BYTES

An accelerated session to support with your planning of Sentinel and to get you up and running!

Sentinel Activation Workshop

Microsoft Sentinel is a scalable, cloud native Security Information and Event Management (SIEM) platform. Microsoft Sentinel provides enterprises with the ability to **ingest data at cloud scale and utilise this to detect threats**, this, coupled with the analytics and threat intelligence that Microsoft provides allows for rapid detection and response for the threats that would previously go undetected.

Bytes believe that customers should be maturing their incident response capabilities by utilising Sentinel, especially in Microsoft Cloud Environments where there are several services enabled. This will allow for a single point to view and track and assess any suspicious activity within the Microsoft Cloud stack.

What to Expect

- ✓ Data Collection
- ✓ Detection of Threats
- ✓ Investigation of Incidents
- ✓ Respond and Contain

Microsoft

To facilitate this belief, **Bytes** are offering a session that will provide a planning & activation exercise to ensure that core considerations are evaluated and planned accordingly.

Additionally, we can investigate the various options around utilising your M365 licensing for greater visibility and explore areas such as Security Co-Pilot for future AI enhancement. Following this, **Bytes** will support you with a basic implementation of Microsoft Sentinel for your Microsoft Cloud Environment.

This acts as a springboard into using Microsoft Sentinel to begin analysing and detecting threats within your cloud environment. The session is a 1-hour session, **free of charge to Bytes Customers**, with the result being that your Microsoft Sentinel instance is configured to your Microsoft Cloud Services to begin receiving insights and alerts on possible threats.

The Workshop Focuses on 6 Key Points:

Requirements Gathering: Get an idea of the business and technical requirements and expectations you have of Sentinel.

Planning and Considerations: Get an understanding of your current environment and provide guidance on how best to deploy Sentinel in a structured manner.

Estimate Pricing: Look to get a rough idea of what log sources you will need to ingest into Sentinel, combined with your assets we can provide an estimated price of Sentinel.

Sentinel Provisioning: We will work with you to implement an instance of Sentinel into your Azure Subscription.

Connecting M365 Data Sources: Walk you through the setup and configuration of Sentinel to begin collecting logs and data from your enabled Microsoft Cloud Services.

Next Steps: Assess and recommend next steps, such as exploring options around further professional services and managed services to support you with enhancing your response capability.

☎ +44 1372 418500 🌐 www.bytes.co.uk ✉ tellmemore@bytes.co.uk