Datasheet

Microsoft Sentinel Workshop

Gain a bird's eye view across your enterprise with SIEM for a modern world

"With everything running through Microsoft Sentinel, we've reduced the time spent on case management and resolution of alerts by approximately 50 percent"

- Stuart Gregg, Cyber Security Operations Lead, ASOS

As IT becomes more strategic, the importance of secuity detection, automation, and response grows. Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges—let alone tomorrow's unimagined risks. Learn to customize playbooks like today's content engineering experts.

With over 300+ Microsoft Sentinel deployments of experience at the heart of the workshop, you will get hands on experience with Microsoft Sentinel, a fully cloud-native SIEM.

See and stop threats before they cause harm with an Microsoft Sentinel Workshop

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.

Do more than just detection with your SIEM. Learn how to secure your cloud and on premises environments with an Microsoft Sentinel Workshop.

Workshop Highlights

- Understand the features and benefits of Microsoft Sentinel
- Gain Visibility into threats across email, identify, and data
- Better understand, prioritize, and mitigate potential threat vectors
- Create a defined deployment roadmap based on your environment and goals.
- Develop join plans and next steps

Choose the approach that's best for you

Every organization is different, so this workshop can be customized to fit your environment and goals. We can provide either of two scenarios:

Remote monitoring

If your organization doesn't have its own security operation center (SOC) or if you want to offload Microsoft specific monitoring tasks, we will demonstrate how BlueVoyant can perform remote monitoring and threat hunting for you.

Joint threat exploration

If your organization 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.

BlueVoyant

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.

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 cybersecurity experts.

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

What we'll do

Analyze 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

*optional component

Discover threats and demonstrate how to automate responses

Recommend next steps on how to proceed with a production implementation of Microsoft Sentinel

Why BlueVoyant

When it comes to compliance, you need an experienced partner.

As the 2022 Microsoft U.S. Security Partner of the Year, along with BlueVoyant's status as a Microsoft Gold Partner with an Advanced Specialization in Cloud Security and Threat Protection and founding member of Microsoft Intelligent Security Alliance (MISA), our mission is to proactively defend organizations of all sizes against today's sophisticated attacks and accelerate detection and response with Microsoft. A Microsoft credentialed advisor delivers all workshops.

BlueVoyant

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**