'excursions', tailstrikes and controlled flight in to terrain. What can we learn in 'cyber' from aviation safety culture, and how can we help improve cyber in aviation?	LIVE IN LONDON LIVE ONLINE
14:40 - 14:50	**GitHub & Security - our platform, products and support for open source** **Paul Hodgkinson,** Field Security Specialist, GitHub GitHub is where the world writes code. We work to produce a secure platform for developers, offer products to help write secure code, and help open source projects and ecosystems build together, securely. This talk covers recent and upcoming innovation in our security products, and describes our wider security work.	LIVE IN LONDON LIVE ONLINE

15:00 - 15:20	**Networking Break**	LIVE IN LONDON
15:20 - 15:40	**Bank of England: SOARing our way to 'enhanced monitoring** **Bill Jeffs,** Cyber Defence Lead, Bank of England **Peter Littler,** Senior Cyber Defence Analyst, Bank of England This presentation covers the Bank of England's Cyber Defence Centre's journey to utilising SOAR technologies to augment its detect and response capability in response to increasing threats facing the Bank. The CDC will demonstrate how its four functions, covering Threat, Detect, Respond and Design, worked together to implement automation in its response functions to tackle the rising threat of ransomware and increased concern over the cyber fall-out of Russia/Ukraine. The presentation will introduce the '5 E's of Automation' - the principles on which the CDC seeks to ensure automation is achieved safely and effectively. We will then dive into the CDC's use of Splunk SOAR and how the CDC built a triage platform, playbooks, and integrations to escalate alerts and take automated response actions to meet the Bank's requirements for 'Enhanced Monitoring' in a sustainable and secure way. The CDC will demonstrate the effectiveness of this approach through real-world examples over the past 6 months.	LIVE IN LONDON
15:45 - 16:05	**Abusing macOS shortcuts** **Parthiban R,** Intelligence analyst, Atlassian **Siva P,** Senior Threat Analyst, Anaplan With an increasing number of macOS being adopted in enterprise endpoints, adversaries are beginning to adapt to a change in the threat landscape for endpoints. The introduction of the macOS shortcuts app released in 12.3 (Monterey) is designed to execute a series of bundled actions in a single triggered execution. Due to its ease of use and sharing capabilities, many app developers, as well as adversaries, have begun adopting it, blurring the line for us investigators. This presentation explores how the shortcuts app can be abused to get a reverse shell and perform various enumeration activities in addition to detecting them.	LIVE IN LONDON
16:10 - 16:40	**Two for One: Firewall 0-day investigations** **Tom Lancaster,** Threat Intel Lead, Volexity In this talk, attendees will hear about two real-world examples of Chinese nation-state attackers using 0-day exploits to compromise firewall devices at Volexity customer sites. This talk will explain the methods used to detect and investigate these attacks, as well as provide unique insights into the actions attackers performed after breaching their target networks.	LIVE IN LONDON

16:45 - 17:10	**Love the way you Liderc: Analysis of an Iran-based threat actor** **Curtis Hanson,** CyberThreat Intelligence Manager, PWC Iran-based threat actor Yellow Liderc, which is commonly known as Tortoiseshell or TA456, first gained public notoriety in 2019 for its specific interests in US military veterans and Middle East IT organisations. PwC has tracked this threat actor targeting a broad range of organisations throughout the US, the Middle East, and Europe, including one from this year that services multiple sectors from energy to aerospace. Yellow Liderc is best known for its social engineering efforts, which include setting up fake social media accounts such as "Marcella Flores". However, this talk will highlight Yellow Liderc's adaptability and persistence, drawing out the threat actor's use of off-the-shelf and custom malware such as PowerShell backdoors and infostealers. We will also present evolutions in Yellow Liderc's tradecraft, discussing new obfuscation techniques and new command and control (C2) methods. Furthermore, while open source has previously attributed Yellow Liderc to Iran's Islamic Revolutionary Guards Corp (IRGC), we will touch on previously unreported associations to Emen Net Pasargad (a.k.a. Ilia Net Gostar) - an organisation most famously known for being sanctioned in late 2021, due to its involvement in an influence campaign targeting the 2020 US presidential election. Ultimately, we will leave attendees with a more comprehensive understanding of Yellow Liderc's activity, by providing granular insights into its victimology, updated visibility into its tactics, and additional context into the threat actor's real-world attribution.	LIVE IN LONDON LIVE ONLINE
17:10 - 17:30	**Closing Remarks & Awards**	LIVE IN LONDON LIVE ONLINE
17:30 - 19:00	**Social Networking**	LIVE IN LONDON

To view the latest Agenda, Attendee Brochure and to find our evaluation forms please click here or scan the QR code:

Thank you for attending

CYBERTHREAT

National Cyber Security Centre
a part of GCHQ

SANS