Defend Against Threats with SIEM Plus XDR Workshop

Consolidated Telecoms Co. Ltd.

www.ctelecoms.com.sa - Info@Ctelecoms.com.sa

Table of Contents

Tel. 012-261 9667
HAS HO Building, Al-Andalus Dist., Ground Floor, Jeddah 21474
Kingdom of Saudi Arabia
P.O. Box 16727

Defend Against Threats with SIEM Plus XDR Workshop

What is Microsoft Defend Against Threats with SIEM Plus XDR?

Microsoft Defend Against Threats with SIEM Plus XDR Workshop consists of two modules:

- Threat Check: is a module with Selected Microsoft 365 security products and features are used to gain visibility into threats to a customer's Microsoft 365 cloud environment
- Microsoft Sentinel: is Security Information and Event Management (SIEM) solution built for yesterday's environments to keep them in pace with today's challenges.

What Selected Microsoft 365 Security products are used in Threat Check?

Microsoft 365 Defender provides access to Microsoft 365 security products needed to detect threats. These products are:

1. Microsoft Defender for Endpoint
   Endpoint protection suite built around powerful behavioral sensors, cloud analytics, and threat intelligence.
2. Microsoft Defender for Office 365
   Advanced protection for your apps and data in Office 365, including email and other collaboration tools.
3. Microsoft Defender for Identity
   Defend against advanced threats, compromised identities, and malicious insiders using correlated Active Directory signals.
4. Microsoft Defender for Cloud Apps
   Identify and combat cyber threats across your Microsoft and third-party cloud services

What is Microsoft Sentinel?

Microsoft Sentinel is a cloud native SIEM solution, which is a solution on top of Log Analytics, works to Detect, Investigate and Respond against threats targeting your users and systems.

Tel. 012-261 9667
HAS HO Building, Al-Andalus Dist., Ground Floor, Jeddah 21474
Kingdom of Saudi Arabia
P.O. Box 16727

The Benefits of the Workshop

- Help to protect against attacks and coordinate defensive responses across the suite through signal sharing and automated actions.
- Narrate the full story of the attack across product alerts, behaviors, and context for security teams by joining data on alerts, suspicious events, and impacted assets to incidents.
- Automate responses to work immediately by triggering self-healing against impacted assets through automated remediation actions.
- Enable security teams to perform detailed and effective threat hunting across endpoint and Office data.
- Understand the features and benefits of Microsoft Sentinel.
- Understand how to discover and Analyze Threats.
- Understand how Microsoft 365 and Azure security products can protect against threats.
- Understand your current data security status and related processes.
- Create a defined deployment roadmap based on your environment and goals.

Workshop Duration and Requirements

- The workshop may require two or more sessions, and this will be agreed on during the first workshop's engagement.
- You will be receiving a satisfaction survey, which is a mandatory activity to finalize the workshop delivery.
- The audience for the workshop would be Microsoft 365 administrators and IT security personnel.
- At least one global admin attendance is required from your organization behalf to conduct the workshop efficiently and smoothly.

The workshop is an interactive session, discussing the Defend Against Threats with SIEM Plus XDR best settings to be assigned.

Tel. 012-261 9667
HAS HO Building, Al-Andalus Dist., Ground Floor, Jeddah 21474
Kingdom of Saudi Arabia
P.O. Box 16727