Project Craton

Accelerating compliance and operational security

CSO50 | pangea

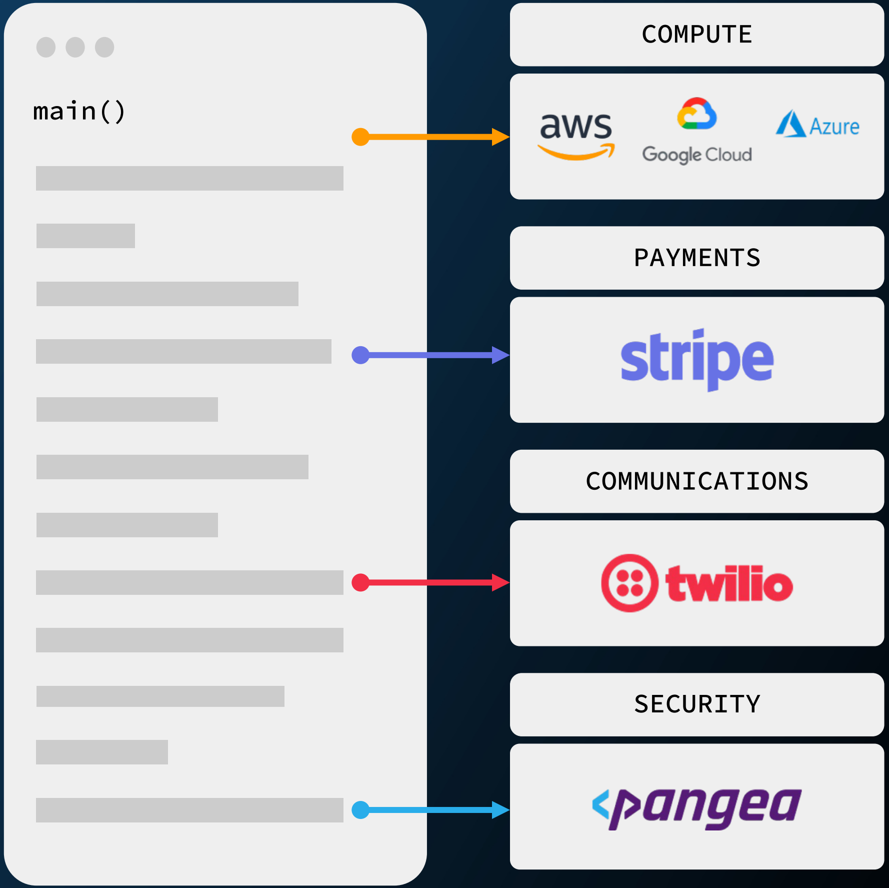
PRODUCED BY CSO

Introduction

- **Sourabh Satish**
  - Co-Founder and CTO, Pangea Cyber
- **Pangea Cyber**
  - ~2 yr old Startup, Series B led by Google Ventures and Ballistic Ventutres
  - First SPaaS (Security Platform as a Service) vendor to provide APIs for your enterprise-ready, security and compliance related features in the Application code.

Composable Apps Accelerate Business Innovation
Gartner Predicts 2023

“By 2025, 60% of the new custom business applications will be built using reusable business services via a shared curated component catalog or marketplace.”



main()

COMPUTE

aws

Google Cloud

Azure

PAYMENTS

stripe

COMMUNICATIONS

twilio

SECURITY

pangea

Security Services for Developers

Security Platform as a Service

pangea

Essential Enterprise Ready

What every secure application needs

Secure Audit Log Tamperproof audit trail	Available
AuthN Secure login & user mgmt	In Beta
AuthZ ReBAC, RBAC & ABAC authorization	Coming soon
Vault Secret and Cryptographic Key Store	Available
Licensing Licensing & Entitlement mgmt	

Data Protection

Secure Data Objects

Secure Object Store Securely store & share file objects	Coming Soon
Secure Ledger Store data on the blockchain	
Sanitize Cleanse file objects	Coming Soon

Threat Analysis

Detect potential threats

File Scan Scan file objects for malware	In Beta
File Detonation Sandbox suspicious files	
URL Detonation Sandbox suspicious URLs	

Compliance

Comply with regulatory requirements

Embargo Limit access by country	Available
Redact Remove sensitive information	Available
Data Classification Classify data by type	Coming Soon

Access

Control Application Access

Bot Detection Detect non human users	
Secure Messaging Send & receive messages securely	

Threat Intelligence

Block known threat actors

File Intel Detect known malicious files	Available
Domain Intel Detect known malicious domains	Available
URL Intel Detect known malicious URLs	Available
User Intel Identify breached credentials	Available
IP Intel Detect known malicious IPs	

IP Reputation	Available
Geolocate	Available
VPN	Available
Proxy	Available
Domain	Available

CROWDSTRIKE DomainTools

REVERSINGLABS SpyCloud

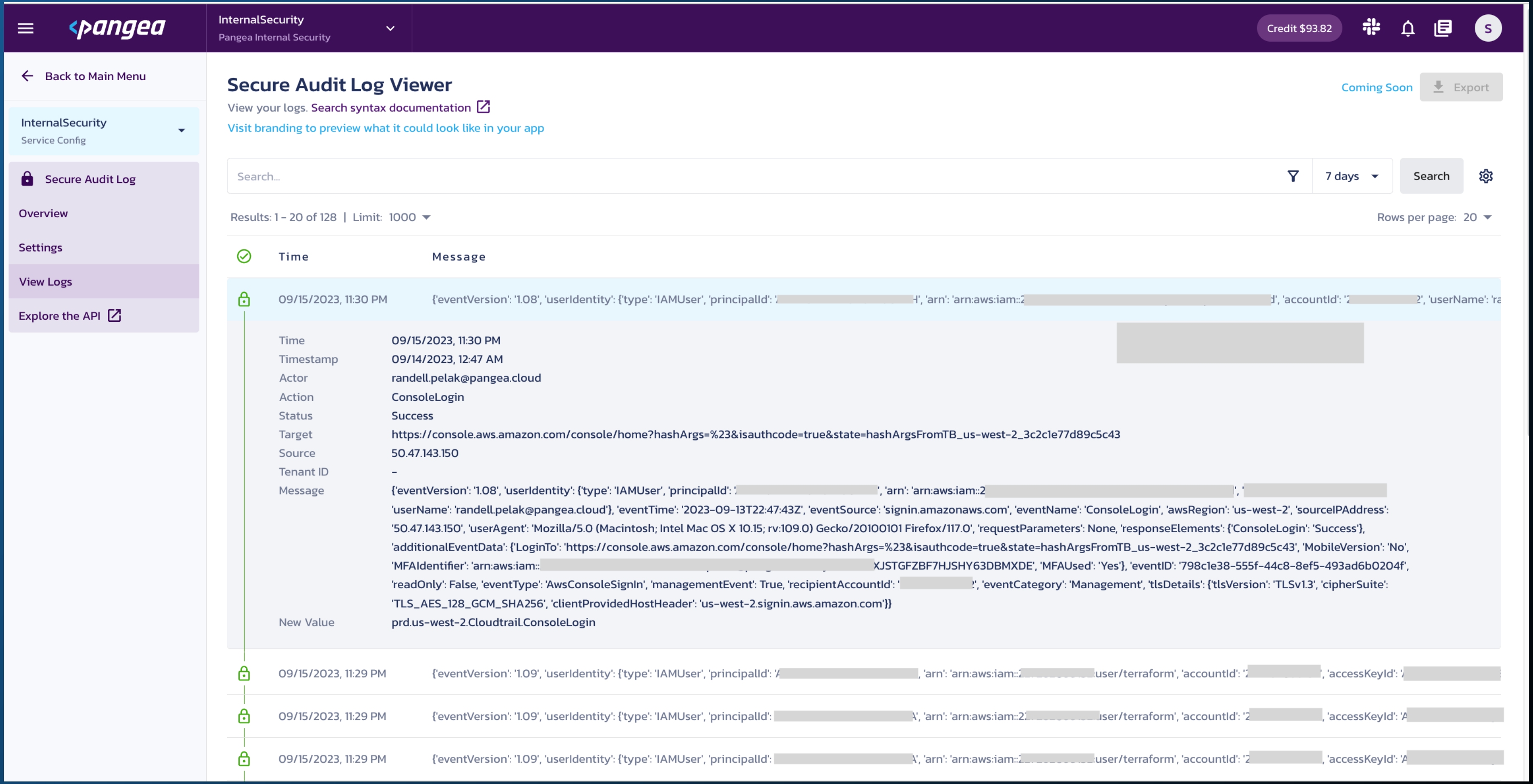
digitalelement TEAM CYMRU

Craton - Business Need

- **Compliance Controls** are a significant burden on small teams
  - Never ending compliance, security obligations and a rapidly evolving threat landscape.
- A need for greater thoroughness and consistency
- A secure and immutable audit log for continuous compliance evidence (vs spot checking)

Craton - definition

- A code-first & automated approach to manage security and compliance tasks
    - Evidence is logged continuously in a secure and tamperproof repository for required retention windows (Secure Audit Log)
    - Evidence is cleansed of sensitive information (Redact)
    - Evidence is enhanced by attaching context (Intel services)
- Automation allows small teams to do more and do consistently.
- Automation extended to include, user breach monitoring, reminder bot and cloud monitoring.



Secure Audit Log Viewer

View your logs. Search syntax documentation

Visit branding to preview what it could look like in your app

Results: 1 – 20 of 128 | Limit: 1000

Rows per page: 20

```
Time                    Message
09/15/2023, 11:30 PM    {'eventVersion': '1.08', 'userIdentity': {'type': 'IAMUser', 'principalId': '[redacted]', 'arn': 'arn:aws:iam::[redacted]', 'accountId': '[redacted]', 'userName': 'ra
```

[redacted]

Time: 09/15/2023, 11:30 PM
Timestamp: 09/14/2023, 12:47 AM
Actor: randell.pelak@pangea.cloud
Action: ConsoleLogin
Status: Success
Target: https://console.aws.amazon.com/console/home?hashArgs=%23&isauthcode=true&state=hashArgsFromTB_us-west-2_3c2c1e77d89c5c43
Source: 50.47.143.150
Tenant ID: -
Message:

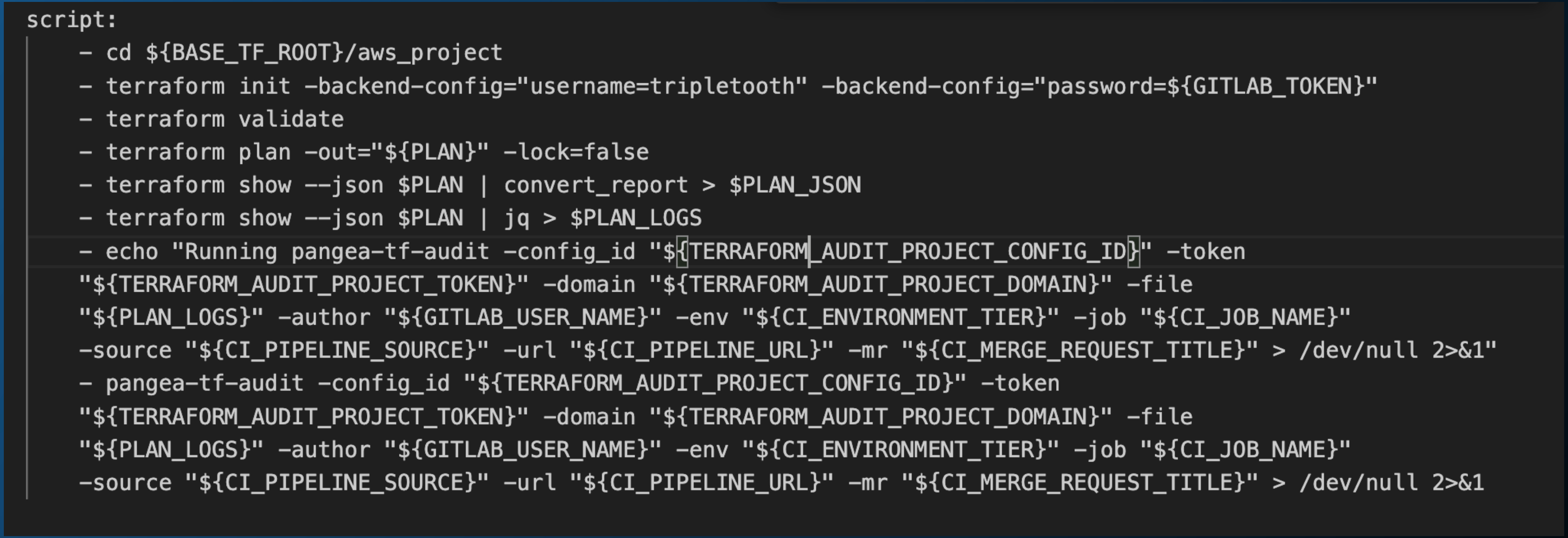
```
{'eventVersion': '1.08', 'userIdentity': {'type': 'IAMUser', 'principalId': '[redacted]', 'arn': 'arn:aws:iam::[redacted]', '[redacted]
'userName': 'randell.pelak@pangea.cloud'}, 'eventTime': '2023-09-13T22:47:43Z', 'eventSource': 'signin.amazonaws.com', 'eventName': 'ConsoleLogin', 'awsRegion': 'us-west-2', 'sourceIPAddress':
'50.47.143.150', 'userAgent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0', 'requestParameters': None, 'responseElements': {'ConsoleLogin': 'Success'},
'additionalEventData': {'LoginTo': 'https://console.aws.amazon.com/console/home?hashArgs=%23&isauthcode=true&state=hashArgsFromTB_us-west-2_3c2c1e77d89c5c43', 'MobileVersion': 'No',
'MFAIdentifier': 'arn:aws:iam::[redacted]XJSTGFZBF7HJSHY63DBMXDE', 'MFAUsed': 'Yes'}, 'eventID': '798c1e38-555f-44c8-8ef5-493ad6b0204f',
'readOnly': False, 'eventType': 'AwsConsoleSignIn', 'managementEvent': True, 'recipientAccountId': '[redacted]', 'eventCategory': 'Management', 'tlsDetails': {'tlsVersion': 'TLSv1.3', 'cipherSuite':
'TLS_AES_128_GCM_SHA256', 'clientProvidedHostHeader': 'us-west-2.signin.aws.amazon.com'}}
```

New Value: prd.us-west-2.Cloudtrail.ConsoleLogin

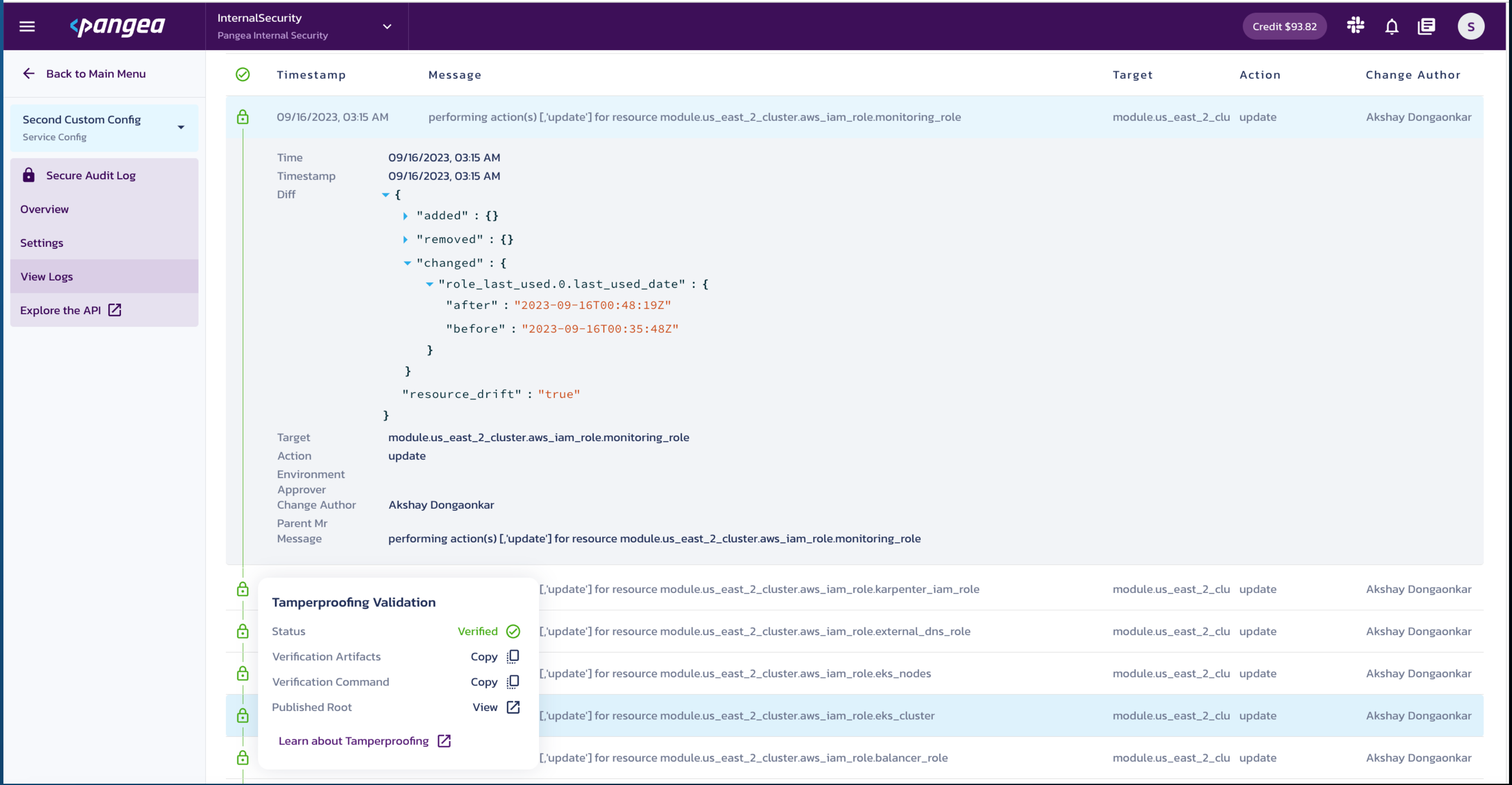
```
09/15/2023, 11:29 PM    {'eventVersion': '1.09', 'userIdentity': {'type': 'IAMUser', 'principalId': '[redacted], 'arn': 'arn:aws:iam::[redacted]user/terraform', 'accountId': '[redacted]', 'accessKeyId': '[redacted]
09/15/2023, 11:29 PM    {'eventVersion': '1.09', 'userIdentity': {'type': 'IAMUser', 'principalId': [redacted]', 'arn': 'arn:aws:iam::[redacted]user/terraform', 'accountId': '[redacted], 'accessKeyId': '[redacted]
09/15/2023, 11:29 PM    {'eventVersion': '1.09', 'userIdentity': {'type': 'IAMUser', 'principalId': [redacted]', 'arn': 'arn:aws:iam::[redacted]user/terraform', 'accountId': '[redacted], 'accessKeyId': '[redacted]
```

Craton – key takeaways

- Once security and compliance data is accessible with code it can quickly be leveraged to meet new use cases.
  - For instance, TF Audit logging can now be used to monitor for resource drift (a new vendor requirement)
- A streamlined compliance audit process with fewer findings.



```
script:
    - cd ${BASE_TF_ROOT}/aws_project
    - terraform init -backend-config="username=tripletooth" -backend-config="password=${GITLAB_TOKEN}"
    - terraform validate
    - terraform plan -out="${PLAN}" -lock=false
    - terraform show --json $PLAN | convert_report > $PLAN_JSON
    - terraform show --json $PLAN | jq > $PLAN_LOGS
    - echo "Running pangea-tf-audit -config_id "${TERRAFORM_AUDIT_PROJECT_CONFIG_ID}" -token
    "${TERRAFORM_AUDIT_PROJECT_TOKEN}" -domain "${TERRAFORM_AUDIT_PROJECT_DOMAIN}" -file
    "${PLAN_LOGS}" -author "${GITLAB_USER_NAME}" -env "${CI_ENVIRONMENT_TIER}" -job "${CI_JOB_NAME}"
    -source "${CI_PIPELINE_SOURCE}" -url "${CI_PIPELINE_URL}" -mr "${CI_MERGE_REQUEST_TITLE}" > /dev/null 2>&1"
    - pangea-tf-audit -config_id "${TERRAFORM_AUDIT_PROJECT_CONFIG_ID}" -token
    "${TERRAFORM_AUDIT_PROJECT_TOKEN}" -domain "${TERRAFORM_AUDIT_PROJECT_DOMAIN}" -file
    "${PLAN_LOGS}" -author "${GITLAB_USER_NAME}" -env "${CI_ENVIRONMENT_TIER}" -job "${CI_JOB_NAME}"
    -source "${CI_PIPELINE_SOURCE}" -url "${CI_PIPELINE_URL}" -mr "${CI_MERGE_REQUEST_TITLE}" > /dev/null 2>&1
```



✓	Timestamp	Message	Target	Action	Change Author
🔒	09/16/2023, 03:15 AM	performing action(s) [,'update'] for resource module.us_east_2_cluster.aws_iam_role.monitoring_role	module.us_east_2_clu	update	Akshay Dongaonkar

Time	09/16/2023, 03:15 AM
Timestamp	09/16/2023, 03:15 AM
Diff	

```
{
  "added" : {}
  "removed" : {}
  "changed" : {
    "role_last_used.0.last_used_date" : {
      "after" : "2023-09-16T00:48:19Z"
      "before" : "2023-09-16T00:35:48Z"
    }
  }
  "resource_drift" : "true"
}
```

Target	module.us_east_2_cluster.aws_iam_role.monitoring_role
Action	update
Environment	
Approver	
Change Author	Akshay Dongaonkar
Parent Mr	
Message	performing action(s) [,'update'] for resource module.us_east_2_cluster.aws_iam_role.monitoring_role

	Message	Target	Action	Change Author
🔒	[,'update'] for resource module.us_east_2_cluster.aws_iam_role.karpenter_iam_role	module.us_east_2_clu	update	Akshay Dongaonkar
🔒	[,'update'] for resource module.us_east_2_cluster.aws_iam_role.external_dns_role	module.us_east_2_clu	update	Akshay Dongaonkar
🔒	[,'update'] for resource module.us_east_2_cluster.aws_iam_role.eks_nodes	module.us_east_2_clu	update	Akshay Dongaonkar
🔒	[,'update'] for resource module.us_east_2_cluster.aws_iam_role.eks_cluster	module.us_east_2_clu	update	Akshay Dongaonkar
🔒	[,'update'] for resource module.us_east_2_cluster.aws_iam_role.balancer_role	module.us_east_2_clu	update	Akshay Dongaonkar

Tamperproofing Validation

Status	Verified ✓
Verification Artifacts	Copy
Verification Command	Copy
Published Root	View

Learn about Tamperproofing

PRODUCED BY

Craton - team

- Baruch Mettler (Sr. Security Engineer)
- Akshay Dongaonkar (Sr. Platform and Infra Engineer)
- Jimmy Jing (Intern)
- Ruchika Muddinagiri (Intern)

Thank You

CSO50

PRODUCED BY CSO