INTEGRATED SOLUTIONS | Digital Solutions Partner

Microsoft Security Anywhere

Empowering employees to securely work from anywhere

The workshop ***Microsoft Security Anywhere*** is designed for organizations looking to increase the security of their IT environment. The workshop will help identify critical points and learn how to immediately respond to threats in a diverse environment.

The scope of practical knowledge covers local, cloud, hybrid as well as multi-cloud environments providing a ***holistic*** approach of modern ***Microsoft Security*** solutions for IT security in organizations.

Solutions such as ***Microsoft Cloud App Security*** provide services for cloud application discovery, monitoring and protection, while ***Azure Sentinel*** collects and analyzes data locally and in cloud environments. ***Microsoft Information Protection*** protects the most important data for an organization from its deliberate or inadvertent unauthorized access. Advanced solutions for ***Identity and Access Management***, protect individual elements of the environment against unauthorized access.

The Most Important Areas

- □ **Modernize security and defend against threat**
- □ **Secure Azure, hybrid and multi cloud**
- □ **Protect and govern sensitive data**
- □ **Manage and investigate risk**
- □ **build Zero Truust foundation**
- □ **Identity and access management**

Threat Protection and modern SOC

A security operations center (SOC) helps organizations detect, monitor, and respond to cyber-threats. SOCs provide services, ranging from log monitoring and analysis to vulnerability management, incident response, and, increasingly, proactive threat hunting.

Azure Hybrid and Multi cloud Security

A multi-cloud strategy involves two or more platforms or providers to handle various business tasks. Azure provides a holistic, seamless, and more secure approach to innovate anywhere across on-premises, multicloud, and edge environments.

Information Protection & Govermance

Microsoft Information Protection & Governance solutions help you protect and govern your data wherever it lives, helping you meet both internal and external security and compliance requirements

Insider Risk Management

Insider risk management policies determine which users are in-scope and which types of risk indicators are configured for alerts. Risk score boosters and anomaly detections help identify user activity that is of higher importance or more unusual.

Identity and access management

is a framework of policies and technology that authenticates and authorizes access to applications, data, systems, and cloud platforms. In basic terms, it helps ensure that the right people have the right access, for the right reasons.

Protect Your Organization

- □ Azure AD Connect
- □ Azure AD Identity & Access Management
- □ Azure Sentinel
- □ Azure Information Protection
- □ Microsoft Threat Protection
- □ Microsoft Cloud App Security
- □ Compliance Manager
- □ Identity and Access Management,

How does it look like ?

Microsoft Security Anywhere

Empowering employees to securely work from anywhere

Introduction

The workshop begins with an introduction and overview section, during which we will discuss the scope and purpose of the workshop.

Analanalysis of the environment

In this part of the workshop, the Integrated Solutions Engineer will conduct an in-depth analysis of the current operating environment. In addition to infrastructure and application analysis, automated discovery processes will be run to check and collect information about threats in the data area including the Data Risk Check Automated Discovery service, which automatically collects data logs from systems, and the User Risk Check service monitors the communications and behavior of a selected group of users and identifies events that may pose a threat to the organization.

Our promise to you

Our workshops will help you achieve your business goals better and faster than the competition

An offer to get you started

- If you are interested please call +48 509 205 000
- or visit our website www.integratedsolutions.pl

Conclusions of the environmental analysis

In this section, the Expert Engineer will present the conclusions of the environment analysis. He will help identify and quantify the risks and vulnerabilities associated with individuals and the way data is processed within the organization.

Demo - Microsoft Security services

This part will present Microsoft's holistic approach to the security. Using previously collected data from environment analysis, scenarios of practical use of security services will be selected based on the current situation of the organization. Through selected scenarios, Microsoft services in the area of security, analysis detection and response to potential threats will be presented in a practical manner. The most common and effective combinations of combinations of services in different environments such as local, cloud, hybrid and multi-cloud will be shown. The goal of this part of the workshop is an analysis and discovery exercise that will help participants learn how to effectively identify cases and possible scenarios.

This area may include the following:

Threat Protection - The end to end protection solution, securing identities, endpoints, user data, cloud apps, and infrastructure
Compliance Manager - This is a feature in the Microsoft 365 Compliance Center that facilitates and simplifies the management of compliance requirements in the organization by measuring progress in the deployment of improvement activities .
Deffender for Cloud Apps – Provide extensive insight, data flow control and advanced analytics to identify and counteract cyber threats across all cloud services.
Azure AD Identity & Access Management – Provide access and identity management functions.
Azure AD Connect – The solution for connecting local identity infrastructure with the Azure AD cloud identity service.
Microsoft Sentinel – This is a scalable, cloud-native solution that delivers intelligent security and threat analytics across the enterprise, providing a single solution for alert detection, threat visibility, proactive threat detection and threat response.
Azure Information Protection – control and secure email, documents and confidential data that is shared outside the organization - from classification to built-in labels and permissions.

Defining the strategy

The final stage of the workshop will be to define a roadmap and appropriate security development strategy based on the company's current and future needs. This assessment will be based on the initial analysis of the environment using the Data Risk Check Automated Discovery tool and selection of the most appropriate solutions based on a prior review of the most suitable usage scenarios and combination of individual Microsoft security services.

Tangible Benefits / Desired Outcomes

- The workshops are conducted by an experienced expert from the Microsoft Competence Center at Integrated Solutions.
- Substantive and practical knowledge is conveyed in an understandable way and adapted to the recipient's expectations.
- Workshops are always based on the latest versions of Microsoft products and services.
- The workshops end with a summary report and a proposal of an action plan.

Why Integrated Solutions Sp. z o.o ?

We are trusted advisor on a market in digital solutions area. As a experienced Microsoft Partner, we advise our Customers how to develop their businesses even better thanks to digitization and modern technologies. We provide ready-made solutions and provide the highest level of security for deployment.