vijilan
IT Security: Enabled

10 QUESTIONS TO ASK

BEFORE CHOOSING AN ITDR PROVIDER

WHY THESE QUESTIONS MATTER

Identity Threat Detection & Response (ITDR) protects the #1 attack vector: credentials. With 80% of breaches involving compromised identities, choosing the right ITDR is critical.

THE QUESTIONS

1 Do you protect Active Directory, cloud identity, or both?

Why it matters: Modern environments span on-prem AD and cloud (Entra ID, Okta). Gaps in coverage leave attack vectors open.

What to look for:
- Active Directory monitoring
- Microsoft Entra ID (Azure AD) protection
- Okta/other IdP integration
- Unified visibility across all identity sources

🚩 Red flag: "Cloud identity is separate" or AD-only coverage.

2 What identity attacks can you detect?

Why it matters: ITDR should catch sophisticated credential attacks, not just brute force.

What to look for:
- Pass-the-hash / Pass-the-ticket
- Kerberoasting / AS-REP roasting
- Golden Ticket / Silver Ticket
- DCSync attacks
- Credential stuffing / spraying
- Token theft

🚩 Red flag: Only detects failed logins or basic anomalies.

3 How do you detect lateral movement?

Why it matters: Attackers move through networks using valid credentials. ITDR must track this movement.

What to look for:
- Cross-system authentication tracking
- Unusual access pattern detection
- Service account monitoring
- Jump host/bastion tracking

🚩 Red flag: No lateral movement detection or "that's a network tool function."

4 Do you provide identity hygiene assessment?

Why it matters: Weak identity configurations enable attacks. Ongoing hygiene finds risks before attackers do.

What to look for:
- Privileged account discovery
- Stale account identification
- Password policy assessment
- Service account audit
- Shadow admin detection

🚩 Red flag: Detection-only with no hygiene/posture capabilities.

5 Can you prevent attacks or only detect them?

Why it matters: Detection without prevention means attackers succeed while you watch.

What to look for:
- Real-time blocking capabilities
- Conditional access integration
- Account lockout/disable
- MFA enforcement triggers
- Honeypot/deception options

🚩 Red flag:** "We alert, you respond."

6 How do you integrate with endpoint detection?

Why it matters: Identity attacks often start at endpoints. Correlated identity + endpoint visibility reveals the full attack story.

What to look for:
- Native EDR integration
- Unified alerts and timeline
- Cross-domain correlation
- Single console for both

🚩 Red flag: Siloed product with no endpoint correlation.

7 What's the deployment impact on domain controllers?

Why it matters: Domain controllers are critical infrastructure. Heavy monitoring agents risk availability.

What to look for:
- Lightweight or agentless options
- No DC performance impact
- No schema changes required
- Non-intrusive monitoring

🚩 Red flag: Requires agents on all DCs or schema modifications.

8 How do you handle service accounts?

Why it matters: Service accounts are often overprivileged, never rotated, and invisible. They're prime attacker targets.

What to look for:
- Service account discovery
- Usage monitoring
- Anomaly detection
- Recommendations for hardening

🚩 Red flag: "Service accounts are treated like regular users."

9 What Zero Trust capabilities are included?

Why it matters: ITDR should enable Zero Trust, not just detect attacks.

**What to look for:
- Risk-based authentication
- Conditional access policies
- Continuous verification
- Least privilege recommendations

🚩 Red flag: Zero Trust mentioned only in marketing.

10 Is managed ITDR available?

Why it matters: Identity attacks require expert investigation. Managed services provide 24/7 protection.

What to look for:
- 24/7 identity monitoring
- Expert investigation included
- Response actions taken on your behalf
- Identity-specific SLAs

🚩 Red flag:** Self-service only.

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
Identity coverage	Critical		
Attack detection	Critical		
Lateral movement	High		
Identity hygiene	High		
Prevention	High		
EDR integration	High		
DC impact	Medium		
Service accounts	High		
Zero Trust	Medium		
Managed services	Medium		
TOTAL		/50	

AICPA SOC

International Organization for Standardization ISO 27001

A-LIGN

HOW VIJILAN ANSWERS

Question	Vijilan Answer
Identity coverage	AD + Entra ID + Okta
Attack detection	All advanced identity attacks
Lateral movement	Full tracking and alerting
Identity hygiene	Continuous assessment
Prevention	Real-time blocking available
EDR integration	Native Falcon integration
DC impact	Lightweight, non-intrusive
Service accounts	Full discovery and monitoring
Zero Trust	Risk-based access enabled
Managed	24/7 identity SOC