

# Bytes Sentinel Activation Workshop

**Microsoft Sentinel** is a scalable, cloud native Security Information and Event Management (SIEM) platform, which enables organisations to securely consume data at cloud scale, whilst monitoring threats. Bringing together optimised threat analytics and intelligence to ensure rapid detection and response.

## Bytes help you utilise your Sentinel

- Providing a tailored introduction to Sentinel.
- Visibility of its analysis and threat detection capabilities.
- 2-hour workshop engagement - free of charge to Bytes Customers.
- Configure Sentinel to your Microsoft Cloud Services – instantly activating insight and threat alert capabilities.

## What does the onboarding include?

- Depending on your Microsoft Licensing and Cloud utilisation, Bytes will determine which services we can ingest into Sentinel.
- Bytes consultants will engage with you prior to the session to ascertain the services in use and which data sources should be ingested as part of this session.

## Four Key Focus Points:

### Intro to Sentinel



Bytes consultants will provide an overview of Sentinel and its capability. What to expect: Data Collection, Detection, investigation and Response.

### Onboarding to Sentinel



Bytes consultants will walk you through the setup and configuration of Sentinel to begin collecting logs and data from your enabled Microsoft Cloud Services.

### Walkthrough of Sentinel



Once your data is ingested, Bytes consultants will walk through the Sentinel portal to show you insights based on your environment.

### Bytes Capabilities & Next Steps



The final part of the session will be to assess and recommend next steps. Connecting Microsoft Cloud data sources is only the first step in the Sentinel Journey.