

	ALCIT	Vendor 2	Vendor 3	Vendor 4
Is MDR offered as a managed service?	Yes			
Can the service ingest security events from all your cloud services?	Yes			
Can the service ingest security events from all your on prem PCs and Servers?	Yes			
Can the service ingest security events from all other on prem devices?	Yes			
Can the service ingest security events from all "work from home" devices?	Yes			
Will the cost of the service increase if your devices send more logs (like when under attack)?	Yes			
Will the service ignore some of your logs if your devices send more vents then your defined threshold?	Yes			
Is the MDR solution capabilities regularly updated with new Indicators of Compromise (IOC)?	Yes			
Does the MDR provider subscribe to multiple threat exchanges to improve its detection capabilities?	Yes			
Does the MDR provider analyze events 24/7?	Yes			
Will a human review the important events and decide what is urgent?	Yes			
Will the MDR vendor notify you of all "urgent" events?	Yes			
Will the MDR vendor notify you of all "non urgent" events?	Yes			
Are "non urgent" events filtered to only provide "important" events?	Yes			
Does the MDR vendor have the ability to leverage containment on managed endpoints to stop (slow down) suspected ongoing attacks?	Yes			
Does the MDR vendor have the ability to leverage containment on other devices to stop (slow down) suspected ongoing attacks?	Yes			
Does the MDR vendor have the ability to investigate and mitigate all "urgent" events in your environment?	Yes			
Does the MDR vendor have the ability to investigate and mitigate all "non-urgent" events in your environment?	Yes			
Will the MDR service provide you reports to help improve your cybersecurity posture?	Yes			
Will the MDR service provider work with you to improve your cybersecurity posture?	Yes			
Does the MDR service allow to perform custom log investigations for custom events?	Yes			
Does the MDR service keep all logs available to match your compliance requirements?	Yes			
Can the MDR service provider have the ability to deploy a complete Cyber Incident Response team?	Yes			
Can the MDR service provider help with the full recovery of services after an incident?	Yes			
Can the MDR service provider deploy their solution in your environment and start protecting you in weeks (not months)?	Yes			