A RICOH Company

G-Cloud 15
Managed Microsoft Sentinel SIEM/SOAR/SOC Service Pricing

MTI's Managed Microsoft Sentinel SIEM/SOAR/SOC is based on the volume of data and logs ingested into the customer's Microsoft Sentinel and Log Analytics workspaces each month. For our Full Managed Service, MTI's UK SOC performs 24x7x365 Monitoring, Analysis, and Detection of events, logs and alerts, threat hunting and conducts manual and automated response actions using the SIEM tooling and available SOAR integrations. We also offer options for out-of-hours only support and a Hybrid / Co-Managed Service.

Full Managed SIEM Service – 24x7x365 Monitoring & Response

Service Item	Monthly Log Data Ingestion Tier					
	0.5 - 1TB	1TB - 2.5TB	2.5TB - 4TB	4TB - 8TB	8TB - 16TB	16TB - 32TB
Once-Off Design, Architecture, Deployment and Onboarding	£37,425	£38,352	£39,278	£40,204	£46,982	£54,223
Annual Fully Managed SIEM Service price	£44,282	£49,840	£55,398	£60,955	£68,366	£75,776

Out-of-hours Only - Managed SIEM Support Service

Service Item	Monthly Log Data Ingestion Tier					
	0.5 - 1TB	1TB - 2.5TB	2.5TB - 4TB	4TB - 8TB	8TB - 16TB	16TB - 32TB
Once-Off Design, Architecture, Deployment and Onboarding	£37,425	£38,352	£39,278	£40,204	£46,982	£54,223
Annual Out of hours only SIEM Service price	£35,945	£38,724	£41,503	£44,282	£47,987	£51,692

Hybrid / Co-Managed SIEM Service

Service Item	Monthly Log Data Ingestion Tier					
	0.5 - 1TB	1TB - 2.5TB	2.5TB - 4TB	4TB - 8TB	8TB - 16TB	16TB - 32TB
Once-Off Design, Architecture, Deployment and Onboarding	£37,425	£38,352	£39,278	£40,204	£46,982	£54,223
Annual Co-Managed SIEM Service price	£38,261	£41,503	£44,282	£47,987	£52,619	£56,787

Notes:

1. Annual Prices are based on a 3-year contract.
2. Payment is provided annually in advance, with invoices payable within 30 days.
3. Pricing excludes VAT, which will be invoiced at the prevailing rate.
4. The Customer is responsible for all their Microsoft Azure, Sentinel, Log Analytics workspace, and storage costs. The pricing above is for MTI-delivered SOC services only.
5. Additional Forensic Incident Response Service is available as an option with a 24x7x365 response time of within 1 hour.
6. Installation / Onboarding cost for ingestion tiers up to the band “4TB to 8TB” allows for onboarding of up to 15 Log Sources that use either existing out-of-the-box Microsoft Sentinel Data Connectors, or ingestion of logs via Syslog. The Tier “8TB to 16TB” includes for 25 out-of-the-box Log Sources and the Tier “16TB to 32TB”, 30 Log sources. Ingestion of custom log parsers / data connectors is quoted for on a case-by-case basis.