OUR PRODUCTS

Expel Managed Detection and Response for Kubernetes

24/7 detection and response for EKS, AKS, and GKE

Your challenge

Kubernetes is the standard for managing containerized workloads, as it allows developers to work quickly and scale efficiently. However, it also adds a new attack surface for threat actors to exploit—and security teams to monitor. With the pace of DevOps releasing Kubernetes-based applications increasing, security teams—especially those without the coverage or cloud expertise—can struggle to catch up and secure the environment. In fact, 67% of organizations[1] have had to slow down deployment due to Kubernetes security concerns.

Our solution

For Amazon Elastic Kubernetes Engine (EKS), Azure Kubernetes Service (AKS), and Google Kubernetes Engine (GKE), Expel® Managed Detection and Response (MDR) for Kubernetes analyzes your audit logs, applies custom detection logic to alert on malicious or interesting activity, and offers clear steps to remediate. We also integrate with container security vendors, including CrowdStrike, Lacework, and Prisma Cloud Compute, so you get more answers from the security tech you already have.

Expel MDR for Kubernetes identifies cluster misconfigurations and references the Center for Information Security (CIS) Kubernetes Benchmark to provide best practices, recommend configuration improvements, and show how you're improving Kubernetes security over time, enabling security operations to shift Kubernetes security from reactive to proactive.

How you'll benefit

✓ Accelerate cloud adoption

Deploy Kubernetes at scale to enable developers without being hindered by security concerns. We'll detect and respond as threats arise in your Kubernetes workloads while your developers continue to build applications that matter to your business.

✓ Demystify Kubernetes security

We filter out the noise, detail findings by Kubernetes cluster, severity and title, and align findings to the MITRE ATT&CK framework so you know exactly what's happening and where to improve across your environment.

✓ Benchmarking to continuously improve

We reference the CIS Kubernetes Benchmark to recommend improvements and benchmark how your Kubernetes risk exposure and security posture is trending against industry best practices over time.

✓ Less employee burnout and alert fatigue

Our security operations platform, Expel Workbench™, filters out low-fidelity alerts, so your team only focuses on what matters. For alerts that require attention, our platform adds context before sending it to Expel analysts for further investigation—a process you have full visibility into.

[1] State of Kubernetes security report 2023

How Expel MDR for Kubernetes Works

Get the best of both technology and people using Expel's software and security analysts.

Monitor:

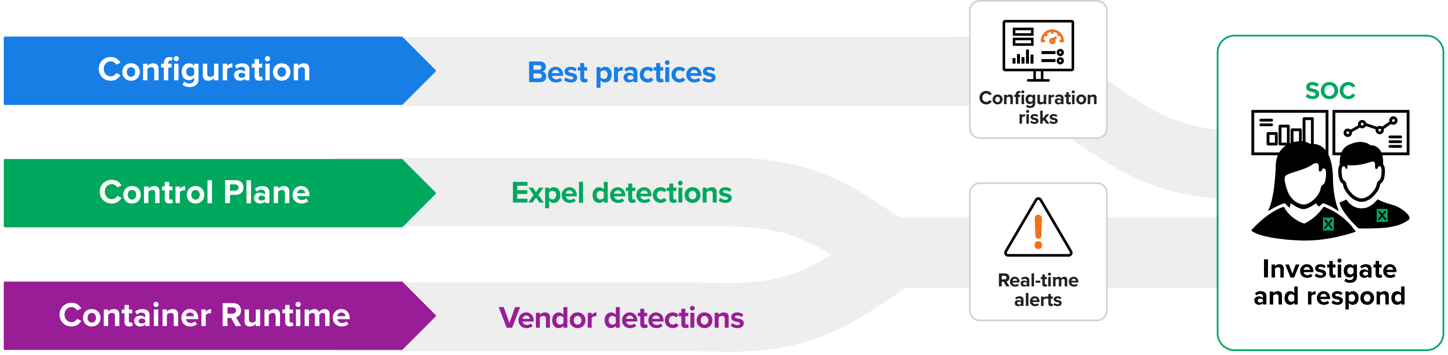
- Cluster configuration
- Control plane
- Container security tech

Detect:

- Configuration risks
- Expel detections from audit logs
- Runtime alerts from third-party vendors

So our bots and analysts can:

- Proactively advise
- Investigate
- Respond



Configuration → Best practices → Configuration risks

Control Plane → Expel detections

Container Runtime → Vendor detections → Real-time alerts

SOC

Investigate and respond

Why Expel

Cloud leadership
Expel offers the first solution of its kind to provide coverage across your cloud environment and detailed insights to improve your Kubernetes security posture.

Custom detections for Kubernetes
Kubernetes detections written by Expel provide another layer of protection and coverage of attacker behaviors.

Alignment to industry standards
Understand not only what happened, but how to improve in alignment with industry standards.

Get more from your security tech
We have 100+ integrations so you get answers, not alerts, from the tech you have.

Software-driven SecOps
Expel combines the power of our security operations platform and analysts to achieve an average 22-minute alert-to-fix time for critical alerts.

Coverage across attack surfaces
Whether you have cloud, on-prem, SaaS apps, or all of the above, we have you covered.

> **"There are two things that differentiated Expel for us: the BYO-tech approach that allowed for quick, frictionless integration and the Expel-written detections that gave us value from day one. As a cloud-native company, we operate a lot in GKE [Google Kubernetes Engine]. Expel MDR for Kubernetes gives us unparalleled visibility into our environment—correlating 'big picture' activities with added context from other integrated technologies and providing increased security observability into our environment."**
>
> **Rahil Parikh,** Security Manager, Engineering & Architecture, Policygenius

Visit www.expel.com to learn more about Expel Managed Detection and Response for Kubernetes and how it can help your organization.