Säkrare molnlösningar utan ett dedikerat säkerhetsteam

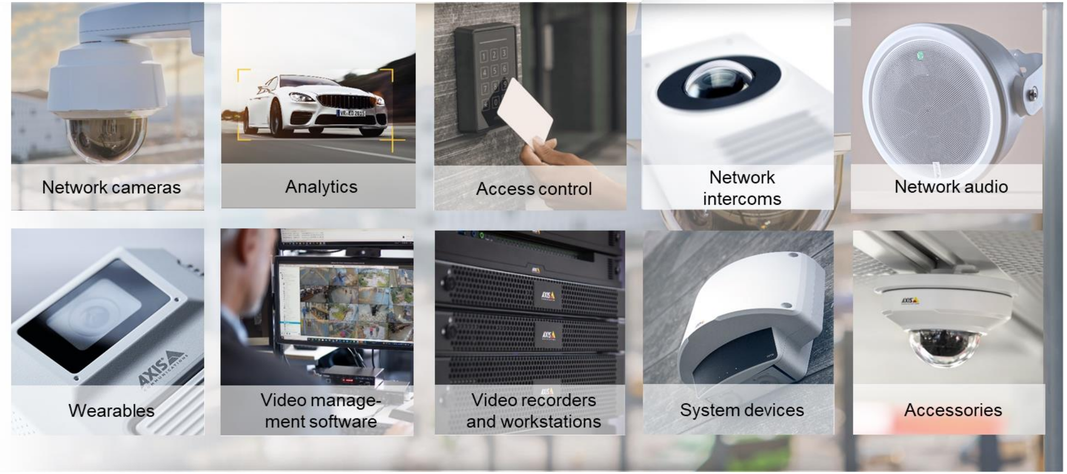
Vägen till utvecklardriven säkerhet

DevLin2024

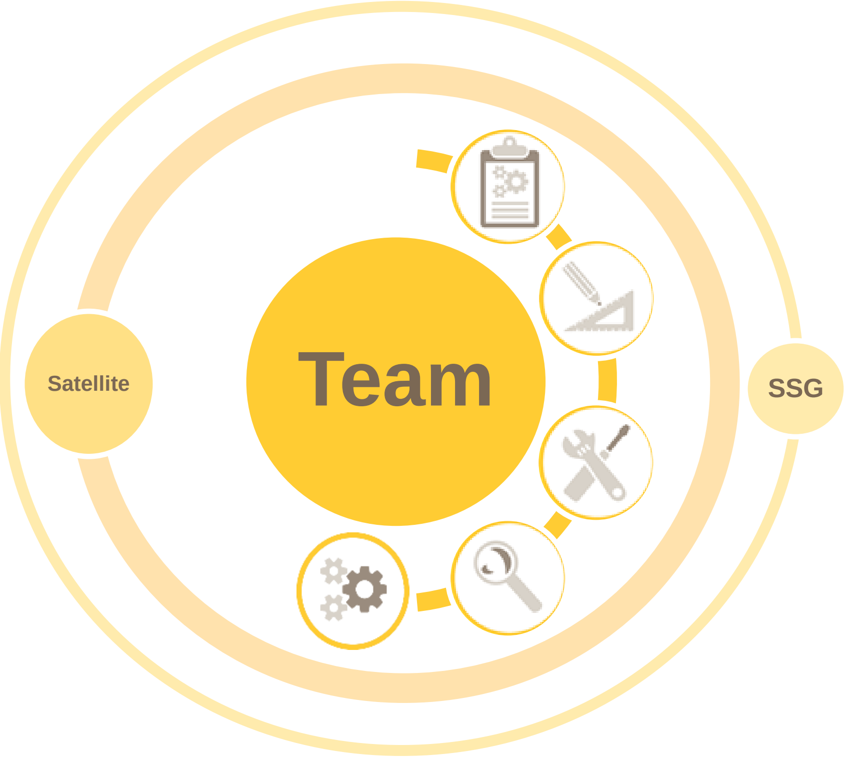
www.axis.com

Whoami?

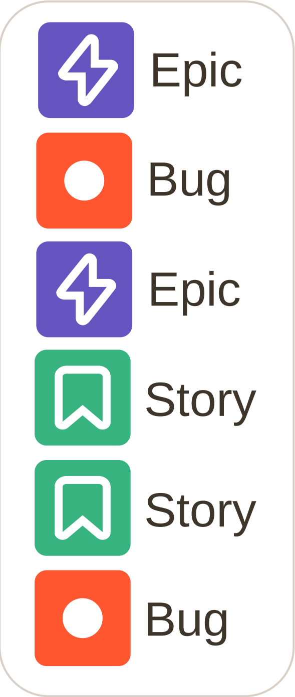
- > Software security coach @ Axis
- > Worked with security for almost 30 years except for two weeks



Team-centric approach



Risk assessment



Epic

Bug

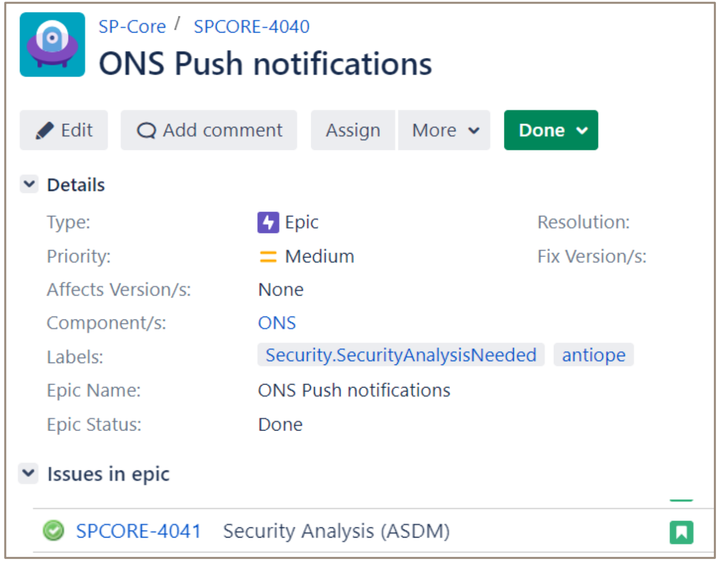
Epic

Story

Story

Bug

Backlog



SP-Core / SPCORE-4040

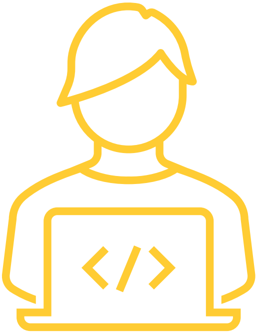
ONS Push notifications

Details

Type:	Epic	Resolution:
Priority:	Medium	Fix Version/s:
Affects Version/s:	None	
Component/s:	ONS	
Labels:	Security.SecurityAnalysisNeeded antiope	
Epic Name:	ONS Push notifications	
Epic Status:	Done	

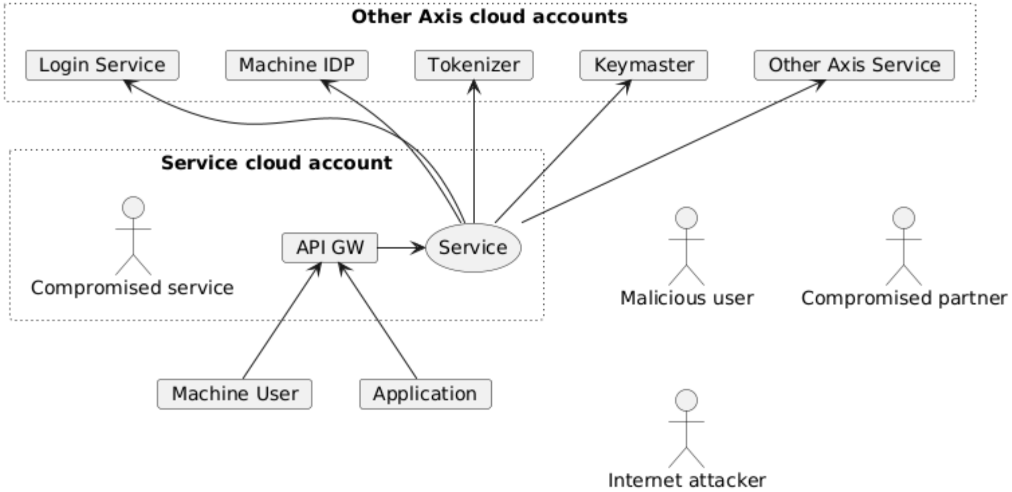
Issues in epic

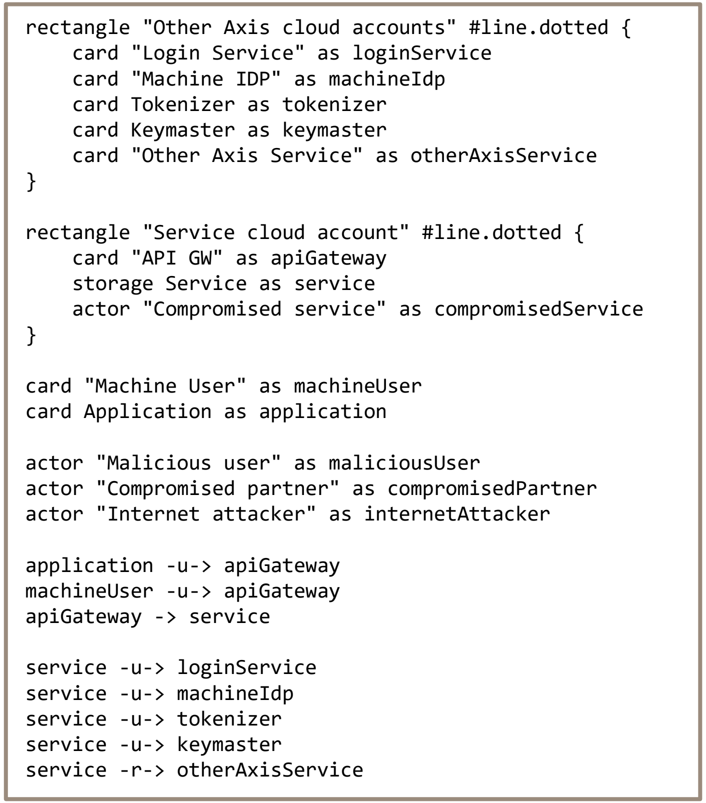
✓ SPCORE-4041 Security Analysis (ASDM)



Team

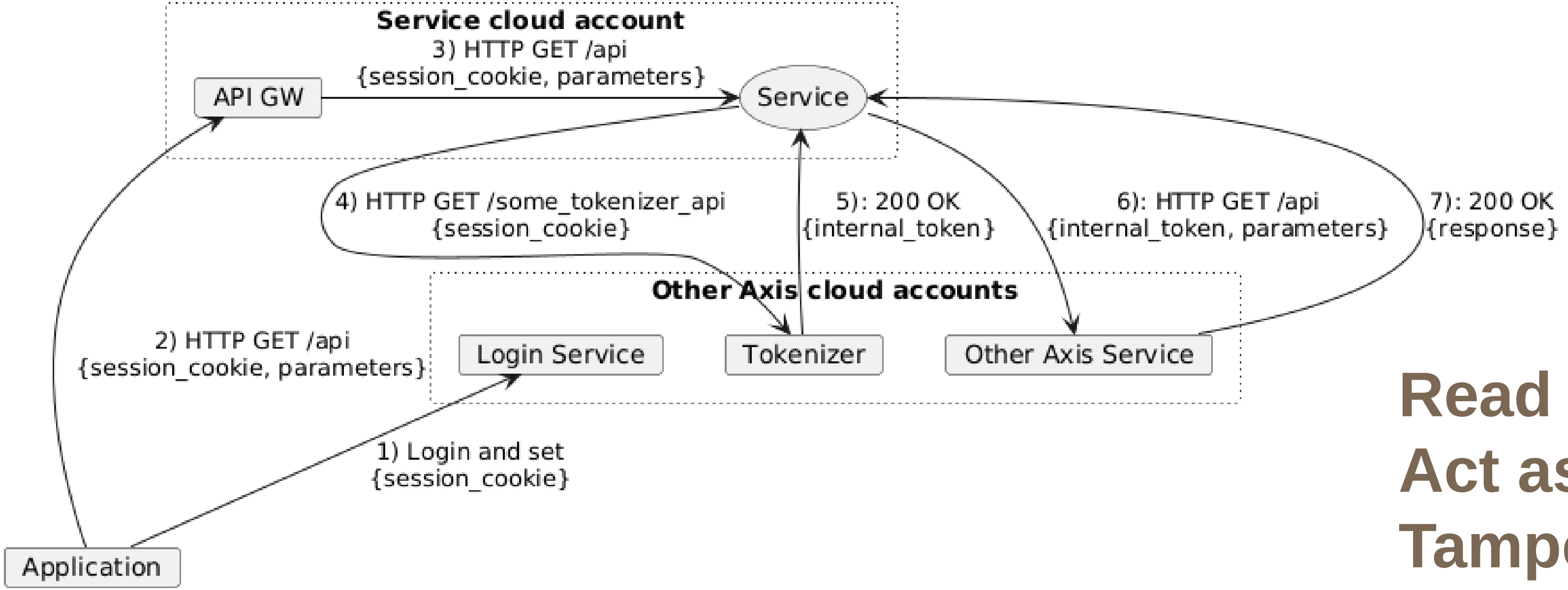
Threat modeling: setting a scope





```
rectangle "Other Axis cloud accounts" #line.dotted {
    card "Login Service" as loginService
    card "Machine IDP" as machineIdp
    card Tokenizer as tokenizer
    card Keymaster as keymaster
    card "Other Axis Service" as otherAxisService
}

rectangle "Service cloud account" #line.dotted {
    card "API GW" as apiGateway
    storage Service as service
    actor "Compromised service" as compromisedService
}

card "Machine User" as machineUser
card Application as application

actor "Malicious user" as maliciousUser
actor "Compromised partner" as compromisedPartner
actor "Internet attacker" as internetAttacker

application -u-> apiGateway
machineUser -u-> apiGateway
apiGateway -> service

service -u-> loginService
service -u-> machineIdp
service -u-> tokenizer
service -u-> keymaster
service -r-> otherAxisService
```

Threat modeling: use-case based data flow diagrams

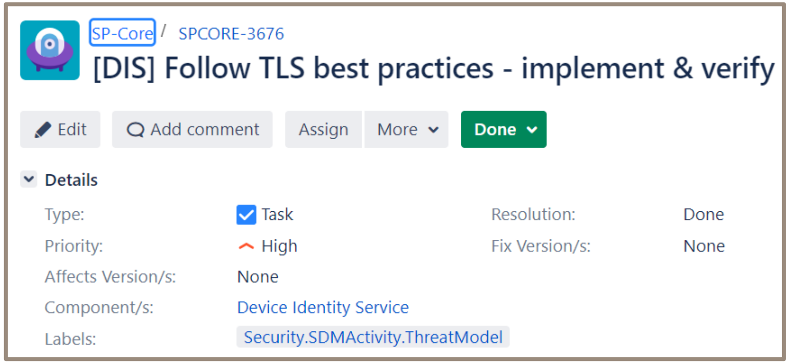


Read
Act as
Tamper
Exhaust
*****

Threat modeling: threats, countermeasures and verification

```
Title: "Threat model: Cloud service"

Threats:
   InternetAttackerMitm:
      Description: |
        An internet attacker reads the session_cookie or session-id to
        impersonate the user
      Countermeasures:
         Description: |
            TLS with server authentication according to:
            TLSBestPractices-Profile1-BrowsertoAxisservice
         Verification: |
            Verify that the TLS configuration follows the TLS Best
            Practices by running testssl.sh
```

Threat	Countermeasure	Verification
An internet attacker reads the session_cookie or session-id to impersonate the user	TLS with server authentication according to: TLSBestPractices-Profile1-BrowsertoAxisservice	Verify that the TLS configuration follows the TLS Best Practices by running for example testssl.sh



SP-Core / SPCORE-3676

[DIS] Follow TLS best practices - implement & verify

Type: ☑ Task

Priority: High

Affects Version/s: None

Component/s: Device Identity Service

Labels: Security.SDMActivity.ThreatModel

Resolution: Done

Fix Version/s: None

Static code analysis

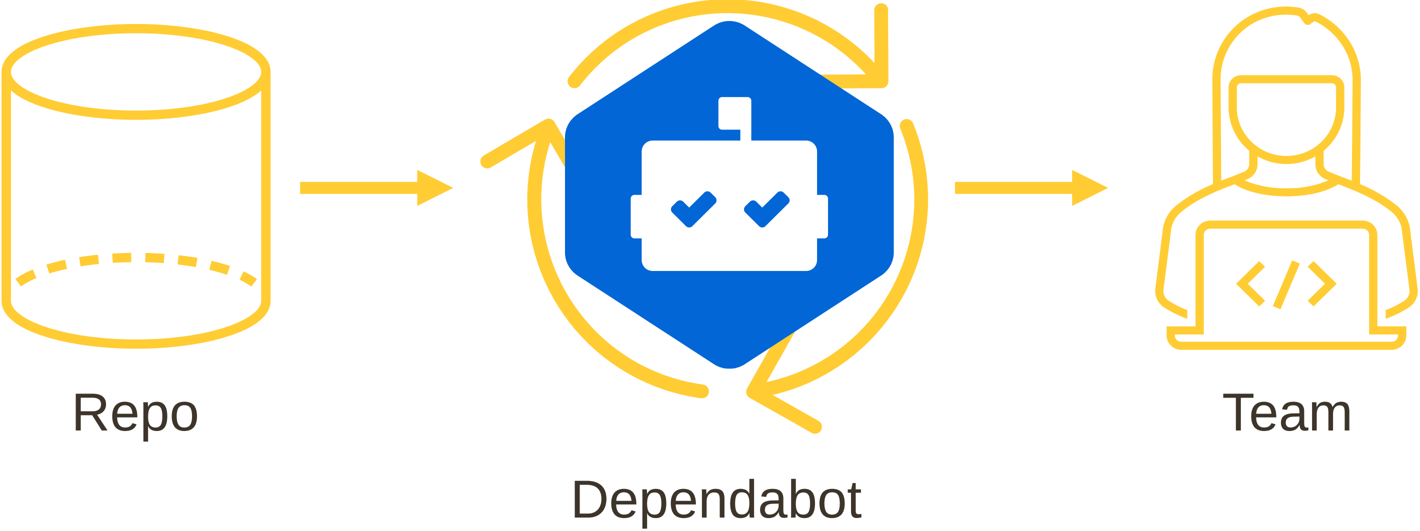
gosec

Golang security checker

Bandit

Python security linter

Software composition analysis

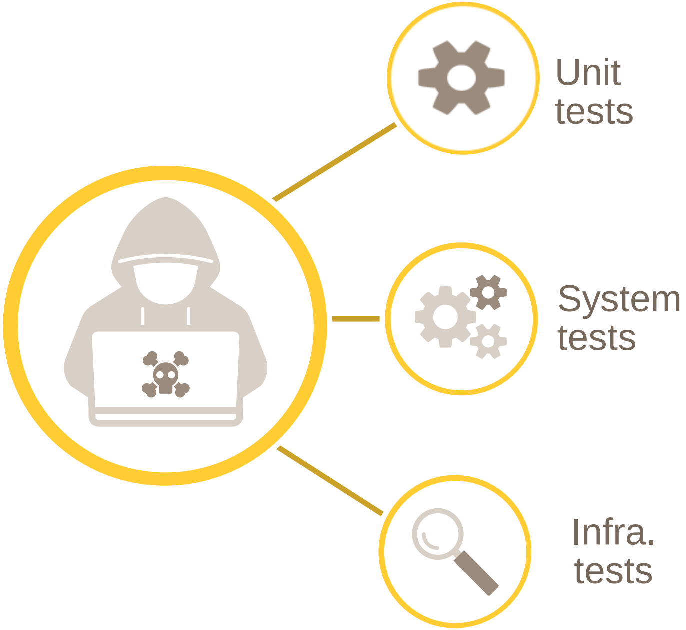


Repo

Dependabot

Team

Security testing

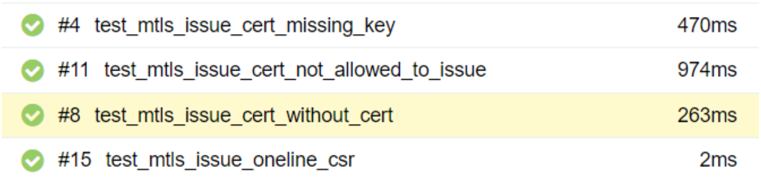


Unit tests

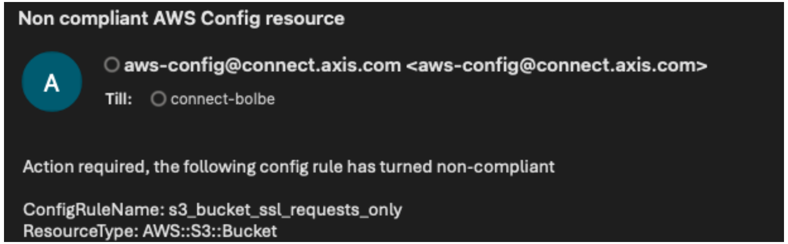
System tests

Infra. tests

```
def test_authorize_revoked_cert(self, cert, mocked_is_revoked):
        mocked_is_revoked.return_value = True

        authorizer = auth.Authorizer(cert)

        msg = "Cert revoked"
        with pytest.raises(auth.InvalidCertificate, match=msg):
            authorizer.authorize()
```



```
✓ #4  test_mtls_issue_cert_missing_key              470ms
✓ #11 test_mtls_issue_cert_not_allowed_to_issue     974ms
✓ #8  test_mtls_issue_cert_without_cert             263ms
✓ #15 test_mtls_issue_oneline_csr                     2ms
```



Non compliant AWS Config resource

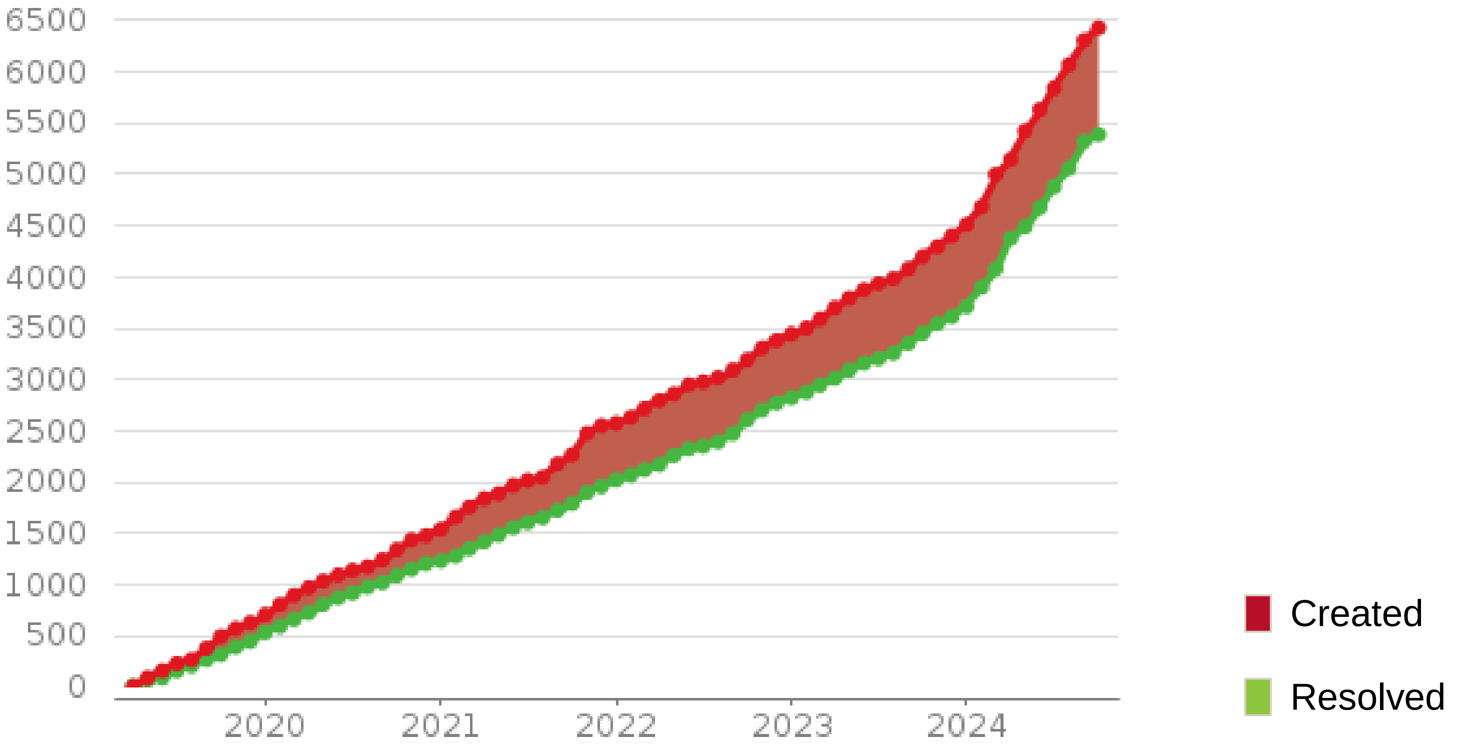
○ **aws-config@connect.axis.com <aws-config@connect.axis.com>**

Till: ○ connect-bolbe

Action required, the following config rule has turned non-compliant

ConfigRuleName: s3_bucket_ssl_requests_only
ResourceType: AWS::S3::Bucket

Security improvements identified by Axis teams



AXIS COMMUNICATIONS