CLOUD4C

A VIRTUAL, VIGILANT WATCHER

FOR YOUR ENTERPRISE

CLOUD4C – MICROSOFT AZURE SENTINEL WORKSHOP

Microsoft Azure Sentinel is a scalable, cloud-native, Security Information Event Management (SIEM) and Security Orchestration Automated Response (SOAR) solution, with an ability to write the custom alert rules and automated playbooks to help you detect threats in your environment in real-time.

AZURE SENTINEL FRAMEWORKS

1

Secure your network, infrastructure, data, and applications on Microsoft Azure effectively.

2

Integrate Artificial Intelligence, Threat Analysis, and Automation for Optimal Security solutions.

3

Investigate possible security breaches and gather forensic evidence to prevent modern cyber threats.

WORKSHOP HIGHLIGHTS

- Understand the features and benefits of Azure Sentinel
- Gain visibility into threats across email, identity, and data
- Better understand, prioritize, & mitigate potential threat vectors
- Create a customised deployment roadmap based on your goals
- Develop joint exploration and execution plans

WORKSHOP OBJECTIVE

Experiencing Azure Sentinel

Discovering and Analyzing Threats

Understanding How To Mitigate Threats

Planning The Next Steps

WORKSHOP SCOPE

Remote Monitoring of Threats

- Incident Monitoring: Provide remote monitoring of Azure Sentinel for incidents during the engagement

- Proactive threat hunting across the organization's data sources (optional) – using Sentinel hunting search and query tools for security threats hunting

Joint Threat Exploration

(Optional – Included in the scope only at customer's discretion)

- Jointly work with the organization's security analysts and engineering team to discover and analyse the threats using Azure Sentinel.

- Demonstration of automation of security operations

- Analysis of threats in an enterprise's on-cloud (Azure) and on-premise environment across email, identify and data to better understand, prioritize and mitigate potential cyber-attack vectors.

WHAT WE'LL DO?

Step 1: Pre-Engagement Call

□ Engagement overview

□ Define scope and identify the right stakeholders

□ Understand business and IT requirements, existing SIEM/SOC tools, data sources to be connected and security operations automation requirements

Step 2: Technical Engagement

□ Setup trial licence with Deploy and Configure Azure Sentinel

□ Connect Azure Sentinel to ingest data from Azure AD Identity Protection, Microsoft Cloud App Security, Agreed 3rd Party Syslog integration and Limited number of on-premises servers

Step 3: Threat Exploration and Report Generation

□ Remote incident monitoring during the data collection phase

□ An optional action of threat hunting to discover indicators of attack in the ingested data

Step 4: Results Presentation

□ Prepare results to gain visibility into threats in your cloud and on-premises environment

□ Get recommendation on how to mitigate or avoid cyberattacks with defined deployment roadmap based on your needs and objectives

WHO ALL SHOULD COME FOR WORKSHOP?

The workshop is intended for security decision-makers such as:

- Chief Information Security Officer
- Chief Information Officer
- Chief Security Officer
- IT Compliance
- Data Protection Officer
- IT Security
- Data Governance Officer
- IT Operations

KEY DIFFERENTIATORS

Cloud4C Security Expertise

- 7+ Reg-tech frameworks
- 40+ Control Objective with 26 security tools
- 700+ customers consuming managed Security services from Cloud4C
- 800000 Events Per Second (EPS)
- 13000 HBSS instances managed
- 3200 UTMs
- 24/7 System Monitoring & Management from Central/Local NOC/SOC

Quick benefits to you

- Conducting the Azure Sentinel Workshop free of cost to you
- 600+ Azure certified resources engaged from the onset
- Customizing workshop to include Microsoft Defender ATP, M365 ATP or Azure Cloud App Security
- Insights based on vast Microsoft and Third-Party Threat Intelligence

Pre-met Global Compliance needs

- **Industry specific -** GDPR, PCI-DSS, GxP, HIPAA, CSA
- **Country specific -** MAS, RBI, FedRAMP, OJK, iRAP, MEITI, SAMA, NESA
- **Worldwide standards –** ISO 27001, ISO 27017, ISO 27018, ISO 20000, ISO 22301, SOC1, SOC2

Cloud4C has deployed Azure Sentinel for customers across the following domains

- **Banks and Financial Institutions**
- **Very Large Government organizations**
- **Large Manufacturer**
- **Retail**
- **Communications**

WHY CLOUD4C?

As an Azure Expert MSP, you can trust our expertise that the workshop will be a highly productive session. It will help you better understand Azure Sentinel's capabilities, determine how it can address your security pain points, and decide whether using managed cybersecurity services – for both detection and incident response can rapidly and cost-effectively raise your security posture.

globalsales@cloud4c.com | www.cloud4c.com