We optimize your SIEM detections

Eliminate false positives and enrich alerts with context, all while reducing storage costs

Common, out-of-the-box SIEM detections **cover only 24%** of MITRE ATT&CK® techniques.

Source

YOUR CHALLENGE

Your security information and event management (SIEM) tech is a critical component of your security operations program.

The way organizations leverage their SIEMs varies, resulting in both unique challenges and benefits.

You may ingest all of your data into your SIEM, making it one of the richest sources of investigative information for detection and response. While there is significant value in having all of your data stored in a unified source for context and correlation, storing all of your data in your SIEM can get expensive quickly.

Your team may also suffer from alert fatigue, with a high volume of false positives without context. The detection coverage you're getting from your SIEM versus your point products is unclear, and while most SIEMs come with built-in detections, you'll need to monitor those and create custom rules to detect anything that's not covered out-of-the-box. Custom rules require continuous monitoring and tuning, adding more detection engineering overhead to the team.

HOW WE HELP

Expel provides industry-leading decision support for your SIEM.

We leverage both your alerts and our Expel-written detections, and assist with tuning (where applicable), to spot incidents faster, eliminate false positives, and enrich your SIEM alerts with meaningful context.

We utilize SIEMs for automated investigative context and correlation in every alert, leverage them for threat hunting, and provide coverage analysis and optimization for your SIEM detections. We help you understand which SIEM detections are providing value—and which aren't—along with recommendations on how to improve. Our automation enriches SIEM alerts with extensive context from our global customer base, all with the benefit of full transparency into the investigative process.

We also don't require you to store all of your data in your SIEM, helping to reduce overall storage cost. By not tying you to a single SIEM, we increase flexibility as your tech stack evolves and can help unlock future savings as your data lake strategy changes.

WHY EXPEL

At Expel, we help you maximize your existing SIEM investment to improve your detection ROI. Here's how we do it:

Fast time-to-value

We work with your specific SIEM needs, with fast onboarding so you start seeing value in days, not months. We tailor your experience to your organization, environment, and goals.

World-class detection and threat intelligence

Expel provides 24/7/365 coverage to detect and respond to any threat with our robust detection library, enabling you to reduce your SIEM detection engineering effort.

Unrivaled visibility, context, and personalization

We enrich your SIEM alerts with context and provide 100% transparency into how we use your SIEM for detection and response.

Industry leading protection

Expel applies both automation and SOC expertise to deliver a 23-minute mean-time-to-response, leveraging your SIEM as a core investigative source for detection and response.

Proactive risk, resilience, and posture analysis

We provide resilience recommendations for every alert, along with full access to our Resilience Library, to shift from reactive to proactive and make the most of your SIEM signal.

WHAT OUR CUSTOMERS SAY

> **"Folding our SIEM into Expel Workbench gives us a more comprehensive view of our Microsoft 365,** Defender, and Azure Active Directory ID security events and alerts. Together, they enable faster and more accurate incident response. And with more streamlined workflows and less manual effort, we gain back valuable time to address other security needs."

MARKEL

Learn more at
expel.com

Awards and Recognition

4.8/5 Stars
on G2 Peer Review

CUSTOMER NPS
75+

FORRESTER
WAVE
LEADER 2023
Managed Detection
And Response