MDR VENDOR EVALUATION · EXPEL VS. BLUEVOYANT

Six questions to ask BlueVoyant

Bring these to your next vendor call. The answers will tell you everything you need to know.

? Use these questions in your evaluation—then see how Expel answers each one.

01	SIEM REQUIREMENT **Do I need to deploy or migrate to Microsoft Sentinel or Splunk before you can monitor my environment?**	EXPEL No. Direct bi-directional API connections to the tools you already own. No proprietary agents, and no SIEM swap.
02	TIME TO VALUE **How long until you're actively detecting and responding in my environment, and who's covering me during the baseline and tuning period?**	EXPEL Customers are up and running in hours. Coverage starts as soon as the connections are live.
03	RESPONSE COMMITMENT **What's your committed response time for a critical alert, measured to containment rather than acknowledgement?**	EXPEL Expel guarantees a 15-minute SLA for critical events and 30 minutes for high-severity events, with a 14-minute MTTR. Commitments, not aspirations.
04	DIRECT SOC ACCESS **Can I talk directly to the analyst working my incident, and see what they're doing as it happens?**	EXPEL Yes. Direct 24x7 access to the analysts working your environment via Slack or Teams, included, with every action visible in Expel Workbench™.
05	CLOUD AND KUBERNETES **How do you cover Kubernetes running in AWS or Google Cloud, and cloud security platforms like Wiz or Orca?**	EXPEL API connections to AWS, Azure, Google Cloud, Kubernetes, Wiz, and more. No agents or sensors.
06	AI SECURITY **If you deploy Microsoft's AI security controls for me, who investigates those alerts after the engagement ends?**	EXPEL Expel monitors AI signals 24x7 across Amazon Bedrock, Azure OpenAI, and Google Vertex AI. It's an ongoing operation, not a project.

YOUR NEXT VENDOR CALL

See how Expel answers every one of these.

Talk to our team—no handoffs, no voicemail, no gap.

expel.com/request-demo