Microsoft Sentinel Workshop

www.overcastmx.com

Get a bird's eye view of your enterprise with SIEM for a modern world

Workshop Highlights

- **Understand** the features and benefits of Azure Sentinel
- Email, identity and data threat **visibility**
- Better **understand, prioritize and mitigate** potential threat vectors
- **Create** a defined implementation roadmap based on your environment and objectives
- **Develop** joint plans and next steps

"With everything running through Azure Sentinel, we've reduced the time spent on case management and alert resolution by about 50 percent."

-**Stuart Gregg, Jefe de Seguridad Cibernética, ASOS**

As IT becomes more strategic, the importance of security grows daily. Security Information and Event Management (SIEM) solutions built for past environments struggle to keep up with present challenges, let alone unimaginable future risks.

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

See and stop threats before they cause damage with an Azure Sentinel Workshop

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

Get an overview of Azure Sentinel along with information on active threats to your Microsoft 365 cloud and on-premises environments with an Azure Sentinel Workshop

Choose the best approach for your needs

Every organization is different, so this workshop can be customized to fit your environment and objectives. We can provide any of these scenarios:

Remote Monitoring

If your organization does not have its own security operations center (SOC) or if you want to offload some monitoring tasks, we will demonstrate how Overcast can perform remote monitoring and threat scanning for you.

Joint threat scanning

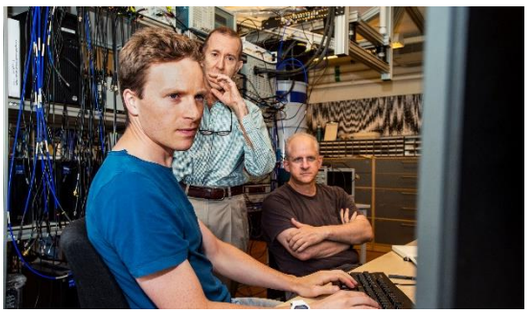
If your organization is interested in learning how to integrate Azure Sentinel into your existing SOC, replacing or extending an existing SIEM, we will work with your SecOps team and provide additional preparation to get them up to speed.

Microsoft Sentinel Workshop

www.overcastmx.com

Workshop Objetives:

Through this workshop, we will work with you to:



- Discover threats to your Microsoft 365 on-premises and cloud 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 the threats you encounter.
- Plan next steps and provide information to create a business case for a production deployment of Azure Sentinel, including a technical implementation roadmap.

In addition, depending on the selected scenario, you will be able to:

Experience the benefits of a managed SIEM with a true cloud-native SIEM, managed and monitored by our cybersecurity experts. (Remote Monitoring Scenario)

Receive hands-on experience, learn how to discover and analyze threats with Azure Sentinel and automate your security operations to make them more effective.(Joint Threat Scanning Scenario)

What are we going to do?

Analyze your requirements and priorities for a SIEM implementation.

Define the scope and deploy Azure Sentinel in your production environment.

Remote monitoring* and proactive threat scanning to uncover indicators of attack*optional component

Discovering threats and demonstrating how to automate responses

Recommend the following steps on how to proceed with a production deployment of Azure Sentinel

Why Overcast?

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

Contact us today to get started!