EVALUATION CHECKLIST

MDR provider evaluation checklist

Compare providers side by side and find the gaps before the demos start. Fill in what each one actually offers, add rows for anything specific to your environment, and take the result into your shortlist conversations.

How to use this checklist

Bring this to your shortlist conversations. Fill in what each provider actually offers, then add rows for anything specific to your environment.

This is a quick yes, no, or maybe pass. It narrows a long list—it won't replace a proof of concept.

Blank cells are as useful as checked ones. Note where a provider couldn't answer.

Criteria for evaluating a managed detection and response (MDR) provider

Criteria	Vendor 1: Expel	Vendor 2:	Vendor 3:
TECHNOLOGY AND COVERAGE			
Endpoint protection support	✓	☐	☐
Cloud environment monitoring (AWS, Azure, Google Cloud, Oracle, etc.)	✓	☐	☐
Kubernetes and container security	✓	☐	☐
Cloud security tool coverage (Wiz, Orca, FortiCNAPP, etc.)	✓	☐	☐
SaaS application monitoring	✓	☐	☐
Network traffic analysis	✓	☐	☐
Email security coverage	✓	☐	☐
Identity and access management	✓	☐	☐
SecOps and SIEM coverage	✓	☐	☐
Notification system coverage	✓	☐	☐
Ticketing system coverage	✓	☐	☐
Bring-your-own-tech approach	✓	☐	☐
API-based connectivity	✓	☐	☐
AI-assisted rule creation	✓	☐	☐
AI-assisted threat scoring	✓	☐	☐
AI-assisted alert prevalence analysis	✓	☐	☐
AI-assisted script analysis	✓	☐	☐
Custom detection support	✓	☐	☐
Can you swap a tool without re-onboarding?	✓	☐	☐
Data normalization across sources	✓	☐	☐
Evidence preservation for forensics	✓	☐	☐
DETECTION AND RESPONSE			
Custom detection engineering	✓	☐	☐
AI-assisted triage	✓	☐	☐
AI-assisted anomaly detection	✓	☐	☐
AI-assisted weak signal correlation	✓	☐	☐
AI-assisted identity classification	✓	☐	☐
False positive reduction	✓	☐	☐
Hypothesis-based threat hunting	✓	☐	☐

VENDOR 1 NOTES: EXPEL

Type your notes...

VENDOR 2 NOTES:

Type your notes...

VENDOR 3 NOTES:

Type your notes...

Criteria	Vendor 1: Expel	Vendor 2:	Vendor 3:
Published mean time to detect (MTTD)	✓	☐	☐
Published mean time to respond (MTTR)	✓	☐	☐
Published mean time to remediate (MTTR)	✓	☐	☐
Contractual SLA for critical alerts	✓	☐	☐
Playbook execution	✓	☐	☐
Active response capabilities	✓	☐	☐
Automated remediation	✓	☐	☐
AI-assisted resolution of low-risk findings	✓	☐	☐
Deep incident investigation	✓	☐	☐
Context enrichment	✓	☐	☐
Cross-environment correlation	✓	☐	☐
ANALYST EXPERTISE			
24x7 coverage	✓	☐	☐
AI-assisted investigations	✓	☐	☐
Experienced security analysts	✓	☐	☐
Specialization depth	✓	☐	☐
Analyst-to-customer ratio	✓	☐	☐
Direct SOC access	✓	☐	☐
Dedicated customer success	✓	☐	☐
Continuous analyst training	✓	☐	☐
Quality control processes	✓	☐	☐
Incident response coordination	✓	☐	☐
Business context understanding	✓	☐	☐
TRANSPARENCY			
Real-time investigation visibility	✓	☐	☐
Full audit trail access	✓	☐	☐
Reporting you can hand to your board	✓	☐	☐
Event search capabilities	✓	☐	☐
Metrics transparency	✓	☐	☐
Detection logic visibility	✓	☐	☐
Roadmap visibility	✓	☐	☐
Direct platform access	✓	☐	☐
Collaboration features	✓	☐	☐
Alert contextualization	✓	☐	☐
AI-assisted incident findings reports	✓	☐	☐
AI-assisted investigation summaries	✓	☐	☐
AI-assisted management reporting	✓	☐	☐
Performance benchmarking	✓	☐	☐
Quality metrics	✓	☐	☐