WHAT IS A SENTINEL STARTER KIT?

A Sentinel Starter Kit is a product designed to introduce, establish, and provide a framework for working with Microsoft Sentinel. The starter kit ingests data from standard sources, creates a valuable dashboard, and onboards the customer onto support for three months to tune and gain a greater understanding of the service. It is designed to provide a solid foundation based upon Microsoft best practices for your Microsoft SIEM. Once the starter kit has been completed, your organisation has complete flexibility in expanding its Sentinel service.

Why Do I Need a Sentinel Starter Kit?

Azured's Starter Kit includes an industry-aligned standard deployment, with standardised inputs and outputs to enable customers to realise immediate benefit from Sentinel whilst establishing a framework for ongoing management, optimisation, and adoption of the service. The Starter Kit answers:

- "Where do I start."
- "Where do I go?", and
- "How can I get there?"

Together, Telstra and Azured will enable your organisation to establish, fine-tune, and onboard Sentinel within their organisation.

What's Included?

The Core Sentinel Starter kit enables your organisation to start realising the benefits of Microsoft Sentinel by implementing a standard configuration. The service will then be fine-tuned for three months to ensure the utmost quality of the Microsoft Sentinel service and the data within it.

> Azured recommends implementing Defender for Cloud Apps (Formerly MCAS) into your environment. Defender for Cloud Apps is an essential component as it provides visibility and control over a company's cloud applications and the third-party platforms its users are accessing. It allows you to get sophisticated analytics to identify and combat cyber threats and control how your data travels.
>
> Without Defender for Cloud Apps, your organisation will be missing out on the ability to better understand their overall cloud posture across

What is delivered to your organisation?

This product provides a solid foundation, a finely tuned configured setup of Sentinel, including analytics, workbooks, watch lists, and automated incident notifications. Allowing you to gain immediate value as well as a clear understanding of how Sentinel can be developed in the future.