Achieve world-class SecOps metrics

Our tech-driven approach to MDR continuously improves as it ingests more telemetry

YOUR CHALLENGE

As your tech stack grows, your security operations center (SOC) inevitably faces more complexity.

New products and attack surfaces pose new risks and require specific expertise, while alerts from more sources require added time to triage, analyze, and investigate.

You need to communicate to your stakeholders the performance of your security operations program, but there are many data sources that contribute to your SOC metrics. With different systems sending telemetry, your SOC needs to connect disparate events together to consolidate and create meaningful metrics for the business.

Most SOCs can't scale as quickly as your environment grows. Not only are your teams experiencing alert fatigue, but the time-based metrics you use to measure your security program—whether it's mean-time-to-detect, -respond, or -remediate—increase as your SOC triages more alerts from more sources. When your SOC metrics increase, threats are in your environment longer, making you more susceptible to risk.

HOW WE HELP

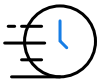
Expel automation and AI enable our SOC analysts to work more efficiently and deliver clear response actions to you sooner, accelerating all of your security program metrics.

Thanks to our purpose-built security operations platform, Expel Workbench™, Expel Managed Detection and Response (MDR) automatically does what other MDRs must accomplish manually—leveraging years of AI learning that optimizes incident filtering, prioritization, severity scoring, and reporting.

Our tech-driven approach filters out false positives, provides our SOC with deep context, and offers cyber resilience recommendations to continuously improve. Our precision enhances as more telemetry is ingested, enabling us to consistently accelerate your mean-time-to-detect, -touch, -triage, -investigate, -respond, and -remediate metrics. When we detect an incident in one organization, we apply that threat intelligence across the Expel ecosystem, so you continuously benefit from our global context, detections and remediation actions.

WHY EXPEL

At Expel, we combine the best of people and technology to deliver the industry-leading MDR service.



Fast time-to-value

We make it easy to onboard and configure your technology, so you realize value quickly from our security operations platform's threat intelligence, with the flexibility to evolve your tech stack.

World-class detection and threat intelligence

We continuously write detections based on new threats and what we see across our platform, providing you with coverage for emerging threats before they impact your business.

Unrivaled visibility, context, and personalization

Expel Workbench provides 100% transparency into all of our automations and detections, providing you with visibility into exactly what we do and how we speed up your response times.

Industry leading protection

We ingest billions of events monthly, cover millions of endpoints and users, and leverage automation to strategically filter out noise to achieve a mean-time-to-response (MTTR) of 23 minutes.

Proactive risk, resilience, and posture analysis

You continuously receive resilience recommendations on how you can shift your program from reactive to proactive, and benefit from the automation and intelligence of our platform.

WHAT OUR CUSTOMERS SAY

"Expel consumes and enriches the findings across all the integrations they have in the platform. With minimal tweaks, **Expel tells us what we need to look at from a security perspective using the big picture**—rather than us writing rules, reviewing alerts, configuring dozens of integrations, and chasing after countless false positives."

FiscalNote

Learn more at
expel.com

Awards and Recognition

4.8/5 Stars
on G2 Peer Review

CUSTOMER NPS
75+