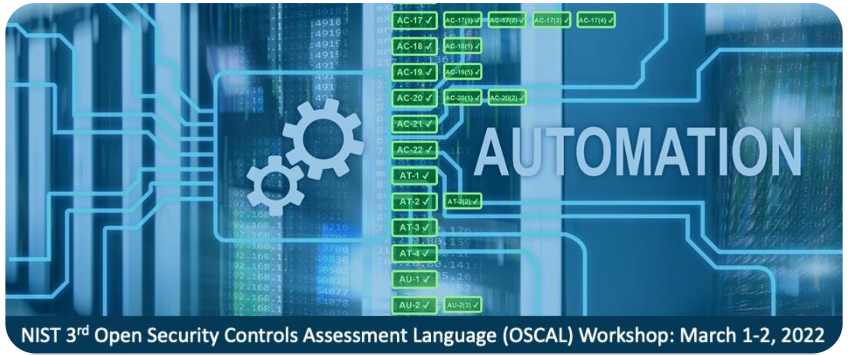
stackArmor



NIST 3rd Open Security Controls Assessment Language (OSCAL) Workshop: March 1-2, 2022

# Accelerating FedRAMP, FISMA/RMF and CMMC 2.0 ATOs with OSCAL

Gaurav "GP" Pal, stackArmor, Inc.
Martin Rieger, stackArmor, Inc.

# About Us

## Gaurav “GP” Pal

Principal
stackArmor

## Martin Rieger

Chief Solutions Officer
stackArmor

GP is subject matter expert in driving cloud adoption and implementing NIST security standards for FedRAMP, FISMA and DFARS/CMMC compliance. He has received the Fed 100 and GCN Rising Star awards in 2015 and 2011 for Cloud ATO’s.

Martin supports all FedRAMP, FISMA/RMF and CMMC 2.0 projects for both Commercial and Federal Agencies. Mr. Rieger has supported multiple 3PAO’s and has over 20 years of progressive information systems experience including active duty with the US Navy.

stackArmor

# About stackArmor

- stackArmor is headquartered in Washington DC and is an Advanced AWS Partner with strong security and compliance experience in Education, DOD & Federal, commercial, public sector and non-profit markets.
- We are 1 of 8 firms selected by AWS globally as inaugural consulting partners as part of the ATO on AWS program.
- stackArmor is the **first and only** AWS Shield Advanced Partner for North America
- Global public sector customer base at the Federal, State and Local Government level.
- Fortune 500 Commercial clients with strong focus on security and compliance.

ISO NIST

**We provide cloud enablement services for regulated industries with strong compliance and security needs.**

FedRAMP | DOD | FISMA/NIST | CMMC

**Government | Public Sector | Defense**
**Aerospace | Space | Healthcare**

Inc. 500 AMERICA'S FASTEST GROWING PRIVATE COMPANIES

aws partner network

**Advanced**
Consulting Partner

SaaS Partner

Public Sector Partner

Security Competency

Government Competency

Microsoft Workloads Competency

aws partner network | authority to operate

The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor's written permission.

# Capabilities

## Our team specializes in technical advisory to include these core services:

- ✓ **NIST Advisement –** ensuring your cloud service meets NIST guidelines
- ✓ **System Documentation** – development of policies, plans and procedures for FedRAMP
- ✓ **DoD A&A –** over ten years of DoD Assessment & Authorization experience
- ✓ **Continuous Monitoring** – Managed services, security and compliance services
- ✓ **Vulnerability Assessments** – perform scans on systems to identify vulnerabilities
- ✓ **Application Security Testing** – detect security holes in software and applications

ATO
DOD CMMC
FedRAMP NIST/RMF

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

CYBERSECURITY MATURITY MODEL
CERTIFICATION

aws partner network | authority to operate

aws CERTIFIED Solutions Architect Associate
aws CERTIFIED Developer Associate
aws CERTIFIED SysOps Administrator Associate
aws CERTIFIED Solutions Architect Professional
aws CERTIFIED DevOps Engineer Professional

NIST
800-171, DFARS & ITAR

# Agenda

- ❑ Growing demand for Cloud Services with NIST Compliance
    - ❑ FedRAMP, StateRAMP, TexRAMP, MARS-E 2.2, DHS 4300…
- ❑ ATO Acceleration with FASTTR
- ❑ Understanding FASTTR
- ❑ How OSCAL helps accelerate ATO’s

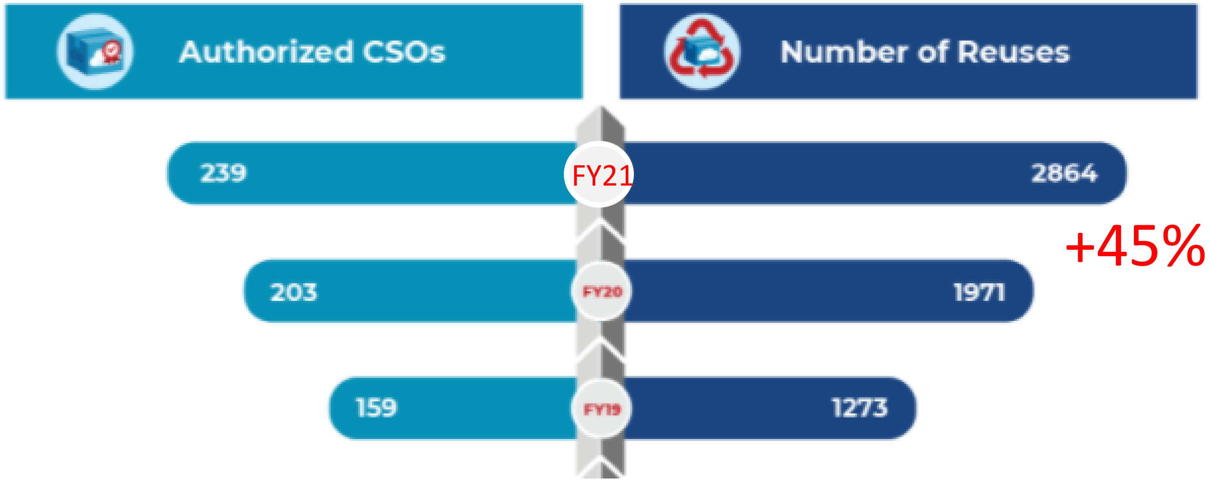
The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor’s written permission.

# FedRAMP Cloud Market Size

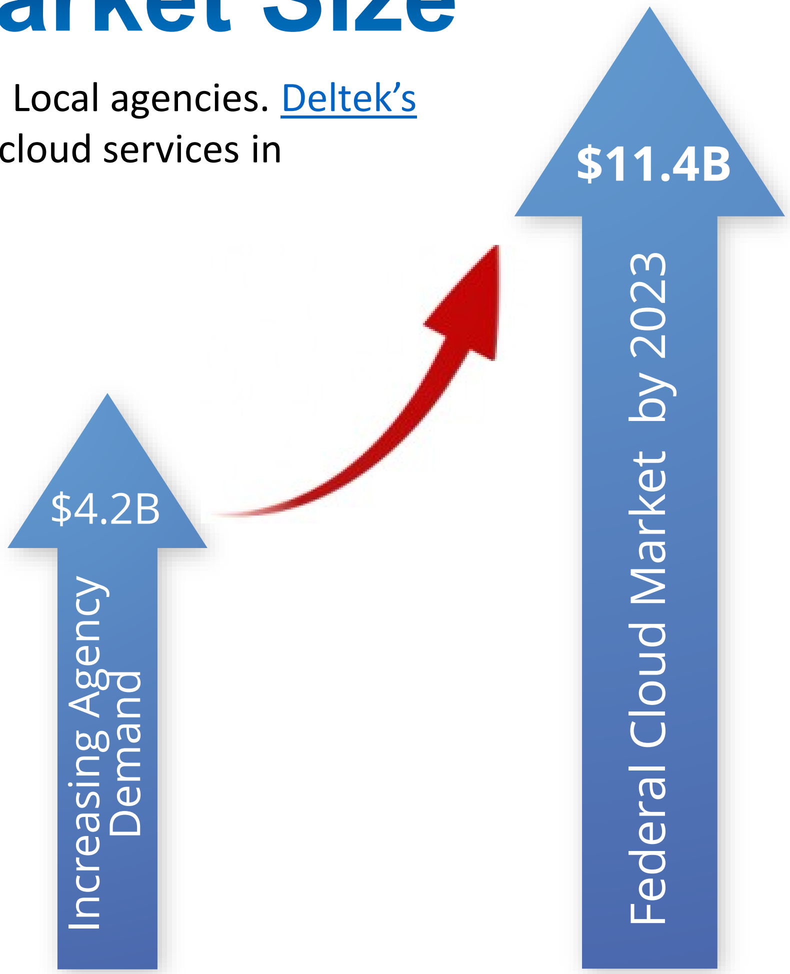
Growing adoption of FedRAMP accredited cloud services by Federal, State and Local agencies. Deltek’s Federal Cloud Market report shows over **$4.2B** spent on FedRAMP accredited cloud services in FY2020/21 with total cloud spending expected to grow to **$11.4 B by 2023**.

FedRAMP

The FedRAMP PMO reports significant jump in agency consumption of FedRAMP accredited cloud services.



Data and graphics were leveraged from the FedRAMP.gov blog published Nov 9, 2021

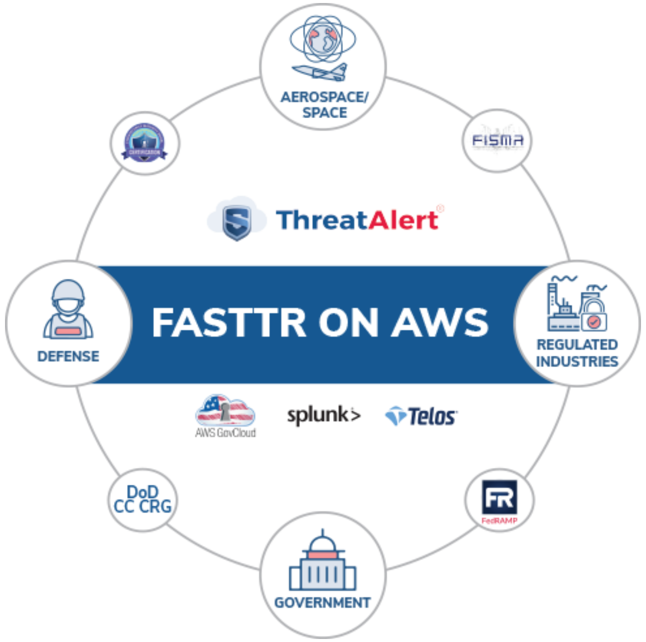


The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor’s written permission.

# Introducing FASTTR on AWS

FASTTR on AWS is a partner led initiative under the ATO on AWS program developed by stackArmor – **an all-in** AWS Partner focused on security and compliance for government centric markets.

As part of the FASTTR on AWS program, we are providing the **ThreatAlert® ATO Accelerator** that reduces the time and cost of FedRAMP, FISMA and CMMC Authority to Operate **by 40%**.



## ThreatAlert® ATO Machine (ATOM)

```
                1 {write-host "Time $($line)" }
                2 {write-host "$($line)"}
                3 {write-host "$($line)"}
                4 {write-host "% $($line)"}
                5 {write-host "$($line)"}
            }
            $i++
        }
} else {
        $i=0
        # ERROR
        write-host "===========ERROR==============="
        write-host "credential ID $($credentialID)"
        foreach ($line in $lines){
            $linenumber = $i
            switch ($linenumber) {
                4 {write-host "$($line)"}
                5 {write-host "$($line)"}
            }
            $i++
        }
}
```

Dedicated "In-boundary" Deployment with Platform-as-code (PaC)

Pre-Audited Security Platform with NIST compliant controls

FedRAMP
XACTA 360
FIPS 140-2
OSCAL

Audit-ready ATO Package with Post-ATO ConMon

The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor's written permission.

# Engineering Approach to ATO’s

## Platform-as-code ThreatAlert® Security Platform

FedRAMP **compliant** landing zone with integrated security services aligned to NIST SP 800-53

## Digital Artifacts in OSCAL

Xacta360 for **OSCAL**

Ready artifacts streamlines and automates FedRAMP

## ThreatAlert® ConMon

Perform scheduled activities and deliver artifacts based on FedRAMP controls and Assist with annual assessment

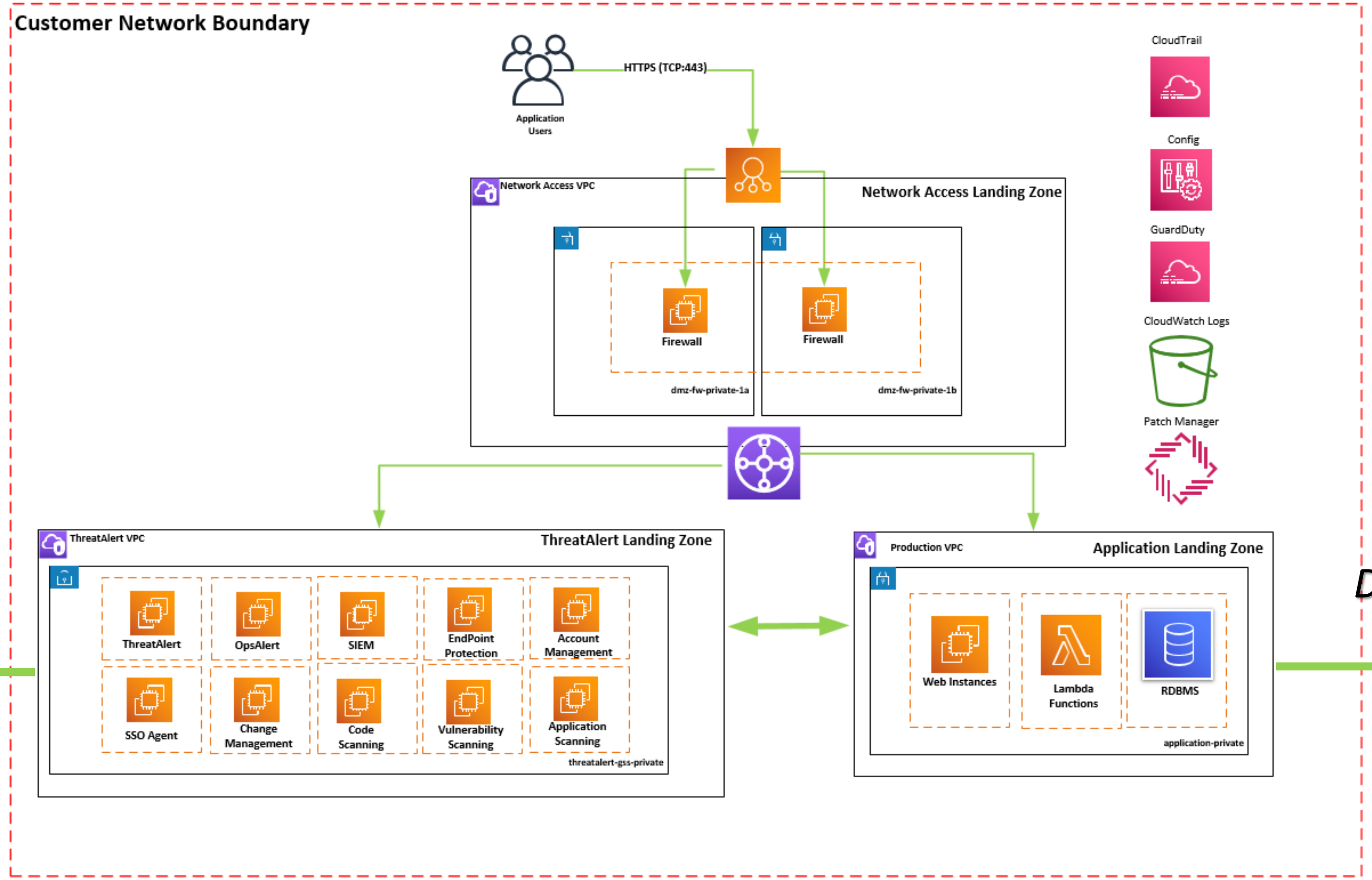
# Compliant Authorization Boundary

ThreatAlert®

*NIST Compliant Security Services*

Detect → Respond → Comply

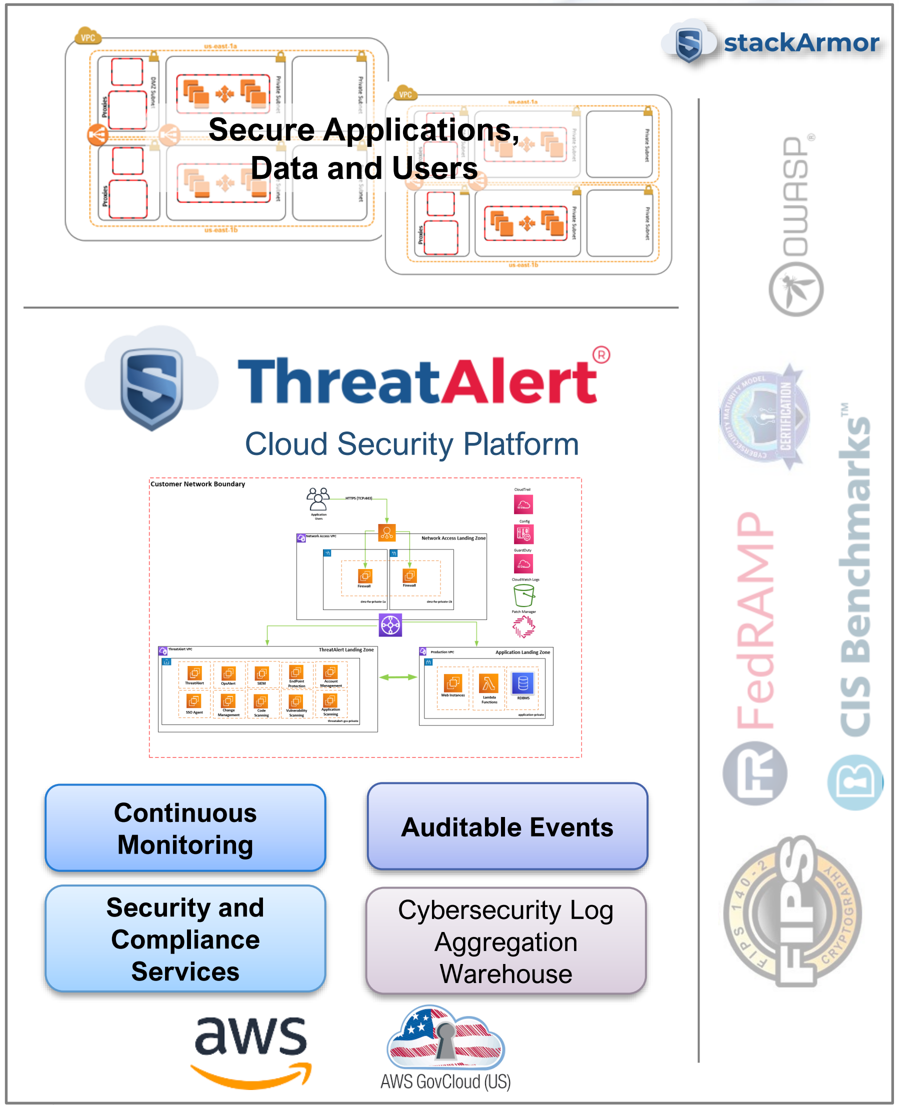
- ✓ User and data monitoring
- ✓ Code vulnerability analysis
- ✓ Container vulnerabilities
- ✓ Web application scan
- ✓ Cloud configuration scan
- ✓ IDS/IPS monitoring
- ✓ SIEM integration
- ✓ Incident management
- ✓ Compliance reporting



*Applications, Data and Users*

The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor's written permission.

# ThreatAlert® Security Platform



| | Security Capability | FIPS/FedRAMP Compliant Service |
|---|---|---|
| 1 | Code analysis | ✓ |
| 2 | Vulnerability Scanning | ✓ |
| 3 | Web Vulnerability Scanning | ✓ |
| 4 | Container vulnerabilities | ✓ |
| 5 | IDS/IPS (Host/Container) | ✓ |
| 6 | Anti-Virus/Malware | ✓ |
| 7 | SIEM | ✓ |
| 8 | Hardening | ✓ |
| 9 | Patch management | ✓ |
| 10 | Observability/Monitoring | ✓ |
| 11 | Alerting | ✓ |
| 12 | Incident management | ✓ |
| 13 | Auditable Cloud system operations monitoring | ✓ |
| 14 | Centralized log aggregation warehouse | ✓ |
| 15 | Centralized account management and MFA | ✓ |
| 16 | Compliance reporting | ✓ |
| 17 | Boundary Protection | ✓ |
| 18 | Secure access management | ✓ |

stackArmor

# What is PaC?

Platform as code is a new paradigm for developing opinionated platforms that meet specific business and security requirements using software development principles of modularity, abstraction and maintainability. The end result is consistency and standardization across the enterprise saving time, money and avoiding costly mistakes.

**PaC**

- Compliance Monitoring
- Incident Management
- IDS/IPS Services
- Web Scanning Services
- Vulnerability Scanning

**"Programming"**

- Python/CDK
- CodePipeline
- CodeBuild
- Step Functions

**IaC**

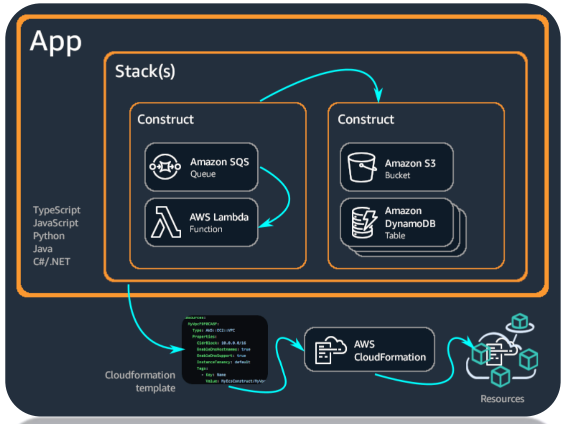
- Basic Policies, IAM Access
- Archival Services
- Storage Services
- Compute Services
- Network Services

**"Scripting"**

- CloudFormation
- Terraform

ATOM
*ATO Machine*

**Our Platform is an App**



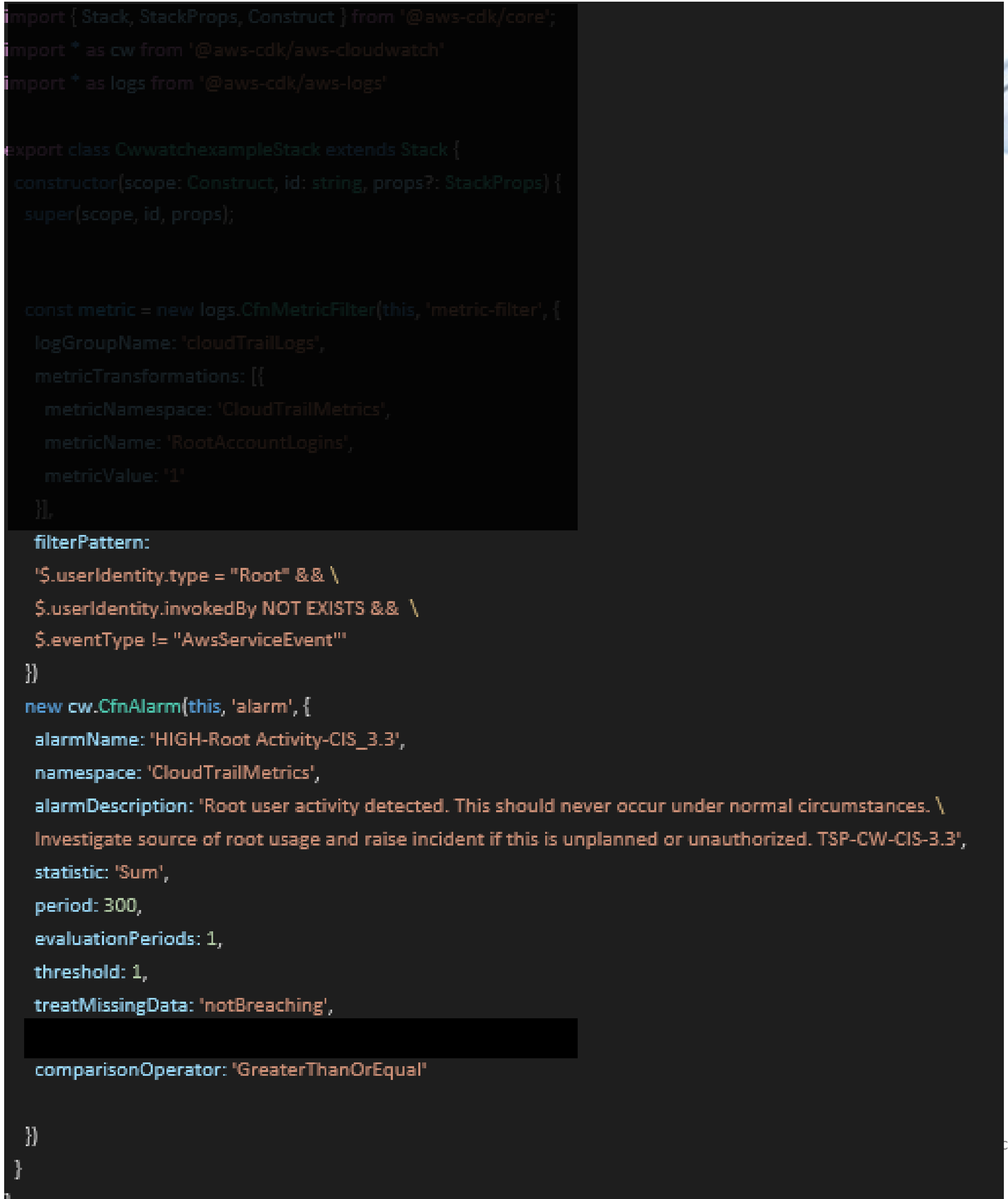
```
Resources:
  MyVpcF9F0CA6F:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: MyEcsConstruct/MyVp
```

ThreatAlert®

AWS : PaaS A

AWS : PaaS B

AWS : PaaS C



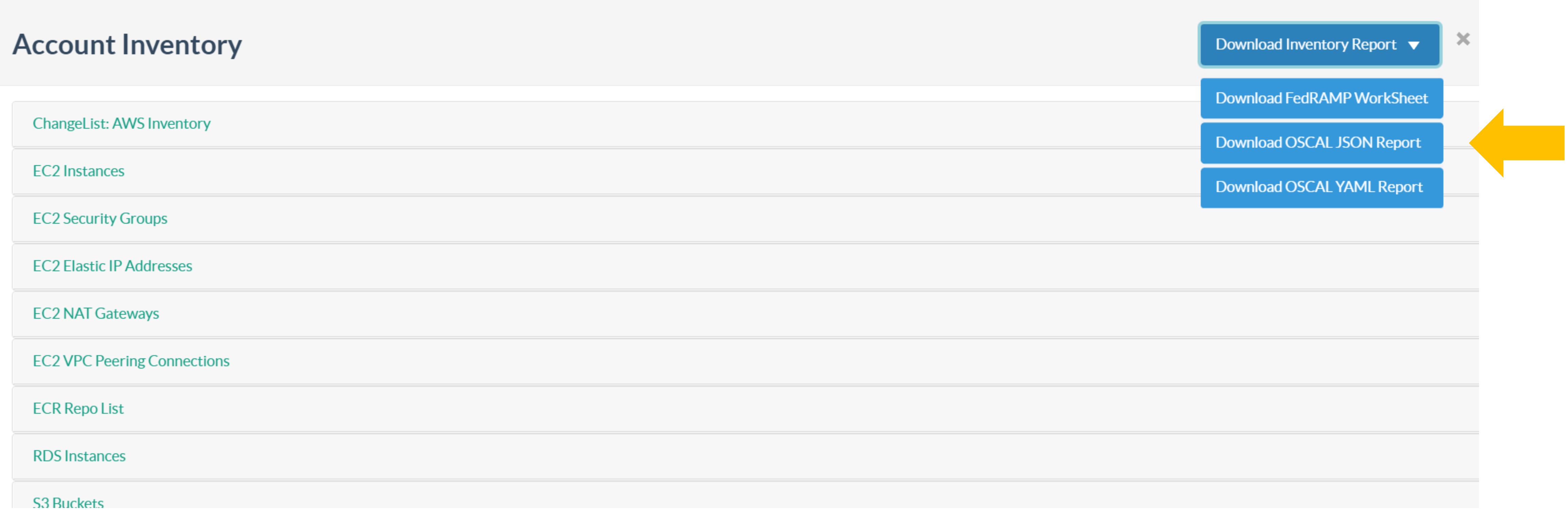
```
import { Stack, StackProps, Construct } from '@aws-cdk/core';
import * as cw from '@aws-cdk/aws-cloudwatch'
import * as logs from '@aws-cdk/aws-logs'

export class CwwatchexampleStack extends Stack {
 constructor(scope: Construct, id: string, props?: StackProps) {
  super(scope, id, props);


  const metric = new logs.CfnMetricFilter(this, 'metric-filter', {
   logGroupName: 'cloudTrailLogs',
   metricTransformations: [{
    metricNamespace: 'CloudTrailMetrics',
    metricName: 'RootAccountLogins',
    metricValue: '1'
   }],
   filterPattern:
   '$.userIdentity.type = "Root" && \
   $.userIdentity.invokedBy NOT EXISTS &&  \
   $.eventType != "AwsServiceEvent"'
  })
  new cw.CfnAlarm(this, 'alarm', {
   alarmName: 'HIGH-Root Activity-CIS_3.3',
   namespace: 'CloudTrailMetrics',
   alarmDescription: 'Root user activity detected. This should never occur under normal circumstances. \
   Investigate source of root usage and raise incident if this is unplanned or unauthorized. TSP-CW-CIS-3.3',
   statistic: 'Sum',
   period: 300,
   evaluationPeriods: 1,
   threshold: 1,
   treatMissingData: 'notBreaching',
  [redacted]
   comparisonOperator: 'GreaterThanOrEqual'

  })
}
```

***Observability as code*** to find data that caused alarm

***Alarm as code*** to satisfy AU-2a and AU-2d

AU-2a auditable events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes

# Enabling cATO with OSCAL



## Account Inventory

Download Inventory Report ▼
×
Download FedRAMP WorkSheet
Download OSCAL JSON Report
Download OSCAL YAML Report

ChangeList: AWS Inventory

EC2 Instances

EC2 Security Groups

EC2 Elastic IP Addresses

EC2 NAT Gateways

EC2 VPC Peering Connections

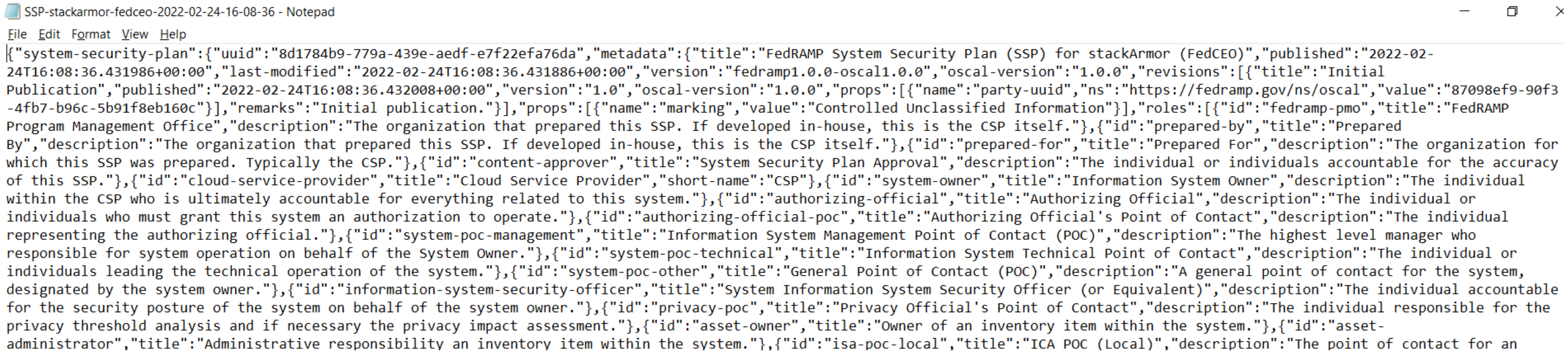
ECR Repo List

RDS Instances

S3 Buckets

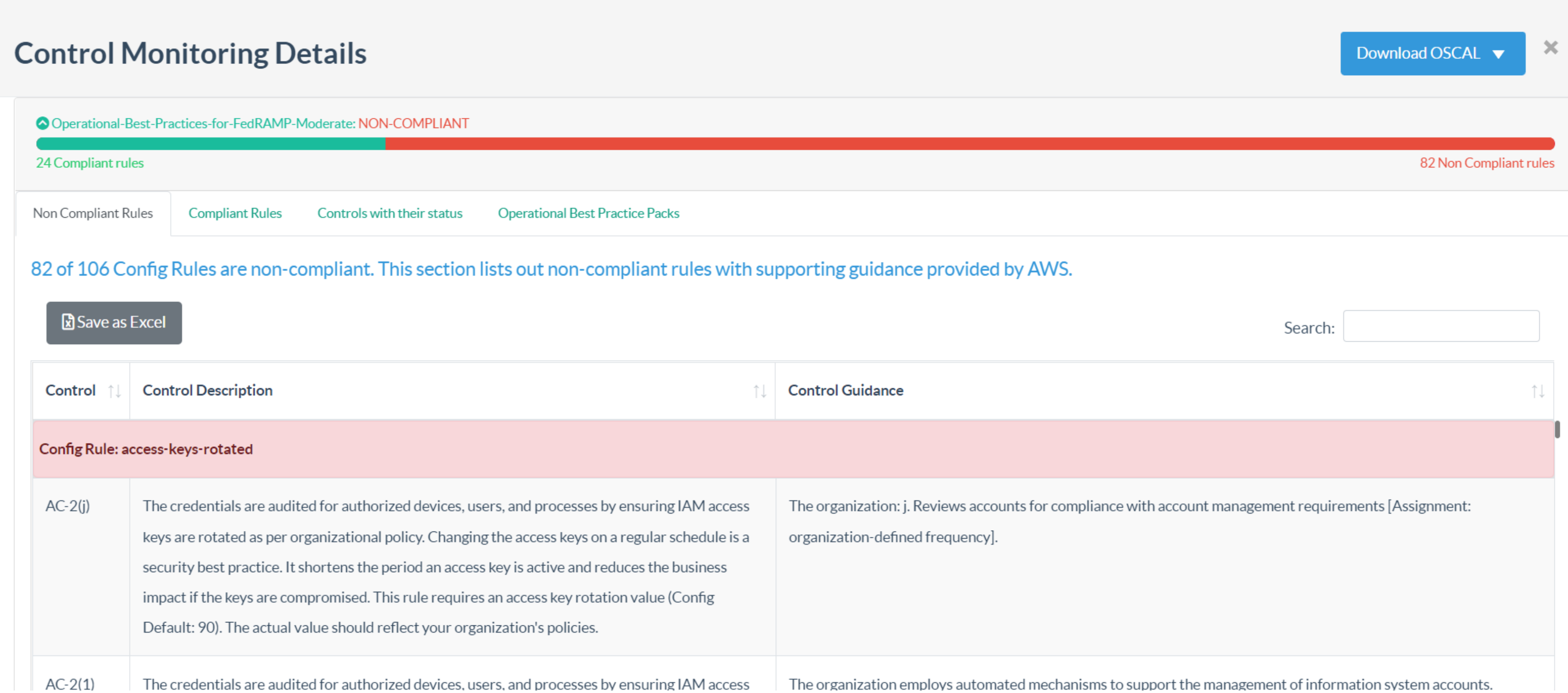
The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor's written permission.

# Digital Inventory in OSCAL



```
{"system-security-plan":{"uuid":"8d1784b9-779a-439e-aedf-e7f22efa76da","metadata":{"title":"FedRAMP System Security Plan (SSP) for stackArmor (FedCEO)","published":"2022-02-
24T16:08:36.431986+00:00","last-modified":"2022-02-24T16:08:36.431886+00:00","version":"fedramp1.0.0-oscal1.0.0","oscal-version":"1.0.0","revisions":[{"title":"Initial
Publication","published":"2022-02-24T16:08:36.432008+00:00","version":"1.0","oscal-version":"1.0.0","props":[{"name":"party-uuid","ns":"https://fedramp.gov/ns/oscal","value":"87098ef9-90f3
-4fb7-b96c-5b91f8eb160c"}],"remarks":"Initial publication."}],"props":[{"name":"marking","value":"Controlled Unclassified Information"}],"roles":[{"id":"fedramp-pmo","title":"FedRAMP
Program Management Office","description":"The organization that prepared this SSP. If developed in-house, this is the CSP itself."},{"id":"prepared-by","title":"Prepared
By","description":"The organization that prepared this SSP. If developed in-house, this is the CSP itself."},{"id":"prepared-for","title":"Prepared For","description":"The organization for
which this SSP was prepared. Typically the CSP."},{"id":"content-approver","title":"System Security Plan Approval","description":"The individual or individuals accountable for the accuracy
of this SSP."},{"id":"cloud-service-provider","title":"Cloud Service Provider","short-name":"CSP"},{"id":"system-owner","title":"Information System Owner","description":"The individual
within the CSP who is ultimately accountable for everything related to this system."},{"id":"authorizing-official","title":"Authorizing Official","description":"The individual or
individuals who must grant this system an authorization to operate."},{"id":"authorizing-official-poc","title":"Authorizing Official's Point of Contact","description":"The individual
representing the authorizing official."},{"id":"system-poc-management","title":"Information System Management Point of Contact (POC)","description":"The highest level manager who
responsible for system operation on behalf of the System Owner."},{"id":"system-poc-technical","title":"Information System Technical Point of Contact","description":"The individual or
individuals leading the technical operation of the system."},{"id":"system-poc-other","title":"General Point of Contact (POC)","description":"A general point of contact for the system,
designated by the system owner."},{"id":"information-system-security-officer","title":"System Information System Security Officer (or Equivalent)","description":"The individual accountable
for the security posture of the system on behalf of the system owner."},{"id":"privacy-poc","title":"Privacy Official's Point of Contact","description":"The individual responsible for the
privacy threshold analysis and if necessary the privacy impact assessment."},{"id":"asset-owner","title":"Owner of an inventory item within the system."},{"id":"asset-
administrator","title":"Administrative responsibility an inventory item within the system."},{"id":"isa-poc-local","title":"ICA POC (Local)","description":"The point of contact for an
```

# cATO as Code for Continuous Compliance



## Control Monitoring Details

Operational-Best-Practices-for-FedRAMP-Moderate: NON-COMPLIANT

24 Compliant rules

82 Non Compliant rules

82 of 106 Config Rules are non-compliant. This section lists out non-compliant rules with supporting guidance provided by AWS.

| Control | Control Description | Control Guidance |
|---|---|---|
| Config Rule: access-keys-rotated | | |
| AC-2(j) | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. | The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]. |
| AC-2(1) | The credentials are audited for authorized devices, users, and processes by ensuring IAM access | The organization employs automated mechanisms to support the management of information system accounts. |

# Highlights

- ❑ Jumpstart FedRAMP, FISMA/RMF, CMMC 2.0 and StateRamp compliance projects with a focus on automation using **NIST OSCAL**
- ❑ **AWS vetted** security & compliance solution - ThreatAlert® ATO Accelerator
- ❑ Telos' Xacta 360® automated compliance solution with AWS control inheritance capabilities and **OSCAL** integration
- ❑ **End to end** solution deployed "on-prem" in customers' or partners' AWS Accounts and includes professional services, licenses and managed services

ThreatAlert®

powered by aws

stackArmor

# Thank You!

*We strive to become a trusted cloud security and operations partner for our customers and deliver customer delight to build long term relationships. We help reduce the time and cost of a FedRAMP, FISMA/RMF and CMMC ATO by 40%.*

- Additional Information
  - Microsite https://stackArmor.com/FASTTR
  - AWS Solutions Offer Listing
  - AWS Marketplace Listing

- Contact us for more information by sending an email at solutions@stackArmor.com