expel

Is your SIEM performing or just running?

Nine questions to answer to know the difference

Investment and value aren't the same thing.

We designed this brief assessment to determine the maturity level of your SIEM. And if it doesn't look great, don't feel bad—we can help with that.

01 ☐

YOUR DATA

Can you name the three log sources that generate the most alert volume—and the three that produce the mostconfirmed true positives? (Bonus: are they the same sources?)

02 ☐

YOUR DATA

Have you audited your ingestion pipeline in the last year to remove data sources not tied to an active detection use case?

03 ☐

YOUR DATA

Are you storing and processing data for compliance only in your SIEM? (Hint: this data isn't contributing to detections.)

04 ☐

YOUR DETECTIONS

Do you know what percentage of your active detection rules have produced a confirmed true positive in the last 90 days?

05 ☐

YOUR DETECTIONS

Can you map your current rule library to the MITRE ATT&CK techniques most relevant to your industry's threat landscape?

06 ☐

YOUR DETECTIONS

Has someone reviewed every active rule in the last six months to verify it still fires correctly?

07 ☐

YOUR DETECTIONS

Do your analysts treat all alert categories equally—or have some become background noise they've learned to tune out?

08 ☐

YOUR TEAM

Do your analysts spend the majority of their time gathering context across multiple tools rather than making decisions and responding to threats?

09 ☐

YOUR TEAM

Is your detection program documented well enough to survive the loss of a key team member?

TALLY YOUR RESULTS

0

PUT IT ALL TOGETHER

What your score means

Count your “yes” answers. Here’s what that number tells you.

0-3 **Your SIEM needs a reset**	You’re not alone—this is where many programs are before they get intentional help. The good news: these gaps are fixable, and the ROI of fixing them is immediate. Let’s talk.
4-6 **There are real gaps worth addressing**	You’ve got some things working, but the holes are meaningful—and they tend to compound. This is the range where teams feel busy but not confident. Expel is built for exactly this.
7-9 **Your program is in good shape**	There are likely still efficiencies to find—but you have a strong foundation. Let’s talk about where Expel can sharpen what’s already working.

How Expel can help improve your SIEM

WHAT WE DO	WHAT THAT MEANS
Own the detection lifecycle end-to-end—engineering, testing, tuning, and retiring rules on an ongoing basis.	No more stale rules, no more alert categories your analysts have learned to ignore.
Build behavioral detections mapped to MITRE ATT&CK—focused on how attackers behave, not just what tools they use.	Detections that hold up even when attackers rotate infrastructure or use valid credentials.
Expel recommends optimizations to ingestion, retention, and data usage to manage SIEM costs, and can implement approved changes on your behalf.	Lower SIEM costs, lower noise floor, and clearer signal from the sources that actually matter.
Our detections are built on 10+ years of detection engineering expertise, refined across 500+ customer environments.	When we learn something in one environment, every environment benefits. Your coverage gets stronger every week, automatically.

Ready to close the gaps?

Ready to close the gaps? Talk to your Expel team or visit expel.com/services/managed-siem