AWS Dome9 CheckUp

Jul 30, 2019 10:00 AM

AWS Dome9 CheckUp.

Cloud Account

AWS (833682875278) , All Regions

TABLE OF CONTENTS

EXECUTIVE SUMMARY

SUMMARY OF TESTS PERFORMED

Tests Performed	Passed	Failed
1018	54.32% (553)	45.68% (465)

FAILED TESTS BY SEVERITY

High	Medium	Low
195	268	2

SUMMARY OF RULES TESTED

Rules Performed	Passed	Failed
67	65.67% (44)	34.33% (23)

Entities by type, Pass Vs Fail

Entity Type	Passed	Failed
AcmCertificate (0)	0	0
AMI (6)	**6**	0
ApplicationLoadBalancer (0)	0	0
CloudFront (0)	0	0
CloudTrail (1)	**1**	0
DynamoDbTable (7)	0	**7**
EcsCluster (0)	0	0
EcsTask (0)	0	0
EFS (0)	0	0
ElastiCache (0)	0	0
ELB (2)	**2**	0
Iam (1)	0	**1**
IamPolicy (617)	**616**	**1**
IamServerCertificate (0)	0	0
IamUser (11)	**5**	**6**
Instance (50)	**22**	**28**

Entity Type	Passed	Failed
Kinesis (0)	0	0
KMS (29)	**29**	0
Lambda (48)	**25**	**23**
List<CloudTrail> (1)	0	**1**
List<Lambda> (1)	0	**1**
RDS (0)	0	0
Redshift (0)	0	0
Region (16)	**2**	**14**
Route53Domain (0)	0	0
Route53HostedZone (0)	0	0
RouteTable (48)	**24**	**24**
S3Bucket (32)	**30**	**2**
SageMakerNotebook (0)	0	0
SecurityGroup (190)	**22**	**168**
Subnet (84)	**57**	**27**
Volume (64)	**63**	**1**
VPC (48)	**5**	**43**
NetworkLoadBalancer (3)	**3**	0

Regions

Name	Passed Tests	Failed Tests	Failed Entities	Failed High	Failed Medium	Failed Low
N. Virginia	**1007**	**11**	**7**	**5**	**6**	0
Ohio	**1005**	**13**	**10**	**6**	**7**	0
Oregon	**1007**	**11**	**7**	**4**	**7**	0
N. California	**1015**	**3**	**3**	**1**	**2**	0
Ireland	**1013**	**5**	**5**	**2**	**3**	0
Frankfurt	**1004**	**14**	**10**	**7**	**7**	0
Singapore	**1013**	**5**	**4**	**1**	**4**	0
Sydney	**1012**	**6**	**5**	**2**	**4**	0
Tokyo	**1013**	**5**	**5**	**2**	**3**	0
Seoul	**1013**	**5**	**5**	**2**	**3**	0
São Paulo	**1013**	**5**	**5**	**2**	**3**	0
Mumbai	**1016**	**2**	**2**	0	**2**	0
Canada Central	**1016**	**2**	**2**	0	**2**	0
London	**1006**	**12**	**8**	**5**	**7**	0

Name	Passed Tests	Failed Tests	Failed Entities	Failed High	Failed Medium	Failed Low
Paris	**1014**	**4**	**4**	**1**	**3**	0
Stockholm	**1014**	**4**	**4**	**2**	**2**	0

Failed Tests Summary

Rule Name	Severity	Tested	Relevant	Non Compliant
Process for Security Group Management - Managing security groups	**High**	**190**	**190**	**114**
Ensure AWS VPC subnets have automatic public IP assignment disabled	**High**	**84**	**84**	**27**
Instance with administrative service: SSH (TCP:22) is too exposed to the public internet	**High**	**50**	**19**	**15**
Instance with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet	**High**	**50**	**18**	**11**
Instance with administrative service: CiscoSecure,websm (TCP:9090) is too exposed to the public internet	**High**	**50**	**12**	**11**
Ensure that AWS DynamoDB is encrypted using customer managed CMKs (Customer Master Key) instead of AWS-owned CMK's	**High**	**7**	**7**	**7**
Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	**High**	**11**	**6**	**6**
Use encrypted storage for instances that might host a database.	**High**	**50**	**2**	**2**
Ensure S3 buckets are not publicly accessible	**High**	**32**	**32**	**2**
Remove Unused Security Groups	**Medium**	**190**	**142**	**99**
Ensure VPC flow logging is enabled in all VPCs	**Medium**	**48**	**48**	**43**
Instance with administrative service: SSH (TCP:22) is exposed to a wide network scope	**Medium**	**50**	**32**	**27**
Ensure AWS NAT Gateways are not being utilized for the default route	**Medium**	**48**	**48**	**24**
Lambda Functions must have an associated tag	**Medium**	**48**	**48**	**23**
Instance with administrative service: Remote Desktop (TCP:3389) is exposed to a wide network scope	**Medium**	**50**	**24**	**17**
Instance with administrative service: CiscoSecure,websm (TCP:9090) is exposed to a wide network scope	**Medium**	**50**	**18**	**17**
Process for Security Group Management - Detection of new Security Groups	**Medium**	**16**	**16**	**14**
Ensure IAM password policy require at least one symbol	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for unauthorized API calls	**Medium**	**1**	**1**	**1**

Rule Name	Severity	Tested	Relevant	Non Compliant
Ensure that your Amazon Lambda functions do not share the same AWS IAM execution role	**Medium**	**1**	**1**	**1**
Ensure AWS EBS Volumes are attached to instances	**Medium**	**64**	**64**	**1**
Ensure IAM password policy expires passwords within 90 days or less	**Low**	**1**	**1**	**1**
Ensure a support role has been created to manage incidents with AWS Support	**Low**	**617**	**1**	**1**

FAILED TESTS

FAILED

HIGH

Process for Security Group Management - Managing security groups

Description:

Security groups should be managed and enforced by Dome9. Dome9 Security Group Full Protection facilitates a formal process for approving and testing all network connections and changes to the firewall and router configurations.

190 TESTED **190** RELEVANT **114** NON COMPLIANT

Network Security

GSL:

```
SecurityGroup should have isProtected = 'true'
```

Remediation:

Change Cloud Guard Dome9 Protection mode for specific security groups from Read-only to Full protection mode

Failed Entities

ID	Name	Region	VPC
sg-08e16c1e483859455	LAMP with PHP 7-1 Certified by Bitnami-7-1-22-1-r40 on Ubuntu 16-04-AutogenByAWSMP-	Singapore	vpc-0278f4095614fd5e8
sg-a5cb6adc	default	Singapore	vpc-4ef04f29
sg-0f8b1b14c0fece642	Management-InstanceSecurityGroup-80NDJH16TT0O	Singapore	vpc-0278f4095614fd5e8
sg-06fb03c2c85991694	default	Singapore	vpc-0278f4095614fd5e8
sg-017cb4f4cbe2995c3	Cluster-InstanceSecurityGroup-19RNWWU9TOO7J	Singapore	vpc-0278f4095614fd5e8

ID	Name	Region	VPC
sg-ae39cad6	default	Tokyo	vpc-f4a23a93
sg-070fe44fd62a0c040	Microsoft Windows Server 2008 R2 Base-2018-07-11-AutogenBy AWSMP-1	Sydney	vpc-0690917dc691a05a8
sg-0b818346e856edad7	launch-wizard-1	Sydney	vpc-0690917dc691a05a8
sg-019df7802c180e1f7	default	Sydney	vpc-0690917dc691a05a8
sg-09a08bcf34beac3dc	launch-wizard-3	Sydney	vpc-0690917dc691a05a8
sg-0d4fb4e5435e8098d	launch-wizard-2	Sydney	vpc-0690917dc691a05a8
sg-9a15ddf0	default	Seoul	vpc-346c4a5c
sg-0485c7bf05cd0727c	Microsoft Windows Server 2008 R2 Base-2018-07-11-AutogenBy AWSMP-	Sydney	vpc-0690917dc691a05a8
sg-047eb512551b97ddb	Microsoft Windows Server 2008 R2 Base-2018-07-11-AutogenBy AWSMP-2	Sydney	vpc-0690917dc691a05a8
sg-f76ba19e	default	Stockholm	vpc-04a8416d
sg-002c5d66c44afd940	launch-wizard-4	Sydney	vpc-0690917dc691a05a8
sg-0d19f9a279066c658	launch-wizard-5	Sydney	vpc-0690917dc691a05a8
sg-08f754d8379194e66	default	Paris	vpc-00d07981fef5aa11b
sg-06b885a39088e997c	default	Frankfurt	vpc-0c99aa94269cda634
sg-0b06406d99951d61f	launch-wizard-1	Frankfurt	vpc-0c99aa94269cda634
sg-0237d8df79395bc47	QA VPC	São Paulo	vpc-0dd7491fcfb1e5739
sg-006a94d3e3b60bc66	default	Sydney	vpc-08c17db27472abd32
sg-0807d08e786df4199	default	Frankfurt	vpc-070e9b1cb4fb74445
sg-00de46f02ee7b6056	default	Frankfurt	vpc-03d3a03126797ecd7
sg-0317eb7b4a5b74d5a	CloudGuard IaaS Security Mana gement - BYOL-R80-10-033-341-AutogenByAWSMP-	Frankfurt	vpc-03d3a03126797ecd7
sg-0662887f0fcdd0fe2	CloudGuard IaaS Security Mana gement - BYOL-R80-10-033-341-AutogenByAWSMP-1	Frankfurt	vpc-03d3a03126797ecd7
sg-011d61286abfba5ec	default	Oregon	vpc-04cd9c4cfa331fb66
sg-0edc488b9375e4e48	CloudGuard IaaS Security Mana gement - BYOL-R80-20-101-427-AutogenByAWSMP-	Oregon	vpc-04cd9c4cfa331fb66
sg-0aa41eb4f8d8ecc2d	sec_group_LB	Oregon	vpc-04cd9c4cfa331fb66
sg-02016fb2ef9dc0eb3	default	Oregon	vpc-09d2ecbb4976ce399

ID	Name	Region	VPC
sg-0db89ceb8079d1072	CloudGuard IaaS R80-20 Security Gateway - BYOL-R80-20-005-376-AutogenByAWSMP-1	Oregon	vpc-09d2ecbb4976ce399
sg-076a662f44ac2f743	CloudGuard IaaS Next Gen Firewall - Threat Prevention Standalone-R80-10-033-341-AutogenByAWSMP-	Oregon	vpc-09d2ecbb4976ce399
sg-04b719f017db1f39c	CloudGuard IaaS Security Management - BYOL-R80-20-101-427-AutogenByAWSMP-1	Oregon	vpc-09d2ecbb4976ce399
sg-05397197b091039e3	Ubuntu 16-04 LTS - Xenial -HVM--Ubuntu 16-04 LTS 20190212-AutogenByAWSMP-2	Oregon	vpc-09d2ecbb4976ce399
sg-011dfd3f4388c481d	SG_OPEN_ISAI	Oregon	vpc-09d2ecbb4976ce399
sg-0d699b93d4832161b	default	Ohio	vpc-002fda6c1746b92a7
sg-05c46db00b8bad7b9	CP-Management-Nottingham-InstanceSecurityGroup-A0ZLJETNQLPW	Ohio	vpc-002fda6c1746b92a7
sg-05b61a514868a24c8	launch-wizard-6	Sydney	vpc-0690917dc691a05a8
sg-062c7903326da3639	default	Ohio	vpc-0d13246ba98f6a395
sg-086e20616091463cb	Check-Point-Transit-VPC-TransitStack-UOPD8YSJWGA2-GatewayB-1J1J3VOXU78PC-SecurityGroup-1I64QQQPOHU15	Ohio	vpc-0d13246ba98f6a395
sg-0957653c8fe04786d	Check-Point-Transit-VPC-TransitStack-UOPD8YSJWGA2-GatewayA-17UPGT337BDDQ-SecurityGroup-WJPUCUZ63T7F	Ohio	vpc-0d13246ba98f6a395
sg-0b17bdebc65976e2a	test-security-group	Ohio	vpc-002fda6c1746b92a7
sg-074f584af096b2c9e	default	Ohio	vpc-081b4cdf31561a49d
sg-0328b41060fccffdc	default	Ohio	vpc-01ec48b32e41b118c
sg-015004d61f2435d43	CloudGuard IaaS R80-20 Security Gateway - BYOL-R80-20-005-376-AutogenByAWSMP-	Ohio	vpc-081b4cdf31561a49d
sg-0c4a293cab4a31991	Management-CHKP	Ohio	vpc-081b4cdf31561a49d
sg-03bab9461a8b554ff	CloudGuard IaaS Security Management - BYOL-R80-20-101-427-AutogenByAWSMP-	Ohio	vpc-081b4cdf31561a49d
sg-0ee760166fa1e72f7	CloudFormer-WebServerSecurityGroup-II9RPD5V5EJ5	Frankfurt	vpc-031c8847c1fe0614d
sg-086ab7563a803f415	default	Frankfurt	vpc-031c8847c1fe0614d

ID	Name	Region	VPC
sg-0d5e4e9af60e8269d	launch-wizard-2	Frankfurt	vpc-0c99aa94269cda634
sg-0d189e0980e0169ec	default	London	vpc-00a5c0fae79e5dfb5
sg-0a849bf9ab5424d6b	Demo-Check-Point-Management-InstanceSecurityGroup-EUM1WJTIBF5W	London	vpc-00a5c0fae79e5dfb5
sg-07ddcbb5adb8f1549	Check-Point-TGW-AutoScaling-MainStack-GVO0TG8L932H-SecurityGatewaysStack-XKOE0FFM6KRW-PermissiveSecurityGroup-VFWKEGYXF9XU	London	vpc-07393d5aece590401
sg-01b3723296973fbd2	default	London	vpc-07393d5aece590401
sg-0e9cab8cab280cfab	default	London	vpc-0635b1031b9fbe1b9
sg-06e5129b028ddc3e1	default	London	vpc-0a1a953743db0df83
sg-0cf7ab913f1518771	launch-wizard-2	London	vpc-0635b1031b9fbe1b9
sg-01d8c435cbfcee92f	launch-wizard-3	London	vpc-0a1a953743db0df83
sg-0e6b6e19e675bda8e	default	London	vpc-01317b8042aff3f2c
sg-0ecc68e6451da2837	Check-Point-Inbound-AutoScaling-PermissiveSecurityGroup-1QTAJJ5838ZD1	London	vpc-01317b8042aff3f2c
sg-0a9eb8561cbc6602f	quick-create-1	London	vpc-01317b8042aff3f2c
sg-058050f9362651705	default	Ohio	vpc-07b020fd98b9806c7
sg-0be427343e25fce76	benoitb-sg	Ohio	vpc-07b020fd98b9806c7
sg-0be626a85e43325b3	default	Ohio	vpc-0890ddc0804e52cc5
sg-0ea0c883c7d115b0b	CloudGuard IaaS Security Management - BYOL-R80-20-101-427-AutogenByAWSMP-1	Ohio	vpc-0890ddc0804e52cc5
sg-02f01a23a75303826	CloudGuard IaaS R80-20 Security Gateway - BYOL-R80-20-005-376-AutogenByAWSMP-1	Ohio	vpc-0890ddc0804e52cc5
sg-07ffa8db38dc925d0	AutoScaling-Security-Group-1	Ohio	vpc-0d13246ba98f6a395
sg-074030344a203e790	GREG_DMZ_SEC_GROUP	Ohio	vpc-0890ddc0804e52cc5
sg-06eee9cedf01c07e5	Kaholo-SG	Frankfurt	vpc-0c99aa94269cda634
sg-024f544fddd285652	Kaholo	Frankfurt	vpc-070e9b1cb4fb74445
sg-0b67c5747c9e8ca2a	Greg-AutoScale-Stack-PermissiveSecurityGroup-9JP816G1ASJQ	Ohio	vpc-0890ddc0804e52cc5
sg-081e896eba10d2d81	launch-wizard-1	Ohio	vpc-0890ddc0804e52cc5
sg-0b5df2a1febcc04f6	launch-wizard-2	Ohio	vpc-0890ddc0804e52cc5

ID	Name	Region	VPC
sg-039056bd22003c32b	CloudGuard IaaS R80-20 Security Gateway - BYOL-R80-20-005-376-AutogenByAWSMP-	London	vpc-0635b1031b9fbe1b9
sg-0d8995d3b66ad591b	default	Ohio	vpc-0eaebca854572960e
sg-091acec2b8062db7f	Check-Point-Management-Hyun-InstanceSecurityGroup-1WI8VP70YRKN7	Ohio	vpc-0eaebca854572960e
sg-0f990bd6cdaced3ac	default	Ohio	vpc-0f907a75820eccb01
sg-053eba5b4981aad3d	Check-Point-Management-test-InstanceSecurityGroup-JL1MHAXJISYJ	Ohio	vpc-0eaebca854572960e
sg-010f6aa7f795ef726	LAMP Certified by Bitnami-7-1-29-0-r50 on Ubuntu 16-04-AutogenByAWSMP-	Ohio	vpc-0eaebca854572960e
sg-0cfbbc4beb5632483	Check-Point-Cluster-Hyun-InstanceSecurityGroup-15AQI4JBRLQOC	Ohio	vpc-0eaebca854572960e
sg-0ec3ae041e8e53572	NGINX Open Source Certified by Bitnami-1-16-0-0-r50 on Ubuntu 16-04-AutogenByAWSMP-	Ohio	vpc-0eaebca854572960e
sg-0d88c8c43cf86c655	launch-wizard-3	Frankfurt	vpc-070e9b1cb4fb74445
sg-021aa98c2c921d3cf	sGJSlondon	London	vpc-0635b1031b9fbe1b9
sg-0ddb4ac5b06fa0ed8	default	London	vpc-06ba88b1e44da29db
sg-0c9588adab9a1f6cb	default	Sydney	vpc-00b10f6ecf81bad13
sg-031c02842b78bb882	launch-wizard-4	Frankfurt	vpc-070e9b1cb4fb74445
sg-089a2de494dcd1882	default	Ohio	vpc-0b9d8b1583875c97c
sg-0c5e8f46c69ac2b15	Check-Point-Cluster-BT-InstanceSecurityGroup-5CS1UISM3WOA	Ohio	vpc-0b9d8b1583875c97c
sg-03fe8ee77148847ab	launch-wizard-5	Frankfurt	vpc-070e9b1cb4fb74445
sg-0283339cb0a6eeb8a	default	Ireland	vpc-0b969103451d7708a
sg-068c012e8861484b1	default	Frankfurt	vpc-07278dd5dff86090a
sg-0d2c320a57855e10e	default	Ireland	vpc-0f36c6405ba7b3377
sg-07811cdb1f9c9dee8	default	Ireland	vpc-0e7e70cca43bfc157
sg-0fe00f16bdd66677e	default	Ireland	vpc-0f114355a917cd98a
sg-0c6c6ab18415e54ae	default	Ireland	vpc-0dcb89a70ed7c3fe2
sg-0768d07aafb38a8cb	JM-1-Check-Point-TGW-AutoScaling-MainStack-IMVJ7A68FM6L-ManagementStack-1M9BEI6WQ0BT8-InstanceSecurityGroup-1JCIPHL7ZKQLB	Ireland	vpc-0dcb89a70ed7c3fe2

ID	Name	Region	VPC
sg-05553021af27ba957	JM-1-Check-Point-TGW-AutoScaling-MainStack-IMVJ7A68FM6L-SecurityGatewaysStack-EX3M7ROGPJB7-PermissiveSecurityGroup-1BXH3SS6C30YY	Ireland	vpc-0dcb89a70ed7c3fe2
sg-02edb3df573c625b1	default	Frankfurt	vpc-0eb54c6cca35cef2c
sg-0f6c1d730b55f20e7	NSaaS Security Group	Frankfurt	vpc-0eb54c6cca35cef2c
sg-0c786cd954633a66e	NSaaS_Host_SG	Frankfurt	vpc-0eb54c6cca35cef2c
sg-05971c438b2f7f103	default	Frankfurt	vpc-005ff9a5d1585605b
sg-0e3ded9cc154e4d81	default	Frankfurt	vpc-0f61ebcb8a5ac5399
sg-0f79ab21c8b9c4ae4	Check-Point-Management-mnoh-InstanceSecurityGroup-TWPQ3HK644ZQ	Frankfurt	vpc-0f61ebcb8a5ac5399
sg-0ea2a171d24927dfd	LAMP Certified by Bitnami-7-1-29-0-r50 on Ubuntu 16-04-AutogenByAWSMP-	Frankfurt	vpc-0f61ebcb8a5ac5399
sg-0c5504c2786b26ec5	default	Frankfurt	vpc-0e8377cbf81339c40
sg-02c5d62cfbca4745e	default	Frankfurt	vpc-0c85f08fc22162d9d
sg-07127644a744a4a86	default	N. California	vpc-0e4b0002161b0bf36
sg-07430abb862281f44	default	Frankfurt	vpc-0249332f781a5791f
sg-0bc6e1ccc146ea818	LAMP Certified by Bitnami-7-1-29-0-r50 on Ubuntu 16-04-AutogenByAWSMP-1	Frankfurt	vpc-0249332f781a5791f
sg-077d18b650cbea636	default	Ireland	vpc-0febe03823903a468
sg-071d538a9aaafc059	default	Ireland	vpc-042fff1c60e196769
sg-0b9ddd400ac70c760	CloudGuard IaaS Security Management -BYOL- - Previous Version-R80-10-033-341-AutogenByAWSMP-	Frankfurt	vpc-070e9b1cb4fb74445
sg-03a88a8e0c6bb9a2f	CloudGuard IaaS Next-Gen Firewall w- Threat Prevention - SandBlast BYOL-R80-20-005-376-AutogenByAWSMP-	Frankfurt	vpc-070e9b1cb4fb74445
sg-0d09f5c4e3033b5de	CloudGuard IaaS Security Management -BYOL--R80-20-101-479-AutogenByAWSMP-	Oregon	vpc-04cd9c4cfa331fb66

FAILED

HIGH

Ensure AWS VPC subnets have automatic public IP assignment disabled

Description:

A VPC subnet is a part of the VPC, with its own rules for traffic. Subnets with automatic Public IP assignment can inadvertently expose the instances within this subnet to the internet. It is recommended to disable this feature for subnets.

84 TESTED **84** RELEVANT **27** NON COMPLIANT

Network Security

GSL:

```
Subnet should not have mapPublicIpOnLaunch=true
```

Remediation:

1. Log in to the AWS console.
2. In the console, select the specific region .
3. Navigate to the 'VPC' service.
4. In the navigation pane, click 'Subnets'.
5. Select the identified Subnet and Select the option 'Modify auto-assign IP settings' under the Subnet Actions.
6. Disable the 'Auto-Assign IP' option and save it.

Failed Entities

ID	Name	Region	VPC
subnet-9787e0cc	-	Tokyo	vpc-f4a23a93
subnet-8da18bc4	-	Tokyo	vpc-f4a23a93
subnet-92d4d1ba	-	Tokyo	vpc-f4a23a93
subnet-139c085f	-	Seoul	vpc-346c4a5c
subnet-1414357c	-	Seoul	vpc-346c4a5c
subnet-3fa5ab47	-	Stockholm	vpc-04a8416d
subnet-bf1ef1d6	-	Stockholm	vpc-04a8416d
subnet-9ce5cdd6	-	Stockholm	vpc-04a8416d
subnet-089568872123af20d	-	São Paulo	vpc-0c797dd4798891a7a
subnet-0ea681392bf94c56c	-	São Paulo	vpc-0c797dd4798891a7a
subnet-0dfe22259d9e1296d	-	Sydney	vpc-08c17db27472abd32
subnet-02f353ed190ac1922	-	Sydney	vpc-08c17db27472abd32
subnet-008792e524acae10e	-	Sydney	vpc-08c17db27472abd32
subnet-0947de130c41ca8a1	-	Frankfurt	vpc-070e9b1cb4fb74445
subnet-0050ca28a2d55dab6	-	Frankfurt	vpc-070e9b1cb4fb74445
subnet-03d90a9ec9d500e1a	-	Frankfurt	vpc-070e9b1cb4fb74445
subnet-0b12817d403c12f9a	Public subnet	Ohio	vpc-002fda6c1746b92a7
subnet-b4b476cf	-	Seoul	vpc-346c4a5c
subnet-022264569b0488de3	Public subnet 2	Ohio	vpc-0d13246ba98f6a395

ID	Name	Region	VPC
subnet-03cf30341ed738bb3	Public subnet 1	Ohio	vpc-0d13246ba98f6a395
subnet-00797b5c689eb6413	Public subnet	Ohio	vpc-081b4cdf31561a49d
subnet-08ce7305eb29d213d	-	Frankfurt	vpc-031c8847c1fe0614d
subnet-0d38419bb82bfec5f	Public subnet 2	London	vpc-07393d5aece590401
subnet-0bf6e48b398899652	Public subnet 1	London	vpc-07393d5aece590401
subnet-0e7fbce489ddbed01	VPC-C-Subnet-Public	Ireland	vpc-0f114355a917cd98a
subnet-0d5d8e4d3c851d72e	Public subnet 2	Ireland	vpc-0dcb89a70ed7c3fe2
subnet-05cd87160bf7139b5	Public subnet 1	Ireland	vpc-0dcb89a70ed7c3fe2

FAILED

HIGH

Instance with administrative service: SSH (TCP:22) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

50 TESTED **19** RELEVANT **15** NON COMPLIANT

Network Ports Security

GSL:

```
Instance where isPublic=true and inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]
```

Remediation:

Delete the rules that allow permissive SSH/Remote/Admin access
As a further protection, use Dome9 Dynamic Access Leasing to limit access to SSH/Remote Desktop only from allowed sources and only when needed.
For more information please refer to: https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_ (https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_)

Failed Entities

ID	Name	Region	VPC
i-0f1b376d28b21add8	Demo-MNG	London	vpc-00a5c0fae79e5dfb5
i-058cbba83aa90a949	-	London	vpc-00a5c0fae79e5dfb5
i-0c5e1696d45c947a6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-088d1cc7ff19a7ba6	Inbound-Gateway	London	vpc-01317b8042aff3f2c

ID	Name	Region	VPC
i-00c6665c1461ce720	Prod-Win-2008	London	vpc-0635b1031b9fbe1b9
i-0e4f8b370d73b1e3f	Chkp-SG	London	vpc-0635b1031b9fbe1b9
i-0acb17ed0d02c498d	NSaaS-SG	Frankfurt	vpc-070e9b1cb4fb74445
i-07fd0dd7506ff7472	Check-Point-Gateway	London	vpc-07393d5aece590401
i-00b65b153ffc4ca68	Check-Point-Gateway	London	vpc-07393d5aece590401
i-0c771682369060b52	monitoring	N. Virginia	vpc-08e4d9606f19e2594
i-068f6edc4a06b324b	DB1	N. Virginia	vpc-08e4d9606f19e2594
i-0b6d2423197706617	ISAI_GW	Oregon	vpc-09d2ecbb4976ce399
i-025806ba9dc1d9485	ISAI_MGMT	Oregon	vpc-09d2ecbb4976ce399
i-0e50738cef07ca04f	transit-gateway	Ohio	vpc-0d13246ba98f6a395
i-0bc51846be38d5d38	transit-gateway	Ohio	vpc-0d13246ba98f6a395

FAILED

HIGH

Instance with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

50 TESTED **18** RELEVANT 11 NON COMPLIANT

Network Ports Security

GSL:

```
Instance where isPublic=true and inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]
```

Remediation:

Delete the rules that allow permissive SSH/Remote/Admin access
As a further protection, use Dome9 Dynamic Access Leasing to limit access to SSH/Remote Desktop only from allowed sources and only when needed.
For more information please refer to: https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_ (https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_)

Failed Entities

ID	Name	Region	VPC

ID	Name	Region	VPC
i-0c5e1696d45c947a6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-088d1cc7ff19a7ba6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-00c6665c1461ce720	Prod-Win-2008	London	vpc-0635b1031b9fbe1b9
i-0e4f8b370d73b1e3f	Chkp-SG	London	vpc-0635b1031b9fbe1b9
i-0acb17ed0d02c498d	NSaaS-SG	Frankfurt	vpc-070e9b1cb4fb74445
i-07fd0dd7506ff7472	Check-Point-Gateway	London	vpc-07393d5aece590401
i-00b65b153ffc4ca68	Check-Point-Gateway	London	vpc-07393d5aece590401
i-068f6edc4a06b324b	DB1	N. Virginia	vpc-08e4d9606f19e2594
i-0b6d2423197706617	ISAI_GW	Oregon	vpc-09d2ecbb4976ce399
i-0e50738cef07ca04f	transit-gateway	Ohio	vpc-0d13246ba98f6a395
i-0bc51846be38d5d38	transit-gateway	Ohio	vpc-0d13246ba98f6a395

FAILED

HIGH

Instance with administrative service: CiscoSecure,websm (TCP:9090) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

50 TESTED **12** RELEVANT 11 NON COMPLIANT

Network Ports Security

GSL:

```
Instance where isPublic=true and inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]
```

Remediation:

Delete the rules that allow permissive SSH/Remote/Admin access
As a further protection, use Dome9 Dynamic Access Leasing to limit access to SSH/Remote Desktop only from allowed sources and only when needed.
For more information please refer to: https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_ (https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_)

Failed Entities

ID	Name	Region	VPC

ID	Name	Region	VPC
i-0c5e1696d45c947a6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-088d1cc7ff19a7ba6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-00c6665c1461ce720	Prod-Win-2008	London	vpc-0635b1031b9fbe1b9
i-0e4f8b370d73b1e3f	Chkp-SG	London	vpc-0635b1031b9fbe1b9
i-0acb17ed0d02c498d	NSaaS-SG	Frankfurt	vpc-070e9b1cb4fb74445
i-07fd0dd7506ff7472	Check-Point-Gateway	London	vpc-07393d5aece590401
i-00b65b153ffc4ca68	Check-Point-Gateway	London	vpc-07393d5aece590401
i-068f6edc4a06b324b	DB1	N. Virginia	vpc-08e4d9606f19e2594
i-0b6d2423197706617	ISAI_GW	Oregon	vpc-09d2ecbb4976ce399
i-0e50738cef07ca04f	transit-gateway	Ohio	vpc-0d13246ba98f6a395
i-0bc51846be38d5d38	transit-gateway	Ohio	vpc-0d13246ba98f6a395

FAILED

HIGH

Ensure that AWS DynamoDB is encrypted using customer managed CMKs (Customer Master Key) instead of AWS-owned CMK's

Description:

AWS DynamoDb should be encrypted using AWS Managed Customer Master Key (CMK), instead of AWS-owned CMK. This is required in order to meet encryption regulatory requirements of Server-Side encryption for the sensitive data that may be stored in th DynamoDB. In addition, encrypting DynamoDb with AWS-managed CMK allows you to view the CMK and its key policy and also audit the encryption/decryption events by examining the DynamoDB API calls using CloudTrail.

7 TESTED **7** RELEVANT 7 NON COMPLIANT

Encryption and Key Management

GSL:

```
DynamoDbTable should have encryptionType='KMS'
```

Remediation:

1. Sign in to AWS console
2. In the console, select the specific region
3. Navigate to 'DynamoDB' dashboard
4. Select the reported table from the list of DynamoDB tables
5. In 'Overview' tab, Navigate to the 'Table Details' section
6. Click the 'Manage Encryption' link available for 'Encryption Type'
7. On 'Manage Encryption' pop up window, select 'KMS' as the encryption type

Failed Entities

ID	Name	Region	VPC

ID	Name	Region	VPC
arn:aws:dynamodb:us-east-2:833682875278:table/Resources	Resources	Ohio	-
arn:aws:dynamodb:us-east-2:833682875278:table/Users	Users	Ohio	-
arn:aws:dynamodb:us-east-2:833682875278:table/users	users	Ohio	-
arn:aws:dynamodb:us-east-2:833682875278:table/TrailDate	TrailDate	Ohio	-
arn:aws:dynamodb:eu-central-1:833682875278:table/Resources	Resources	Frankfurt	-
arn:aws:dynamodb:eu-central-1:833682875278:table/TrailDate	TrailDate	Frankfurt	-
arn:aws:dynamodb:eu-central-1:833682875278:table/Users	Users	Frankfurt	-

FAILED

HIGH

Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password

Description:

Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a username and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their username and password as well as for an authentication code from their AWS MFA device. It is recommended that MFA be enabled for all accounts that have a console password.

Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential.

11 TESTED **6** RELEVANT **6** NON COMPLIANT

Identity and Access Management

GSL:

```
IamUser where passwordEnabled='true' should have mfaActive='true'
```

Remediation:

Perform the following to enable MFA:
1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/ (https://console.aws.amazon.com/iam/)
2. In the navigation pane, choose Users.
3. In the User Name list, choose the name of the intended MFA user.
4. Choose the Security Credentials tab, and then choose Manage MFA Device.
5. In the Manage MFA Device wizard, choose A virtual MFA device, and then choose Next Step.
IAM generates and displays configuration information for the virtual MFA device, including a QR code graphic. The graphic is a representation of the 'secret configuration key' that is available for manual entry on devices that do not support QR codes.
6. Open your virtual MFA application. (For a list of apps that you can use for hosting virtual MFA devices, see Virtual MFA Applications.) If the virtual MFA application supports multiple accounts (multiple virtual MFA devices), choose the option to create a new account (a new virtual MFA device).
7. Determine whether the MFA app supports QR codes, and then do one of the following:
7.1 Use the app to scan the QR code. For example, you might choose the camera icon or choose an option similar to Scan code, and then use the device's camera to scan the code.
7.2 In the Manage MFA Device wizard, choose Show secret key for manual configuration, and then type the secret configuration key into your MFA application.
When you are finished, the virtual MFA device starts generating one-time passwords.
8. In the Manage MFA Device wizard, in the Authentication Code 1 box, type the one-time password that currently appears in the virtual MFA device. Wait up to 30 seconds for the device to generate a new one-time password. Then type the second one-time password into the Authentication Code 2 box. Choose Active Virtual MFA.

Additional Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html#enable-virt-mfa-for-iam-user (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html#enable-virt-mfa-for-iam-user)
CIS Amazon Web Services Foundations Benchmark v1.1.2
https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf (https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf)
IAM Best Practices at the following link:
http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html)
Virtual MFA Applications guidance by AWS:
https://aws.amazon.com/iam/details/mfa/#Virtual_MFA_Applications (https://aws.amazon.com/iam/details/mfa/#Virtual_MFA_Applications)

Failed Entities

ID	Name	Region	VPC
AIDAIOFX72ANX2XDZEWRQ	MMatysik		-
AIDA4EG27EOHJLGSHWNOF	shayl		-
AIDA4EG27EOHB3W2KBUR7	Admin		-
AIDA4EG27EOHL7AQ2MOMM	matankadosh		-

ID	Name	Region	VPC
AIDA4EG27EOHKDMWNUNUD	bob		-
AIDA4EG27EOHFCUVM5X7Y	arikblumin		-

FAILED

HIGH

Use encrypted storage for instances that might host a database.

Description:

Ensure that storage is encrypted by KMS on instances that, based on their name, might host a database. Covered DBs include: couchbase, riak,redis, hbase, Oracle, SAP Hana, Postgres, cassandra, hadoop, Mongo, Neo4j and any server with DB, SQL, database or graph in name

50 TESTED **2** RELEVANT 2 NON COMPLIANT

Encryption and Key Management

GSL:

```
Instance where (name like '%db%') or (name like '%database%' ) or (name like '%sql%' ) or (name like '%couchbase%' ) or (name like '%riak%' ) or (name like '%redis%' ) or (name like '%hbase%' ) or (name like '%oracle%' ) or (name like '%hana%' ) or (name like '%postgres%' ) or (name like '%cassandra%' ) or (name like '%hadoop%' ) or (name like '%mongo%' ) or (name like '%graph%' ) or (name like '%Neo4j%' ) should have volumes with [kmsKeyId and encrypted='true']
```

Remediation:

On the AWS console, configure the filesystem on the instance(s) to be encrypted, using a key that is stored in a file on an S3 bucket (created for this purpose).
This involves creating an S3 bucket, with a permissions policy, creating & encrypting an encryption key and storing it in the bucket, and then configuring the instances to use the key to encrypt the filesystems, all from the AWS console.

Follow the steps in https://aws.amazon.com/blogs/security/how-to-protect-data-at-rest-with-amazon-ec2-instance-store-encryption (https://aws.amazon.com/blogs/security/how-to-protect-data-at-rest-with-amazon-ec2-instance-store-encryption) in particular the section 'Implementing the Solution'

Failed Entities

ID	Name	Region	VPC
i-078cdfff016cdda38	mongodb	N. Virginia	vpc-08e4d9606f19e2594
i-068f6edc4a06b324b	DB1	N. Virginia	vpc-08e4d9606f19e2594

FAILED

HIGH

Ensure S3 buckets are not publicly accessible

Description:

Misconfigured S3 buckets can leak private information to the entire internet or allow unauthorized data tampering / deletion. Dome9 Clarity intuitively map network traffic sources, security groups, instances, rds, elbs and traffic flow thus facilitating the adherence to maintaining a network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.

32 TESTED **32** RELEVANT **2** NON COMPLIANT

Network Security

GSL:

```
S3Bucket should not have ( acl.grants contain [uri like 'http://acs.amazonaws.com/groups/global/%'] or policy.Statement contain [Effect='Allow' and (Principal='*' or Principal.AWS='*')])
```

Remediation:

1. Dome9 Clarity is available to all Dome9 Customers and no extra cost, thus Dome9 customers can maintain proper security posture and comply with regulatory requirements.
2. Review the S3 bucket ACL list and the IAM policy document. Remove all world accessible entries and set a proper policy. You might wish to use the AWS Policy Generator at: https://awspolicygen.s3.amazonaws.com/policygen.html (https://awspolicygen.s3.amazonaws.com/policygen.html)

Failed Entities

ID	Name	Region	VPC
yvducp	yvducp	Frankfurt	-
dome9-s3bucket1-f27nkwvgkfxz	dome9-s3bucket1-f27nkwvgkfxz	N. Virginia	-

FAILED

MEDIUM

Remove Unused Security Groups

Description:

A security group should always have attached protected assets. Removing Unused Security Groups is the expected outcome of the firewall and router rule sets review.

190 TESTED **142** RELEVANT **99** NON COMPLIANT

Network Security

GSL:

```
SecurityGroup where name != 'default' should not have networkAssetsStats contain-all [ count = 0 ]
```

Remediation:

Delete Unused Security Groups detected by the Dome9 Report.

Failed Entities

ID	Name	Region	VPC
sg-08e16c1e483859455	LAMP with PHP 7-1 Certified by Bitnami-7-1-22-1-r40 on Ubuntu 16-04-AutogenByAWSMP-	Singapore	vpc-0278f4095614fd5e8
sg-0f8b1b14c0fece642	Management-InstanceSecurityGroup-80NDJH16TT0O	Singapore	vpc-0278f4095614fd5e8
sg-017cb4f4cbe2995c3	Cluster-InstanceSecurityGroup-19RNWWU9TOO7J	Singapore	vpc-0278f4095614fd5e8
sg-070fe44fd62a0c040	Microsoft Windows Server 2008 R2 Base-2018-07-11-AutogenByAWSMP-1	Sydney	vpc-0690917dc691a05a8
sg-0b818346e856edad7	launch-wizard-1	Sydney	vpc-0690917dc691a05a8
sg-09a08bcf34beac3dc	launch-wizard-3	Sydney	vpc-0690917dc691a05a8
sg-0d4fb4e5435e8098d	launch-wizard-2	Sydney	vpc-0690917dc691a05a8
sg-0485c7bf05cd0727c	Microsoft Windows Server 2008 R2 Base-2018-07-11-AutogenByAWSMP-	Sydney	vpc-0690917dc691a05a8
sg-047eb512551b97ddb	Microsoft Windows Server 2008 R2 Base-2018-07-11-AutogenByAWSMP-2	Sydney	vpc-0690917dc691a05a8
sg-0b9633f2d0e4e4268	Dome9-AlbSG-IEOFDWKPWO21	N. Virginia	vpc-08e4d9606f19e2594
sg-03a8bcc0fff0bb8cb	Dome9-DevopSG-17NL7W0KJ11ZG	N. Virginia	vpc-08e4d9606f19e2594
sg-01839290cc73abc70	QA	São Paulo	vpc-0dd7491fcfb1e5739
sg-002c5d66c44afd940	launch-wizard-4	Sydney	vpc-0690917dc691a05a8
sg-0d19f9a279066c658	launch-wizard-5	Sydney	vpc-0690917dc691a05a8
sg-01c9cbcab5f1de99e	blobb	N. Virginia	vpc-08e4d9606f19e2594
sg-0b06406d99951d61f	launch-wizard-1	Frankfurt	vpc-0c99aa94269cda634
sg-0237d8df79395bc47	QA VPC	São Paulo	vpc-0dd7491fcfb1e5739
sg-0b71906b6e48d3eb8	take14theteam	São Paulo	vpc-0dd7491fcfb1e5739
sg-00e112e9a436b0f4a	ericc	São Paulo	vpc-0dd7491fcfb1e5739
sg-0fdd82ec45afb9b59	DPO Security Group	São Paulo	vpc-0dd7491fcfb1e5739
sg-0ea74ea7a87fa333d	BenNZ	São Paulo	vpc-0dd7491fcfb1e5739
sg-0d96ac2f2c6db049f	Jeremy	São Paulo	vpc-0dd7491fcfb1e5739
sg-0c4e985c2f70394c6	test	São Paulo	vpc-0c797dd4798891a7a
sg-0317eb7b4a5b74d5a	CloudGuard IaaS Security Management - BYOL-R80-10-033-341-AutogenByAWSMP-	Frankfurt	vpc-03d3a03126797ecd7

ID	Name	Region	VPC
sg-0662887f0fcdd0fe2	CloudGuard IaaS Security Management - BYOL-R80-10-033-341-AutogenByAWSMP-1	Frankfurt	vpc-03d3a03126797ecd7
sg-0edc488b9375e4e48	CloudGuard IaaS Security Management - BYOL-R80-20-101-427-AutogenByAWSMP-	Oregon	vpc-04cd9c4cfa331fb66
sg-01a288dbf171a4bf8	FL_Test	São Paulo	vpc-0c797dd4798891a7a
sg-0c8d827744624ba8f	Dome9 Test QA	São Paulo	vpc-0dd7491fcfb1e5739
sg-0bfbeb71ae4351688	ReadySG	São Paulo	vpc-0dd7491fcfb1e5739
sg-07e133add4dcae210	ReadySG1	São Paulo	vpc-0dd7491fcfb1e5739
sg-0db89ceb8079d1072	CloudGuard IaaS R80-20 Security Gateway - BYOL-R80-20-005-376-AutogenByAWSMP-1	Oregon	vpc-09d2ecbb4976ce399
sg-076a662f44ac2f743	CloudGuard IaaS Next Gen Firewall - Threat Prevention Standalone-R80-10-033-341-AutogenByAWSMP-	Oregon	vpc-09d2ecbb4976ce399
sg-05397197b091039e3	Ubuntu 16-04 LTS - Xenial -HVM--Ubuntu 16-04 LTS 20190212-AutogenByAWSMP-2	Oregon	vpc-09d2ecbb4976ce399
sg-081bbddb16ca08a4e	test-carsten	São Paulo	vpc-0dd7491fcfb1e5739
sg-0b893f608f70017fc	fasfddgasf	São Paulo	vpc-0dd7491fcfb1e5739
sg-0714623f3a1475f62	TESTMK	São Paulo	vpc-0dd7491fcfb1e5739
sg-0888b40261b216ef9	jwalkersecgroup	São Paulo	vpc-0dd7491fcfb1e5739
sg-03ce1ae7e24e9c37d	VIC-SG	São Paulo	vpc-0c797dd4798891a7a
sg-05c46db00b8bad7b9	CP-Management-Nottingham-InstanceSecurityGroup-A0ZLJETNQLPW	Ohio	vpc-002fda6c1746b92a7
sg-05b61a514868a24c8	launch-wizard-6	Sydney	vpc-0690917dc691a05a8
sg-0e30455f4f8abdfa4	Test-QATEST	São Paulo	vpc-0dd7491fcfb1e5739
sg-06a818b0534733e8a	D9_SG_Test	São Paulo	vpc-0dd7491fcfb1e5739
sg-0ccacb628030331bf	EW-Test	São Paulo	vpc-0dd7491fcfb1e5739
sg-0b17bdebc65976e2a	test-security-group	Ohio	vpc-002fda6c1746b92a7
sg-080a57d56f58727d2	inbound-http-ssh-locked-sao-paulo	São Paulo	vpc-0dd7491fcfb1e5739
sg-0793d8b0ffe5f2520	locked-sao-paulo-test-sg	São Paulo	vpc-0dd7491fcfb1e5739
sg-0c4a293cab4a31991	Management-CHKP	Ohio	vpc-081b4cdf31561a49d
sg-0ee760166fa1e72f7	CloudFormer-WebServerSecurityGroup-II9RPD5V5EJ5	Frankfurt	vpc-031c8847c1fe0614d

ID	Name	Region	VPC
sg-0d5e4e9af60e8269d	launch-wizard-2	Frankfurt	vpc-0c99aa94269cda634
sg-01d8c435cbfcee92f	launch-wizard-3	London	vpc-0a1a953743db0df83
sg-0a9eb8561cbc6602f	quick-create-1	London	vpc-01317b8042aff3f2c
sg-0be427343e25fce76	benoitb-sg	Ohio	vpc-07b020fd98b9806c7
sg-02f01a23a75303826	CloudGuard IaaS R80-20 Security Gateway - BYOL-R80-20-005-376-AutogenByAWSMP-1	Ohio	vpc-0890ddc0804e52cc5
sg-07ffa8db38dc925d0	AutoScaling-Security-Group-1	Ohio	vpc-0d13246ba98f6a395
sg-074030344a203e790	GREG_DMZ_SEC_GROUP	Ohio	vpc-0890ddc0804e52cc5
sg-024f544fddd285652	Kaholo	Frankfurt	vpc-070e9b1cb4fb74445
sg-02019636708329d2e	test-ca	Oregon	vpc-09d2ecbb4976ce399
sg-0b67c5747c9e8ca2a	Greg-AutoScale-Stack-PermissiveSecurityGroup-9JP816G1ASJQ	Ohio	vpc-0890ddc0804e52cc5
sg-08202e4d3a8cd0541	SP I/O	São Paulo	vpc-0dd7491fcfb1e5739
sg-06fa4ced361272da9	N.V I/O	N. Virginia	vpc-08e4d9606f19e2594
sg-091acec2b8062db7f	Check-Point-Management-Hyun-InstanceSecurityGroup-1WI8VP70YRKN7	Ohio	vpc-0eaebca854572960e
sg-053eba5b4981aad3d	Check-Point-Management-test-InstanceSecurityGroup-JL1MHAXJISYJ	Ohio	vpc-0eaebca854572960e
sg-010f6aa7f795ef726	LAMP Certified by Bitnami-7-1-29-0-r50 on Ubuntu 16-04-AutogenByAWSMP-	Ohio	vpc-0eaebca854572960e
sg-0cfbbc4beb5632483	Check-Point-Cluster-Hyun-InstanceSecurityGroup-15AQI4JBRLQOC	Ohio	vpc-0eaebca854572960e
sg-0ec3ae041e8e53572	NGINX Open Source Certified by Bitnami-1-16-0-0-r50 on Ubuntu 16-04-AutogenByAWSMP-	Ohio	vpc-0eaebca854572960e
sg-0d88c8c43cf86c655	launch-wizard-3	Frankfurt	vpc-070e9b1cb4fb74445
sg-021aa98c2c921d3cf	sGJSlondon	London	vpc-0635b1031b9fbe1b9
sg-031c02842b78bb882	launch-wizard-4	Frankfurt	vpc-070e9b1cb4fb74445
sg-03fe8ee77148847ab	launch-wizard-5	Frankfurt	vpc-070e9b1cb4fb74445
sg-0a0e6213071b37415	mySecurityGroupNW	N. Virginia	vpc-08e4d9606f19e2594
sg-08efefcc29cf191a9	calvin	N. Virginia	vpc-08e4d9606f19e2594
sg-0236a8cbb126ed80b	Jim T test	N. Virginia	vpc-08e4d9606f19e2594

ID	Name	Region	VPC
sg-0f79ab21c8b9c4ae4	Check-Point-Management-mnoh-InstanceSecurityGroup-TWPQ3HK644ZQ	Frankfurt	vpc-0f61ebcb8a5ac5399
sg-0ea2a171d24927dfd	LAMP Certified by Bitnami-7-1-29-0-r50 on Ubuntu 16-04-AutogenByAWSMP-	Frankfurt	vpc-0f61ebcb8a5ac5399
sg-0bbc529cc869356bc	MyWebservergroup	São Paulo	vpc-0dd7491fcfb1e5739
sg-0dcdd6b1ca620d055	Mywebservergroup	N. Virginia	vpc-08e4d9606f19e2594
sg-076dae938783af2ec	Demo-VPN	N. Virginia	vpc-08e4d9606f19e2594
sg-0fe231bd43358cc1e	Jarod-Test	N. Virginia	vpc-08e4d9606f19e2594
sg-02961b00fa3df3a69	blabla	São Paulo	vpc-0dd7491fcfb1e5739
sg-0de60e30524b16123	Jarod-Test2	N. Virginia	vpc-08e4d9606f19e2594
sg-087cf98ddfe4fa253	jtest	N. Virginia	vpc-08e4d9606f19e2594
sg-016811c44881197fa	1	N. Virginia	vpc-08e4d9606f19e2594
sg-07b6406cde085c13f	Demo35	N. Virginia	vpc-08e4d9606f19e2594
sg-09757fb033cfa0707	Robs_QAVPC_Security_Group	São Paulo	vpc-0dd7491fcfb1e5739
sg-01d3c17950a9b767c	Rob_HTTPand_SSH_From_Internet	N. Virginia	vpc-08e4d9606f19e2594
sg-0e48b58c08677bb36	matt-k	São Paulo	vpc-0dd7491fcfb1e5739
sg-0b477b9fb3eca64c7	matthew-test	N. Virginia	vpc-08e4d9606f19e2594
sg-059b8ea7ec53005a8	CSC	São Paulo	vpc-0dd7491fcfb1e5739
sg-0561266947733e981	CSC_NV	N. Virginia	vpc-08e4d9606f19e2594
sg-023e3ebfdad988186	nwtestgrp	N. Virginia	vpc-08e4d9606f19e2594
sg-016741dfb4b868ec3	nwSecGrp	São Paulo	vpc-0c797dd4798891a7a
sg-0bdc153d97560255e	test	São Paulo	vpc-0dd7491fcfb1e5739
sg-0f235c39c6dd89514	SSH&http inbound NV	N. Virginia	vpc-08e4d9606f19e2594
sg-0921fbbb038a1981c	dbullard-lab-25-jul-2019	São Paulo	vpc-0dd7491fcfb1e5739
sg-0191948a9ce342212	dbullard-lab	N. Virginia	vpc-08e4d9606f19e2594
sg-086df1ad209343f88	SG_Test	São Paulo	vpc-0dd7491fcfb1e5739
sg-070f01d92af8b9ed4	BB	Oregon	vpc-09d2ecbb4976ce399
sg-0d09f5c4e3033b5de	CloudGuard IaaS Security Management -BYOL--R80-20-101-479-AutogenByAWSMP-	Oregon	vpc-04cd9c4cfa331fb66
sg-0990a63a596dd224c	maya-test-sg	N. Virginia	vpc-08e4d9606f19e2594

FAILED

MEDIUM

Ensure VPC flow logging is enabled in all VPCs

Description:
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs. VPC Flow Logs provide visibility into network traffic that traverses the VPC and can be used to detect anomalous traffic or insight during security workflows.

48 TESTED **48** RELEVANT **43** NON COMPLIANT

Network Security

GSL:

```
VPC should have hasFlowLogs=true
```

Remediation:
Perform the following to determine if VPC Flow logs is enabled:
Via the Management Console:
1. Sign into the management console
2. Select Services then VPC
3. In the left navigation pane, select Your VPCs
4. Select a VPC
5. In the right pane, select the Flow Logs tab.
6. If no Flow Log exists, click Create Flow Log
7. For Filter, select Reject
8. Enter in a Role and Destination Log Group
9. Click Create Log Flow
10. Click on CloudWatch Logs Group

Additional Reference:
CIS Amazon Web Services Foundations Benchmark v1.1.2
https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf
(https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf)

Failed Entities

ID	Name	Region	VPC
vpc-4ef04f29	-		vpc-4ef04f29
vpc-0278f4095614fd5e8	Shay-Training		vpc-0278f4095614fd5e8
vpc-f4a23a93	-		vpc-f4a23a93
vpc-0690917dc691a05a8	Training		vpc-0690917dc691a05a8
vpc-346c4a5c	-		vpc-346c4a5c
vpc-0dd7491fcfb1e5739	QA VPC		vpc-0dd7491fcfb1e5739
vpc-04a8416d	-		vpc-04a8416d
vpc-00d07981fef5aa11b	test		vpc-00d07981fef5aa11b

ID	Name	Region	VPC
vpc-0c99aa94269cda634	Kaholo		vpc-0c99aa94269cda634
vpc-0c797dd4798891a7a	Bill QA VPC		vpc-0c797dd4798891a7a
vpc-08c17db27472abd32	-		vpc-08c17db27472abd32
vpc-070e9b1cb4fb74445	Default-VPC		vpc-070e9b1cb4fb74445
vpc-03d3a03126797ecd7	Manoj1		vpc-03d3a03126797ecd7
vpc-04cd9c4cfa331fb66	VPC_LB		vpc-04cd9c4cfa331fb66
vpc-09d2ecbb4976ce399	VPC_Isai		vpc-09d2ecbb4976ce399
vpc-002fda6c1746b92a7	AWS-Training		vpc-002fda6c1746b92a7
vpc-0d13246ba98f6a395	Check-Point-Transit-VPC-VPCStack-1IPVWVAXL4V5X		vpc-0d13246ba98f6a395
vpc-081b4cdf31561a49d	AWS-Training		vpc-081b4cdf31561a49d
vpc-01ec48b32e41b118c	JoelTraining		vpc-01ec48b32e41b118c
vpc-031c8847c1fe0614d	CloudformerVPC		vpc-031c8847c1fe0614d
vpc-00a5c0fae79e5dfb5	Demo-MNG-VPC		vpc-00a5c0fae79e5dfb5
vpc-07b020fd98b9806c7	benoitb-vpc		vpc-07b020fd98b9806c7
vpc-0890ddc0804e52cc5	GREG-VPC		vpc-0890ddc0804e52cc5
vpc-0eaebca854572960e	HyunVPC		vpc-0eaebca854572960e
vpc-0f907a75820eccb01	allen-vpc		vpc-0f907a75820eccb01
vpc-06ba88b1e44da29db	vpcjs		vpc-06ba88b1e44da29db
vpc-00b10f6ecf81bad13	vpc-a		vpc-00b10f6ecf81bad13
vpc-0b9d8b1583875c97c	BT-AWS-Demo-2		vpc-0b9d8b1583875c97c
vpc-0b969103451d7708a	Internal-VPC		vpc-0b969103451d7708a
vpc-07278dd5dff86090a	AWS Training Minuk		vpc-07278dd5dff86090a
vpc-0e7e70cca43bfc157	VPC-A-Internal		vpc-0e7e70cca43bfc157
vpc-0f36c6405ba7b3377	VPC-B-Internal		vpc-0f36c6405ba7b3377
vpc-0f114355a917cd98a	VPC-C-DMZ		vpc-0f114355a917cd98a
vpc-0dcb89a70ed7c3fe2	JM-1-Check-Point-TGW-AutoScaling-VPCStack-1448CF8M0C95Q		vpc-0dcb89a70ed7c3fe2
vpc-0eb54c6cca35cef2c	NSaaS_User		vpc-0eb54c6cca35cef2c
vpc-005ff9a5d1585605b	dp_henrique_mmt		vpc-005ff9a5d1585605b
vpc-0f61ebcb8a5ac5399	AWS-Training mnoh		vpc-0f61ebcb8a5ac5399
vpc-0c85f08fc22162d9d	henrique_aws_training		vpc-0c85f08fc22162d9d
vpc-0e8377cbf81339c40	vpc_dedicated_henrique		vpc-0e8377cbf81339c40
vpc-0e4b0002161b0bf36	Jarod		vpc-0e4b0002161b0bf36
vpc-0249332f781a5791f	mnoh-Training		vpc-0249332f781a5791f
vpc-0febe03823903a468	JM-tgw-internal-vpc-b		vpc-0febe03823903a468

ID	Name	Region	VPC
vpc-042fff1c60e196769	JM-tgw-internal-vpc-a		vpc-042fff1c60e196769

FAILED

MEDIUM

Instance with administrative service: SSH (TCP:22) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

50 TESTED **32** RELEVANT 27 NON COMPLIANT

Network Ports Security

GSL:

```
Instance where inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]
```

Remediation:

Delete the rules that allow permissive SSH/Remote/Admin access
As a further protection, use Dome9 Dynamic Access Leasing to limit access to SSH/Remote Desktop only from allowed sources and only when needed.
For more information please refer to: https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_ (https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_)

Failed Entities

ID	Name	Region	VPC
i-0f1b376d28b21add8	Demo-MNG	London	vpc-00a5c0fae79e5dfb5
i-058cbba83aa90a949	-	London	vpc-00a5c0fae79e5dfb5
i-0c5e1696d45c947a6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-088d1cc7ff19a7ba6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-076da3f9f1bcfb849	LB_ManagementR80.20	Oregon	vpc-04cd9c4cfa331fb66
i-0764e9401f5625e64	Production-Instance	London	vpc-0635b1031b9fbe1b9
i-00c6665c1461ce720	Prod-Win-2008	London	vpc-0635b1031b9fbe1b9
i-0e4f8b370d73b1e3f	Chkp-SG	London	vpc-0635b1031b9fbe1b9
i-0ba02993961346b80	-	Frankfurt	vpc-070e9b1cb4fb74445
i-0acb17ed0d02c498d	NSaaS-SG	Frankfurt	vpc-070e9b1cb4fb74445
i-07fd0dd7506ff7472	Check-Point-Gateway	London	vpc-07393d5aece590401

ID	Name	Region	VPC
i-00b65b153ffc4ca68	Check-Point-Gateway	London	vpc-07393d5aece590401
i-0bdcf56ebbd439d1f	MLM	Ohio	vpc-081b4cdf31561a49d
i-09d3fe20cba169650	SME	Ohio	vpc-081b4cdf31561a49d
i-0a5e8de8303ead318	Gw-1	Ohio	vpc-081b4cdf31561a49d
i-08c83fcd8dfcbeaf3	Greg-SMS	Ohio	vpc-0890ddc0804e52cc5
i-0a2fb88cea8c30d27	Greg-Micro-AZ2	Ohio	vpc-0890ddc0804e52cc5
i-009f872d456514d8f	Greg-Micro-AZ1	Ohio	vpc-0890ddc0804e52cc5
i-0c771682369060b52	monitoring	N. Virginia	vpc-08e4d9606f19e2594
i-068f6edc4a06b324b	DB1	N. Virginia	vpc-08e4d9606f19e2594
i-0655da436768fbfa2	-	N. Virginia	vpc-08e4d9606f19e2594
i-0b6d2423197706617	ISAI_GW	Oregon	vpc-09d2ecbb4976ce399
i-0aabd4466f8601e3f	ISAI_UBUNTU_WEB	Oregon	vpc-09d2ecbb4976ce399
i-025806ba9dc1d9485	ISAI_MGMT	Oregon	vpc-09d2ecbb4976ce399
i-03d10f55653565b4c	Kali-Staging	London	vpc-0a1a953743db0df83
i-0e50738cef07ca04f	transit-gateway	Ohio	vpc-0d13246ba98f6a395
i-0bc51846be38d5d38	transit-gateway	Ohio	vpc-0d13246ba98f6a395

FAILED

MEDIUM

Ensure AWS NAT Gateways are not being utilized for the default route

Description:

NAT Gateway is a scalable and resilient method for allowing outbound internet traffic from your private VPC subnets. It is recommended to use NAT gateways, and not the default route which permits all traffic, in Route Tables.

48 TESTED **48** RELEVANT **24** NON COMPLIANT

Network Security

GSL:

```
RouteTable where routes contain [ state='active' and instanceId!='null' ] should not have routes contain [ destinationCidrBlock='0.0.0.0/0' ]
```

Remediation:

To create a NAT gateway:
1. Sign into the AWS console
2. In the console, select the specific region
3. Navigate to VPC Dashboard
4. In the navigation pane, select 'NAT Gateways'
5. Click 'Create NAT Gateway', Specify the subnet in which to create the NAT gateway, and select the allocation ID of an Elastic IP address to associate with the NAT gateway. When you're done, click 'Create a NAT Gateway'. The NAT gateway displays in the console. After a few moments, its status changes to Available, after which it's ready for you to use.

To update Route Table:
After you've created your NAT gateway, you must update your route tables for your private subnets to point internet traffic to the NAT gateway. We use the most specific route that matches the traffic to determine how to route the traffic.
1. Sign into the AWS console
2. In the console, select the region
3. Navigate to VPC Dashboard
4. In the navigation pane, select 'Route Tables'
5. Select the reported route table associated with your private subnet
6. Select 'Routes' and Click 'Edit routes'
7. Replace the current route that points to the NAT instance with a route to the NAT gateway
8. Click 'Save routes'.

Failed Entities

ID	Name	Region	VPC
rtb-aa7f43cd	-	Singapore	vpc-4ef04f29
rtb-3144ab57	-	Tokyo	vpc-f4a23a93
rtb-097e76091cd9da05c	-	Sydney	vpc-0690917dc691a05a8
rtb-6a08ee01	-	Seoul	vpc-346c4a5c
rtb-0555ff2c104d2715c	-	N. Virginia	vpc-08e4d9606f19e2594
rtb-d15eb7b8	-	Stockholm	vpc-04a8416d
rtb-003cb70c4dd878894	-	Frankfurt	vpc-0c99aa94269cda634
rtb-0dece9c909110c994	-	São Paulo	vpc-0c797dd4798891a7a
rtb-02c05b8b3aa803b3e	-	Sydney	vpc-08c17db27472abd32
rtb-051799a4263fa757c	Default-VPC-RT	Frankfurt	vpc-070e9b1cb4fb74445
rtb-0aad4327f75a54ac6	to Internet	Oregon	vpc-04cd9c4cfa331fb66
rtb-0fe3d827a6e4a0e10	ToInternet_ISAI	Oregon	vpc-09d2ecbb4976ce399
rtb-037158de1ccb4a524	-	Ohio	vpc-081b4cdf31561a49d
rtb-0f1d10f53684e3602	-	London	vpc-00a5c0fae79e5dfb5
rtb-0f3e557b0f68efa02	-	London	vpc-07393d5aece590401
rtb-020ae917bfeb244dc	-	London	vpc-0635b1031b9fbe1b9
rtb-09c325d37b09a0395	-	London	vpc-0a1a953743db0df83

ID	Name	Region	VPC
rtb-09a40082f3433fd87	-	London	vpc-01317b8042aff3f2c
rtb-09582ba69afdffcf8	-	Ohio	vpc-0890ddc0804e52cc5
rtb-02d36ade0bc65d02e	-	Sydney	vpc-00b10f6ecf81bad13
rtb-00d03c5e00fb34f33	-	Ireland	vpc-0f114355a917cd98a
rtb-02e78599013c4f0c0	-	Ireland	vpc-0dcb89a70ed7c3fe2
rtb-0d61f0a35651b7a78	-	Ireland	vpc-0febe03823903a468
rtb-03ed399f9a7364ca1	-	Ireland	vpc-042fff1c60e196769

FAILED

MEDIUM

Lambda Functions must have an associated tag

Description:

Tags are key-value pairs that you attach to AWS resources to better organize them. They are particularly useful when you have many resources of the same type, which in the case of AWS Lambda, is a function. By using tags, customers with hundreds of Lambda functions can easily access and analyze a specific set by filtering on those that contain the same tag. Two of the key advantages of tagging your Lambda functions are: Grouping and Filtering and Cost allocation.

48 TESTED **48** RELEVANT 23 NON COMPLIANT

Cloud Assets Management

GSL:

```
Lambda should have tags
```

Remediation:

Navigate to https://console.aws.amazon.com/lambda/ (https://console.aws.amazon.com/lambda/)

You can add tags to your function under the Tags section in the configuration tab.

For more information: https://docs.aws.amazon.com/lambda/latest/dg/tagging.html#how-to-tag-console (https://docs.aws.amazon.com/lambda/latest/dg/tagging.html#how-to-tag-console)

Failed Entities

ID	Name	Region	VPC
arn:aws:lambda:us-east-2:833682875278:function:getUsersResources	getUsersResources	Ohio	-
arn:aws:lambda:eu-central-1:833682875278:function:scanTrailUpdateResources	scanTrailUpdateResources	Frankfurt	-

ID	Name	Region	VPC
arn:aws:lambda:eu-central-1:833682875278:function:deleteLoadBalancer	deleteLoadBalancer	Frankfurt	-
arn:aws:lambda:eu-central-1:833682875278:function:getUserResources	getUserResources	Frankfurt	-
arn:aws:lambda:eu-central-1:833682875278:function:deactivateUser	deactivateUser	Frankfurt	-
arn:aws:lambda:eu-central-1:833682875278:function:saveInstanceStateToTable	saveInstanceStateToTable	Frankfurt	-
arn:aws:lambda:eu-central-1:833682875278:function:shutdownInstances	shutdownInstances	Frankfurt	-
arn:aws:lambda:eu-central-1:833682875278:function:deleteUsers	deleteUsers	Frankfurt	-
arn:aws:lambda:eu-central-1:833682875278:function:createUserLink	createUserLink	Frankfurt	-
arn:aws:lambda:us-east-1:833682875278:function:scanTrailUpdateCloudFormation-us-east-1	scanTrailUpdateCloudFormation-us-east-1	N. Virginia	-
arn:aws:lambda:eu-west-1:833682875278:function:scanTrailUpdateCloudFormation-eu-west-1	scanTrailUpdateCloudFormation-eu-west-1	Ireland	-
arn:aws:lambda:ap-northeast-2:833682875278:function:scanTrailUpdateCloudFormation-ap-northeast-2	scanTrailUpdateCloudFormation-ap-northeast-2	Seoul	-
arn:aws:lambda:us-east-2:833682875278:function:scanTrailUpdateCloudFormation-us-east-2	scanTrailUpdateCloudFormation-us-east-2	Ohio	-
arn:aws:lambda:us-west-1:833682875278:function:scanTrailUpdateCloudFormation-us-west-1	scanTrailUpdateCloudFormation-us-west-1	N. California	-

ID	Name	Region	VPC
arn:aws:lambda:ap-south-1:833682875278:function:scanTrailUpdateCloudFormation-ap-south-1	scanTrailUpdateCloudFormation-ap-south-1	Mumbai	-
arn:aws:lambda:sa-east-1:833682875278:function:scanTrailUpdateCloudFormation-sa-east-1	scanTrailUpdateCloudFormation-sa-east-1	São Paulo	-
arn:aws:lambda:ap-southeast-2:833682875278:function:scanTrailUpdateCloudFormation-ap-southeast-2	scanTrailUpdateCloudFormation-ap-southeast-2	Sydney	-
arn:aws:lambda:us-west-2:833682875278:function:scanTrailUpdateCloudFormation-us-west-2	scanTrailUpdateCloudFormation-us-west-2	Oregon	-
arn:aws:lambda:eu-west-3:833682875278:function:scanTrailUpdateCloudFormation-eu-west-3	scanTrailUpdateCloudFormation-eu-west-3	Paris	-
arn:aws:lambda:ca-central-1:833682875278:function:scanTrailUpdateCloudFormation-ca-central-1	scanTrailUpdateCloudFormation-ca-central-1	Canada Central	-
arn:aws:lambda:ap-northeast-1:833682875278:function:scanTrailUpdateCloudFormation-ap-northeast-1	scanTrailUpdateCloudFormation-ap-northeast-1	Tokyo	-
arn:aws:lambda:eu-west-2:833682875278:function:scanTrailUpdateCloudFormation-eu-west-2	scanTrailUpdateCloudFormation-eu-west-2	London	-
arn:aws:lambda:ap-southeast-1:833682875278:function:scanTrailUpdateCloudFormation-ap-southeast-1	scanTrailUpdateCloudFormation-ap-southeast-1	Singapore	-

FAILED

MEDIUM

Instance with administrative service: Remote Desktop (TCP:3389) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

50 TESTED **24** RELEVANT 17 **NON COMPLIANT**

Network Ports Security

GSL:

```
Instance where inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]
```

Remediation:

Delete the rules that allow permissive SSH/Remote/Admin access
As a further protection, use Dome9 Dynamic Access Leasing to limit access to SSH/Remote Desktop only from allowed sources and only when needed.
For more information please refer to: https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_ (https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_)

Failed Entities

ID	Name	Region	VPC
i-0c5e1696d45c947a6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-088d1cc7ff19a7ba6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-076da3f9f1bcfb849	LB_ManagementR80.20	Oregon	vpc-04cd9c4cfa331fb66
i-0764e9401f5625e64	Production-Instance	London	vpc-0635b1031b9fbe1b9
i-00c6665c1461ce720	Prod-Win-2008	London	vpc-0635b1031b9fbe1b9
i-0e4f8b370d73b1e3f	Chkp-SG	London	vpc-0635b1031b9fbe1b9
i-0ba02993961346b80	-	Frankfurt	vpc-070e9b1cb4fb74445
i-0acb17ed0d02c498d	NSaaS-SG	Frankfurt	vpc-070e9b1cb4fb74445
i-07fd0dd7506ff7472	Check-Point-Gateway	London	vpc-07393d5aece590401
i-00b65b153ffc4ca68	Check-Point-Gateway	London	vpc-07393d5aece590401
i-0a5e8de8303ead318	Gw-1	Ohio	vpc-081b4cdf31561a49d
i-068f6edc4a06b324b	DB1	N. Virginia	vpc-08e4d9606f19e2594
i-0b6d2423197706617	ISAI_GW	Oregon	vpc-09d2ecbb4976ce399
i-0aabd4466f8601e3f	ISAI_UBUNTU_WEB	Oregon	vpc-09d2ecbb4976ce399
i-03d10f55653565b4c	Kali-Staging	London	vpc-0a1a953743db0df83
i-0e50738cef07ca04f	transit-gateway	Ohio	vpc-0d13246ba98f6a395
i-0bc51846be38d5d38	transit-gateway	Ohio	vpc-0d13246ba98f6a395

FAILED

MEDIUM

Instance with administrative service: CiscoSecure,websm (TCP:9090) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

50 TESTED **18** RELEVANT 17 NON COMPLIANT

Network Ports Security

GSL:

```
Instance where inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]
```

Remediation:

Delete the rules that allow permissive SSH/Remote/Admin access
As a further protection, use Dome9 Dynamic Access Leasing to limit access to SSH/Remote Desktop only from allowed sources and only when needed.
For more information please refer to: https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_ (https://helpcenter.dome9.com/hc/en-us/articles/360003963234-Dynamic-Access-Leasing#_Dynamic_Access_Leasing_)

Failed Entities

ID	Name	Region	VPC
i-0c5e1696d45c947a6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-088d1cc7ff19a7ba6	Inbound-Gateway	London	vpc-01317b8042aff3f2c
i-076da3f9f1bcfb849	LB_ManagementR80.20	Oregon	vpc-04cd9c4cfa331fb66
i-0764e9401f5625e64	Production-Instance	London	vpc-0635b1031b9fbe1b9
i-00c6665c1461ce720	Prod-Win-2008	London	vpc-0635b1031b9fbe1b9
i-0e4f8b370d73b1e3f	Chkp-SG	London	vpc-0635b1031b9fbe1b9
i-0ba02993961346b80	-	Frankfurt	vpc-070e9b1cb4fb74445
i-0acb17ed0d02c498d	NSaaS-SG	Frankfurt	vpc-070e9b1cb4fb74445
i-07fd0dd7506ff7472	Check-Point-Gateway	London	vpc-07393d5aece590401
i-00b65b153ffc4ca68	Check-Point-Gateway	London	vpc-07393d5aece590401
i-0a5e8de8303ead318	Gw-1	Ohio	vpc-081b4cdf31561a49d
i-068f6edc4a06b324b	DB1	N. Virginia	vpc-08e4d9606f19e2594
i-0b6d2423197706617	ISAI_GW	Oregon	vpc-09d2ecbb4976ce399

ID	Name	Region	VPC
i-0aabd4466f8601e3f	ISAI_UBUNTU_WEB	Oregon	vpc-09d2ecbb4976ce399
i-03d10f55653565b4c	Kali-Staging	London	vpc-0a1a953743db0df83
i-0e50738cef07ca04f	transit-gateway	Ohio	vpc-0d13246ba98f6a395
i-0bc51846be38d5d38	transit-gateway	Ohio	vpc-0d13246ba98f6a395

FAILED

MEDIUM

Process for Security Group Management - Detection of new Security Groups

Description:

Dome9 Newly Detected Groups Behavior should be set to Full protection or lock to enforce Security Groups management process

16 TESTED **16** RELEVANT **14** NON COMPLIANT

Network Security

GSL:

```
Region should not have behavior='ReadOnly'
```

Remediation:

Change Cloud Guard Dome9 Protection mode for specific security groups from Read-only to Full protection mode

Failed Entities

ID	Name	Region	VPC
us-west-1	N. California	N. California	-
eu-west-1	Ireland	Ireland	-
ap-southeast-1	Singapore	Singapore	-
ap-northeast-1	Tokyo	Tokyo	-
us-west-2	Oregon	Oregon	-
ap-southeast-2	Sydney	Sydney	-
eu-central-1	Frankfurt	Frankfurt	-
ap-northeast-2	Seoul	Seoul	-
ap-south-1	Mumbai	Mumbai	-
us-east-2	Ohio	Ohio	-
ca-central-1	Canada Central	Canada Central	-
eu-west-2	London	London	-
eu-west-3	Paris	Paris	-
eu-north-1	Stockholm	Stockholm	-

FAILED

MEDIUM

Ensure IAM password policy require at least one symbol

Description:

It is recommended that the password policy require at least one symbol. Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure passwords consist of different character sets. Setting a password complexity policy increases account resiliency against brute force login attempts.

1 TESTED **1** RELEVANT **1** NON COMPLIANT

Identity and Access Management

GSL:

```
Iam should have passwordPolicy.requireSymbols=true
```

Remediation:

Perform the following to set the password policy as prescribed:
1. Login to AWS Console (with appropriate permissions to View Identity Access Management Account Settings)
2. Go to IAM Service on the AWS Console
3. Click on Account Settings on the Left Pane
4. Check "Require at least one non-alphanumeric character"
5. Click "Apply password policy"

Additional Reference:
CIS Amazon Web Services Foundations Benchmark v1.1.2
https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf
(https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf)
IAM Best Practices:
http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html)

Failed Entities

ID	Name	Region	VPC
833682875278	Account Summary		-

FAILED

MEDIUM

Ensure a log metric filter and alarm exist for unauthorized API calls

Description:

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for unauthorized API calls.
Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

1 TESTED **1** RELEVANT **1** NON COMPLIANT

Monitoring

GSL:

```
List<CloudTrail> should have items with [hasSNSSubscriber='true' and metricFilters with [filterPattern isFilterPatternEqual('{ ($.errorCode = *UnauthorizedOperation) || ($.errorCode =AccessDenied*) }')] length() > 0]
```

Remediation:

Perform the following to setup the metric filter, alarm, SNS topic, and subscription:
1. Create a metric filter based on filter pattern relevant for this check. For More details, refer to CIS Amazon Web Services Foundations Benchmark v1.1.2
https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf (https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf)
2. Create an SNS topic that the alarm will notify Note: you can execute this command once and then re-use the same topic for all monitoring alarms.
3. Create an SNS subscription to the topic created in step 2 Note: you can execute this command once and then re-use the SNS subscription for all monitoring alarms.
4. Create an alarm that is associated with the CloudWatch Logs Metric Filter created in step 1 and an SNS topic created in step 2

Additional Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CountingLogEventsExample.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CountingLogEventsExample.html)

Failed Entities

ID	Name	Region	VPC
N/A	List<CloudTrail>		-

FAILED

MEDIUM

Ensure that your Amazon Lambda functions do not share the same AWS IAM execution role

Description:

It is recommended to have one IAM role per each Lambda function in order to follow the Principle of Least Privilege. This way you can ensure that your Lambda functions will have the minimum privileges needed to perform the required tasks.

1 TESTED **1** RELEVANT **1** NON COMPLIANT

Identity and Access Management

GSL:

```
List<Lambda> should not have items groupBy [executionRoleArn] contain [values length() > 1]
```

Remediation:
1. Navigate to Lambda dashboard at https://console.aws.amazon.com/lambda/.
(https://console.aws.amazon.com/lambda/.)

2. In the navigation panel, go to AWS Lambda section and select Functions.

3. Choose the relevant Lambda function, and click on it to access its configuration page.

4. Select the Configuration tab and click Execution role.

5. Apply an existing execution role by choosing an existing role from the first dropdown list, then select the name of the existing IAM role from the second dropdown list.
Note: The chosen IAM role cannot be associated with another Lambda function and must follow the Principle of Least Privilege

Failed Entities

ID	Name	Region	VPC
N/A	List<Lambda>		-

FAILED

MEDIUM

Ensure AWS EBS Volumes are attached to instances

Description:
Checks for EBS volumes that are unattached to instances, for example, if they persist after an EC2 instance has been terminated. It is recommended to review of these volumes regularly, since they may contain sensitive company data, application, infrastructure or users.
In addition, removing unattached instances will lower your AWS bill.

64 TESTED **64** RELEVANT **1** NON COMPLIANT

Operational

GSL:

```
Volume should have attachments contain [ state='attached' ]
```

Remediation:

Periodically review EBS volumes. Archive them to Glacier, remove the volume entirely, or reattach them if they were inadvertently orphaned.

1. Navigate to the the AWS console EC2 dashboard
2. In the navigation pane, select Volumes
3. Sort using the State column and locate the volumes marked 'available'
4. Review the volume information (create date, size, status, etc)
5. Determine if you wish to retain or remove each volume

Failed Entities

ID	Name	Region	VPC
vol-0adea425f94498b94	-	Paris	-

FAILED

LOW

Ensure IAM password policy expires passwords within 90 days or less

Description:

IAM password policies can require passwords to be rotated or expired after a given number of days. It is recommended that the password policy expire passwords after 90 days or less.
Reducing the password lifetime increases account resiliency against brute force login attempts. Additionally, requiring regular password changes help in the following scenarios:
- Passwords can be stolen or compromised sometimes without your knowledge. This can happen via a system compromise, software vulnerability, or internal threat.
- Certain corporate and government web filters or proxy servers have the ability to intercept and record traffic even if it's encrypted.
- Many people use the same password for many systems such as work, email, and personal.
- Compromised end user workstations might have a keystroke logger.

1 TESTED **1** RELEVANT 1 NON COMPLIANT

Identity and Access Management

GSL:

```
Iam should have passwordPolicy.maxPasswordAge>0 and passwordPolicy.maxPasswordAge<91
```

Remediation:

Perform the following to set the password policy as prescribed: Via AWS Console:
1. Login to AWS Console (with appropriate permissions to View Identity Access Management Account Settings)
2. Go to IAM Service on the AWS Console
3. Click on Account Settings on the Left Pane
4. Check "Enable password expiration"
5. Set "Password expiration period (in days):" to 90 or less

Additional Reference:
CIS Amazon Web Services Foundations Benchmark v1.1.2
https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf
(https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf)

Failed Entities

ID	Name	Region	VPC
833682875278	Account Summary		-

FAILED

LOW

Ensure a support role has been created to manage incidents with AWS Support

Description:
AWS provides a support center that can be used for incident notification and response, as well as technical support and customer services. Create an IAM Role to allow authorized users to manage incidents with AWS Support.
By implementing least privilege for access control, an IAM Role will require an appropriate IAM Policy to allow Support Center Access in order to manage Incidents with AWS Support.

617 TESTED **1** RELEVANT 1 NON COMPLIANT

Identity and Access Management

GSL:

```
IamPolicy where name='AWSSupportAccess' should not have users isEmpty() and roles isEmpty() and groups isEmpty()
```

Remediation:
For each account that failed this rule, on the IAM console.Navigate to Roles, and create a new role (assign it any name, but it should suggest the Support role). Assign the AWSSupportAccess policy to this role.
Alternatively, instead of a Role, define a Group with the support policy.

Additional Reference:
CIS Amazon Web Services Foundations Benchmark v1.1.2
https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html#accessing-support
(https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html#accessing-support)

Failed Entities

ID	Name	Region	VPC
ANPAJSNKQX2OW67GF4S7E	AWSSupportAccess		-

PASSED TESTS

PASSED

HIGH

ApplicationLoadBalancer with administrative service: SSH (TCP:22) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

```
ApplicationLoadBalancer where isPublic=true and inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]
```

PASSED

HIGH

ApplicationLoadBalancer with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

ApplicationLoadBalancer where isPublic=true and inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]

PASSED

HIGH

ApplicationLoadBalancer with administrative service: CiscoSecure,websm (TCP:9090) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

ApplicationLoadBalancer where isPublic=true and inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]

PASSED

HIGH

Use encrypted connection between CloudFront and origin server

Description:

Enforce HTTPS-only traffic between a CloudFront distribution and the origin.
It is recommended to use HTTPS for secure communications between your CloudFront distribution and end users to guarantee encryption of traffic and prevent malicious actors from intercepting your traffic.

Note: This rule runs on all the origins except S3 Buckets

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

CloudFront where not distributionConfig.origins.items with [s3OriginConfig] should have distributionConfig.origins.items with [customOriginConfig.originProtocolPolicy='https-only' or distributionConfig.defaultCacheBehavior.viewerProtocolPolicy='redirect-to-https']

PASSED

HIGH

ECS Cluster At-Rest Encryption

Description:

Ensure that AWS ECS clusters are encrypted. Data encryption at rest, prevents unauthorized users from accessing sensitive data on your AWS ECS clusters and associated cache storage systems.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

```
EcsCluster where( not containerInstances isEmpty()) should have containerInstances with [ instance.volumes contain [ encrypted=true ] ]
```

PASSED

HIGH

Ensure that your Amazon EFS file systems are encrypted

Description:

Enable encryption of your EFS file systems in order to protect your data and metadata from breaches or unauthorized access and fulfill compliance requirements for data-at-rest encryption within your organization.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

```
EFS should have encrypted=true
```

PASSED

HIGH

Ensure AWS ElastiCache Redis clusters have encryption for data at rest enabled

Description:

In order to protect sensitive data, AWS ElastiCache Redis clusters should be encrypted rest. Encryption of data at rest prevents unauthorized access to your sensitive data stored on AWS ElastiCache Redis clusters and associated cache storage.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

```
ElastiCache where engine='redis' should have atRestEncryptionEnabled=true
```

PASSED

HIGH

ELB - Recommended SSL/TLS protocol version

Description:
Using insecure ciphers for your ELB Predefined or Custom Security Policy, could make the SSL connection between the client and the load balancer vulnerable to exploits. TLS 1.0 was recommended to be disabled by PCI Council after June 30, 2016

2 TESTED **2** RELEVANT **0** NON COMPLIANT

Encryption and Key Management

GSL:

```
ELB should not have elbListeners with [ policies contain [ attributes contain-any [$ in ('Protocol-SSLv3', 'Protocol-TLSv1') ] ] ]
```

PASSED

HIGH

ELB with administrative service: SSH (TCP:22) is too exposed to the public internet

Description:
Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

2 TESTED **0** RELEVANT **0** NON COMPLIANT

Network Ports Security

GSL:

```
ELB where isPublic=true and inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]
```

PASSED

HIGH

ELB with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet

Description:
Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

2 TESTED **0** RELEVANT **0** NON COMPLIANT

Network Ports Security

GSL:

```
ELB where isPublic=true and inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL') and scope isPublic() and scope
```

numberOfHosts() > 32]

PASSED

HIGH

ELB with administrative service: CiscoSecure,websm (TCP:9090) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

2 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

ELB where isPublic=true and inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]

PASSED

HIGH

Ensure VIRTUAL MFA is enabled for the "root" account

Description:

The root account is the most privileged user in an AWS account. MFA adds an extra layer of protection on top of a username and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their username and password as well as for an authentication code from their AWS MFA device.
Note: When virtual MFA is used for root accounts, it is recommended that the device used is NOT a personal device, but rather a dedicated mobile device (tablet or phone) that is managed to be kept charged and secured independent of any individual personal devices. ("non-personal virtual MFA") This lessens the risks of losing access to the MFA due to device loss, device trade-in or if the individual owning the device is no longer employed at the company.

Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential.

11 TESTED **1** RELEVANT 0 NON COMPLIANT

Identity and Access Management

GSL:

IamUser where name like '%root_account%' should have mfaType='Virtual'

PASSED

HIGH

Instances with Direct Connect virtual interface should not have public interfaces

Description:

Ensure that instances with direct connect virtual interface do not have public interfaces

50 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Security

GSL:

```
Instance where vpc.vpnGateways contain [directConnectVirtualInterfaces] should have isPublic=false
```

PASSED

HIGH

AWS Kinesis streams are encrypted with KMS customer master keys

Description:

Use KMS customer-managed keys (CMK) to protect the Kinesis Streams and metadata. Using KMS CMK, you gain full control over who can use the keys to access AWS Kinesis data (including the system metadata). The AWS KMS service allows you to create, rotate, disable and audit CMK encryption keys.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

```
Kinesis should have encryptionKey.isCustomerManaged=true
```

PASSED

HIGH

Ensure rotation for customer created CMKs is enabled

Description:

AWS Key Management Service (KMS) allows customers to rotate the backing key which is key material stored within the KMS which is tied to the key ID of the Customer Created customer master key (CMK). It is the backing key that is used to perform cryptographic operations such as encryption and decryption. Automated key rotation currently retains all prior backing keys so that decryption of encrypted data can take place transparently.
Rotating encryption keys helps reduce the potential impact of a compromised key as data encrypted with a new key cannot be accessed with a previous key that may have been exposed.

29 TESTED **0** RELEVANT 0 NON COMPLIANT

Logging

GSL:

```
KMS where isCustomerManaged=true and deletionDate <=0 should have rotationStatus=true
```

PASSED

HIGH

Use Encrypted RDS storage

Description:

Encrypt Amazon RDS instances and snapshots at rest, by enabling the encryption option for your Amazon RDS DB instance.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

```
RDS should have isStorageEncrypted = 'true' and kmsKeyId
```

PASSED

HIGH

RDS should not have Public Interface open to a public scope

Description:

RDS should not be open to a public scope. Firewall and router configurations should be used to restrict connections between untrusted networks and any system components in the cloud environment.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Security

GSL:

```
RDS where isPublic='true' should not have inboundRules with [scope isPublic()]
```

PASSED

HIGH

RDS Databases with Direct Connect virtual interface should not have public interfaces

Description:

Ensure that RDS databases with direct connect virtual interface should not have public interfaces

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Security

GSL:

```
RDS where vpc.vpnGateways contain [directConnectVirtualInterfaces] should have isPublic=false
```

PASSED

HIGH

Use KMS CMK customer-managed keys for Redshift clusters

Description:

Use customer-managed KMS keys instead of AWS-managed keys, to have granular control over encrypting and encrypting data.
Encrypt Redshift clusters with a Customer-managed KMS key. This is a recommended best practice.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

Redshift should have dataEncrypted and kmsKeyId

PASSED

HIGH

Expired Route 53 Domain Names

Description:

Identify any expired domain names registered with AWS Route 53

0 TESTED **0** RELEVANT 0 NON COMPLIANT

DNS Management

GSL:

Route53Domain should not have expirationTime before(-1, 'minutes')

PASSED

HIGH

Use Route53 for scalable, secure DNS service in AWS.

Description:

Use AWS Route 53 Domain Name System (DNS) service within your AWS account to manage DNS zones for your domains

0 TESTED **0** RELEVANT 0 NON COMPLIANT

DNS Management

GSL:

Route53HostedZone should have recordSets

PASSED

HIGH

Ensure SageMaker Notebook Instance Data Encryption is enabled

Description:

SageMaker is a fully-managed AWS service that enables developers and data engineers to quickly and easily build, train and deploy machine learning models at any scale. An AWS SageMaker notebook instance is a fully managed ML instance that is running the Jupyter Notebook open-source web application. It is highly recommended that the data stored on Machine Learning (ML) storage volumes attached to your AWS SageMaker notebook instances is encrypted in order to protect your data from breaches or unauthorized access and fulfill compliance requirements for data-at-rest encryption within your organization.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

SageMakerNotebook should have kmsKey

PASSED

HIGH

NetworkLoadBalancer with administrative service: SSH (TCP:22) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

3 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

NetworkLoadBalancer where isPublic=true and inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]

PASSED

HIGH

NetworkLoadBalancer with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

3 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

NetworkLoadBalancer where isPublic=true and inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]

PASSED

HIGH

NetworkLoadBalancer with administrative service: CiscoSecure,websm (TCP:9090) is too exposed to the public internet

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

3 TESTED **0** RELEVANT **0** NON COMPLIANT

Network Ports Security

GSL:

NetworkLoadBalancer where isPublic=true and inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL') and scope isPublic() and scope numberOfHosts() > 32]

PASSED

MEDIUM

Ensure expired certificates are removed from the AWS Certificate Manager (ACM)

Description:

Checks for expired certificates in the AWS Certificate Manager. It is recommended to delete expired certificates.

0 TESTED **0** RELEVANT **0** NON COMPLIANT

Encryption and Key Management

GSL:

AcmCertificate should not have status='EXPIRED'

PASSED

MEDIUM

Public AMI

Description:

One or more AMI exposed to the public internet. It is recommended to not publicly shared with the other AWS accounts in order to avoid sensitive data exposure. If required, AMI images should only be shared with relevant AWS accounts without making them public.

6 TESTED **6** RELEVANT **0** NON COMPLIANT

Network Security

GSL:

AMI should have isPublic=false

PASSED

MEDIUM

ApplicationLoadBalancer with administrative service: SSH (TCP:22) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

0 TESTED **0** RELEVANT **0** NON COMPLIANT

Network Ports Security

GSL:

ApplicationLoadBalancer where inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]

PASSED

MEDIUM

ApplicationLoadBalancer with administrative service: Remote Desktop (TCP:3389) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

0 TESTED **0** RELEVANT **0** NON COMPLIANT

Network Ports Security

GSL:

ApplicationLoadBalancer where inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]

PASSED

MEDIUM

ApplicationLoadBalancer with administrative service: CiscoSecure,websm (TCP:9090) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

ApplicationLoadBalancer where inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]

PASSED

MEDIUM

Ensure multi-regions trail exists for each AWS CloudTrail

Description:

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. CloudTrail provides a history of AWS API calls for an account, including API calls made via the Management Console, SDKs, command line tools, and higher-level AWS services (such as CloudFormation).

1 TESTED **1** RELEVANT 0 NON COMPLIANT

Logging

GSL:

CloudTrail should have isMultiRegionTrail=true

PASSED

MEDIUM

ECS Cluster should have active services only

Description:

Amazon ECS uses services: run and maintain number of instances of a task definition simultaneously in an ECS cluster. Idle ECS clusters running services should be removed to reduce container attack surface

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Security

GSL:

EcsCluster should have activeServicesCount > 0

PASSED

MEDIUM

ELB with administrative service: SSH (TCP:22) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

2 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

ELB where inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]

PASSED

MEDIUM

ELB with administrative service: Remote Desktop (TCP:3389) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

2 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

ELB where inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]

PASSED

MEDIUM

ELB with administrative service: CiscoSecure,websm (TCP:9090) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

2 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

```
ELB where inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]
```

PASSED

MEDIUM

Instances are Configured under Virtual Private Cloud

Description:

Instance should be configured in vpc. AWS VPCs provides the controls to facilitate a formal process for approving and testing all network connections and changes to the firewall and router configurations.

50 TESTED **50** RELEVANT 0 NON COMPLIANT

Network Security

GSL:

```
Instance should have vpc
```

PASSED

MEDIUM

Security Groups must be defined under a Virtual Private Cloud

Description:

All security groups must be associated with a VPC, EC2 Classic not allowed. VPCs provides the controls to facilitate a formal process for approving and testing all network connections and changes to the firewall and router configurations.

190 TESTED **142** RELEVANT 0 NON COMPLIANT

Network Security

GSL:

```
SecurityGroup where not name='default' should have vpc
```

PASSED

MEDIUM

Ensure there is an up to date Network Diagram for your cloud network

Description:

Dome9 Clarity allows you to visualize your Amazon Network Security configurations in real time.

1 TESTED **1** RELEVANT **0** NON COMPLIANT

Network Security

GSL:

```
TRUE
```

PASSED

MEDIUM

NetworkLoadBalancer with administrative service: SSH (TCP:22) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

3 TESTED **0** RELEVANT **0** NON COMPLIANT

Network Ports Security

GSL:

```
NetworkLoadBalancer where inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 22 and portTo >= 22 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]
```

PASSED

MEDIUM

NetworkLoadBalancer with administrative service: Remote Desktop (TCP:3389) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

3 TESTED **0** RELEVANT **0** NON COMPLIANT

Network Ports Security

GSL:

NetworkLoadBalancer where inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 3389 and portTo >= 3389 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]

PASSED

MEDIUM

NetworkLoadBalancer with administrative service: CiscoSecure,websm (TCP:9090) is exposed to a wide network scope

Description:

Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.

3 TESTED **0** RELEVANT 0 NON COMPLIANT

Network Ports Security

GSL:

NetworkLoadBalancer where inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL')] should not have inboundRules contain [port <= 9090 and portTo >= 9090 and protocol in ('TCP','ALL') and scope numberOfHosts() > 32]

PASSED

LOW

ALB secured listener certificate about to expire in one month

Description:

Ensure that SSL/TLS certificates stored in AWS IAM are renewed one month before expiry.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

ApplicationLoadBalancer should not have listeners contain [certificates contain [expiration before(30, 'days')]]

PASSED

LOW

Invalid CPU or Memory Value Specified

Description:

When registering a task, if you specify an invalid cpu or memory value, you receive the following error:

An error occurred (ClientException) when calling the RegisterTaskDefinition operation: Invalid 'cpu' setting for task. For more information, see the Troubleshooting section of the Amazon ECS Developer Guide.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Operational

GSL:

EcsTask where launchType= 'FARGATE' should have memory= '1024' or memory= '256' or memory= '512' or memory= '2048' or memory= '4096'

PASSED

LOW

SSL/TLS certificates expire in one month

Description:

Ensure that SSL/TLS certificates stored in AWS IAM are renewed one month before expiry.

0 TESTED **0** RELEVANT 0 NON COMPLIANT

Encryption and Key Management

GSL:

IamServerCertificate should not have expiration before(30, 'days')