focus group

Microsoft Solutions Partner

Microsoft Sentinel workshop

As IT becomes more strategic, the importance of security grows daily. Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges - let alone tomorrow's unknown risks.

That's why Microsoft developed Sentinel, a fully cloud-native SIEM.

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting and threat response.

Get an overview of Microsoft Sentinel along with insights on active threats to your Microsoft 365 cloud and on-premises environments with a Microsoft Sentinel workshop.

Workshop highlights

- **Understand the features and benefits of Microsoft Sentinel**
- **Gain visibility into threats across email, identity and data**
- **Better understand, prioritise and mitigate potential threat vectors**
- **Create a defined deployment roadmap based on your environment and goals**
- **Develop joint plans and next steps**

Choose the approach that's right for you

Every organisation is different, so this workshop can be customised to fit your environment and goals within the following two scenarios:

Remote monitoring

If your organisation doesn't have its own security operations centre (SOC) or if you want to offload some monitoring tasks, we will demonstrate how Focus Group can perform remote monitoring and threat hunting for you.

Joint threat exploration

If your organisation is interested in learning how to integrate Microsoft Sentinel in your existing SOC by replacing or augmenting an existing SIEM, we will work with your SecOps team and provide additional readiness to bring them up to speed.

In addition, depending on the selected scenario, you will also:

Experience the benefits of a managed SIEM with a true cloud native SIEM, managed and monitored by our cyber security experts. (Remote monitoring scenario)

Receive hands-on experience, learn how to discover and analyse threats using Microsoft Sentinel and how to automate your Security Operations to make it more effective. (Joint threat exploration scenario)

Workshop objectives

Through this workshop, we will work with you to:

- **Discover threats** to your Microsoft 365 cloud and on-premises environments across email, identity and data.
- Understand how to **mitigate threats** by showing how Microsoft 365 and Azure security products can help mitigate and protect against threats that are found.
- Plan next steps and provide information to **build a business case** for a production deployment of Microsoft Sentinel including a technical deployment roadmap.

What we'll do

- Analyse your requirements and priorities for a SIEM deployment
- Define scope & deploy Microsoft Sentinel in your production environment
- Remote monitoring* and proactive threat hunting to discover attack indicators
- Discover threats and demonstrate how to automate responses
- Recommend next steps on how to proceed with a production implementation of Microsoft Sentinel

*optional component

Fill in this form and a member of the team will call you back, or you can contact us now on 0330 500 2500.

> Our digital services are instrumental to our student experience and Focus Group are a valuable asset in ensuring our security is keeping pace with the digital strategy
>
> ~ James King, Head of IT at Royal College of Art

Royal College of Art

focusgroup.co.uk/enterprise