Amazon Inspector

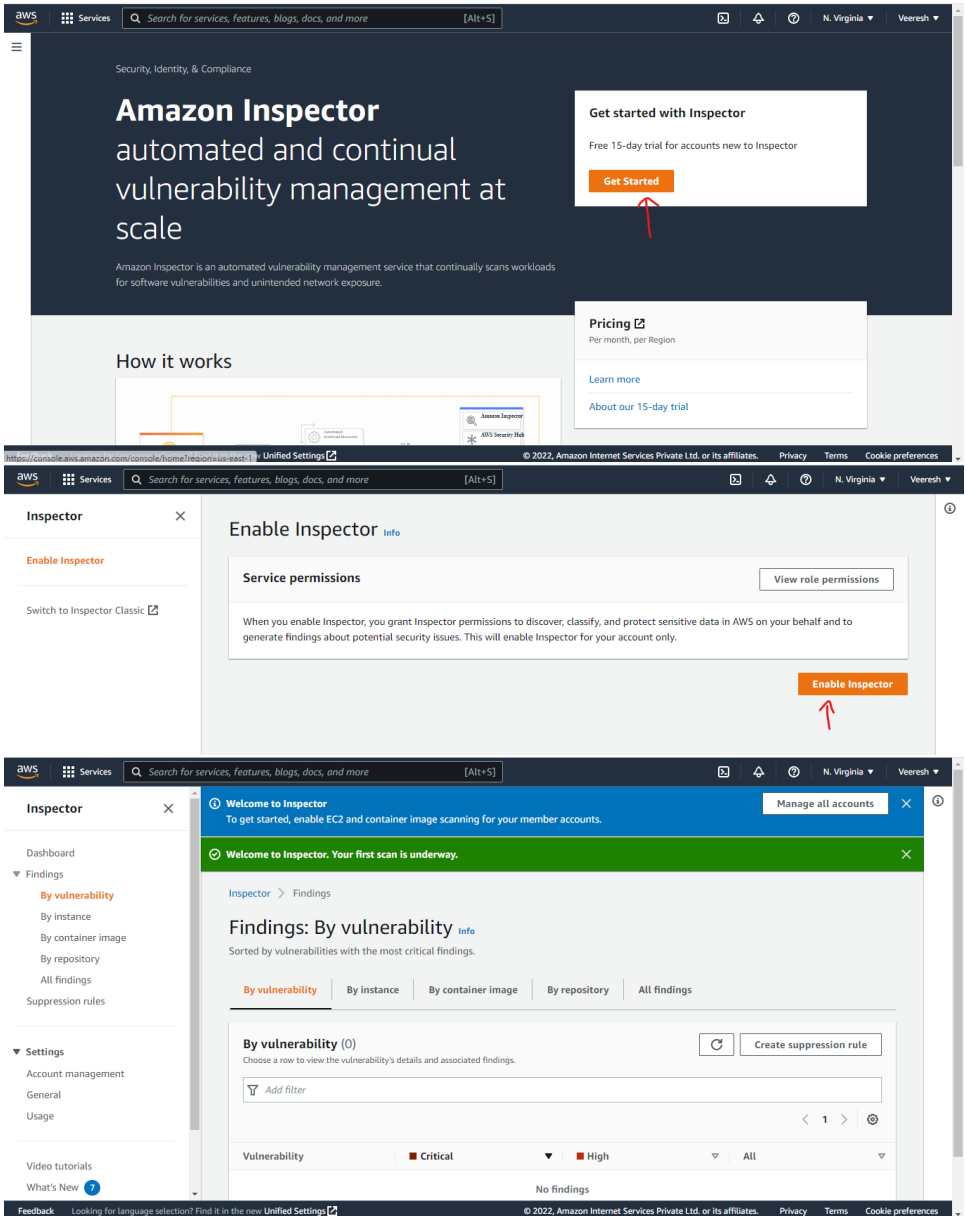
Amazon Inspector is an automated security assessment service and to test network accessibility of EC2 instance. It helps you to identify vulnerabilities within your EC2 instances and applications. And allows you to make security testing more regular occurrence as part of the development and IT operations.

Amazon Inspector provides a clear list of security and compliance findings assigned a priority by the severity level. Moreover, these findings can be analysed directly or as part of comprehensive assessment records available via the API or AWS Inspector console. AWS Inspector security assessments help you check for unintended network accessibility of EC2 instances and vulnerabilities on those EC2 instances.

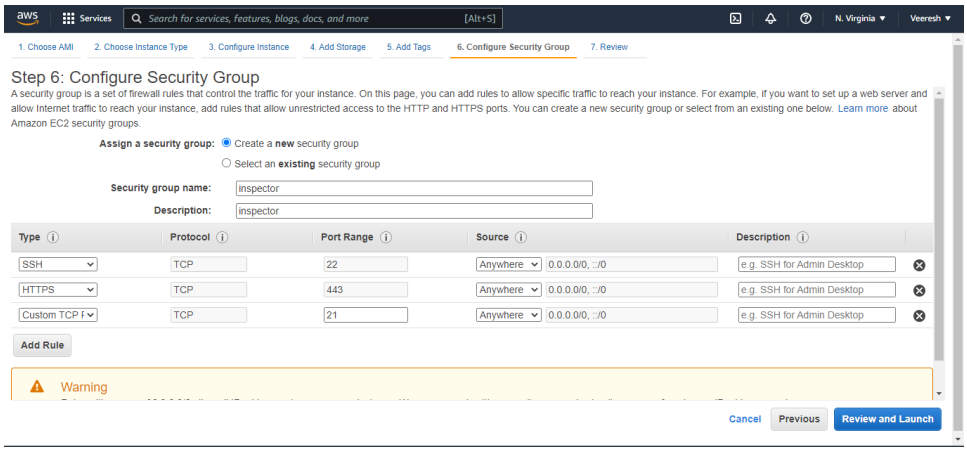
Hands on:

Step 1 :

- Goto amazon inspector dashboard, select get started.
- Next enable the inspector.

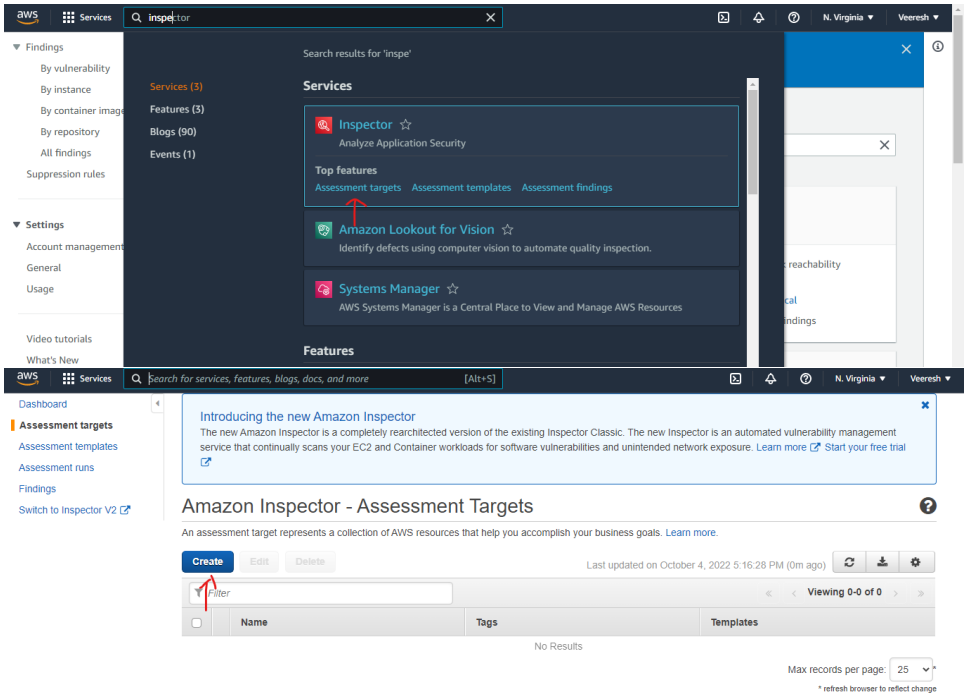


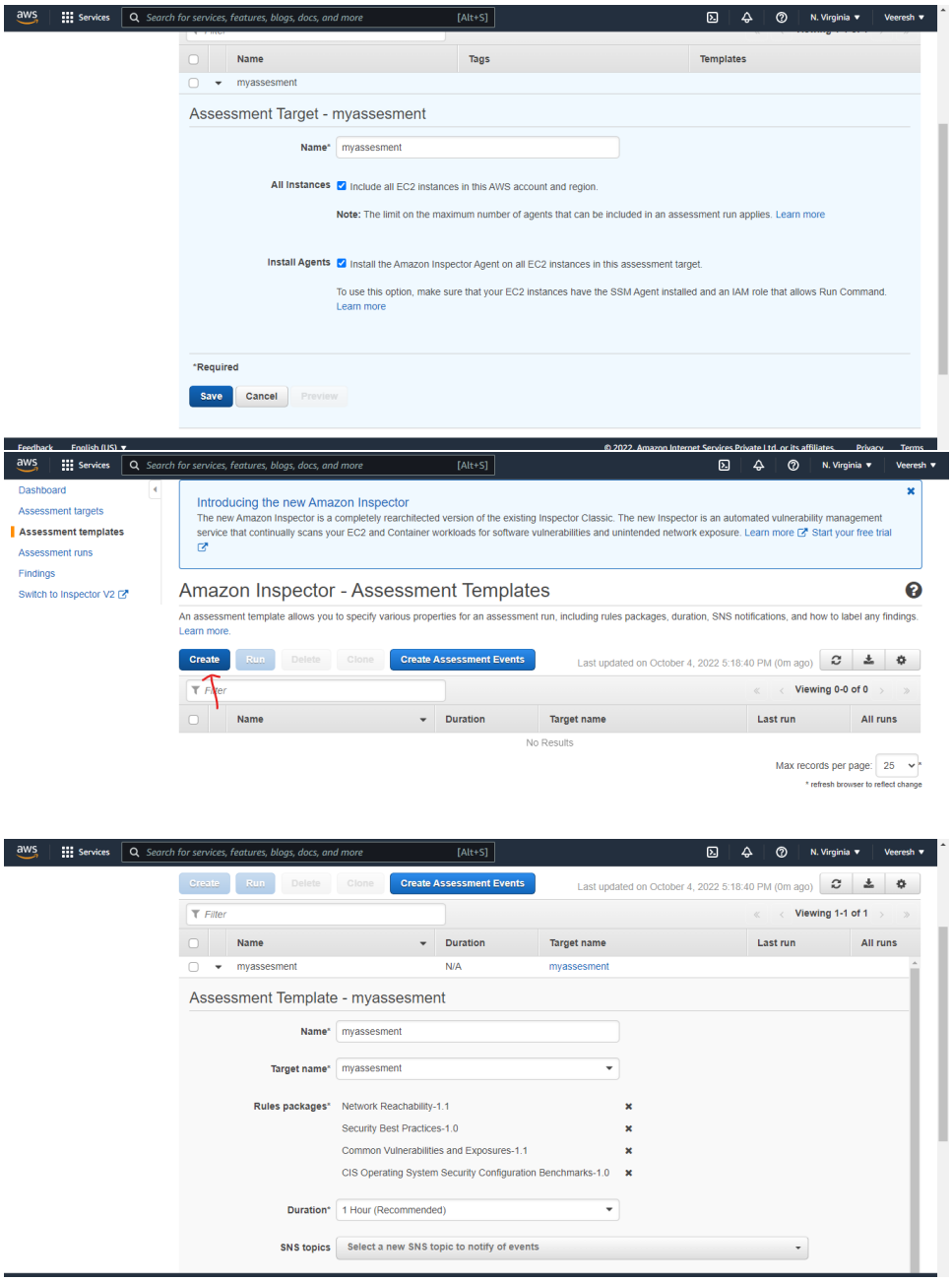
Step 2: Launch an EC2 instance with security group ports , 21,22, 443 at source everywhere. This is for we can track the vulnerabilities.

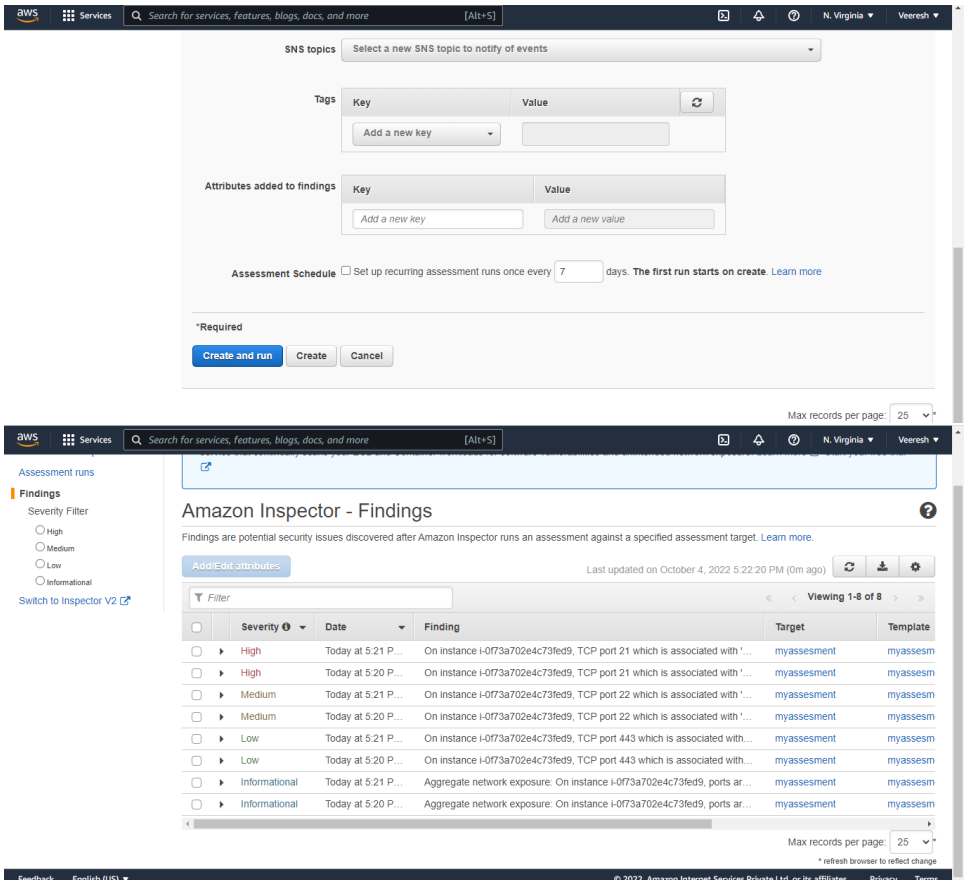


Step 3 :

- Goto the inspector assessment targets, create the target with all instances.
- Create and run assessment templetes with the assessment target which are previously created.
- We can get the data of vulnerabilities as TCP port 21 for High risk, TCP port 22 for medium risk.

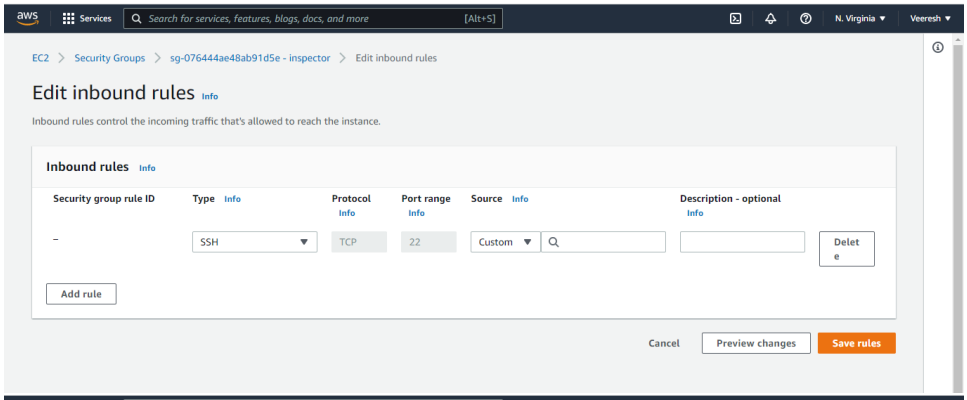


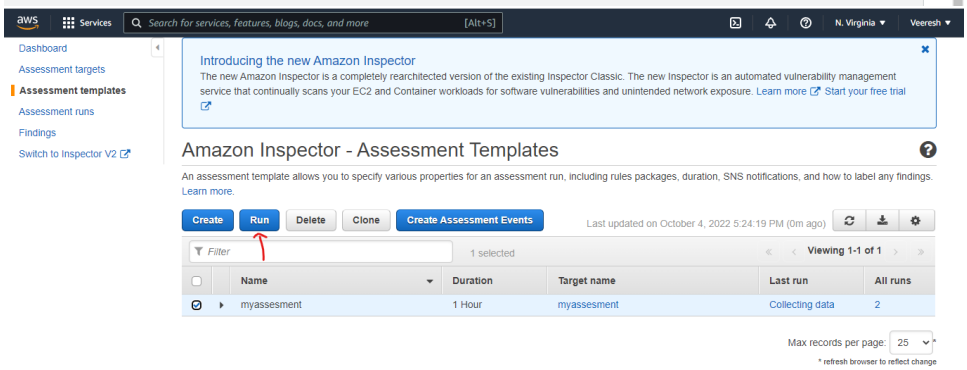

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Veeresh
Name
Tags
Templates
myassesment
Assessment Target - myassesment
Name*
myassesment
All Instances
Include all EC2 instances in this AWS account and region.
Note: The limit on the maximum number of agents that can be included in an assessment run applies. Learn more
Install Agents
Install the Amazon Inspector Agent on all EC2 instances in this assessment target.
To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command.
Learn more
*Required
Save
Cancel
Preview
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings
Switch to Inspector V2
Introducing the new Amazon Inspector
The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more
Start your free trial
Amazon Inspector - Assessment Templates
An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings.
Learn more.
Create
Run
Delete
Clone
Create Assessment Events
Last updated on October 4, 2022 5:18:40 PM (0m ago)
Filter
Viewing 0-0 of 0
Name
Duration
Target name
Last run
All runs
No Results
Max records per page: 25
* refresh browser to reflect change
Create
Run
Delete
Clone
Create Assessment Events
Last updated on October 4, 2022 5:18:40 PM (0m ago)
Filter
Viewing 1-1 of 1
Name
Duration
Target name
Last run
All runs
myassesment
N/A
myassesment
Assessment Template - myassesment
Name*
myassesment
Target name*
myassesment
Rules packages*
Network Reachability-1.1
Security Best Practices-1.0
Common Vulnerabilities and Exposures-1.1
CIS Operating System Security Configuration Benchmarks-1.0
Duration*
1 Hour (Recommended)
SNS topics
Select a new SNS topic to notify of events

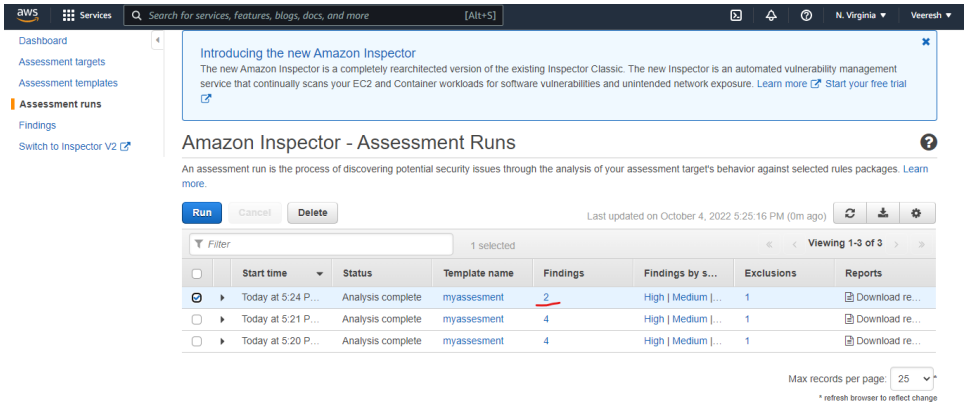


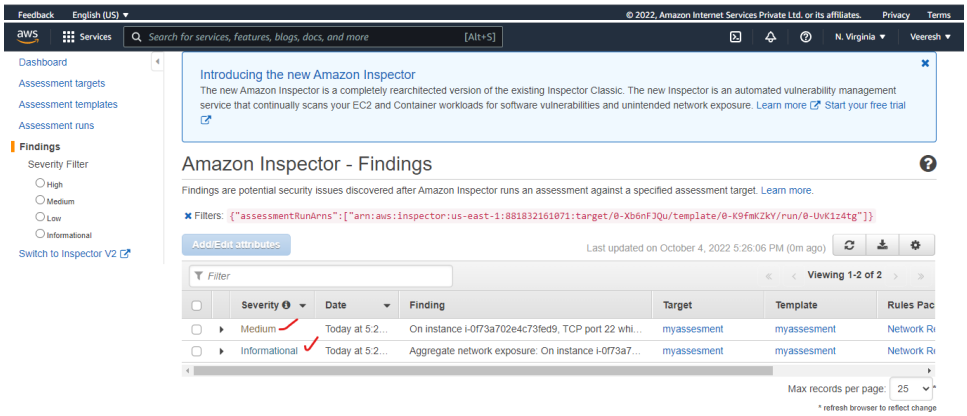
Step 4 : now get back to the EC2 instance security group and remove all previously created protocols and add the ssh 22 custom source and save it.

- Then goto the assessment templets select and run the templets.
- Then we will find the medium and informational severity.


Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Veeresh
EC2 > Security Groups > sg-076444ae48ab91d5e - inspector > Edit inbound rules
Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
-
SSH
TCP
22
Custom
Delet e
Add rule
Cancel
Preview changes
Save rules


Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Veeresh
Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings
Switch to Inspector V2
Introducing the new Amazon Inspector
The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial
Amazon Inspector - Assessment Templates
An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. Learn more.
Create
Run
Delete
Clone
Create Assessment Events
Last updated on October 4, 2022 5:24:19 PM (0m ago)
Filter
1 selected
Viewing 1-1 of 1
Name
Duration
Target name
Last run
All runs
myassesment
1 Hour
myassesment
Collecting data
2
Max records per page: 25
* refresh browser to reflect change


Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Veeresh
Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings
Switch to Inspector V2
Introducing the new Amazon Inspector
The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial
Amazon Inspector - Assessment Runs
An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior against selected rules packages. Learn more.
Run
Cancel
Delete
Last updated on October 4, 2022 5:25:16 PM (0m ago)
Filter
1 selected
Viewing 1-3 of 3
Start time
Status
Template name
Findings
Findings by s...
Exclusions
Reports
Today at 5:24 P...
Analysis complete
myassesment
2
High | Medium |...
1
Download re...
Today at 5:21 P...
Analysis complete
myassesment
4
High | Medium |...
1
Download re...
Today at 5:20 P...
Analysis complete
myassesment
4
High | Medium |...
1
Download re...
Max records per page: 25
* refresh browser to reflect change


Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Veeresh
Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings
Severity Filter
High
Medium
Low
Informational
Switch to Inspector V2
Introducing the new Amazon Inspector
The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial
Amazon Inspector - Findings
Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. Learn more.
Filters: {"assessmentRunArns":["arn:aws:inspector:us-east-1:881832161071:target/0-Xb6nFJQu/template/0-K9fmKZkV/run/0-UvK1z4tg"]}
Add/Edit attributes
Last updated on October 4, 2022 5:26:06 PM (0m ago)
Filter
Viewing 1-2 of 2
Severity
Date
Finding
Target
Template
Rules Pac
Medium
Today at 5:2...
On instance i-0f73a702e4c73fed9, TCP port 22 whi...
myassesment
myassesment
Network R
Informational
Today at 5:2...
Aggregate network exposure: On instance i-0f73a7...
myassesment
myassesment
Network R
Max records per page: 25
* refresh browser to reflect change