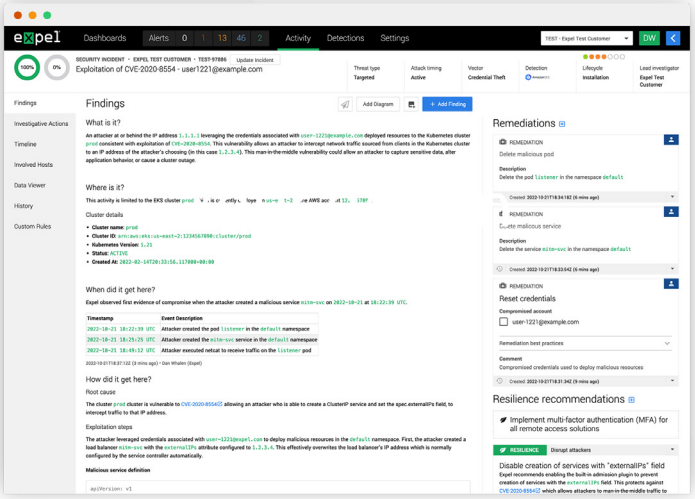
Expel MDR for Kubernetes

Gain visibility to secure your Kubernetes environment

Kubernetes is the standard for managing container applications. Traditional MDR solutions do not monitor Kubernetes, which puts organizations at risk. 53% of organizations using Kubernetes have identified a misconfiguration and 38% have uncovered a major vulnerability that was not uncovered by their detection and response technology[1].



Remove blind spots and mitigate Kubernetes risk

- Deploy Kubernetes–securely and at scale
- Reap Kubernetes advantages while minimizing risks
- Safeguard across all cloud attack surfaces
- Translate Kubernetes event logs into usable insights
- Shift security posture from reactive to proactive

What you get

Expel MDR for Kubernetes eliminates security blind spots, arms DevOps to maintain a secure cloud infrastructure and lets developers do what they do best—build applications that matter to the business.

We identify Kubernetes cluster misconfigurations and reference the Center for Information Security (CIS) benchmark to **recommend improvements**.

We integrate with your Amazon Elastic Kubernetes Service (EKS) and Google Kubernetes Engine (GKE) environments to analyze logs and apply custom detection logic to alert on abnormal activity.

We integrate with container security vendors to get the answers you need with the tech you already use (spanning CrowdStrike, Lacework and Prisma Cloud Compute).

1 Red Hat 2022 state of Kubernetes report

Why Expel?

Expel MDR for Kubernetes is the first to provide coverage across your cloud environment and detailed insights to improve your Kubernetes security posture.

Accelerate cloud adoption; practical intelligence helps contextualize and prioritize what matters most.

Demystify Kubernetes with answers, not alerts, through Expel-written detections that adapt with your environment and align with the MITRE ATT&CK Framework.

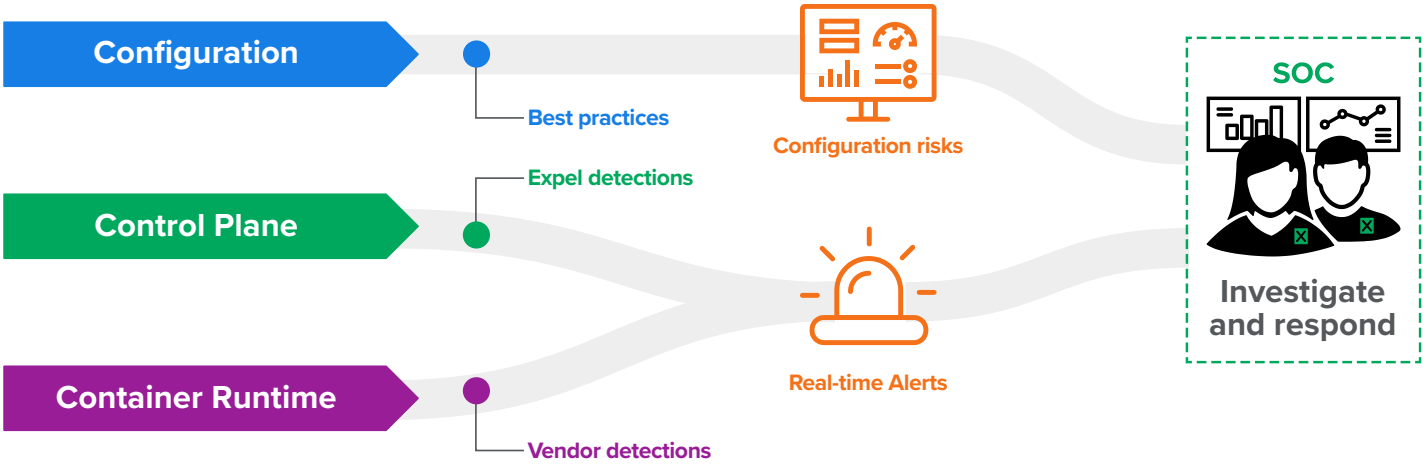
Put your existing tech to work improving ROI; align DevOps and security to securely adopt Kubernetes at scale.

Qlik

"Expel was already using Kubernetes for their development — the team knew how it worked and how to secure it. So it was very easy for me to say, 'Okay, these are the guys we're going to partner with because they understand exactly where we are today in our security journey.' It was an easy decision."

– Principal Architect, Qlik

How it works



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

Learn more at www.expel.com/solutions/secure-kubernetes.