

Managed Microsoft SOC and MDR Tender Questions

* Please note this is a generic guide for Microsoft Sentinel and Microsoft Defender customers: suggested questions and why each matter. Questions should be tailored for your organisation and technology stack.

1. Company Information

Ref	Question	Why it's important
1.1	How many years has your company been in business?	Checking credibility and longevity for business continuity reasons.
1.2	Please outline management and staff capabilities including: • Number and categories of staff employed; • Management structure chart; • Your company's relevant experience in carrying out an implementation of this scale; • The levels of experience within the team proposed to work with and support us; • Flexibility of interaction with staff, given your location and your ability to support our sites.	Checking quality, credibility, expertise and support of company and employees.
1.3	Please confirm that you can provide your financial accounts for the last three years and details of your company directors on request, and state whether any exclusion grounds under applicable public procurement rules (where relevant) apply to your organisation or its associated persons.	Financial standing and statutory due diligence.
1.4	Please provide details of relevant accreditations, for example ISO 27001, ISO 9001, Cyber Essentials or Cyber Essentials Plus.	Checking for proof of audits to recognised security and quality standards.
1.5	Where does the SOC Team Operate from? Include how many security operations centres (SOCs) you have.	Checking for local support and redundant SOC.
1.6	How many years have you been providing managed SIEM services, and what percentage of your business is derived from managed SIEM services?	Checking for credibility of performing the SOC/SIEM service.
1.7	How many employees does your company have, and how many of them are aligned to the managed SIEM business unit/service?	Understanding whether it is a core focus of the business and therefore likely to have more investment and attention in the service.
1.8	Describe the process for screening and hiring your security monitoring staff.	Due diligence on the provider's employees.
1.9	Explain the process of initial and ongoing training of your security monitoring staff.	Ensuring the SOC provider continuously trains staff and keeps them current to provide a good service.
1.10	Do you have up-to-date liability insurance? If so, please provide evidence.	Due diligence.
1.11	Please share the details of any significant third-party dependencies, the nature of these dependencies and any integration challenges they may pose.	Assessing business continuity risk.

Ref	Question	Why it's important
1.12	Do you or your affiliated companies process our data outside the UK, the European Economic Area, or any other jurisdiction we specify? If so, state where, why, and under what transfer mechanism.	Checking for data protection compliance.
1.13	Tenderers must provide contact details for two reference sites and include: organisation name, contact name and details, SIEM/SOC solution provided, similarity of solution scope, and duration of contract to date. At least one reference should be a customer using the proposed SIEM.	Due diligence of existing customers.
1.14	Can you provide case studies or references from customers in regulated or public sector environments, and explain how you support their compliance and reporting needs (for example GDPR)?	Checking they understand how to keep the organisation compliant and what information is needed on an ongoing basis.
1.15	State your managed service customer retention rate over the last three years.	Customer retention is a measure of service quality and long-term partnership.
1.16	How will we be prioritised alongside your largest customers? State the typical size of your customers and where we would sit within your customer base.	Checking the organisation receives the same attention and senior engagement as any larger customer.

2. Commercial, Contractual and Legal

Ref	Question	Why it's important
2.1	Indicate the licensing and pricing model(s) for your managed SOC and MDR service, and state clearly which components are licensed through Microsoft and which through you.	Understanding a predictable cost model to avoid hidden costs.
2.2	Describe the base cost and pricing methodology.	Understanding a predictable cost model to avoid hidden costs.
2.3	Provide details on one-time costs and recurring costs.	Understanding a predictable cost model to avoid hidden costs.
2.4	How are costs negotiated for upgrading or expanding the service? Can standard log sources be added without affecting pricing and service levels?	Understanding how pricing will change as the organisation grows and what additional costs are associated with the service.
2.5	Please complete the Inclusion Schedule in Appendix A. For each item, state whether it is included in the base fee, chargeable (with the rate), or not offered.	One consistent format allows costs to be compared like for like.
2.6	Separate Microsoft costs (for example Microsoft Sentinel ingestion, retention and data lake charges, Microsoft Defender and Security Copilot licences, and Azure Logic Apps) from your service fees. State any margin or handling charge you apply to Microsoft consumption, and who holds the billing relationship.	Showing which costs are set by Microsoft and which by the provider.

Ref	Question	Why it's important
2.7	Define what you classify as a standard log source and what you classify as a custom log source, and state the charge, if any, for each.	Avoiding disputes about what is included as the environment changes.
2.8	Please provide pricing for the current scope across all our sites, and for scenarios of +50% log volume, +100% log volume, and 10 additional log sources. Show any threshold at which charges change.	Showing how cost scales over the life of the contract.
2.9	State your price hold period, indexation cap, minimum term, auto-renewal terms, and the service credits that apply if service levels are missed.	Cost certainty over the contract term.
2.10	Please confirm you will act as a data processor under applicable data protection law (for example UK GDPR and the Data Protection Act 2018, or EU GDPR) and will enter into a Data Processing Agreement with us.	Compliance.
2.11	Detail how your SOC service ensures compliance with applicable data protection law (for example UK or EU GDPR) and relevant national cyber security guidance.	Compliance.
2.12	Tenderers must outline how they support and implement environmental and sustainable efficiencies in their practices and in the delivery of services.	Environmental practices of third-party suppliers are often needed for the organisation's own ESG metrics.
2.13	What social and governance initiatives does your organisation conduct? Please cite examples.	Often needed for the organisation's own ESG metrics.
2.14	Describe where any remotely stored data is kept, including logs, alerts, cases, backups and disaster recovery locations.	Compliance.

3. Partnership and Service Experience

Ref	Question	Why it's important
3.1	Name the roles that would act as our single point of contact, how we can reach them 24/7, and your target response time for non-incident queries.	The organisation should be able to reach the right people quickly, without chasing for updates.
3.2	Which people would be named and dedicated to us, and which would be drawn from a shared pool? Please state the roles and their experience.	Confirming the organisation will work with named people who understand its environment.
3.3	Describe your meeting cadence (for example weekly operational, monthly service, quarterly executive), who attends from your side, and how actions are tracked and followed through from one meeting to the next.	A strong relationship includes regular contact initiated by the provider.
3.4	If we made no contact for a month, what proactive contact would we receive? Provide an example of a typical month.	Testing how proactive the service is.
3.5	Provide anonymised examples of improvements or recommendations you raised with customers, without being asked, in the last three months.	Checking the provider proactively leads improvement.

Ref	Question	Why it's important
3.6	State analyst turnover for the team proposed to support us over the last 24 months, the proportion of customer contact handled by the same named individuals, and your handover process when personnel change.	A stable team builds knowledge of the organisation, which matters most during an incident.
3.7	Describe how your analysts come to understand our environment (for example asset criticality, key users, runbooks and what normal activity looks like) and how that knowledge is kept up to date.	Familiarity with the organisation before an incident speeds and improves response.
3.8	Beyond monitoring and response, describe how the service builds our cyber resilience over time, including roadmap, posture reviews and exercises. State which are included in the base fee.	Checking the service improves the organisation's security posture as well as monitoring it.

4. Service Requirements

Ref	Question	Why it's important
4.1	Describe your SOC model (for example 24/7 in one location, based in our region, Follow the Sun) and where your analysts are located.	To understand whether there are multiple SOC's, time zones, understanding of local laws and regulations, and compliance with data protection law.
4.2	Describe the delivery model of the managed SOC service (shared, dedicated, hybrid).	Will the organisation have access to the same resources who understand its environment and business?
4.3	Describe the structure of the delivery team of the managed SOC (levels/tiers).	The organisation needs to know who is doing what so it can trust the right actions are taken at each step of the response lifecycle, and that critical incidents will not be missed or delayed.
4.4	Describe how the team is organised in seniority, skillset and competencies.	Evaluating competency.
4.5	At what level of experience are your analysts? Please include anonymised sample CVs or role profiles for senior staff members.	Evaluating competency.
4.6	What is the number of employees in the SOC (permanent and contracted staff)? Detail how the SOC team is organised in terms of size, structure, seniority, skillset and competencies, including the number of staff in your SOC team and their experience levels.	Assessing the provider's capacity, reliability and consistency of service. High reliance on contractors may mean inconsistent analyst quality.
4.7	Define how service levels are maintained outside of core working hours.	Assessing whether teams are in place outside core business hours.
4.8	Outline your approach to continuous development of your SOC staff. What on-the-job training or professional development plans are in place?	Ensuring staff are kept well trained and up to date.

Ref	Question	Why it's important
4.9	Detail the rate of SOC staff retention.	Low retention can mean different analysts who do not understand the organisation's business.
4.10	Outline the experience and qualifications of your SOC personnel, including anonymised sample CVs or role profiles for SOC Manager, Tier 1, Tier 2 and Tier 3 analysts.	Evidence of competency.
4.11	Clearly describe the SOC offering and how it provides 24/7 monitoring, investigation and alerting, including create, manage, monitor and respond to SIEM events.	Explaining how the SOC operates to meet objectives.
4.12	Describe how you expect to manage staff turnover, staff career progression, leave, etc., for your personnel assigned to provide services.	Ensuring consistent staff.
4.13	How are you demonstrating thought leadership in cyber security?	For example, publishing whitepapers, speaking at conferences, and engaging in community events.

5. Incident Management and Incident Response

Ref	Question	Why it's important
5.1	What level of incident response capabilities do you offer, including first response triage and escalation procedures?	Does the SOC have a structured process to investigate incidents?
5.2	How do you handle escalation procedures for high-priority incidents?	Demonstrating the process.
5.3	How does your SOC coordinate with our internal teams, third-party vendors and relevant authorities (for example the data protection regulator) during security incidents or breaches?	Is there a structured workflow for communication?
5.4	What level of engagement and coordination can we expect between your SOC team and our management, especially during critical incidents or breaches?	How much will the organisation be kept informed during a breach?
5.5	How do you ensure that communication channels remain open and clear throughout ongoing incidents?	What backup procedures are in place if your systems are down?
5.6	Describe how you classify and prioritise incidents based on their severity and potential impact.	How severity is decided to meet response time SLAs.
5.7	What is the default retention period for security event logs and incidents?	Does it match the organisation's compliance requirements?
5.8	Clearly describe how your solution handles incident response workflows, from detection to resolution, and how you would ensure effective communication and collaboration between your SOC team and our internal team during critical incidents. Provide a detailed breakdown of the steps involved.	Outlining a structured process.

Ref	Question	Why it's important
5.9	Describe your containment authority model for our organisation. State which actions (for example isolating a device, disabling an account, blocking an indicator) are pre-authorised, which require our approval, and which are recommended only. Please use Microsoft Defender and Microsoft Sentinel as the reference.	Agreeing in advance who can act, and how quickly, protects the organisation's operations and speeds containment.
5.10	Describe any advanced incident response and digital forensic services that are included or available as a retainer with the managed SIEM monitoring service offering.	Are there additional costs for investigations that are outside traditional incident investigations?
5.11	Detail how you support forensic investigations and provide evidence for legal or regulatory proceedings, if necessary.	Can the provider carry out forensic investigations?
5.12	Do you assist with creating specific incident response use cases and maintain a runbook? If so, please describe how this is achieved.	A structured approach keeps the IR capability proactive, tailored and continuously improving.
5.13	What incident response methodologies do you follow (for example NIST, SANS)?	Does the provider follow industry best practice?

6. Operating the SOC

Ref	Question	Why it's important
6.1	Describe the process of upkeep and maintaining the detection rules in the SIEM to ensure coverage of the latest threats and the effectiveness of existing use cases.	How will the provider optimise the SIEM to ensure nothing is missed?
6.2	Monitor and measure the efficiency and quality of rules.	Will rules be continuously reviewed or only set up at the start?
6.3	Develop use cases employing advanced threat detection techniques.	Will the provider continuously optimise the environment as the threat landscape changes?
6.4	Leverage the MITRE ATT&CK framework to develop use cases and ensure full coverage.	Does the provider track TTPs against industry frameworks to keep use cases up to date?
6.5	State how many new detection use cases you deliver per customer per year as standard. Provide an example of the most recent one delivered for a comparable customer.	Detection capability needs to improve continuously as the environment and threats change.
6.6	How often are existing detections reviewed against changes in the environment and MITRE ATT&CK coverage, and how is coverage reported to us? State whether this is included in the base fee.	Keeping detections current as the environment changes.
6.7	How would we know its detection capability is better after 12 months than at the start? State the metrics and how they are reported.	Evidence of measurable improvement.
6.8	Who owns false-positive tuning? Describe how you proactively recommend tuning and how we are shown what was tuned and why. State whether tuning is included in the base fee.	A well-managed service becomes more accurate over time.

Ref	Question	Why it's important
6.9	Who maintains the mix of Microsoft-native, custom and provider-developed detection content, and how often is it updated?	Clear accountability for detection quality.
6.10	Indicate whether your company provides any of the following activities: SIEM health check, log source review, implementation of default analytics (rules, signatures, behaviours, etc.), and analytics tuning against the priorities of our organisation. Describe how each will be achieved.	Checking the SOC provider will continuously uplift the organisation's security maturity and posture.
6.11	Describe the log collection process and how it is supported, including how standard and custom log sources are onboarded. State the charge, if any, for each and any limit on the number of sources.	Understanding engineering capability and avoiding unexpected charges for new log sources.
6.12	Do you implement a regular cadence of new use cases and perform life cycle management? If yes, describe the process and frequency. Is this included in the base service price, or is it a premium service?	Is use case development included in the price?
6.13	How will continuous analytics tuning and optimisation be performed in order to reduce false positives?	A structured approach to reducing noise and alert fatigue allows greater attention on real incidents.
6.14	Tenderers must clearly describe how they will carry out fine tuning of analytics and alerts to meet our needs.	Getting the most out of the organisation's security investments.
6.15	Tenderers must clearly describe how new log sources are onboarded, including custom log sources.	Does the provider have engineering capability to bring in new log sources and build custom parsers?
6.16	Clearly describe your event correlation and analysis approach, highlighting how you identify patterns and anomalies.	Does the provider rely only on SIEM alerts, or also look at user behaviour and other trends?
6.17	What tools and technologies do you incorporate into your SOC service?	For example ticketing systems, SOAR platforms and custom-built tools that provide value.
6.18	How do you ensure every alert is reviewed and actioned?	Outlining controls and processes used in a mature SOC to ensure alert accountability and timely response.
6.19	How do you ensure log sources are always active and properly sending data to the SIEM?	What people, process and technology are in place to check the organisation is covered?

7. Threat Intelligence and Threat Hunting

Ref	Question	Why it's important
7.1	Describe the threat intelligence service provided as part of the offering.	How is threat intelligence used to enrich alerts and give analysts more information when triaging?
7.2	What threat intelligence sources or feeds do you use to enhance monitoring and detection capabilities?	Is there a broad range of feeds?
7.3	Which threat intelligence frameworks do you use to guide your SOC activities?	Following best practice (for example MITRE ATT&CK, STIX/TAXII).
7.4	Describe how you notify customers of new vulnerabilities and attack campaigns, the timeframe, and how you assess and explain whether they affect the customer's environment.	The organisation should hear about relevant threats before it needs to ask.
7.5	Describe how threat intelligence is contextualised to our Microsoft estate and how often we would receive relevant advisories. Provide an anonymised example from the last three months.	Intelligence is most useful when it is relevant to the organisation's own environment and risk.
7.6	Do we have access to your wider security expertise (for example senior analysts, threat intelligence and incident response specialists) as part of the service? State any limits on hours or access.	Checking for access to a security organisation as well as a monitoring service.
7.7	Describe your threat hunting service and the types of threat hunting methods delivered by leveraging industry frameworks.	Proactively looking for threats using best practice such as MITRE ATT&CK, DeTT&CT and the Cyber Kill Chain.
7.8	Is threat hunting performed as standard, or available as an additional service? State the frequency included in the base fee and how findings feed back into detection engineering.	Will the organisation need to pay extra?

8. Onboarding and Transition

Ref	Question	Why it's important
8.1	Approximately how long will the onboarding process take, given our requirements and log sources across all our sites?	Will it meet the organisation's deadline?
8.2	Provide the approach and methodology you will apply to the SOC migration, taking into account working with the current provider and tools, your experience with Microsoft Sentinel and Microsoft Defender, and access requirements.	Does the provider have a structured approach and demonstrable experience with the chosen platforms?
8.3	What is your process for onboarding a new client, particularly when transitioning security operations for a regulated or public sector organisation?	Demonstrating the approach.
8.4	What timeframes do you propose for the initial setup, onboarding and full deployment of your SOC services to an operational service?	How long will it take to reach an acceptable level of service?

Ref	Question	Why it's important
8.5	Describe your approach to building out the full detailed migration plan and highlight the proposed timeline, when it will be completed, and any prerequisites or dependencies, particularly on us.	Sharing the plan and what is needed from the organisation for a successful transition.
8.6	Outline what proactive steps will be taken to mitigate potential service interruptions during the migration plan, taking into account the desire to achieve the appropriate balance between risk and cost. Please show the structure of your proposed SOC migration team and how you expect it to align with our team.	Which risks could the organisation face, and which teams and resources are needed for a successful transition?
8.7	Describe how you would sequence onboarding across all our sites, how long standard and custom log sources typically take to onboard, and whether any parallel running period is charged.	Planning realistic timelines and costs across the whole estate.
8.8	How do you integrate with our existing security infrastructure (for example Microsoft Defender, endpoint protection, firewall systems) to enhance the effectiveness of the SOC?	Can the provider integrate with the organisation's infrastructure?
8.9	Describe the handover process, including transition and operational phase.	Checking the SOC provider will share information and uplift the knowledge of the organisation's staff.

9. Offboarding and Handover

Ref	Question	Why it's important
9.1	Tenderers must clearly describe how they will support an exit strategy to an alternative provider. This should include details on migration of data, temporary co-existence with the new platform, any charges for exit and data export, and other relevant information.	What activities will the provider perform and what will the organisation be left with?

10. Additional Services

Ref	Question	Why it's important
10.1	Tenderers are to state the availability of advanced security management services within their portfolio, include any additional relevant services, and provide day rates for these roles in the price response template.	Can the provider perform additional services and offer a competitive rate card to draw down on in the future?
10.2	What additional security services can you provide that will help with the overall service?	What other services can the provider offer to support this?
10.3	What additional services can you include as part of your proposal?	For example regular tabletop exercises, purple teaming, simulations and incident response tests.

11. AI-Enabled SOC and Microsoft Security

Ref	Question	Why it's important
11.1	Describe how you use the Microsoft Stack and AI agents in triage, investigation and response?	Understanding how AI is used to operate at machine speed.
11.2	For each stage (enrichment, triage, investigation, containment), state which actions are automated, which require analyst approval, and what audit trail and rollback exist.	Governance of automated actions.
11.3	State which AI capabilities require specific Microsoft licences or consumption (for example Microsoft 365 E5/7 or Security Copilot capacity), what we would pay Microsoft or you for them, and the assumptions you have made.	Avoiding surprise costs.
11.4	Describe your human oversight model for AI: who validates AI outputs, how accuracy is monitored, and how analyst decisions feed back into triage logic.	Accountability for decisions with material consequence.
11.5	Where are AI prompts, responses and our data processed and stored? Is our telemetry used to train any model, whether yours or a third party's?	Data protection and confidentiality.
11.6	Which AI components are proprietary to you and which depend on third-party providers? What happens to the service if a provider is withdrawn?	Business continuity of AI-enabled services.

12. Microsoft Sentinel and Defender Platform

Ref	Question	Why it's important
12.1	Indicate your experience managing Microsoft Sentinel and Microsoft Defender, including the number of customers, years of experience and relevant staff certifications.	Checking for experience with the organisation's platforms.
12.2	Our security team will require access to the SIEM platform. Please confirm that logins will be made available and whether any restrictions are associated with those logins.	Some SOC providers do not allow access to the SIEM.
12.3	What types of events and logs do you recommend collecting and monitoring?	Does the provider understand what needs to be collected to be a true security partner?
12.4	Does your solution support collection of all data source types from common cloud providers such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP)?	Does the platform support different cloud environments?
12.5	What data sources and log formats can your SIEM ingest?	Checking it can integrate easily.
12.6	How do you integrate with existing tools such as firewalls, EDR, IAM or cloud platforms?	Checking it can integrate easily.
12.7	To what extent can your solution address log management and reporting; incident investigations; forensic analysis; correlation of machine data; behaviour profiling and anomaly detection; application monitoring; integration with automation and orchestration solutions; and integration with UBA solutions?	How comprehensive is the solution?

Ref	Question	Why it's important
12.8	How scalable is the architecture? What data volumes can be ingested per day, and how is cost controlled as volume grows?	Can it grow with the organisation without unexpected cost?
12.9	Can you bring in multiple pieces of data during an incident (alerts, notes, attachments, reports, outputs of queries) and place them on a timeline? Can this information be used to produce incident reports?	Giving the organisation more information to understand an incident.
12.10	Can your solution automatically log analyst activities taken throughout the investigation?	Important for forensic investigations.
12.11	Does your solution have the ability to place, compare and track events, notable events, analyst notes and analyst actions within a single timeline or view?	Important for incident response.

13. Service Governance

Ref	Question	Why it's important
13.1	For SLA non-compliance, tenderers must detail how SLA non-compliances will be managed, what service credits apply, and what measures will be put in place to prevent recurrence.	Does the provider have a process for missed SLAs, and are there financial implications?
13.2	Describe a real-world example of how a client's risk reporting was tuned over time to identify real threats and minimise false positives. Provide timelines and the process required. Quantify the number of threats communicated during the tuning period.	An example of how the provider has improved a customer's security maturity and reduced risk.
13.3	Tenderers must clearly describe the reporting function of their solution, including analysis and customisation capabilities. Provide sample weekly, monthly and quarterly reports, and show how reporting demonstrates whether our security posture is improving over time in a form suitable for the Board and executive team.	Reporting should show whether the organisation is becoming more secure as well as what the SOC did.
13.4	Detail the frequency and format of meetings, including Service, Project, Change, Demand Management and general governance meetings.	A high-touch service that keeps the organisation updated and acts as a true partner.
13.5	Describe the structure of your Quarterly Business Review, including how actions and roadmap items are carried forward.	Continuity and governance.
13.6	Describe how service management is integrated as part of the service offering. Service management would include change management, incident, problem, asset and service compliance.	How does the provider ensure service governance is implemented?
13.7	What are the standard service levels offered, with clear linkage to service delivery? Describe your standard performance level metrics to indicate the effective delivery of the services.	Standard SLAs and performance metrics.
13.8	Do you provide any compliance reporting support, such as generating reports, custom reports and ad hoc reports? Please provide examples or templates.	Can the provider produce additional reports when needed, and is it an extra cost?

Ref	Question	Why it's important
13.9	Confirm the frequency of security reports you provide to clients and what key performance indicators (KPIs) are included in these reports (daily, weekly, monthly, quarterly, etc.).	How often will the organisation receive reports?
13.10	What are your guaranteed response times for different types of security incidents within the SOC?	SLAs against priorities.
13.11	Can you commit to a specific uptime percentage for your SOC services? What redundancy or failover mechanisms do you have in place?	Does the organisation need to account for any downtime?
13.12	Describe your performance review structure (weekly, quarterly, annual, etc.).	How will the provider review its own performance?
13.13	Can you provide detailed reporting on incidents, including root cause analysis and post-incident reviews? State your timescales for post-incident reports and how actions are tracked to closure.	How strong are the reports, and do they give the organisation the information to build resilience?
13.14	Provide details of any real-time incident dashboards or reporting tools for stakeholders to track the status of ongoing incidents.	How will the provider keep the organisation updated on incidents?
13.15	How do you ensure continuous improvement in your threat detection capabilities within the SOC?	What continuous improvement mechanisms are in the process to ensure the organisation keeps moving forward?
13.16	How do you incorporate lessons learned from past incidents into future improvements of your SOC operations?	Is the provider learning from incidents?
13.17	Tenderers must clearly describe how the service provides alerting.	How will the organisation be kept updated (email, phone, ticketing system)?
13.18	Tenderers must clearly describe how the service will give us full visibility of the security status of our assets and the performance of the SOC provider from a single real-time dashboard. State whether access is included in the base fee and the number of users.	Visibility of the organisation's security and of any missed SLAs.
13.19	Tenderers must clearly describe the roles and responsibilities between us and your organisation, to include Service, Project and Change Management and overall compliance.	A RACI to understand who is responsible.
13.20	Can we request custom dashboards for our own audiences, such as the Board, IT leadership and audit? State who builds them, the turnaround time, the number included in the base fee, and the charge for each additional one.	Dashboards for different audiences should not become a surprise cost.

Appendix A: Inclusion Schedule

For each item, mark whether it is included in the base fee, chargeable (and state the rate), or not offered. Use the notes column for any limits, caps or conditions.

Ref	Item	Included in base fee	Chargeable (state rate)	Not offered / notes
A.1	Standard log source integration (as defined in your response)			
A.2	Custom connectors and parsers			
A.3	Ingestion volume above the baseline			
A.4	New detection use cases			
A.5	Review of existing detections			
A.6	False-positive tuning			
A.7	Threat intelligence advisories specific to our organisation			
A.8	Threat hunting (state frequency)			
A.9	Incident response hours, forensics and onsite attendance			
A.10	Out-of-hours and bank holiday support			
A.11	Containment and response actions			
A.12	Custom, ad hoc and compliance reports			
A.13	Quarterly Business Reviews and executive reporting			
A.14	Named analysts and Service Delivery Manager			
A.15	Premium or enhanced support tiers			
A.16	Customer portal users and API access			
A.17	Onboarding, migration and parallel running			
A.18	Change requests, additional sites or tenants			
A.19	Health checks, posture reviews and tabletop exercises			
A.20	AI and agent features, including third-party agent licensing			
A.21	Microsoft Sentinel workspace and retention management			
A.22	Exit, offboarding and data export			