vijilan
IT Security: Enabled

10 QUESTIONS TO ASK

BEFORE CHOOSING A MANAGED SOC PROVIDER

WHY THESE QUESTIONS MATTER

Not all managed SOC providers are created equal. Some stop at alerting. Others provide true 24/7 coverage. A few actually remediate threats.

These 10 questions will help you separate marketing claims from operational reality—and find a SOC partner that actually protects your organization.

THE QUESTIONS

1 What is your actual response time SLA?

Why it matters: "Average" response times are meaningless. A 15-minute average could mean some incidents take hours. Look for *guaranteed* SLAs with penalties.

What to look for:
- Guaranteed response time (not average)
- Different SLAs by severity (P1 vs P4)
- Contractual commitment with remedies
- 15-30 minutes for critical threats

🚩 Red flag: "We respond as quickly as possible" or "industry-leading response times" without specific numbers.

2 Who actually reviews the alerts—humans or automation?

Why it matters: AI and automation are great for initial triage, but critical decisions should involve human judgment. Pure automation leads to missed context and false negatives.

What to look for:
- Human analysts review critical alerts
- Clear escalation from automated to human
- Named analysts or dedicated team
- Analyst certifications (GCIA, GCIH, OSCP)

🚩 Red flag: "Our AI handles 99% of alerts automatically" without human oversight.

3 Do you provide full remediation or just containment?

Why it matters: Containment stops the bleeding. Remediation fixes the wound. Many providers isolate a threat and hand it back to you—at 2 AM on a Saturday.

What to look for:
- Full remediation included (not just alerting)
- Malware removal and system restoration
- Root cause elimination
- Clear definition of where their responsibility ends

🚩 Red flag: "We detect and alert; remediation is your responsibility."

4 What happens after business hours?

Why it matters: 76% of ransomware attacks are deployed outside business hours. A SOC that scales down at night isn't truly 24/7.

What to look for:
- Same staffing levels nights/weekends
- No "on-call only" coverage gaps
- Same SLAs regardless of time
- Global SOC locations for follow-the-sun coverage

🚩 Red flag: "After-hours alerts are queued for morning review" or "on-call analyst will respond within 4 hours."

5 How do you handle identity-based attacks?

Why it matters: 80% of breaches involve compromised credentials. EDR alone won't catch attackers who log in with valid credentials.

What to look for:
- Identity threat detection (ITDR) included
- Active Directory monitoring
- Lateral movement detection
- Credential theft prevention (pass-the-hash, etc.)

🚩 Red flag: "Identity protection is available as an add-on" or not mentioned at all.

6 What's included vs. what costs extra?

Why it matters: Many providers advertise low base prices, then charge extra for incident response, threat hunting, or additional endpoints.

What to look for:
- Clear, all-inclusive pricing
- No per-incident fees
- Threat hunting included (not add-on)
- Defined endpoint/user limits

🚩 Red flag: Vague pricing, "contact us for IR fees," or long lists of paid add-ons.

7 Can I see a sample incident report?

Why it matters: The quality of communication during an incident matters as much as the technical response. Vague reports waste your time and don't support compliance.

What to look for:
- Detailed timeline of events
- Clear root cause analysis
- Specific remediation steps taken
- Recommendations for future prevention
- Compliance-ready format

🚩 Red flag: Refusal to share samples, or generic "threat detected and resolved" summaries.

8 What's your customer retention rate?

Why it matters: High churn suggests customers aren't getting value. Happy customers stay.

What to look for:
- 90%+ retention rate
- Average customer tenure (3+ years is good)
- References from long-term customers
- Case studies with named companies

🚩 Red flag: Evasive answers, no references available, or "we don't track that."

9 What security technology do you use?

Why it matters: The platform matters. A SOC built on legacy SIEM can't match one built on modern cloud-native technology.

What to look for:
- Named platforms (CrowdStrike, Sentinel, etc.)
- Cloud-native architecture
- Single-agent approach (less overhead)
- Integration with your existing tools

🚩 Red flag: Proprietary or unnamed technology, or "we're platform-agnostic" (often means lowest-common-denominator).

10 How do you demonstrate value over time?

Why it matters: Security is hard to measure. A good SOC partner proactively shows ROI, not just monthly invoice.

What to look for:
- Regular business reviews (monthly/quarterly)
- Metrics dashboard with trending
- Comparison to industry benchmarks
- Continuous improvement recommendations

🚩 Red flag: No proactive reporting, or "reports available upon request."

vijilan
IT Security: Enabled

vijilan.com
info@vijilan.com
+1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN

EVALUATION SCORECARD

Question	Weight	Score (1-5)	Notes
Response SLA	High		
Human vs. Automation	High		
Remediation scope	Critical		
After-hours coverage	Critical		
Identity protection	High		
Pricing transparency	Medium		
Report quality	Medium		
Retention rate	Medium		
Technology platform	High		
Value demonstration	Medium		
TOTAL		/50	

Scoring Guide:
- 45-50: Excellent candidate
- 35-44: Good, clarify gaps
- 25-34: Significant concerns
- Below 25: Keep looking

AICPA SOC | ISO 27001 | A-LIGN

HOW VIJILAN ANSWERS

Question	Vijilan Answer
Response SLA	15 minutes guaranteed (Premium)
Human review	Certified analysts (GCIA, GCIH, OSCP)
Remediation	Full remediation included
After-hours	Same coverage 24/7/365
Identity	ITDR included in Premium
Pricing	All-inclusive, no surprise fees
Reports	Detailed incident reports, weekly summaries
Retention	95%+ customer retention
Technology	CrowdStrike Falcon platform
Value	Monthly business reviews, risk trending

READY TO EVALUATE?

Schedule a call with Vijilan to see how we answer these questions—and any others you have.

vijilan
IT Security: Enabled

vijilan.com
info@vijilan.com
+1 (954) 334-9988

SCAN HERE TO BOOK A FREE DEMO