PHOENIX

Microsoft Partner
Microsoft
2021 Partner of the Year Winner
United Kingdom

Sentinel Essentials

Inform and advise
24 hours | 7 days a week | 365 days a year

Reliable and efficient data and system security is paramount in today's dynamic digital landscape. With constant developments challenging organisations to remain ahead of potential threats and protect their systems, its vital that your cyber security solutions can identify and respond to threats quickly and effectively.

What is Sentinel Essentials?

Sentinel Essentials is a managed service provided by Phoenix that leverages the power of Microsoft Sentinel to provide you with a thorough understanding of what security events, issues, and threats are happening in real-time within your on-premise and cloud environments.

Through the analysis of log data constantly captured from your existing systems, Sentinel Essentials proactively identifies threats and supports you with a response to manage them.

Our cyber security analysts will work with you to identify security threats and provide a targeted response, utilising our industry experience alongside AI and machine learning algorithms developed by Microsoft.

Threat intelligence data within Sentinel provides further confidence by identifying security incidents that may be triggered and their relevant severities and impacts.

The benefits of Sentinel Essentials

Choosing our Sentinel Essentials service gives you access to our cyber security specialists who will analyse log data, identify current security threats, and respond quickly to cyber security incidents. The service is tailored specifically to your organisation's requirements and gives you confidence that your systems and data are protected.

> **"Sentinel Essentials proactively identifies threats and supports you with a response to manage them."**

What's included in Sentinel Essentials?

Security Information and Event Management (SIEM)

At the centre of our Sentinel Essentials service, we offer proactive management on an ongoing basis covering all aspects of Security Information and Event Management (SIEM).

This includes:

- Assessment, onboarding, and analysis of new log sources
- Assessment and breakdown of available threat intelligence
- Identification, verification, communication, and escalation of significant alerts and incidents
- Ongoing proactive management and support 24/7/365
- Provision of additional intelligence for significant alerts and incidents
- Trend analysis alerts to identify tactical and strategic security improvements
- Identification, analysis, and development of bespoke Sentinel workbooks (dashboards)
- Identification, analysis, and development of bespoke Sentinel playbooks, which builds automation into the service delivery

Platform management

In addition to identification and management of security incidents, Sentinel Essentials manages the core components of Sentinel's technology and other associated tools required to effectively deliver service excellence.

This management covers 'housekeeping' tasks, including feature and security updates (where applicable), and ongoing configuration to keep the service running and up-to-date.

Core platform management activities include:

- Monitoring and maintaining the availability and integrity of configured components
- Monitoring Microsoft's threat intelligence feed
- Monitoring of data sources connected to Sentinel
- Supporting Sentinel configuration changes resulting from customer change requests
- Supporting the investigation of technical issues relating to Sentinel
- Providing recommendations on Sentinel configuration improvements and implementing those recommendations where applicable
- Providing guidance on new Sentinel features and Sentinel platform upgrades
- Providing guidance on additional and optional features within or related to Sentinel
- Acting as point of contact to raise and monitor Sentinel issues flagged with Microsoft

Tiered service levels

Below is a high-level overview of the service attributes and different service tiers available with our Sentinel Essentials service, allowing us to tailor your service to meet your requirements.

SERVICE FEATURES	INFORM	ADVISE
Support hours[1]	8am – 6pm or 24/7/365	8am – 6pm or 24/7/365
Service level agreement	●	●
Support portal	●	●
Unlimited portal users	●	●
Email support	●	●
Security monitoring and alerting	●	●
Security bulletins	●	●
Nominated contacts	●	●
Service reporting dashboard	●	●
Customer success manager	●	●
Microsoft vendor escalation[2]	●	●
Incident management	●	●
Telephone support		●
Sentinel security management		●
Sentinel health check	Annual	Bi-annual
Essential data connector onboarding	Unlimited	Unlimited
Advanced data connector onboarding[2]		6
Premium data connector onboarding[2]		2
Security advice and guidance		●
Rule management		●
Custom rules per quarter[2]		8
Custom workbooks per quarter[2]		4
Custom automated playbooks per quarter[3]		1
Vendor escalation[4]		●
Regular service reviews		●
Computer security incident response plan (TBC)		●

[1]24/7/365 available as an upgrade to standard service levels.
[2]For platform issues and Microsoft created connectors.
[3]Additional can be purchased (charged on time spent)
[4]Non Microsoft vendors if vendor support is available

Strengthen your cyber security defences now

To speak with one of our cyber security specialists about how our Sentinel Essentials managed service will support your organisation's cyber security approach, arrange a call at a time that's convenient to you below.

BOOK NOW

01904 562200
hello@phoenixs.co.uk
www.phoenixs.co.uk

PHOENIX