expel | sumo logic

PARTNER BRIEF

See everything, stop anything: MDR + SIEM for simple security

Navigating SIEM costs, complexity, and coverage

Whether you are using a SIEM for data retention or for detection and response, there are often challenges. Storage costs can add up quickly, and legacy SIEM solutions are noisy and require continuous monitoring and tuning of custom rules, which means more work for your team. And with the recent market consolidation of legacy SIEM providers, many customers like you, are looking to make a change. That's where Expel Managed Detection and Response (MDR) and Sumo Logic can help.

Level up your security with Expel + Sumo Logic

Expel, a leader in The Forrester Wave™: Managed Detection & Response, Q2, 2023, has teamed up with Sumo Logic, a disrupter in the SIEM space, to deliver an alternative way to manage SIEM complexities—all while helping you save on data storage costs. Together, we help organizations make sense of their data from across disparate sources and alert you to threats before they can cause harm.

Sumo Logic's Cloud SIEM enhances security teams' efficiency with actionable, context-enriched insights. The product scales as you grow and consolidates security log management across SecOps, ITOps, and DevOps. Rapid SIEM deployment, intuitive interfaces, and out-of-the-box integrations ensure quick time-to-value, empowering teams to act smarter and faster.

Through an expanded partnership with Sumo Logic, Expel provides expert-managed detection and response in conjunction with their cloud-based SIEM and log storage options—helping you get the most from your current or planned investment.

Expel supports Sumo Logic's Cloud SIEM in two ways:

- Organizations with straightforward, long-term data storage needs can leverage a cost-effective data lake as an MDR investigative source, supporting both compliance and storage requirements.
- Organizations that need a full-service SIEM can leverage Sumo Logic's Cloud SIEM for rich, customizable alerts that power MDR investigations. Expel integrates seamlessly, combining data from Sumo Logic with other key security sources to deliver a unified view of your security landscape.

This partnership offers you enhanced visibility, consolidating all the security data you need in one centralized location. Expel supports Sumo Logic custom and out-of-the-box rules with our own custom detections, automatically updating SIEM alerts based on the status of Expel investigations. You'll also gain access to Expel's evaluations of your SIEM rule configurations, identifying supportability and recommending optimizations for improved security. Together, Expel and Sumo Logic help you amplify the effectiveness of your security–empowering your team with the tools they need to mitigate risk.

Addressing your security challenges

Meet compliance requirements

Combine Expel MDR with low-cost data storage, meeting compliance needs while our experts handle detection and response alongside your SOC.

Replace your current SIEM

Unhappy with your SIEM? Switch to Expel MDR and Sumo Logic's Cloud SIEM for simpler, optimized detection and response.

Overcome skills gaps

Expel SOC analysts bring valuable staffing and expertise to the table, helping you bridge gaps in your security expertise and resources.

Assess if SIEM is right for you

New to SIEM? No problem. Expel MDR and Sumo Logic's Cloud SIEM is delivered in a single package and streamlined under one contract. Offload detection and response to our SOC, freeing your team to focus on strategic SIEM management and optimization, with support to kickstart your SIEM journey.

expel | sumo logic

How you'll benefit from the Expel and Sumo Logic partnership

Maximize ROI on your SIEM investment

- Leverage Expel's data lake as a lower-cost storage solution for compliance and audits.
- Free up internal resources to focus on strategic initiatives while Expel experts handle day-to-day threat detection and investigations.
- Gain insights into which SIEM detections are effective and receive recommendations for efficiency improvements.

Holistic visibility and coverage

- Expel maintains comprehensive visibility across your environment–ensuring gaps are covered and conducting root cause analysis when incidents arise.
- Expel can leverage data stored in the data lake during investigations to bring context to alerts.
- Expel provides advanced integration support of Sumo Logic's Cloud SIEM, including out-of-the-box and custom rules support and access to SIEM tuning guidance.

Unburden your SecOps

- Purchase professional service hours for easy SIEM onboarding, migration, or content development delivered by Sumo Logic technical experts.
- Enhance your SOC with 24x7 coverage and our extensive detection library, reducing the burden on detection engineering.

WHAT OUR CUSTOMERS SAY

"Folding our SIEM into Expel Workbench gives us a more comprehensive view of our security events and alerts. Together, they enable faster and more accurate incident response—we gain back valuable time to address other security needs."

LEWIS MCINTYRE
DIRECTOR OF CYBERSECURITY AND INCIDENT RESPONSE

MARKEL

Ready for a new way to detect and respond to SIEM alerts?

Don't let today's complex threat landscape undermine your organization's security. Harness the combined power of Expel and Sumo Logic to strengthen your security posture, minimize the noise for your SecOps, and protect your business continuity–all while making the most of your SIEM investment.

Contact your Expel sales representative to learn more about Expel + Sumo Logic pricing and packaging options

Contact sales →

02/05/25