GSE Enterprise Security Working Group – Next Meeting

We are pleased to confirm that the next meeting of the GSE UK Enterprise Security Working Group, is scheduled as follows:

Date	Thursday 6th February 2020 (09:00 – 16:15, UK time)
Venue	SAS London Office, 7th Floor, 199 Bishopsgate, London, EC2M 3TY
Webex availability	Yes – you can attend in person or via Webex. Please indicate your preference when you register
Registration	Click here
CPE hours	Up to a maximum of 6 hours (full attendance required to claim maximum number of hours)

This meeting is suitable for anyone with an interest in Mainframe Security, including Mainframe Security Professionals (newbies to experienced), Cyber Security Specialists, System Programmers, Auditors and Managers. Attending this meeting will grow your professional knowledge and skills in the following areas:

- Latest security innovations from vendors and how they help enhance security for your organisation
- Current threats, trends, including regulatory and compliance updates to help you prioritise security and compliance efforts
- Share problems, knowledge, best practices with working group members
- Give feedback to vendors on their offerings, including product direction
- Earn CPEs (continuing professional education) to support maintenance of certifications, such as CISA, CISM, CISSP, CRISC

Please read on for the agenda line up. We look forward to seeing you in February!

Jamie Pease CISA, CISM, CISSP, CITP, MBCS
Chairman of the GSE UK Enterprise Security Working Group

Agenda

Start	End	Topic	Who
08:30	09:00	**Registration & Coffee**	All
09:00	09:15	**Introduction from the Chair** • Membership • GSE UK Conference 2020 & other Security events • CPEs • Future topics & venue • Feedback	Jamie Pease (Working Group Chairman)
09:15	09:30	**Welcome to SAS** An introduction from our host!	Andy Gadsby (SAS)
09:30	10:30	**New Pen Test War Stories** During 2019 Mark and the RSM team undertook well over 20 mainframe penetration tests (z/OS, RACF, ACF2 and TSS and subsystems such as MQ, CICS and Db2). The team also performed several business application tests, which revealed some interesting results! During this session, Mark will reveal some of the vulnerabilities that were discovered and some of the ways that they were exploited. The session will contain technical details of the vulnerability and also some of the code used to exploit them.	Mark Wilson (RSM Partners)

10:30	11:00	**From the CISO's perspective** And the focus for us security professionals in 2020 should be? James Loftus, the CISO for RSM Partners will share his thoughts and insights into where we should be channeling our efforts for the year ahead; where are we going wrong; how to get senior management buy-in to fix those security issues.	James Loftus (RSM Partners)
11:00	11:15	**Break for refreshments and networking**	All
11:15	12:00	**The story of an application owners' quest to clean-up their act** Jamie will share with you an interesting case study where some application owners went on a mission to reduce a large amount of access to their applications. What drove them to it, what did they need, how did they implement it and what was the result? Join this session to find out more!	Jamie Pease (Working Group Chairman)
12:00	13:00	**I smell a rat - A Windows Forensic approach** The threats landscape changes every day. New bots, rootkits, malware, ransomware, phishing campaigns, as well as other forms of sensitive data stealing methods can be read about in security bulletins daily, or even twice a day. For every organisation that store and processes personal or sensitive data, or deals with credit card payments, or bookings, or research it is not a matter of if they will be hacked, but a matter of when this will happen. This is the same in the case of dealing with insiders. In every organisation there's a disgruntled employee, or one who does not agree with its policies, has money issues, or holds other grudges against management and therefore wants to punish the organisation for his/hers unhappiness. In most of the cases this punishment will mean that organisation's sensitive data are sold or leaked to third parties, sometimes with catastrophic consequences. In this presentation we will explore some very subtle and in the same time extraordinary dangerous methods to leak sensitive data undetected. We will explore base64 encryption, file embedding, extension alteration (without changing the file type), and steganography from a fresh perspective (or a twist).	Cristian Coraci (The Open University)
13:00	13:45	**Lunch and networking**	All

13:45	14:45	**IBM zSecure Update** Rob van Hoboken will provide us with a technical talk on what's new in IBM zSecure V2.4.0 and recent service stream enhancements.	Rob van Hoboken (IBM Netherlands)
14:45	15:00	**Break for refreshments and networking**	All
15:00	16:00	**All hands session** Do you have any questions, ideas, conundrums you would like to share with the group? This 'all hands' session is your opportunity to share it with the group. We would also like to use this session to understand the challenges / priorities for the year ahead for Mainframe sites, to help the working group get a better understanding of the direction of travel for security on the Mainframe.	All
16:00	16:15	**Closing comments from the Chair**	Jamie Pease (ESWG Chair)
16:15		**End of meeting**	

Future GSE UK Security meetings for your calendar

More details of our schedule can be found here: http://www.racf.gse.org.uk/content/content_events.php