New feature: Amazon GuardDuty Extended Threat Detection now supports Amazon EKS
GuardDuty Extended Threat Detection connects individual findings and signals into an attack sequence, a critical severity finding. This capability now includes coverage for multi-stage attacks targeting Amazon EKS clusters in your AWS environment. GuardDuty correlates multiple security signals across Amazon EKS audit logs, runtime behavior of processes, and AWS API activity to detect sophisticated attack patterns. Enable EKS Protection, Runtime Monitoring (EKS), or both to maximize your detection coverage. Feature availability varies in AWS GovCloud (US) and AWS China Regions. Learn more

GuardDuty > Summary

Summary Info

View and analyze security trends based on GuardDuty findings in your AWS environment.

Updated a few seconds ago | Today

Overview

Attack sequences - *new*	Total findings	Resources with findings	Accounts with findings
3	364	18	1

Findings - *new*

Prioritize triaging and remediating topmost severity detections.

Critical	High	Medium	Low
3	148	150	63

Top threats | Top attack sequences only

Findings	Severity
Potential credential compromise of IAMUser/[redacted] indicated by a sequence of actions.	Critical
Potential data compromise of one or more S3 buckets involving a sequence of actions associated with IAMUser/john_doe.	Critical
Potential Kubernetes cluster compromise of eks-demo-cluster indicated by a sequence of actions.	Critical
The EC2 instance i-99999999 is behaving in a manner that may indicate it is being used to perform a Denial of Service (DoS) attack using the TCP protocol.	High
The EC2 instance i-99999999 may be the target of a DNS rebinding attack.	High
A user successfully logged into an RDS database in your account from a known malicious IP address.	High
A container escape via runc was detected in EC2 instance i-99999999.	High
A DGA domain name was queried by EC2 instance i-99999999.	High

View all findings

Introducing the new AWS Security Hub - *public preview*

The new Security Hub is your unified cloud security solution that prioritizes critical issues and helps you respond at scale to protect your cloud environment. Learn more

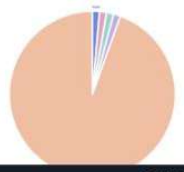
Try Security Hub

Runtime Monitoring coverage

Monitor runtime activity to detect threats to your compute workloads on Amazon ECS (including AWS Fargate), Amazon EKS, and Amazon EC2.

Enable Runtime Monitoring

Most common finding types



© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences