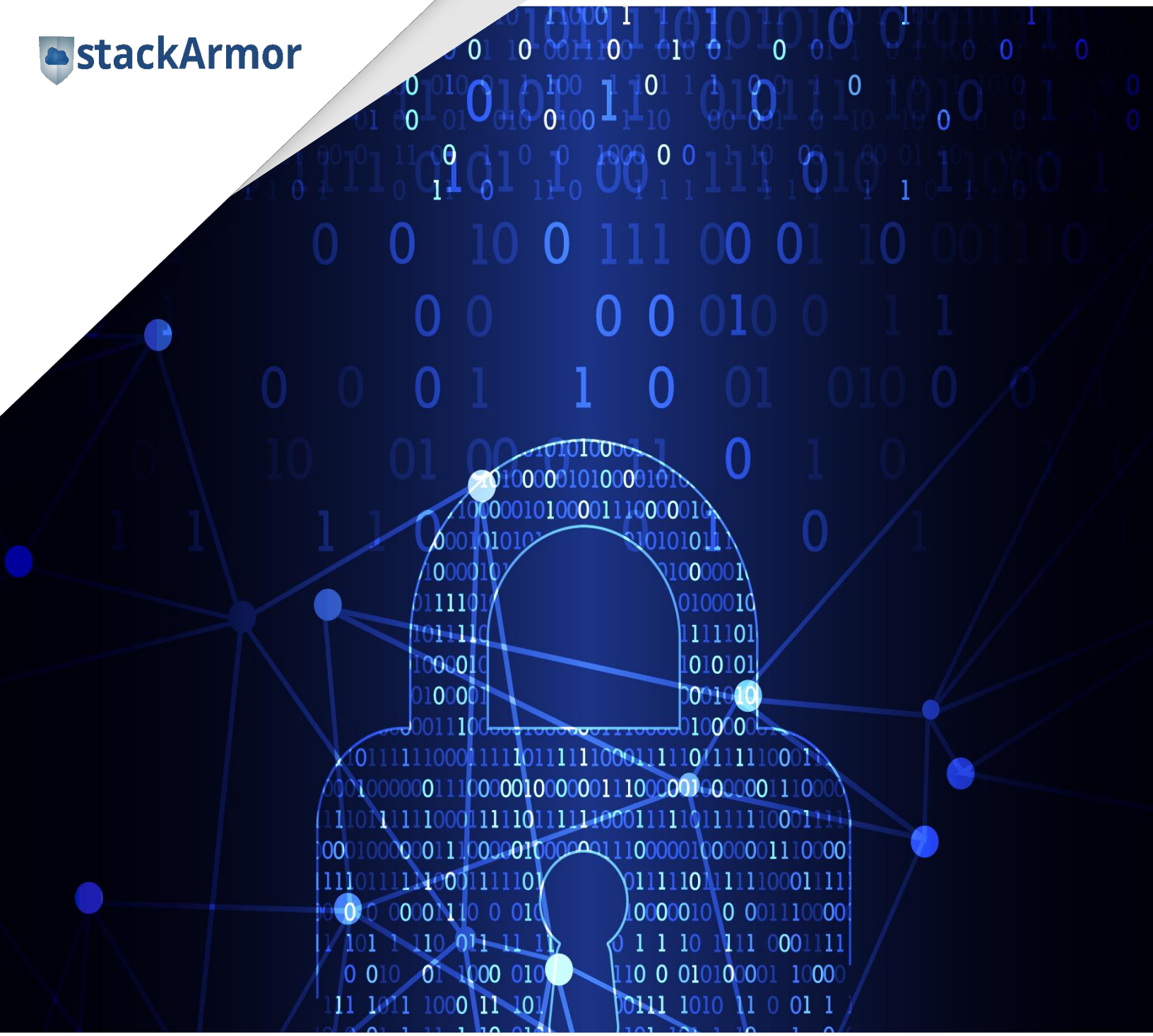


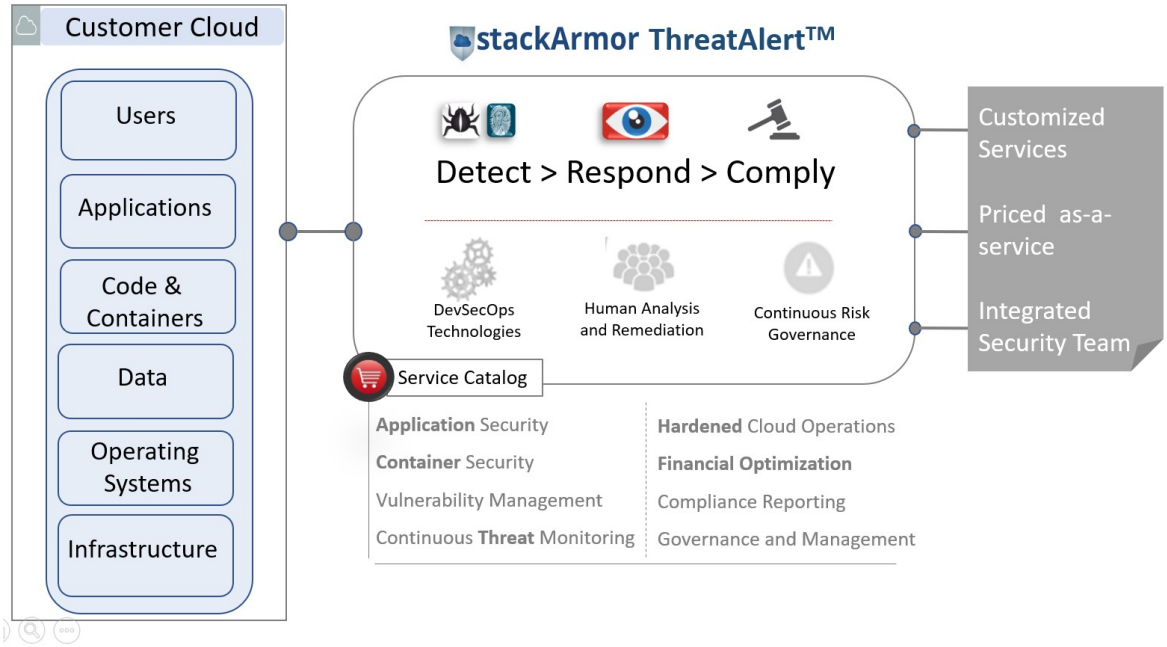
stackArmor ThreatAlert™ Solution Brief:

Continuous Cloud Threat Monitoring and Compliance

Table of Contents

1. stackArmor ThreatAlert™ Continuous Threat Monitoring and Response

stackArmor ThreatAlert™ is an in-boundary continuous cloud security monitoring and compliance solution for regulated industries. Organizations in healthcare, education and public sector must ensure that their cloud environment follows strict regulatory and compliance requirements. Constant configuration changes, code & container vulnerabilities and providing compliance reports is challenging for most compliance-driven organizations. stackArmor ThreatAlert™ provides security services from code to container to cloud as an integrated solution.

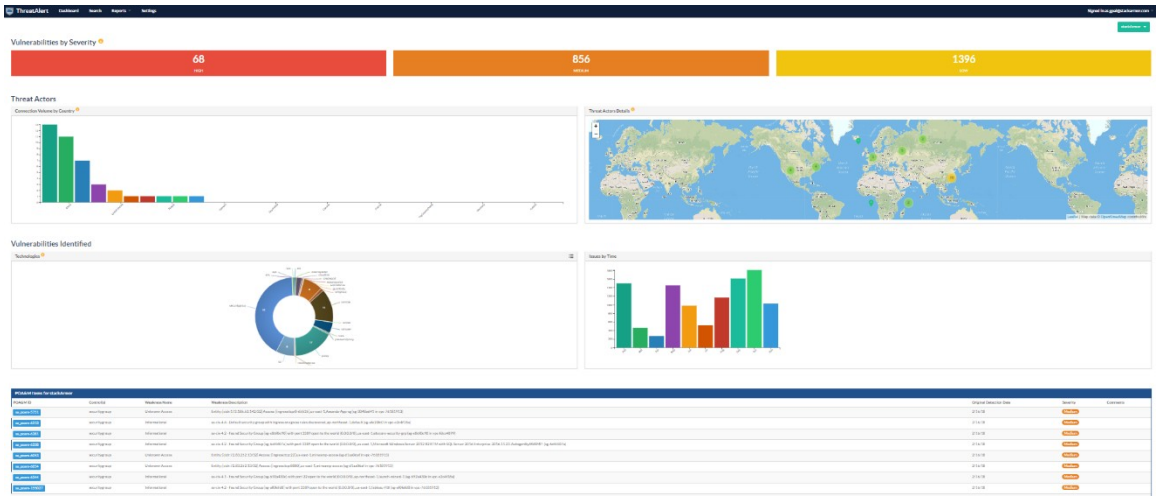


stackArmor ThreatAlert™ service for threat monitoring, management and incident response for security focused customers in Public sector, Healthcare and Education markets.

stackArmor ThreatAlert™ provides comprehensive full-stack threat monitoring and incident response support. The solution has been developed by stackArmor's Security and Cloud Solution Architects that have supported cloud migrations and security operations since 2009 for US Federal and Department of Defense customers.

2. Managed DevSecOps with stackArmor ThreatAlertTM

The US National Institute of Standards and Technology (NIST) has developed a comprehensive information systems security requirements framework for protecting the confidentiality, integrity and availability of digital systems. stackArmor's cloud architecture, security and compliance experts have distilled these requirements into a cloud-specific DevSecOps framework for organizations looking to meet or exceed FedRAMP, FISMA, HIPAA, MARS 2.0 E or similar security and compliance standards. stackArmor ThreatAlert™ provides a set of robust integrations that include Amazon GuardDuty, Security Hub, Inspector and other additional services like IDS/IPS into a single integrated view. The service is designed to help reduce the time and cost associated with managing cloud security and compliance. The screenshot below shows our integrated dashboard with High, Medium and Low findings.

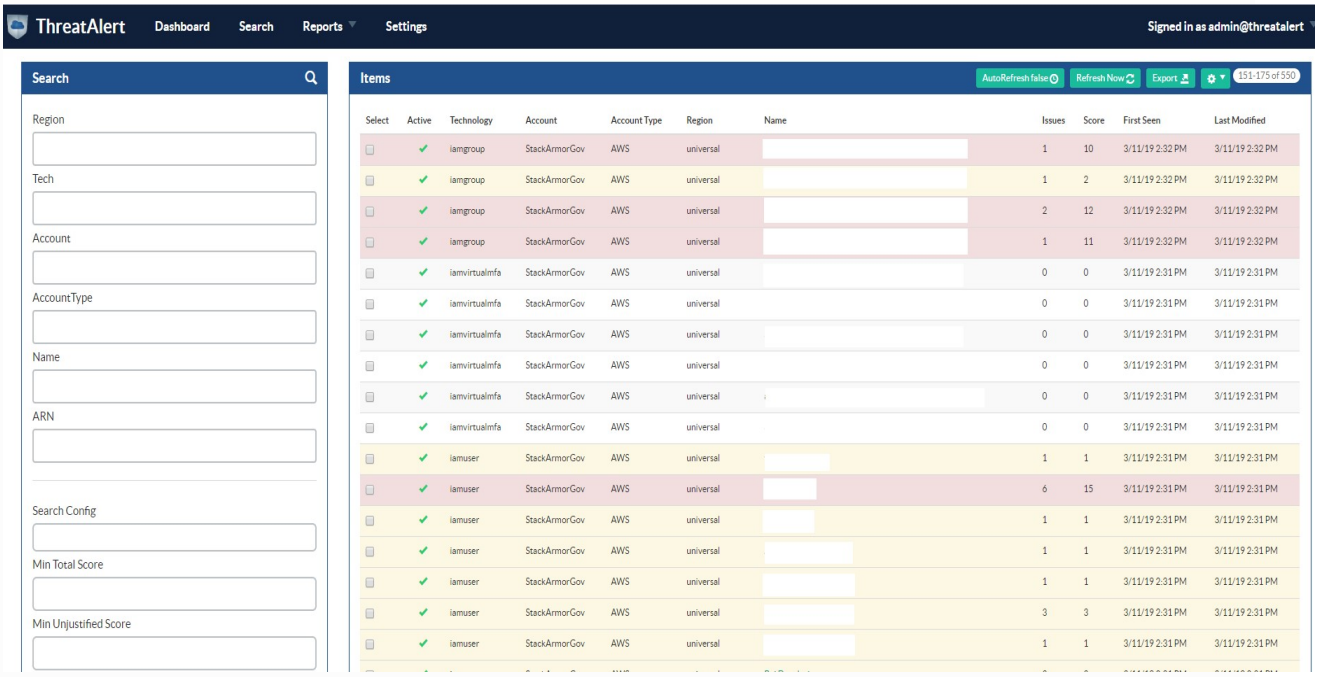


Screenshot of stackArmor ThreatAlert™ Dashboard and POAM Management System for compliance and continuous monitoring with incident response management.

The stackArmor ThreatAlert™ solution detects and reports on security and systems operations issues detected in the environment to provide a holistic solution for security and compliance focused customers. Further, the stackArmor ThreatAlert™ solution includes human-based analysis, remediation and incident response support with native integrations with ITSM/Service Management platforms like ServiceNow or Jira.

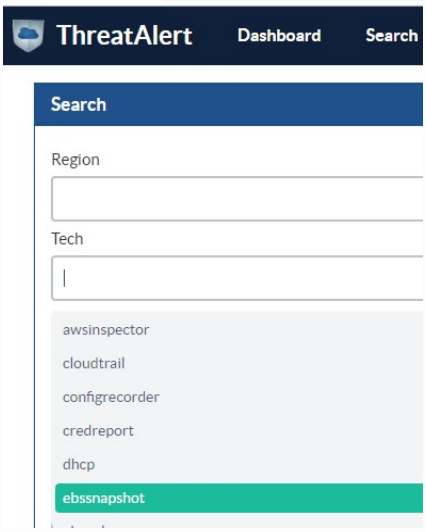
3. Searching in ThreatAlert Web UI

On the Web UI, click the **Search** button at the top left. These items are colored if they have issues. Yellow is for minor issues like friendly cross account access while red indicates more important security issues, like an S3 bucket granting access to “AllUsers” or a security group allowing 0.0.0.0/0. The newest results are always at the top.

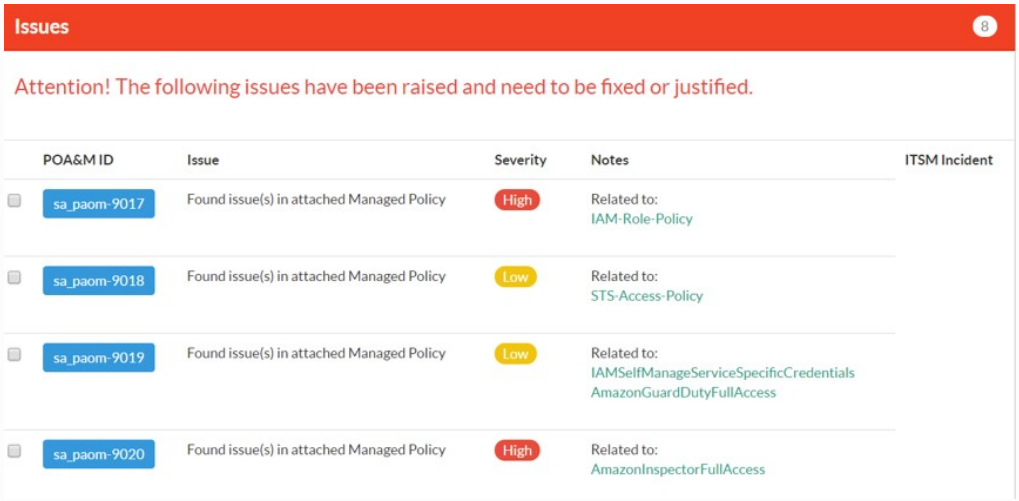


Select ‘Audit Issues’ in Type to filter out only the compliance/ security issues.

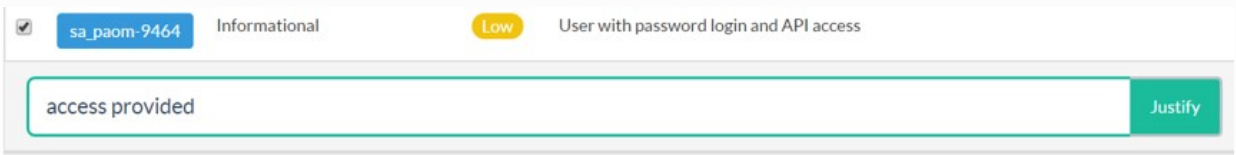
We can filter these results using the ‘Search’ box on the left. The Region, Tech, Account, and Name fields use auto-complete to help you find what you need as shown in the snapshot below.



Clicking on the **Item Name** will bring up all the vulnerabilities related to the issue with their respective severity. It will also show the instance IDs, Instance Names, VPCs the issue item is attached to.



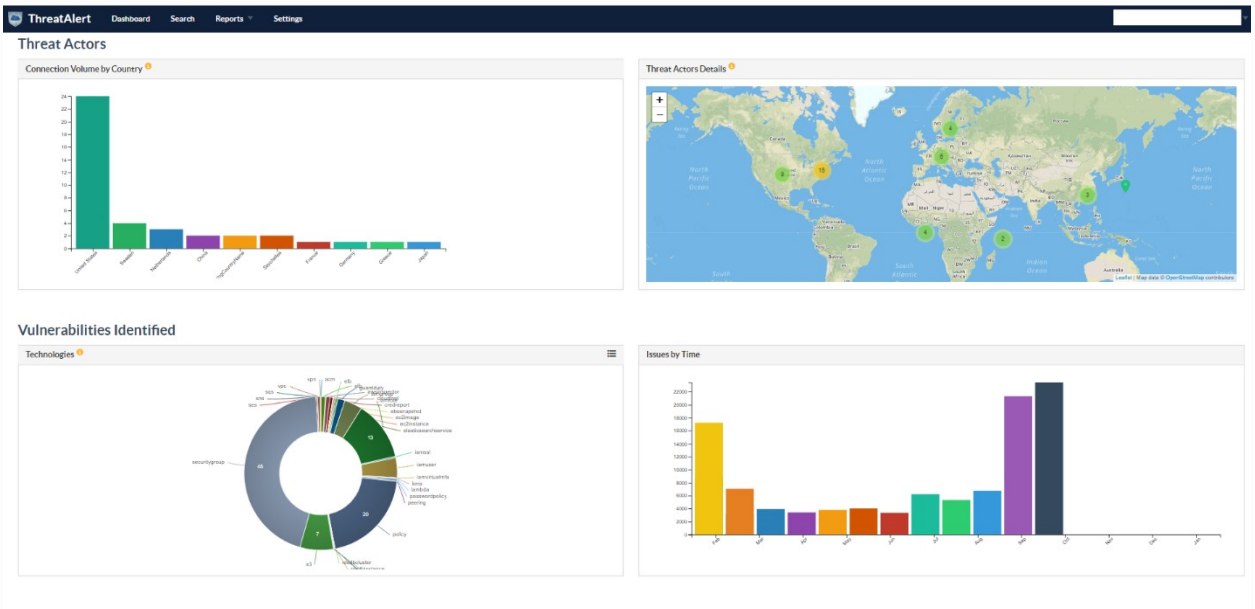
If you think, something is required as in 443 for the load balancer should be open to the internet, you can justify the issue as well. To justify, select the check box adjacent to the issue, add comments and click justify.



4. ThreatAlert Dashboard

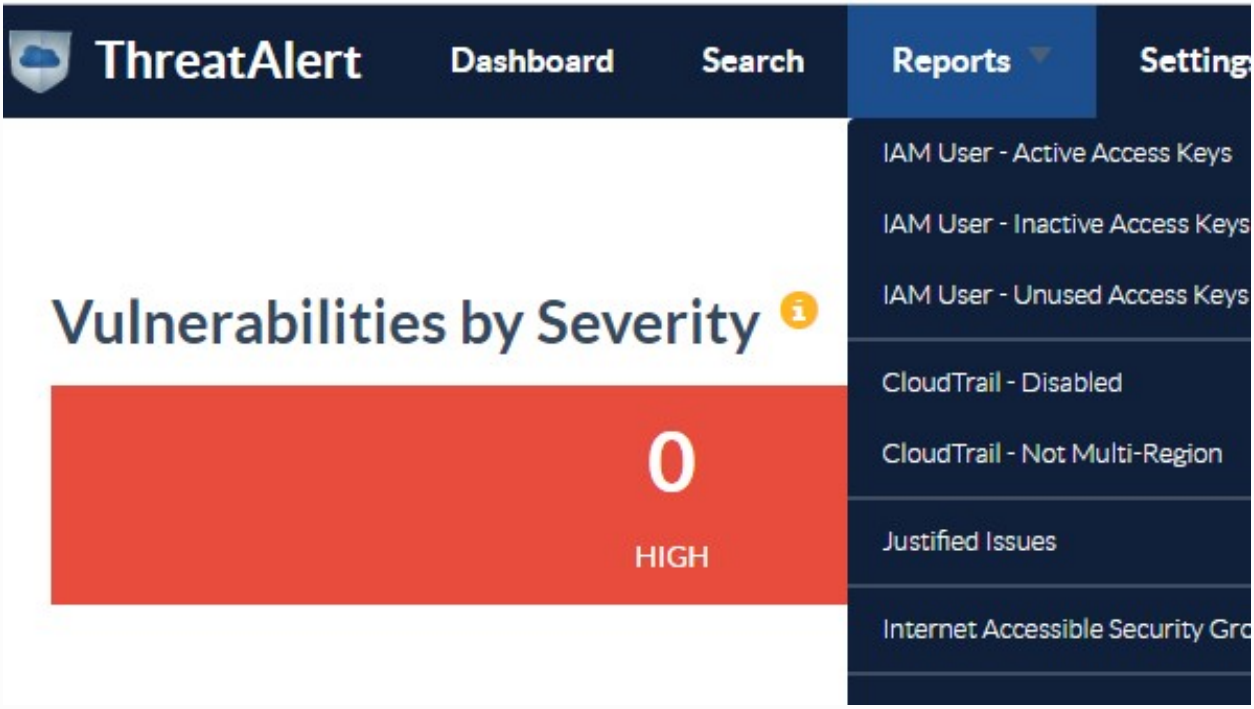
Dashboard Panel is a visual representation of the vulnerabilities in the environment. For multiple accounts, clicking on 'All Accounts' tab lets you select a specific AWS environment and filters out security threats only for the selected account. Also Clicking on 'High', 'Medium' or 'Low' filters out the vulnerabilities.

These Dashboard Panels show the threat actors from different countries. Clicking on one of the locations will show you exact location and IP address the instance and ports being hit on. The bottom two panels group the security threats according to the technologies (SecurityGroup, Policy, IAMUser, etc.)



5. ThreatAlert Reports

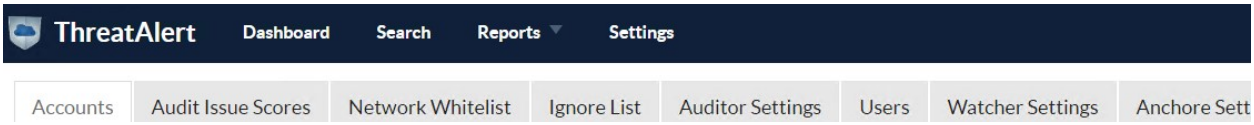
Reports makes it easier to filter out data. Selecting one of them filters out the vulnerabilities which makes it easier to download and export the report in .csv format. To export just hit on the 'Export' tab on the right corner.



6. Adding Accounts to ThreatAlert

Follow these steps to add the accounts on ThreatAlert portal.

1. Go to the settings -> Accounts tab as shown in the picture.



2. Click on the "+" under Accounts as shown in the picture.

3. Fill in the information below.

Name – Name of the account

Type – AWS (select from dropdown)

Number - AWS account number

Role Name* - Name of the role you created in AWS account (case sensitive)

NOTE: - Make sure role name is same as the one on AWS console. (Case Sensitive)

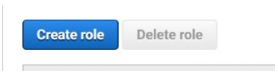
4. Make sure on selecting active and saving the information you just filled in. (Leave the remaining values blank)

7. Adding accounts to ThreatAlert (AWS Console)

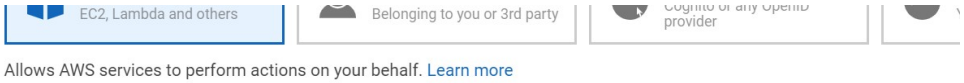
Please follow these steps on AWS console to finish adding AWS accounts to ThreatAlert.

On AWS account you want to add in:

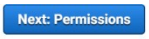
1. Under Services >Security, Identity & Compliance. Create an IAM role. Select Roles from left navigation bar. Select Create Role.



2. Choose EC2 service.



Allows AWS services to perform actions on your behalf. Learn more

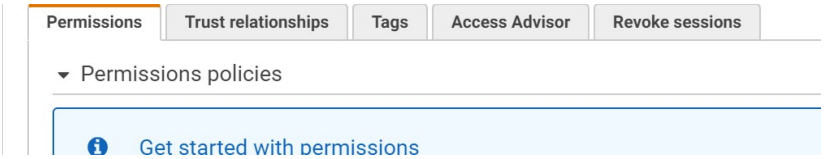
3. Click 

4. Click 

5. Click

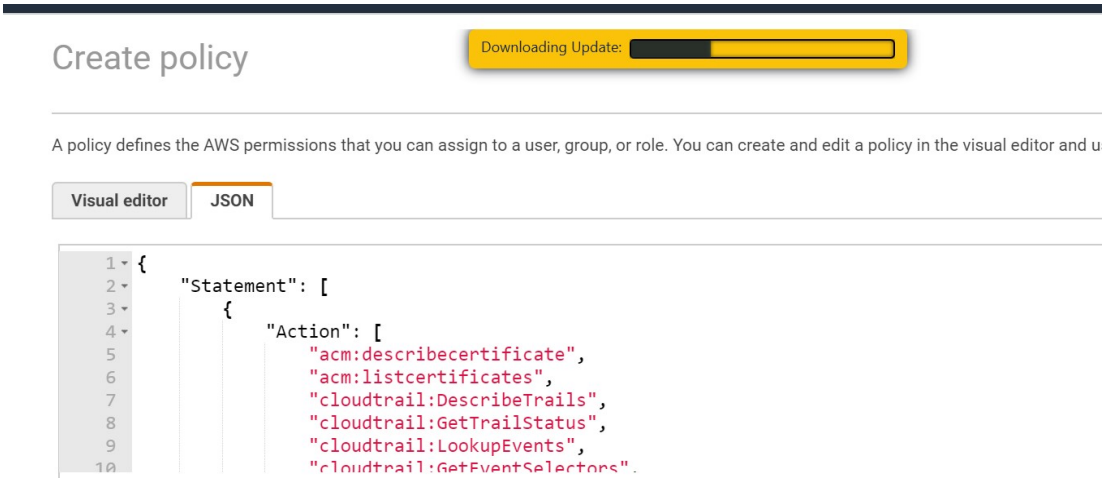
6. This is the Role Name* you add on ThreatAlert admin panel. Ec2.

7. Click on the new Role created and click Attach Policies.



8. Select Create Policy.

9. Select JSON. Copy and Paste the policy below. Click Review Policy.



10. Attach this inline policy to the role created. This is a read only IAM role that gives ThreatAlert instance the permission to scan your AWS environment.

```
{
   "Statement": [
      {
         "Action": [
            "acm:describecertificate",
            "acm:listcertificates",
            "cloudtrail:DescribeTrails",
            "cloudtrail:GetTrailStatus",
            "cloudtrail:LookupEvents",
            "cloudtrail:GetEventSelectors",
            "cloudwatch:DescribeAlarmsForMetric",
            "config:describeconfigrules",
            "config:describeconfigurationrecorders",
            "directconnect:describeconnections",
            "guardduty:GetDetector",
            "guardduty:GetMasterAccount",
            "guardduty:GetInvitationsCount",
            "guardduty:GetFindings",
            "guardduty:ListDetectors",
            "guardduty:GetIPSet",
            "guardduty:GetFindingsStatistics",
            "guardduty:ListThreatIntelSets",
            "guardduty:GetThreatIntelSet",
            "guardduty:ListInvitations",
            "guardduty:ListIPSets",
            "guardduty:GetMembers",
            "guardduty:ListFindings",
            "inspector:ListFindings",
```

"inspector:DescribeAssessmentRuns",

"inspector:ListAssessmentRunAgents",

"inspector:DescribeCrossAccountAccessRole",

"inspector:ListEventSubscriptions",

"inspector:ListAssessmentTargets",

"inspector:PreviewAgents",

"inspector:ListAssessmentRuns",

"inspector:DescribeResourceGroups",

"inspector:ListAssessmentTemplates",

"inspector:GetTelemetryMetadata",

"inspector:DescribeAssessmentTargets",

"inspector:DescribeAssessmentTemplates",

"inspector:ListTagsForResource",

"inspector:DescribeRulesPackages",

"inspector:ListRulesPackages",

"inspector:DescribeFindings",

"iam:GetCredentialReport",

"iam:GenerateCredentialReport",

"ec2:describeaddresses",

"ec2:describedhcpoptions",

"ec2:describeflowlogs",

"ec2:describeimages",

"ec2:describeimageattribute",

"ec2:describeinstances",

"ec2:describeinternetgateways",

"ec2:describekeypairs",

"ec2:describenatgateways",

"ec2:describenetworkacls",

"ec2:describenetworkinterfaces",

"ec2:describeregions",

"ec2:describeroutetables",

"ec2:describesecuritygroups",

"ec2:describesnapshots",

"ec2:DescribeSnapshotAttribute",

"ec2:describesubnets",

"ec2:describetags",

"ec2:describevolumes",

"ec2:describevpcendpoints",

"ec2:describevpcpeeringconnections",

"ec2:describevpcs",

"ec2:describevpnconnections",

"ec2:describevpngateways",

"elasticloadbalancing:describeloadbalancerattributes",

"elasticloadbalancing:describeloadbalancerpolicies",

"elasticloadbalancing:describeloadbalancers",

"elasticloadbalancing:describelisteners",

"elasticloadbalancing:describerules",

"elasticloadbalancing:describesslpolicies",

"elasticloadbalancing:describetags",

"elasticloadbalancing:describetargetgroups",

"elasticloadbalancing:describetargetgroupattributes",

"elasticloadbalancing:describetargethealth",

"es:describeelasticsearchdomainconfig",

"es:listdomainnames",

"glacier:DescribeVault",

"glacier:GetVaultAccessPolicy",

"glacier:ListTagsForVault",

"glacier:ListVaults",

"iam:GetAccountPasswordPolicy",

"iam:getaccesskeylastused",

"iam:getgroup",

"iam:getgrouppolicy",

"iam:getloginprofile",

"iam:getpolicyversion",

"iam:getrole",

"iam:getrolepolicy",

"iam:GetSAMLProvider",

"iam:getservercertificate",

"iam:getuser",

"iam:getuserpolicy",

"iam:listaccesskeys",

"iam:listattachedgrouppolicies",

"iam:listattachedrolepolicies",

"iam:listattacheduserpolicies",

"iam:listentitiesforpolicy",

"iam:listgrouppolicies",

"iam:listgroups",

"iam:listinstanceprofilesforrole",

"iam:listmfadevices",

"iam:listpolicies",

"iam:listrolepolicies",

"iam:listroles",

"iam:listsamlproviders",

"iam:listservercertificates",

"iam:listsigningcertificates",

"iam:listuserpolicies",

"iam:listusers",

"kms:describekey",

"kms:getkeypolicy",

"kms:getkeyrotationstatus",

"kms:listaliases",

"kms:listgrants",

"kms:listkeypolicies",

"kms:listkeys",

"lambda:getfunctionconfiguration",

"lambda:getpolicy",

"lambda:listaliases",

"lambda:listeventsourcemappings",

"lambda:listtags",

"lambda:listversionsbyfunction",

"lambda:listfunctions",

"logs:describemetricfilters",

"rds:describedbclusters",

"rds:describedbclustersnapshots",

"rds:describedbinstances",

"rds:describedbsecuritygroups",

"rds:describedbsnapshots",

"rds:describedbsnapshotattributes",

"rds:describedbsubnetgroups",

"redshift:describeclusters",

"route53:listhostedzones",

"route53:listresourcerecordsets",

"route53domains:listdomains",

"route53domains:getdomaindetail",

"s3:getacceleratеconfiguration",

"s3:getbucketacl",

"s3:getbucketcors",
"s3:getbucketlocation",
"s3:getbucketlogging",
"s3:getbucketnotification",
"s3:getbucketpolicy",
"s3:getbuckettagging",
"s3:getbucketversioning",
"s3:getbucketwebsite",
"s3:getlifecycleconfiguration",
"s3:listbucket",
"s3:listallmybuckets",
"s3:getreplicationconfiguration",
"s3:getanalyticsconfiguration",
"s3:getmetricsconfiguration",
"s3:getinventoryconfiguration",
"ses:getidentityverificationattributes",
"ses:listidentities",
"ses:listverifiedemailaddresses",
"ses:sendemail",
"sns:gettopicattributes",
"sns:listsubscriptionsbytopic",
"sns:listtopics",
"sqs:getqueueattributes",
"sqs:listqueues",
"iam:GetAccountSummary",
"iam:ListVirtualMFADevices"
],
"Resource": "*",
"Effect": "Allow"

```
      }
    ]
}
```

11. Add any Name

12. Go under trust relationship of that role and edit it to:

```
{
 "Version": "2008-10-17",
 "Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "ec2.amazonaws.com",
      "AWS": "INSTANCE PROFILE ARN GOES HERE"
    },
    "Action": "sts:AssumeRole"
  }
 ]
}
```

13. Replace the “INSTANCE PROFILE ARN GOES HERE” line to the actual instance profile of ThreatAlert.

ThreatAlert scans your environment every hour. So, if everything is created well, you should be able to see your newly added account vulnerabilities from next scan.

8. About stackArmor

stackArmor is an Advanced AWS certified provider of Cloud migration, Cloud managed services and Cloud managed security & compliance services for Government, Education, Healthcare and Non-profits customers. Our certified experts help protect customers from cyberthreat challenges through systems engineering best practices developed over decades while working with US Federal Agencies requiring compliance with ISO 27001, NIST, FFIEC, FISMA, FedRAMP, DHS and DISA standards. stackArmor is recognized by Amazon Web Services (AWS) for strong Government, Public Sector and Security competencies and was selected as 1 of 10 inaugural launch partners globally for the AWS Security Competency.

stackArmor

Washington DC Office
8300 Greensboro Drive, #990
Tysons VA 22102, USA

Email: solutions@stackarmor.com
Website: www.stackArmor.com

CONNECT WITH US

https://www.linkedin.com/company/stackarmor-inc-/

https://twitter.com/stackArmor

We are an Advanced AWS Partner and 1 of 10 firms selected globally by AWS for the Security competency launch. We enable your company's transition to secure cloud computing through the lifecycle that includes the design of secure environments; implementation of automated intrusion detection, vulnerability and log management services; and helping modernize Enterprise IT operations through automation of cybersecurity, development and operations activities. We deliver secure and compliant architectures with decades of experience working with US Federal and Department of Defense meeting NIST, FFIEC, FISMA, FedRAMP, DHS and DISA standards.