vijilan
IT Security: Enabled

10 QUESTIONS TO ASK

BEFORE CHOOSING A SIEM PROVIDER

WHY THESE QUESTIONS MATTER

SIEM is often the most expensive security investment —and the most disappointing. These questions help you avoid costly mistakes and find a platform that actually delivers value.

THE QUESTIONS

1 How is pricing calculated?

Why it matters: Volume-based pricing punishes you for better visibility. Ingesting more logs shouldn't bankrupt your security budget.

What to look for:
- Predictable pricing model
- No penalties for data volume spikes
- Clear understanding of total cost
- No hidden fees for features

Red flag: Per-GB pricing without caps, or "it depends on your data."

2 How fast is search across large data sets?

Why it matters: Investigations require fast queries. If search takes minutes, analysts waste hours waiting.

What to look for:
- Sub-second search (even at scale)
- Demo with realistic data volumes
- No performance degradation over time
- Real-time streaming queries

Red flag: "Search times vary" or demos only on small datasets.

3 What's the architecture—index-based or streaming?

Why it matters: Traditional index-based SIEMs are expensive and slow at scale. Modern streaming architectures (like LogScale) eliminate these constraints.

What to look for:
- Index-free or streaming architecture
- Cloud-native design
- Horizontal scalability
- No infrastructure bottlenecks

Red flag: Heavy on-prem infrastructure requirements.

4 What log sources are supported out-of-box?

Why it matters: Custom parsers take months to build. Pre-built integrations accelerate time-to-value.

What to look for:
- 100+ pre-built integrations
- Common sources included (Windows, firewalls, cloud)
- Easy custom parser creation
- Community content available

Red flag: "We can build custom parsers" as the primary answer.

5 What detection content is included?

Why it matters: A SIEM without detections is just expensive log storage. Pre-built rules accelerate your security program.

What to look for:
- 500+ pre-built detection rules
- MITRE ATT&CK mapping
- Regular rule updates
- Easy custom rule creation

Red flag: "Detections are your responsibility" or minimal out-of-box content.

6 How long does deployment typically take?

Why it matters: Legacy SIEM deployments take 12-18 months. Modern platforms deploy in weeks.

What to look for:
- Weeks, not months
- Cloud-native (minimal infrastructure)
- Phased onboarding approach
- Quick time-to-first-detection

Red flag: "Plan for 6-12 months" or extensive professional services required.

7 What's the retention policy and cost?

Why it matters: Compliance often requires 1+ year retention. Storage costs can explode with legacy architectures.

What to look for:
- 1+ year retention affordable
- Tiered storage (hot/warm/cold)
- No surprise storage fees
- Easy data replay from archive

Red flag: Short retention defaults or expensive long-term storage.

8 Do you offer managed SIEM services?

Why it matters: Even great platforms require expertise to operate. Managed options reduce your operational burden.

What to look for:
- Fully managed option available
- 24/7 monitoring included
- Tuning and optimization
- Detection engineering support

Red flag:** "Platform only—you operate it."

9 How do you handle compliance reporting?

Why it matters: Manual compliance reporting wastes analyst time. Built-in reports accelerate audits.

What to look for:
- Pre-built compliance dashboards
- HIPAA, PCI, SOC 2, CMMC templates
- Automated evidence collection
- Audit-ready exports

Red flag: "Build your own reports" or generic templates only.

10 What's the migration path from our current SIEM?

Why it matters: Switching SIEMs is painful. A clear migration path reduces risk and accelerates transition.

What to look for:
- Documented migration methodology
- Detection rule translation
- Parallel running support
- Professional services for migration

Red flag: "Start fresh" or no migration support.

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
Pricing model	Critical		
Search speed	Critical		
Architecture	High		
Log sources	High		
Detection content	High		
Deployment time	Medium		
Retention/storage	High		
Managed services	Medium		
Compliance reports	Medium		
Migration support	Medium		
TOTAL		/50	

AICPA SOC

ISO 27001

A-LIGN

HOW VIJILAN ANSWERS

Question	Vijilan Answer
Pricing	Predictable, not volume-based
Search speed	Sub-second (LogScale)
Architecture	Index-free streaming
Log sources	100+ pre-built
Detections	500+ rules, MITRE mapped
Deployment	2-4 weeks
Retention	1 year standard
Managed	Fully managed available
Compliance	HIPAA, PCI, CMMC dashboards
Migration	Full migration services

vijilan
IT Security: Enabled
vijilan.com
info@vijilan.com
+1 (954) 334-9988

SCAN HERE TO BOOK A FREE DEMO