**SASIG Daily Webinars 26th April 30th April**

**Monday 26 April 2021, 11am-12noon (BST)**

**Insider threats: An interactive crisis simulation**

**https://www.thesasig.com/calendar/event/21-04-26-tabletop/**

**Tuesday 27 April 2021, 11am-12.30pm (BST)**

**Online scenario exercise: Kaspersky’s Interactive Protection Simulation (KIPS)**

**https://www.thesasig.com/calendar/event/21-04-27-tabletop/**

**Wednesday 28 April 2021, 11am-12noon (BST)**

**DCMS Cyber Security Breaches Survey 2021 results**

**https://www.thesasig.com/calendar/event/21-04-28-intelligence/**

**Thursday 29 April, 11am-12noon (BST)**

**Who do you trust? Explore the true realities of Zero Trust**

**https://www.thesasig.com/calendar/event/21-04-29-incident/**

**Friday 30 April, 11am-12noon (BST)**

**Is your dishwasher trying to kill you? (The dangers of IoT in the smart home)**

**https://www.thesasig.com/calendar/event/21-05-12-aiiot/**

**SASIG Daily Webinars 26th April 30th April**

**Monday 26 April 2021, 11am-12noon (BST)**

**Insider threats: An interactive crisis simulation**

Every day, sensitive enterprise data is compromised by trusted users who, knowingly or accidentally, expose critical information to the outside world. Such compromises can cost your organisation dearly in liability, loss of intellectual property, and loss of customer and supplier trust.

Do you have the tools, skills, and staffing needed to prevent such a breach? Do you know what steps you must take in the event of a compromise? Join us to experience the impact of an insider compromise first-hand.

This interactive webinar will throw attendees into an emerging insider threat simulation taking place at a fictional pharmaceutical company. You must use your decision-making skills to find the insider threat, manage the growing crisis, and prevent the loss of potentially billions of dollars.

Join us for this interactive webinar to:

* See the impact of the human element in crisis management and response
* Gain a greater understanding of how decisions in a threat scenario have a business-wide impact
* Discover how to strengthen your organisation on both sides of ‘the boom’, so it’s as ready before the impact as it is after it

**Tuesday 27 April 2021, 11am-12.30pm (BST)**

**Online scenario exercise: Kaspersky’s Interactive Protection Simulation (KIPS)**

We are delighted to once again be partnering with Kaspersky to host their Interactive Protection Simulation (KIPS) – remotely and all online.

Utilising the latest learning techniques and addressing all levels of the organisational structure, this exercise is effective in establishing a better security understanding amongst staff of varying roles, levels of management experience and technical knowledge. The activity allows players to discover and analyse the typical mistakes made in building cybersecurity and incident response procedures while demonstrating the real role of cybersecurity in business continuity and profitability. By establishing a better cybersecurity understanding, organisations can successfully lower the number of cyber-incidents and reduce associated financial losses, with an impact which lasts well into the longer-term.

During the exercise, participants will:

* Access the simulation through Kaspersky’s online KIPS portal
* Make business decisions on cybersecurity strategy with real-time threat updates and dynamic outcomes
* Follow live scoreboard of all participating teams
* Communicate over voice chat with your team

You’ll compete in teams of up to six players, so what better way to spend a Tuesday morning than through an informative and entertaining session… with considerable kudos for the winning team.

**Watch a short video about the simulation exercise here.**

**https://www.youtube.com/watch?v=y\_ihFMwUTQU**

**Spaces are limited and will be granted on a first come, first served basis – so book early to avoid missing out.**

**Wednesday 28 April 2021, 11am-12noon (BST)**

**DCMS Cyber Security Breaches Survey 2021 results**

Join DCMS to hear the latest findings from the Cyber Security Breaches Survey 2021. The report explores how the cyber risk to organisations is heightened due to the Covid-19 pandemic, a situation which has made securing digital environments more challenging as organisational resources are diverted to facilitating home working for staff.

The Cyber Security Breaches Survey is a DCMS commissioned annual official statistic that surveys businesses, charities and the education sector about their approach to cyber security, and the costs and impacts of cyber breaches and attacks.

The findings of the survey help organisations understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports Government to understand changes to cyber security risk across the UK, and to shape future policy in this area.

**You can read the full report here.**

**https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021**

**Thursday 29 April, 11am-12noon (BST)**

**Who do you trust? Explore the true realities of Zero Trust**

In the good old days of working from an office, organisations typically ‘trusted’ an employee when they issued them with a security badge to get in through the front door. How bizarre does that seem when most of us are working from home and recruitment in many organisations continues as usual!

Changes in working patterns and the expansion of VDI, VPN and internet-based remote access has introduced new attack vectors. This has certainly led to the explosion of vendor noise around ZERO TRUST, and typically we see every vendor has twisted aspects of what they do into a ‘Zero Trust Story’.

In this session, Secrutiny explores what Zero Trust really is from both an analyst and common view. It’s not another theoretical discussion about Zero Trust and how important it is, we’ll look at common approaches, including practical steps you can take now to start the journey, and share our views on the operational side of it all.

**Friday 30 April, 11am-12noon (BST)**

**Is your dishwasher trying to kill you? (The dangers of IoT in the smart home)**

In an increasingly connected world, more devices than ever are now online. From fridges to toothbrushes, the world is getting smarter. The data harvested can often lead to a more efficient and tailored experience, but what risks do they possess? Many IoT devices collect sensitive and even very personal data which could potentially become a treasure trove to attackers.

Smart devices have taken the market by storm but how easily can they be hacked? And what about privacy? ESET researchers have looked into this modern attack vector, so join Cyber Security Specialist Jake Moore as he unravels the potential hacks and data leaks that malicious actors could use to target unsuspecting victims.