SUMMIT AGENDA

We strive to present the most relevant, timely and valuable content. As a result, this agenda is subject to change. Please check back frequently for changes and updates.

Tuesday, February 27th

08:00 - 09:00

Registration & coffee
09:00 - 09:20

Welcome Address & Opening Remarks

Paul Chichester, Director of Operations at NCSC

James Lyne, Head of R&D, SANS Institute
09:20 - 10:00

Technology Forwards: Seemingly Simpler, More Complex & Exploitable

As we strive to make technology simpler to use, more integrated and intelligent we are opening up new opportunities for attackers. Delving into new trends in exploitation and attack James' session will be live demo packed showing you some of the new techniques cyber criminals are capitalizing on. This session will leave you with tools and techniques you can use and plenty of technical gore.

Keynote by: James Lyne, Head of R&D, SANS Institute
10:00 - 10:30

Morning Break & Vendor Networking Area
10:30 - 11:30

CTF & Hackathon
11:30 - 12:00

Hunting Memory Anomalies

The use of memory injection techniques for nefarious purposes has now become common place in many real world compromises being used by both low and high sophistication attackers. In this talk I'll discuss ways in which defenders can begin to detect such anomalies at scale and the challenges involved.

Alex Davies, Senior Threat Hunter at Countercept
12:00 - 13:00

Luncheon & Vendor Networking Area
13:00 - 13:30

Hacking Civil Drones

This talk will cover: Security issues of Civil Drones; Laws in UK for using private Drones; Video Demonstration of hacking Civil Drone.

Aatif Khan, Independent Cyber Security Researcher
13:30 - 14:00

Smashing CTF Challenges – Live Demos of Reversing, Code Breaking and Problem Solving

Wondering how that CTF challenge worked? Why couldn't you quite get it to spit out the key you expected? What IDA oddity prevented you spotting that sequence of bytes? Live demos from some of the challenge creators that will teach you new techniques, offer salacious spoilers and be a lot of fun!

Conor Kelly, Owen Hayman & Simon McNamee, CTF Designers for CyberThreat
14:00 - 15:00

CTF & Hackathon
15:00 - 15:30

Afternoon Break & Vendor Networking Area
15:30 - 16:00

A Senior Researcher from the NCSC will discuss the organisation's journey thus far.

Senior Researcher, NCSC
16:00 - 16:30

Hunting for Lateral Movement: Foundation, Attacker Actions, and Repeatable Methodology to Detect

After a compromise, most attackers go sideways. Progressively moving deeper in the network, compromising systems while searching for key assets/data. Would you spot this lateral movement on your network? In this technical session, we'll review various techniques used to spread through a network, which data sets you can use to reliably find them, and techniques for detecting lateral movement.

Ryan Nolette, Security Technologist at Sqrrl
16:30 - 17:30

CTF & Hackathon
17:30 - 17:45

Day 1 Closing Remarks

Paul Chichester, Director of Operations at NCSC

James Lyne, Head of R&D, SANS Institute
18:00 - 20:00

Sponsored Networking / Cocktail Reception

Wednesday, February 28th

09:00 - 09:05

Day 2 Opening Remarks

Paul Chichester, Director of Operations at NCSC

James Lyne, Head of R&D, SANS Institute
09:05 - 09:45

Keynote

A surprise with something very cool, fun and technically brilliant.

David Litchfield
09:45 - 10:15

Hunting Pastebin for Fun and for Profit

From a security analytics and Threat Intelligence perspective Pastebin is a treasure trove of information. All content that is uploaded to pastebin and not explicitly set to private (which requires an account) is listed and can be viewed by anyone. Hackers and script kiddies are quick to push their warez on to the site for the world to see and developers / network engineers are prone to accidentally leaking internal configurations and credentials.

Kevin Breen, SANS Certified Malware and Forensic Analyst and currently leads the UK CIRT Team for Leonardo MW Ltd.
10:15 - 10:35

Analysing the Bad for a Greater Good

A case study on turning inside out a leaked booter database from a threat intel position and also from a defender position. The aim is to offer insight into the DDoS "market" and in the same time understand the type of data available for a better protection against these types of attack, the ideal combination between attribution leads and threat intel.

Bogdan Necula, Operational Analyst at OLAF - European Anti-Fraud Organisation
10:35 - 11:35

CTF & Hackathon
11:35 - 12:05

Think Your VPN is Secure? Think Again...

In this session the speaker will describe how common VPN architectures have evolved over the years, however the protocols we use today were designed nearly 20 years ago. Have these protocol stood the test of time? We shall investigate a number of attack vectors against VPNs (live demonstrations will be attempted) along with common mistakes that result in insecure architectures. Finally, we shall look to the future of VPNs and investigate what the threat of a quantum computer brings to modern day IPsec VPN designs.

Graham Bartlett, Senior Technical Leader at Cisco
12:05 - 13:00

Luncheon & Vendor Networking Area
13:00 - 13:30

Threat Intelligence in Practice: Operation Cloud Hopper and the After Effects

An account of our investigation into one of the largest sustained espionage campaigns focused on the supply chain. Rachel and Jason will cover the discovery and initial investigation of the compromise, which targeted IT Managed Service Providers, how we tracked the actor and the aftereffects of publicly reporting on the actor including how they evolved in response.

Jason Smart & Rachel Mullan, Threat Intel at PWC
13:30 - 14:00

A Senior Researcher from the NCSC will discuss the organisation's journey thus far.

Senior Researcher, NCSC
14:00 - 15:00

CTF & Hackathon
15:00 - 15:20

Afternoon Break & Vendor Networking Area
15:20 - 15:50

Proactive Hunting for Active Subdomain Takeovers

The talk will explain the technical details of subdomain takeover, which is an emerging threat in the cybersecurity. The concepts and techniques were demonstrated on a high-profile organization. Details of proper remediation and collaboration with CIRT teams of the affected organization will be described as well.

Stijn Vande Casteele, Co-Founder & CEO at Sweepatic

Patrik Hudak, Security Researcher, Sweepatic
15:50 - 16:30

Secure Code: Not Actually That Easy Smarty Pants

Security often blames development. Development often blames security. Rachelle takes a look at some of the new challenges of producing secure code with technical examples of why it isn’t always as simple as it sounds in a policy document.

Rachelle Saunders, Helical Levity
16:30 - 17:00

Closing Remarks

Paul Chichester, Director of Operations at NCSC

James Lyne, Head of R&D, SANS Institute