Amesto Fortytwo

Managed Sentinel

amesto
Fortytwo

Managed Sentinel

- A standardized and effective way of managing Microsoft Sentinel configuration.
- Built on infrastructure-as-code to enable for controlled and trackable deployment.
- Enables fast onboarding of Microsoft Sentinel with a Common set of rules and configuration as a baseline serving different needs, ranging from insourcing to MDR/SOC as a service.

MANAGED SENTINEL

Why Managed Sentinel?

- Fast setup of Microsoft Sentinel
- Functionable configuration baseline from day one, including detection rules
- Shared, collaborative effort for development of detection rules – best of both worlds
- Avoid pitfalls and cumbersome reconfiguration at a later stage
- Built and maintained by a dedicated Microsoft security team

What is included in Managed Sentinel

Let us take care of your Sentinel platform so you can focus on your core business. Our security experts will ensure that your Microsoft Sentinel solution is always up to date with the latest threat detection mechanisms and properly integrated with other Microsoft security products, as well as 3.rd party integrations.

- Continuously updated Sentinel instance in your own Azure environment.
- Access to global threat intelligence and analysis.
- Analytics rules and ML based anomaly detection.
- Watchlists for extra correlation against critical entities.
- Incident creation logic with optional alerting to customer.
- Workbooks with response routines for most common alerts.

amesto
Fortytwo

www.amestofortytwo.com
Hello@amestofortytwo.com