aws | Search [Alt+S] | United States (Ohio) | bayateAWS

Security Hub > Findings

Security Hub

Dashboard
- Summary
- Exposure
- Threats
- Vulnerabilities
- Posture management
- Sensitive data

Inventory
- Findings
- Resources

Management
- Integrations
- Automations

Settings
- General

Detection engines
- GuardDuty
- Inspector
- Security Hub CSPM
- Macie

Findings (40+)

A finding is a record of a security check or security-related detection. This screen organizes all of your findings in one place. You can filter and view your findings by severity, resource, status, and other fields.

Update status

Saved filter sets: Choose a filter set | Add filter | Group by: None

Quick filters

Severity
- Critical (3)
- High (148)
- Medium (150)
- Low (63)
- Informational (13)

Top 10 attributes

Account ID
[redacted]

Resource type
[redacted]

Resource type
[redacted]

Resource type
[redacted]

Resource type
[redacted]

View more (+5)

Top 10 accounts

[redacted] (377)

Top 10 resource types
- AWS::EC2::Instance (292)
- Cloud::Container::Container (126)
- Cloud::Container::KubernetesCluster (91)

Finding	Severity	Resource	Age	Status	Account	Region
The API ListAttachedRolePolicies was invoked using root credentials.	Low	AWS::IAM::AccessKey ASIAVMZUIIHNAEA6XQUE	about 1 hour	New	[redacted]	[redacted]
The API GetFindingsStatistics was invoked using root credentials.	Low	AWS::IAM::AccessKey ASIAVMZUIIHNPPM2TNFE	about 1 hour	New		
A container has mounted a host directory.	Medium	AWS::EC2::Instance i-99999999	about 1 hour	New		
A container has mounted a host directory.	Medium	Cloud::Container::Container GeneratedFindingContainerId	about 1 hour	New		
A container has mounted a host directory.	Medium	AWS::ECS::Cluster GeneratedFindingECSClusterName	about 1 hour	New		
A container has mounted a host directory.	Medium	Cloud::Container::Container GeneratedFindingContainerId	about 1 hour	New		
A resource of type KubernetesCluster has executed a suspicious command.	Low	Cloud::Container::Container GeneratedFindingContainerId	about 1 hour	New		
A Kubernetes API commonly used in Impact tactics invoked by the anonymous user.	High	AWS::EKS::Cluster GeneratedFindingEKSClusterName	about 1 hour	New		
The EC2 instance i-99999999 is communicating with a domain name related to a known abused domain name.	Medium	AWS::EC2::Instance i-99999999	about 1 hour	New		
A container has mounted a host directory.	Medium	Cloud::Container::Container GeneratedFindingContainerId	about 1 hour	New		
A resource of type Container has executed a suspicious command.	Low	Cloud::Container::Container GeneratedFindingContainerId	about 1 hour	New		
A resource of type EKSCluster has executed a suspicious command.	Low	Cloud::Container::Container GeneratedFindingContainerId	about 1 hour	New		
A resource of type ECSCluster has executed a suspicious command.	Low	AWS::ECS::Cluster GeneratedFindingECSClusterName	about 1 hour	New		
A resource of type Instance has executed a suspicious command.	Low	AWS::EC2::Instance i-99999999	about 1 hour	New		
A Kubernetes API commonly used in Impact tactics invoked from a Tor exit node IP address.	High	AWS::IAM::AccessKey GeneratedFindingAccessKeyId	about 1 hour	New		
The EC2 instance i-99999999 is communicating with a Drop Point.	Medium	AWS::EC2::Instance i-99999999	about 1 hour	New		