**SASIG Daily Webinars 4th May 7th May**

**Monday 3rd May – No Event**

**Tuesday 4 May 2021, 11am-12noon (BST)**

**Public & Hybrid SaaS with absolute Zero Trust: A ‘Made in Germany’ perspective**

**https://www.thesasig.com/calendar/event/21-05-04-incident/**

 **Wednesday 5 May 2021, 11am-12noon (BST)**

**How can you adapt your approach to human factors in a changing security landscape?**

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

**Thursday 6 May 2021, 11am-12noon (BST)**

**The strategic value in infosec: How to be more than a cost centre**

**https://www.thesasig.com/calendar/event/21-05-06-boardroom/**

**Friday 7 May 2021, 3pm-4.30pm (BST)**

**SASIG Academy Cyber Health Session 1 – How to assess cyber health and risks: Build**

**Members Only**

**https://www.thesasig.com/calendar/event/21-05-07-incident/**

**SASIG Daily Webinars 4th May 7th May**

**Monday 3rd May – No Event**

**Tuesday 4 May 2021, 11am-12noon (BST)**

**Public & Hybrid SaaS with absolute Zero Trust: A ‘Made in Germany’ perspective**

**The cloud. A form of outsourcing which gave us challenges, including the governance and trust model applied to what are in fact third-party contractors. Should you implicitly trust them for IAM controls? Or not adopt SaaS at all? Or only adopt hybrid or some complex, in-between solution? Should you trust your contractor for the integrity of the authentication, verification, or authorisation processes?**

**IDEE GmbH – the European champion for verifiable, zero-trust, password-less authentication, offers a disruptive new model whereby organisations need not trust their IDP and can stay in control of their authentication, verification, and authorisation processes – including the policy decision point (PDP) as defined by the NIST Zero-Trust Architecture. Come along and discuss with us how the German standards for privacy and security by design shape the architecture choices that you can make today.**

**Wednesday 5 May 2021, 11am-12noon (BST)**

**How can you adapt your approach to human factors in a changing security landscape?**

**Before the pandemic, less than 30% of people in the UK had ever worked remotely. By April 2020, nearly half of all UK employees were working at home. And 74% of employees now see a mix of office-based and remote working as the best way forward. As hybrid working goes from being a ‘future possibility’ to an impending reality, how do security professionals adapt their approach to human factors?**

**Thursday 6 May 2021, 11am-12noon (BST)**

**The strategic value in infosec: How to be more than a cost centre**

**One of the most important factors in determining the return on investment (ROI) of a security programme is the perception of risk management at board level. Despite the importance of the security team in protecting the business, it can sometimes be perceived as a cost centre rather than delivering clear strategic value to the business. So how can security professionals redress this perception? Join us for a webinar where we’ll look at ways for infosec to position themselves in the way they should be seen – as core to the security, reputation and value of the business.**

**Friday 7 May 2021, 3pm-4.30pm (BST)**

**SASIG Academy Cyber Health Session 1 – How to assess cyber health and risks: Build**

**Members Only**

**Our May Academy series looks at how to assess cyber health and risks.**

**Hackers gain access to systems by exploiting a series of vulnerabilities in their escalation to achieving data theft or destruction. A concept widely known as the ‘kill chain’, it is best represented by a pyramid where the available surface area (or systems) that are exploited at each level narrows on their approach to targeted services, network(s), user rights and behaviours, and ultimately – data. Although there is a greater risk of exploitation at the lower tiers, it is spread out. Yet at higher levels, it is more focused – and has more impact that leads to damage. This paradigm of cyber risk provides a context for assessing the health of an organisation’s cybersecurity.**

**In our first of four sessions, we will review the methods of assessing cyber health and identifying common cyber risks from the ‘build’ layer of the pyramid. It will include scripts, demonstrations, data analysis techniques and references useful for collating information.**

**Session 2 – Assessing your services**

**Session 3 – Assessing your networks**

**Session 4 – Assessing your users and data**