inara TECHNOLOGIES

The Enterprise Buyer's Guide to Selecting a Managed Security Provider

5-Dimension evaluation framework · 20-question RFP scorecard · SLA structure · onboarding governance

Due Diligence Framework for MSSP Procurement

DOCUMENT TYPE	PUBLISHER	YEAR	AUDIENCE
Industry Whitepaper	Inara Technologies	2026	Enterprise & Government

TABLE OF CONTENTS

S. No.		Pg. No.
01-	Why MSSP Selection Fails	4
02-	The Five-Dimension Capability Framework	5
03-	SLA Structure: What to Demand	6
04-	Onboarding Governance	7
05-	Tooling Transparency & Data Portability	8
06-	Regulatory & Compliance Alignment	9
07-	MSSP Due Diligence Scorecard	10

Executive Summary

The managed security services market is among the most crowded in enterprise technology. Every provider claim 24/7 monitoring, advanced threat detection, and rapid incident response. The reality — visible to any buyer who looks past the marketing claims — is that the gap between claimed and delivered capability is wider in this market than in almost any other IT services segment.

This guide gives enterprise and government security buyers the tools to close that gap: a structured evaluation framework, the right due diligence questions, and a 20-item RFP scorecard that separates genuine managed security operations from managed detection theatre.

Central Argument: The most important MSSP evaluation dimension is not technology. It is the quality of the response playbook library, the escalation governance model, and the transparency of the reporting framework. These three dimensions predict operational outcomes more reliably than any technology stack comparison.

WHY MSSP SELECTION FAILS

Common Procurement Mistakes

Enterprise and government buyers consistently make the same mistakes in MSSP procurement. Understanding these failure patterns is the first step to avoiding them.

Technology-First Evaluation

Selecting based on the vendor's SIEM/SOAR platform before evaluating the operational team that runs it. A world-class tool operated by an under-resourced team delivers poor outcomes. An average tool operated by a disciplined, well-governed team delivers good ones.

Treating "24/7 Monitoring" as a Meaningful Differentiator

"24/7 monitoring" is a baseline expectation, not a capability claim. The relevant questions are: What is the analyst-to-alert ratio on the overnight shift? What is the escalation time for a P1 detection at 3 a.m.? How many analysts are actively monitoring vs on-call?

Ignoring Onboarding Governance

The onboarding phase – telemetry integration, detection baseline, playbook development – is where most MSSP engagements underdeliver. A provider that cannot describe their onboarding process in detail has not thought about it carefully.

Accepting Vague SLA Commitments

Response time SLAs without corresponding resolution SLAs and measurement methodology are commercially meaningless. Demand MTTD and MTTR commitments by priority, with defined measurement periods and consequences for repeated misses.

The Five-Dimension Capability Framework

Evaluating MSSP Maturity Across Five Dimensions

Use the following five dimensions to structure your evaluation. Score each provider 1–4 per dimension. A provider scoring below 2.5 average across all five should not be shortlisted, regardless of commercial attractiveness.

#	Dimension	What to Evaluate
01	Analyst Depth & Team Structure	Size and seniority of the analyst team. Shift coverage model. Analyst-to-client ratio on overnight shifts. Career development and retention indicators.
02	Detection Engineering Quality	How detection rules are written, tuned, and maintained. False positive rate and how it is managed. Process for adding new detections in response to emerging threats.
03	Response Playbook Library	Number of documented playbooks. Coverage of priority threat scenarios. Playbook testing cadence (tabletop and simulated). Customization capability.
04	Tooling Transparency & Data Portability	Clarity on SIEM/SOAR ownership model. Data retention policy and export capability. What happens to client data and detections if the engagement ends.
05	Reporting Quality & Transparency	Sample reports – are they operational data or management insight? Frequency of client-facing reviews. CISO-level briefing capability.

SLA Structure:
What to Demand

Moving Beyond "24/7 Monitoring"

A meaningful managed SOC SLA includes four components: detection commitment (MTTD), response commitment (analyst acknowledgement), resolution commitment (MTTR), and reporting commitment. All four must be defined, measured, and subject to consequences for repeated misses.

SLA Component	What to Demand	Red Flags in Provider Response
MTTD	Defined per threat category; not a single average	"We detect everything" – not a real commitment
Response Time	P1: ≤15 min; P2: ≤30 min; P3: ≤2 hrs	Response time only without resolution SLA
MTTR	P1: ≤4 hrs; P2: ≤8 hrs; measured and reported	MTTR not tracked or "client-dependent" deflection
Reporting Cadence	Weekly operational; monthly management review	Reports available "on request" – no proactive cadence
SLA Breach Consequence	Defined escalation + service credit mechanism	No consequence model – SLAs are aspirational
Measurement Period	Rolling monthly with published methodology	Unmeasured or self-reported only

Onboarding Governance

The 30/60/90-Day Milestone Model

A responsible MSSP should be able to describe their onboarding process in detail before a contract is signed. The onboarding phase is where the provider's operational discipline is most visible — and where the gap between well-run and poorly-run providers is most apparent.

Phase	Timeline	Key Deliverables	Client Input Required
Discovery & Access	Days 1–14	Asset inventory; telemetry source mapping; existing security tool audit; stakeholder RACI defined	Asset list; tool access; security contacts
Telemetry Integration	Days 15–30	SIEM ingestion confirmed for all in-scope sources; data quality validation; baseline alert noise	Tool access; firewall rules for log forwarding
Detection Baseline	Days 31–60	Custom detection rules tuned to environment; false positive rate below agreed threshold	Environment-specific context; approval of rules
Playbook Completion	Days 45–75	Priority playbooks completed and reviewed; tabletop exercise conducted; escalation path tested	Attendance at tabletop; CISO/IT sign-off
Full Operations	Day 90	Full 24/7 coverage; first monthly report delivered; formal SLA measurement begins	Monthly review attendance; feedback on reports

Tooling Transparency & Data Portability

Avoiding Lock-In and Protecting Data Portability

SIEM and SOAR tooling creates data and intellectual property that has long-term operational value: detection rules, investigation notebooks, playbooks, and historical alert data. Understanding the ownership model for this content – and what happens to it if the MSSP engagement ends – is a critical due diligence question.

Key Questions on Tooling and Data

- Who owns the SIEM license – the MSSP or the client? What happens to the license and data if the engagement ends?
- Can client-specific detection rules and playbooks be exported in a standard format? What are the portability constraints?
- What is the data retention policy? Where is data stored? Does storage comply with the client's data residency requirements?
- Is the MSSP's tooling stack disclosed upfront? Are there undisclosed sub-processors or third-party telemetry sharing arrangements?
- What is the MSSP's process for accommodating new telemetry sources? Is there a cost per source, or is integration included?

Regulatory & Compliance Alignment

Pakistan PDPA, ISO 27001, and Sector-Specific Requirements

For organizations in regulated sectors, MSSP compliance alignment is not optional. The provider must demonstrate that their operational model, data handling practices, and delivery team are compatible with the applicable regulatory framework. This is particularly relevant for government and defense buyers with Pakistan-based delivery requirements.

Requirement	What to Verify	Documentation to Request
Data residency	All client data processed and stored within Pakistan	Data Processing Agreement with residency clause
ISO 27001	Provider holds current certification	Certificate + scope statement
Team background screening	All SOC analysts with client data access have been screened	Screening policy + process description
Access governance	Role-based access with full audit trail	Access management policy; sample audit report
Incident reporting	Defined process for regulatory breach notification	Incident notification SLA; escalation procedure
Subcontractor disclosure	No undisclosed sub-processors with client data access	Sub-processor list; DPA flow-down requirements

The 20-Question MSSP Due Diligence Scorecard

Use the following questions in RFP responses, provider presentations, and reference checks. Score each response 0 (not addressed), 1 (partially addressed), or 2 (fully addressed). A provider scoring below 30/40 should not advance to commercial evaluation.

#	Category	Question	Score /2
Q1	Analyst Operations	How many analysts are on shift during overnight weekday hours? What is the analyst-to-client ratio?	__ /2
Q2	Analyst Operations	What is the average tenure and seniority profile of your SOC analyst team?	__ /2
Q3	Analyst Operations	Describe your analyst escalation path for a P1 detection – from detection to L3 in detail.	__ /2
Q4	Detection Engineering	How are detection rules developed, maintained, and tuned? How often are they reviewed?	__ /2
Q5	Detection Engineering	What is your current false positive rate across clients? How is it measured?	__ /2
Q6	Detection Engineering	Describe how you operationalize new threat intelligence – from feed to deployed detection rule.	__ /2
Q7	Response Playbooks	How many documented response playbooks do you maintain? List coverage for ransomware, phishing, identity compromise, and lateral movement.	__ /2
Q8	Response Playbooks	How are playbooks customized for a new client environment? What is the timeline?	__ /2
Q9	Response Playbooks	Describe your last tabletop exercise – scenario, participants, and output.	__ /2
Q10	SLA Commitments	What are your committed MTTD and MTTR targets by priority level? How are they measured?	__ /2
Q11	SLA Commitments	What is the consequence model for repeated SLA misses?	__ /2
Q12	SLA Commitments	Provide a sample monthly report from a comparable client (redacted).	__ /2

Q13	Tooling & Data	Who owns the SIEM license? What happens to client data and detection rules if the engagement ends?	__ /2
Q14	Tooling & Data	Where is client data stored? Does your data residency model comply with Pakistan PDPA requirements?	__ /2
Q15	Tooling & Data	List all third-party sub processors with access to client telemetry data.	__ /2
Q16	Onboarding	Describe your standard onboarding process – key milestones, client input required, and go-live criteria.	__ /2
Q17	Onboarding	How long does full telemetry integration typically take? What are the most common delays?	__ /2
Q18	Onboarding	Provide the escalation contact list for a hypothetical P1 incident at 2 a.m. on a public holiday.	__ /2
Q19	Compliance	Do you hold current ISO 27001 certification? Provide the certificate and scope statement.	__ /2
Q20	References	Provide two references from clients in comparable sectors who have been with you for more than 12 months.	__ /2

Scoring Guide: Below 24/40: Do not advance | 24–32/40: Conditional — address gaps before contracting | 33–40/40: Qualified for commercial evaluation