AGENDA

Monday, November 20

CYBERTHREAT 2023

Time (GMT)	Description
8:00 am - 10:00 am	Live in London **Registration & Networking**
10:00 am - 10:20 am	Live in London and Online **Opening Remarks** James Lyne, Chief Technology and Innovation Officer Paul Chichester, Director of Operations, NCSC Sophia N, Deputy Head of IM, NCSC
10:20 am - 11:00 am	Live in London and Online **Keynote: Frontier Challenges: Black Boxes, Closed Ecosystems and Scale** Ollie Whitehouse, CTO, National Cyber Security Centre A threat and technology focused view of the R&D opportunities that we can collectively go after to help to make the UK the safest place to live and work online.
11:05 am - 11:30 am	Live in London and Online **Crisis Management - What Could Go Wrong?** Ellie Watts, Security Consulting Manager, Accenture Crisis management, crisis simulation, crisis response. These terms are currently being banded around somewhat interchangeably. There is a constant undercurrent of cyber incident related anxiety, for obvious reasons. Very few have visibility of what actually happens when a cyber crisis occurs, let alone how they should prepare themselves. Perhaps they have a run an annual mandatory IT team tabletop exercise for the IT team, or compulsory incident training. Conversely, Crisis Management simulations are hugely in demand from enterprise clients, but after initial conversations it becomes clear that this exercise may be to appease the board and tick a box, as opposed to truly exposing an organisation to the wide-scale chaos of a cyber crisis causing wide spread business impact. Very few clients know what a Crisis Management simulation might entail, let alone what they should be looking to achieve. There are some basic principles that will help an organisation be more resilient to this type of incident, and practical insights that can be shared from those who have seen it, warts and all.
11:30 am - 11:50 am	Live in London and Online **Networking Break**

Monday, November 20

CYBERTHREAT 2023

Time (GMT)	Description
11:50 am - 12:15 pm	**Live in London and Online** **Busy Bees - The Transformation of BumbleBee** Patrick Staubmann, Threat Researcher, VMRay In early 2022, a new malicious loader named BumbleBee was discovered. Multiple cyber-attacks have been identified that use BumbleBee to deliver well-known malware families to harm systems. While analyzing different BumbleBee samples, we identified many structural changes and improvements implemented since its first sighting. These changes are a strong indicator that the family is still under heavy development, and we expect more changes in the future. This makes the family an interesting and important object of research. To protect itself against detection and manual as well as automated analysis, BumbleBee uses various techniques to detect sandboxes and analysis environments. Most of this logic is taken from an open-source sandbox detection project. This talk shares our insights and thoughts collected over the past months while analyzing and tracking this malware family.
12:20 pm - 12:40 pm	**Live in London and Online** **ENISA's View on the Yearly Threat Landscape 2023** Ifigeneia Lella, Cyber Security Officer, ENISA ENISA Threat Landscape (ETL) report provides a general overview of the cybersecurity threat landscape. Over the years, the ETL has been used as key instrument in understanding the current status of cybersecurity across the EU and provide insight in terms of trends and patterns, leading to relevant decisions, prioritisation of actions and recommendations. The ETL report is partly strategic and partly technical, with information relevant to both technical and non-technical readers.This presentation will give a view from the EU on trends and tactics considering active threat actors and the most prominent threats that were observed during the year.
12:45 pm - 1:10 pm	**Live in London** **Defending The UK Against State-Sponsored Cyber Attacks: Lessons Learned** Thomas Griffith, Senior Threat Intelligence Analyst, Microsoft Daniel W, NCSC Dan C, Incident Management Deputy Technical Director, NCSC Over the past year, Microsoft and the National Cyber Security Centre (NCSC) have collaborated to respond to several incidents involving sophisticated cyber actors. This talk will delve into the lessons we've learned from these incidents, covering everything from victim notification to remediation. We will discuss the tactics, techniques, and procedures (TTPs) we've observed, as well as provide guidance on how to prepare for a cyber-attack notification. We hope to showcase the power of collaboration between government and industry, and how it can lead to the best possible outcomes. Specifically, for this talk we will focus on the lessons learned from an APT29 compromise, which can be applied to a variety of other scenarios.

Monday, November 20

CYBERTHREAT 2023

Time (GMT)	Description
1:10 pm - 2:15 pm	**Live in London and Online** **Networking Lunch**
2:15 pm - 2:40 pm	**Live in London and Online** **King of Thieves: Black Alicanto and the Ecosystem of North Korea-Based Cyber Operations** Sveva Vittoria Scenarelli, Cyber Threat Intelligence Manager, PwC 3 billion US Dollars: the (likely underestimated) profit of North Korea-based threat actors' cyber operations over the past 5 years. As the White House assesses that cyber activity now funds up to a half of North Korea's missile program, and new cryptocurrency heists continue hitting the news, this presentation takes an in-depth look at a financially-motivated North Korea-based threat actor known by many names: Black Alicanto, DangerousPassword, APT38, Bluenoroff. Covering intrusion chains, malware, infrastructure and targeting in the Financial Services sector and beyond, this presentation aims to offer a comprehensive and up-to-date understanding of Black Alicanto's TTPs, operations, and mission. Finally, it will also touch on strategic aspects: it will highlight how Black Alicanto's activity supports strategic objectives in line with the national interests of North Korea, and clarify to the audience how Black Alicanto fits within the broader ecosystem of North Korea-based threat actors - including the infamous Lazarus Group.
2:45 pm - 3:05 pm	**Live in London and Online** **ThreatIntelGPT: Structure from Chaos** David Greenwood, Product, EclecticIQ ChatGPT 3.0 made waves across almost every industry when it hit the market in late November last year. Far from a silver bullet for the cyber-security industry, ChatGPT, and more specifically the GPT-3 model, do have many practical uses, namely the automation of highly repetitive tasks. Ask any threat intelligence analyst and they will concur; extraction and dissemination of threat intelligence often requires many hours of ctrl+c, ctrl+v. Earlier this year I set out to use ChatGPT to create structured knowledge graphs from a variety of intelligence reports in my inbox. In this session I will explain the trial and error that went into generating prompts that accurately extract artefacts and their relationships from unstructured intelligence reports (including: PDFs, emails, and Slack messages). Taking it a step further, I will also talk you through my attempts at using Chat-GPT to model the intelligence as rich STIX 2.1 Objects for easy dissemination into existing security tooling. Rest easy, the content covered in this talk will not replace your job.
3:10 pm - 3:30 pm	**Live in London and Online** **Practical Cybercrime Intelligence** Will Thomas, Co-author and Instructor, SANS Institute Cybercrime intelligence is sometimes viewed as navigating forbidden parts of the darkweb and is too risky to perform on your own. I want to show you how straightforward it can be be showcasing my investigation and method for gathering intelligence on one of the longest running ransomware operations, who've been active for up to seven years. My talk will include all techniques I used to investigate this group using various disciplines in cybercrime intelligence. I will share OSINT tips and tricks and how to manually research and navigate the darkweb, as well as how to perform blockchain analysis. I will also show how I use malware sandbox detonations and pivot on malware sandbox submissions, as well as MITRE ATT&CK TTP extraction. The investigation will also conclude with some cybercriminal digital dossier creation and threat actor profiling.

Monday, November 20

CYBERTHREAT 2023

Time (GMT)	Description
3:30 pm - 3:50 pm	Live in London and Online **Networking Break**
3:50 pm - 4:10 pm	SPONSORED TALK Live in London and Online **SCATTERED Landscape – A Look at this eCrime Adversary** Stuart Wiggins, Strategic Threat Advisor, CrowdStrike SCATTERED SPIDER has been one of the more active and brazen eCrime adversary groups tracked by CrowdStrike beginning in 2022. This presentation will look at how their tactics and objectives have shifted in recent activity, highlighting their latest techniques and goals, as well as what organisations can do to best defend and respond to this evolving campaign.
4:15 pm - 4:25 pm	SPONSORED TALK Live in London and Online **Case Study: Investigating a Citrix NetScaler 0day (CVE-2023-4966)** Mathias Frank, Principal Incident Response Consultant, Mandiant, part of Google Cloud A recent critical vulnerability in Citrix NetScaler appliances has allowed threat actors to hijack user sessions and gain access to internal applications and networks. This talk provides a frontline view of the exploitation of this vulnerability, CVE-2023-4966.
4:30 pm - 4:55 pm	Live in London and Online **Hunting down a New Activity Group Targeting Governments in the Middle East and Africa** Lior Rochberger, Security Researcher, Palo Alto Networks In the era of ever-evolving world of cyber warfare, the global cyber landscape has become a battlefield where nation-states deploy new, cutting-edge techniques to obtain non-public and confidential information. An example for such a player is the newly discovered activity group, “CL-STA-0043”, whose level of sophistication, determination and espionage motives bear the hallmarks of a true advanced persistent threat. In our talk, we will step into the depths of the cyber landscape, where we unfold the story behind the activity group “CL-STA-0043”. We will showcase our research on the activity group’s attacks on governments in the Middle East and Africa. This research offers an exclusive glimpse into some very rare and previously unreported tactics, techniques, and procedures designed to penetrate even the most fortified defenses and evade traditional security measures. By dissecting their never-before-seen TTPs, we aim to equip cybersecurity professionals with hands-on knowledge and tips needed to stay one step ahead and hunt down these highly sophisticated threats. Join us as we unveil previously undisclosed information and lay out the attackers' playbook, while shedding light on the intricate web of attribution and clustering surrounding this emerging activity group.

Monday, November 20

CYBERTHREAT 2023

Time (GMT)	Description
5:00 pm - 5:25 pm	**Live in London and Online** **Advanced Persistent Art - The Counterintuitive Complexity & Rising Relevance of Mobile Signalling in Cyber** Rowland Corr, Vice President & Head of Government Relations, Enea AB (formerly AdaptiveMobile Security Limited) Drawing from real-world examples recently observed by Enea TIU, this presentation will explain the evolving nature (& anatomy) of mobile signalling attacks as hostile state-level surveillance threats. The presentation will outline: • Specific commands & TTPs used by the case study attacker • How to identify and defend against such activity Also highlighted will be a yet nascent but important trend towards integration of signalling competency into SOC teams and CERTS (something historically absent from them).
5:30 pm - 9:00 pm	**Live in London and Online** **Closing Remarks** James Lyne, Chief Technology and Innovation Officer Paul Chichester, Director of Operations, NCSC Sophia N, Deputy Head of IM, NCSC
5:30 pm - 9:00 pm	**Live in London** **Networking, Buffet & Drinks** **Bonus Talk with Ken Munro, Pentest Partners** **Session Title**: Why plane hacking in the media is (usually) misleading This bonus talk will dismantle most of the 'airplane hacks' seen on TV and film and show why they don't work in the real world. Given Die Hard 2 will be part of it, the talk should be quite entertaining, but with a serious message.

Tuesday, November 21

CYBERTHREAT 2023

Time (GMT)	Description
9:00 am - 10:00 am	**Live in London and Online** **Registration & Networking**
10:00 am - 10:10 am	**Live in London and Online** **Opening Remarks** James Lyne, Chief Technology and Innovation Officer Paul Chichester, Director of Operations, NCSC Sophia N, Deputy Head of IM, NCSC
10:10 am - 10.50 am	**Live in London and Online** **Keynote: Wartime Cyber Threat Intelligence** Juan Andrés Guerrero-Saade, AVP, SentinelLabs at SentinelOne The nascent development of private-sector Cyber Threat Intelligence (CTI) benefitted from consistently low stakes. Even the most notable CTI discoveries of the past decade were mostly insulated from properly substantiated discussions of relative risk, potential loss of life, and the need for timely disclosures to select parties. The Russian invasion of Ukraine changed that drastically as hot conflicts with 'cyber' support components meant governments overtly enlisted the CTI industry. With a second parallel cyber-supported war unfolding with Israel-Hamas, and a third looming in the not so distant horizon, it's a good time to account for our failures and successes and substantiate the relative value of Wartime CTI.
10:55 am - 11:20 am	**Live in London and Online** **War-Driven Victimology: A Transformative Odyssey** Nazar Tymoshyk, Lead Specialist, CERT-UA
11:20 am - 11:40 am	**Live in London and Online** **Networking Break**
11:40 am - 12:05 pm	**Live in London and Online** **Everyone Gets a Web Shell! Or, Backdooring Web Hosting Companies in Scale** Daniel Frank, Principal Threat Researcher, Palo Alto Networks In this talk, we will provide analysis of the custom-built backdooring tool that was used to compromise at least hundreds of websites, together with other selected tools from the attacker's arsenal. In addition, we will share our threat hunting methodology that led to this discovery, starting with the initial anomalous behavioral findings that kicked off our long investigative journey. We shall share our challenges with big-data hunting, how to effectively conduct an investigation on nearly three years worth of data, and how we dealt with certain research gaps. By the end of the talk the audience will be acquitted with previously undiscovered custom tools, the modus-operandi of a rarely seen threat actor, and of course actionable intelligence on how to hunt for similar threats.

Tuesday, November 21

CYBERTHREAT 2023

Time (GMT)	Description
12:10 pm - 12:30 pm	SPONSORED TALK Live in London and Online **Sandboxing and Threat Intelligence: Alerts Are No Longer Enough** Ertugrul Kara, Senior Product Marketing Manager, VMRay As SOC and Incident Response units grapple with a rise in alerts and increasingly advanced malware and phishing threats, working to block such problems is an ever increasing issue. Handling just the alerts is purely reactive, harvesting as much threat intelligence and then ensuring all systems can use this threat intelligence is proactive. This talk will explore the use of advanced technologies for malware and phishing analysis to streamline triage, investigation, and response processes. Understand when to depend on your sandbox, how to benchmark your sandbox, and to ensure you make use of the valuable data it produces.
12:35 pm - 12:55 pm	Live in London and Online **Supporting Victims of Cybercrime and Online Harm** Charlotte Hooper, Helpline Manager, The Cyber Helpline The Cyber Helpline is a UK charity that supports over 2000 victims of cybercrime every month by linking them with cybersecurity experts for free, expert help. Cybersecurity professionals are best placed to fill the gap in support for individuals experiencing cybercrime, but the impact, trends and the importance of giving safe advice means that it differs from 'traditional' cybersecurity. Individuals facing cybercrime face unique challenges and require tailored support and expertise, which isn't always available. This presentation provides an insight into the threats facing individuals in the online space, the impact it has on them, why the advice that you might give your friends and family could be inadvertently dangerous and how you can use your experience to make a difference in peoples lives with the skills you already have, just by learning to apply them to a different audience.
12:55 pm - 2:00 pm	Live in London and Online **Networking Lunch**
2:00 pm - 2:25 pm	Live in London and Online **BYOVD (Bring Your Own Vulnerable Driver): The Adversaries Return to the Kernel** Paul Moon, Director, Technical Analysis Cell, CrowdStrike Despite Microsoft's efforts to increase mitigation within the Windows Kernel the adversaries' access is on the rise. One reason for this increase is the widespread use of the BYOVD technique, where legitimate but vulnerable drivers are exploited to gain access at ring0. This technique enables the adversary to perform sensor tampering, disable driver signing, install bootkits and allow them to evade detection. This talk covers real world examples of this trend, digs into observed techniques in practice, discusses the difficulties in defending BYOVD and provides you with suggested mitigations including what to look out for. Key take aways of this talk: • The trend for BYOVD incidents is on the increase and what this means for your defensive posture • Which adversaries are using this technique and how are they using it. • What makes this threat challenging to detect. • What are the best mitigation strategies to prevent this threat.

Tuesday, November 21

CYBERTHREAT 2023

Time (GMT)	Description
2:30 pm - 2:55 pm	**Live in London and Online** **Behind the Scenes: A Look at Iran's Contracting Landscape** Saher Naumaan, Principal Threat Intelligence Analyst, BAE Systems Digital Intelligence Molly Elliott, Threat Intelligence Analyst, BAE Systems Digital Intelligence Both of the main security agencies in Iran - the Islamic Revolutionary Guard Corps and the Ministry of Intelligence and Security - use private companies and individual contractors for malware development, operational activity, and support/training. Using recent and historical examples, we will discuss how researchers have linked companies and individuals back to threat groups (and security agencies) through OSINT and technical links, and outline the types of services contractors likely provide to Iran's government. These are comprised of a range of different activities, including espionage, cyber-enabled influence, and disruptive operations. This talk identifies ongoing trends and remaining areas of uncertainty when it comes to Iran's contracting landscape, including contractors' remits, tactics, and relationships to the government. We explore questions about the talent pools used to build Iran's contractors, the comparisons with other countries' contracting models, how Western sanctions and indictments have addressed these third-party companies and how they've informed the UK and US's policies towards Iran.
3:00 pm - 3:25 pm	**Live in London and Online** **Analyzing Volatile Memory on a Google Kubernetes Engine Node** Marcus Hallberg, Security Engineer, Spotify This talk focuses on how we can access and analyze volatile memory in the kernel on a Google Kubernetes Engine (GKE) node using AVML. The purpose of this is to collect a memory snapshot to get granular information about running processes and activities on the GKE node as well as pods and containers running on that node. By using the memory snapshot we can troubleshoot current node activities or use it to collect additional information as part of a security investigation. I will also cover how this method is applicable to other cloud instances running Linux distributions that are supported by AVML. In my talk I will show how we can: • Build a custom privileged docker container running AVML. • Deploy it to a specific GKE node we want to take a memory snapshot of. • Access the kernel space on the GKE node in /proc/kcore and take a snapshot of it. • Get a copy of the unencrypted vmlinux file for the active running version of the GKE node. • Build an intermediate symbol file (ISF) of the kernel using dwarf2json to analyze the memory dump using the vmlinux file. • Provide methods for how to analyze the snapshot, using for example Volatility3.
3:25 pm - 3:50 pm	**Live in London and Online** **Networking Break**
3:50 pm - 4:15 pm	**Live in London and Online** **Beyond Sophistication: Leveraging Threat Actor Attributes to Improve Security Outcomes** Jamie Collier, Principal Threat Intelligence Advisor, Mandiant, part of Google Cloud Jay Christiansen, Senior Consulting Manager, Mandiant, part of Google Cloud Sophistication is a misleading descriptor for threat actors and has become amorphous in the various ways it is used. This talk proposes a more precise discussion of adversaries' attributes to meaningfully differentiate between threats. Our central argument will be that adopting a richer vocabulary of descriptors offers far more than just nuanced understanding. Rather, our focus will be on the way that focusing on actor attributes can improve security outcomes. We do this by demonstrating how actor attributes can enable threat intelligence to be applied more effectively to wider range of use cases beyond the security operation centre. Here, we will focus on how adversary attributes can be used to improve threat-led red teaming and cyber risk assessments.

Tuesday, November 21

CYBERTHREAT 2023

Time (GMT)	Description
4:20 pm - 4:30 pm	**SPONSORED TALK** **Live in London and Online** **Now, Next, -Never-** Magpie Graham, Technical Director of Intelligence, Dragos, Inc. The OT/ICS Threat Landscape is rapidly changing, fuelled by evolutions in technology that increase the attack surface whilst decreasing the cost to the adversary. This talk will explore some of the challenges facing industrial organisations today, highlight some trends Threat Groups exhibit in offensive developments and reveal insights into the defensive developments some Nations are investing in to stay ahead of future threats.
4:35 pm - 5:00 pm	**Live in London and Online** **The Certificate Enrollment Agent's Underestimated Superpower** Dagmar Heidecker, Consultant, Microsoft Andreas Luy, Consultant, Microsoft In Microsoft's Compromise Recovery team we fight cyber attacks besides our customers almost every day. Our work includes different technologies, but Active Directory is our main focus in most cases as it is still an attractive target for attackers. Active Directory has a long history with certificate-based authentication, with smart card authentication being the most widely known use case. Having some technical knowledge of certificate-based authentication in Active Directory allows to correctly assess the sensitivity of a Certification Authority's private key for Active Directory security. Unexpectedly, not only Certification Authorities are entitled of verifying incoming certificate requests, in some cases this sensitive task is delegated to a role called "Certificate Enrollment Agent". A (Certificate) Enrollment Agent is a user who can enroll for a certificate on behalf on another client or user. The permission to do so is based on the requirement of a digital counter-signature with an Enrollment Agent certificate. In other words, a counter-signature from an entitled Enrollment Agent will result in a certificate issued by the Certification Authority. This session will deal with the Certificate Request Agent's superpower, how it can be abused during attacks and how to protect.
5:00 pm - 5:10 pm	**Live in London and Online** **Closing Remarks** James Lyne, Chief Technology and Innovation Officer Paul Chichester, Director of Operations, NCSC Sophia N, Deputy Head of IM, NCSC
5:10 pm - 6:30 pm	**Live in London** **Networking & Farewell Drinks**