Microsoft Sentinel in 30 Days

Accelerate your Security Information and Event Management (SIEM) migration to a cloud-based platform

The Challenge

On-premise SIEM platforms are typically difficult to manage. There are limited integrations with modern platforms, as well as often hit ingestion and storage limits that require additional hardware or appliances continue to provide necessary capabilities.

The Solution

The Spyglass MTG Microsoft Sentinel Jumpstart is a 4-Week Implementation that helps our customers accelerate their move to Microsoft Sentinel to provide a scalable, cost effective, and secure cloud based SIEM. As part of the deployment, we will do the following:

- Review existing SIEM platform to understand the current state as well as discuss current strategy for security operations
- Review existing cloud strategy to understand how public cloud is being used
- Using the information gathered, define an architecture for Microsoft Sentinel that would be scalable and secure as you move along your cloud journey
- Deploy and configure Microsoft Sentinel with the initial log sources, analytic rules/workbooks, initial automation framework and access control model to help them scale their usage of Microsoft Sentinel

Core Components

- Sentinel deployment and configuration
- Initial log source onboarding
- Initial Sentinel content based on current logs
- SOC knowledge transfer and process integration
- Initial automation of routine processes

Agenda

- Week 1: Analysis & Inventory
- Weeks 2: Design & Deployment
- Weeks 2-4: Onboarding & Integration
- Week 4: Response

Spyglass MTG Can Help!

We can help you accelerate your move to the cloud. <u>Contact us today</u>!

Infrastructure Azure
Data & AI Azure
Digital & App Innovation Azure
Modern Work
Security