expel

Provider checklist criteria for evaluating MDR

How to use this checklist

This checklist operates as a brief comparison document to support you through budget evaluation (and consequently, vendor shopping) season. Use it to compare MDR vendor basic offerings, and add in specifics for your org to make sure you know what you're getting across the board.

This is meant to be a yes/no/maybe quick evaluation. You'll always want to take a deeper dive into vendor tools and platforms, and even complete a proof of concept if possible.

Criteria	Vendor 1: Expel	Vendor 2:	Vendor 3:
Technology & coverage			
Endpoint protection support	✓	☐	☐
Cloud environment monitoring (AWS, Azure, Google Cloud, Oracle, etc.)	✓	☐	☐
Kubernetes & container security	✓	☐	☐
Cloud security solutions (Wiz, Orca, FortiCNAPP, etc.)	✓	☐	☐
SaaS application monitoring	✓	☐	☐
Network traffic analysis	✓	☐	☐
Email security integration	✓	☐	☐
Identity & access management	✓	☐	☐
Sec Ops & SIEM integrations	✓	☐	☐
Notification systems integration	✓	☐	☐
Ticketing system integrations	✓	☐	☐
Bring-your-own tech approach	✓	☐	☐
API-based connectivity	✓	☐	☐
AI-assisted rule creation	✓	☐	☐
AI-assisted threat scoring	✓	☐	☐
AI-assisted alert prevalence	✓	☐	☐
AI-assisted script translation	✓	☐	☐
Custom detection support	✓	☐	☐
Tool flexibility and swap capabilities	✓	☐	☐
Data normalization across sources	✓	☐	☐
Evidence preservation for forensics	✓	☐	☐
Detection & response			
Advanced threat detection	✓	☐	☐
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

Vendor 2 Notes:

Vendor 3 Notes:

Criteria	Vendor 1: Expel	Vendor 2	Vendor 3
Fast mean time to detect (MTTD)	✓	☐	☐
Fast mean time to respond (MTTR)	✓	☐	☐
Playbook execution	✓	☐	☐
Active response capabilities	✓	☐	☐
Automated remediation	✓	☐	☐
AI resolutions (AIR)	✓	☐	☐
Deep incident investigation	✓	☐	☐
Context enrichment	✓	☐	☐
Cross-environment correlation	✓	☐	☐
Continuous analyst training	✓	☐	☐
Analyst expertise			
24x7x365 coverage	✓	☐	☐
AI assisted investigations	✓	☐	☐
Experienced security analysts	✓	☐	☐
Specialization depth	✓	☐	☐
Appropriate 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	✓	☐	☐
Comprehensive reporting	✓	☐	☐
Event search capabilities	✓	☐	☐
Metrics transparency	✓	☐	☐
Detection logic visibility	✓	☐	☐
Product roadmap access	✓	☐	☐
Direct platform access	✓	☐	☐
Collaboration features	✓	☐	☐
Alert contextualization	✓	☐	☐
AI-assisted incident findings reports	✓	☐	☐
AI-assisted investigation summaries	✓	☐	☐
AI-assisted management reporting	✓	☐	☐
Performance benchmarking	✓	☐	☐
Quality metrics	✓	☐	☐