
nuvibit
cloud foundation

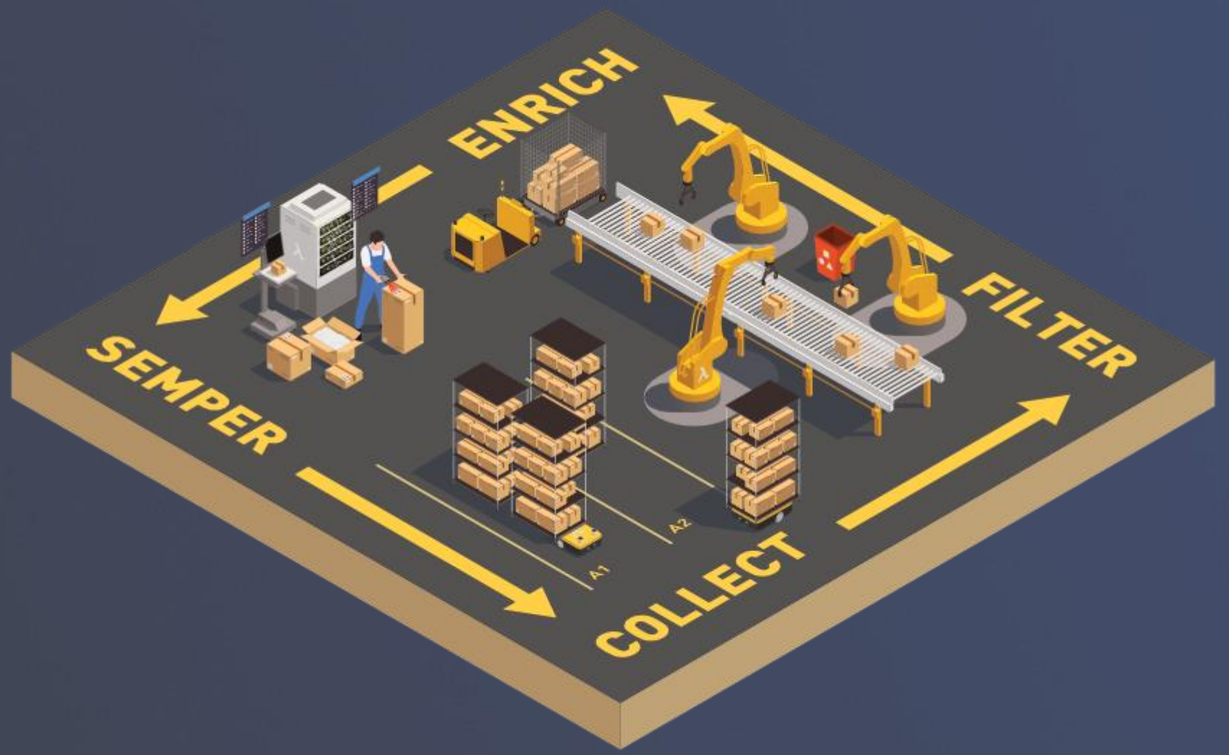
aws partner network

Select
Consulting Partner

Public Sector Partner

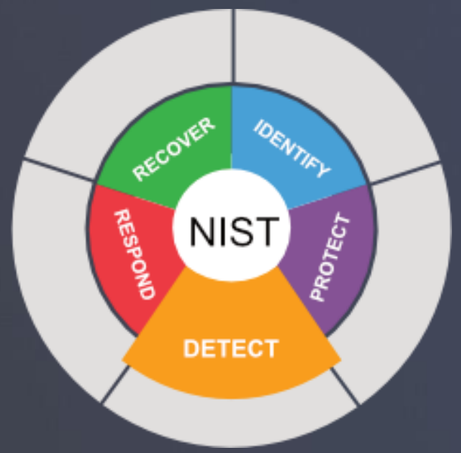
# Nuvibit SEMPER

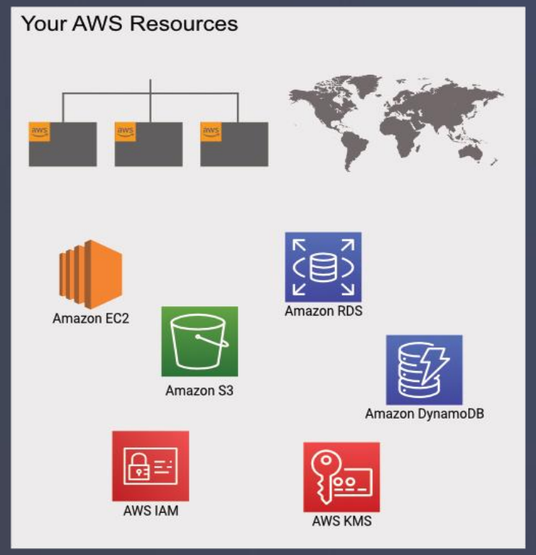
AWS Native Security Finding Management



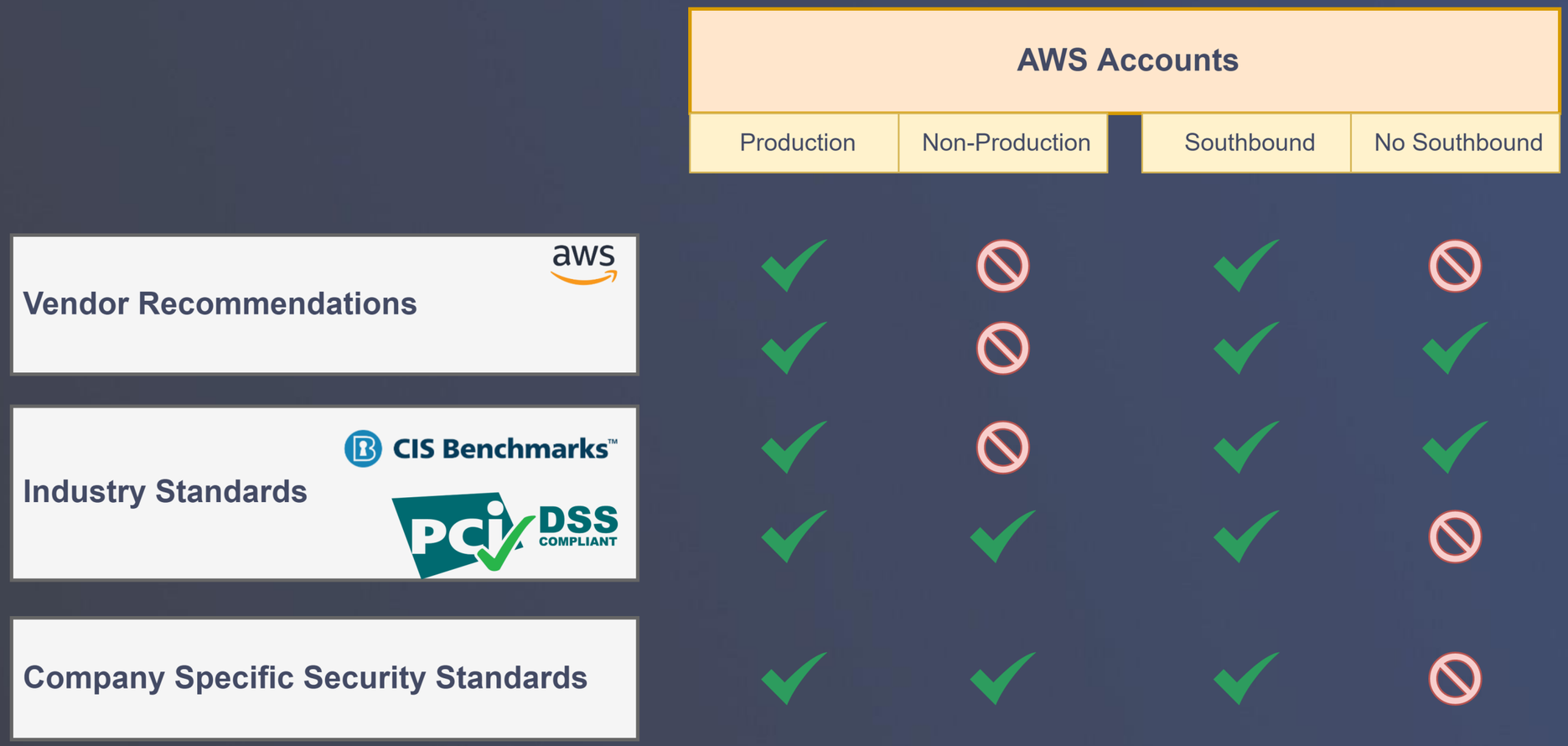
# Are your Workloads spread across multiple AWS Accounts or even AWS Regions?

# How to measure Compliance and detect Security Events of your important AWS resources?




# Your AWS Accounts are heterogeneous!
# You need good Tailoring!

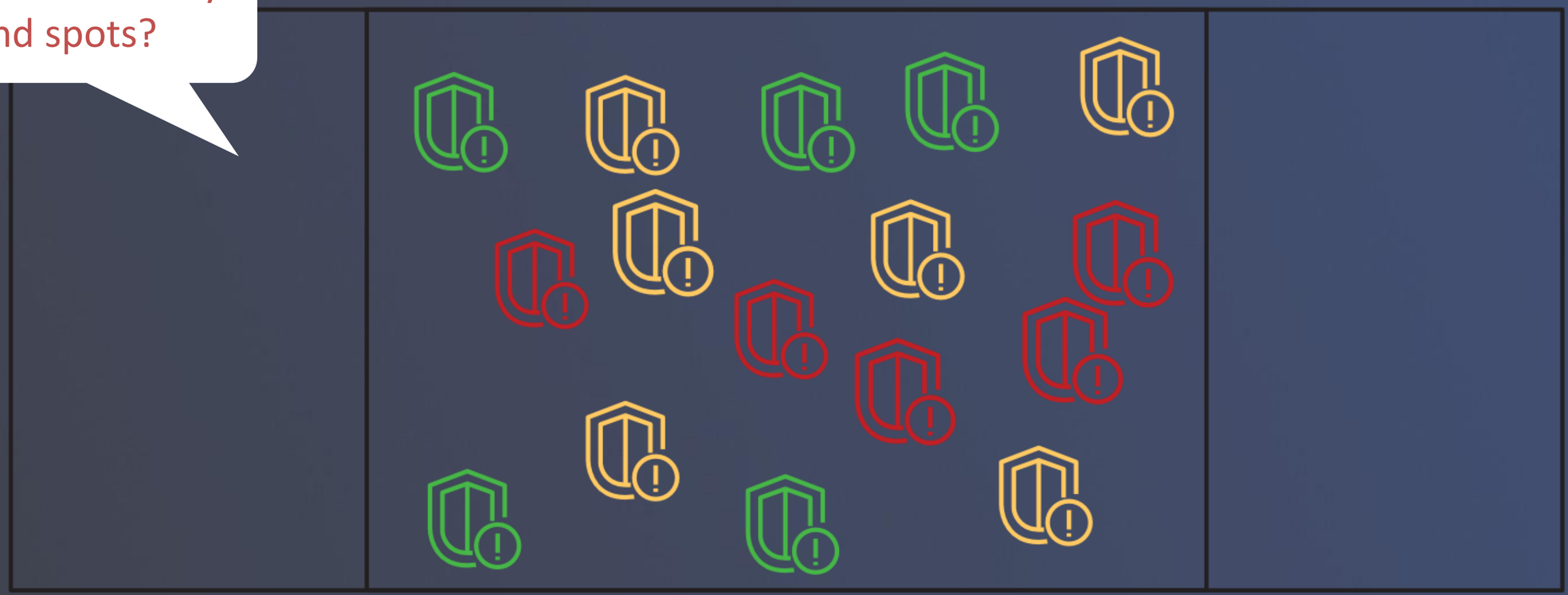



1. AWS Foundational Security Best Practices standard
2. CIS AWS Foundations Benchmark controls
3. PCI DSS controls

nuvibit cloud foundation

# ...but there is still a lot of room for improvement!

How can I cover my blind spots?



nuvibit cloud foundation

# ...but there is still a lot of room for improvement!

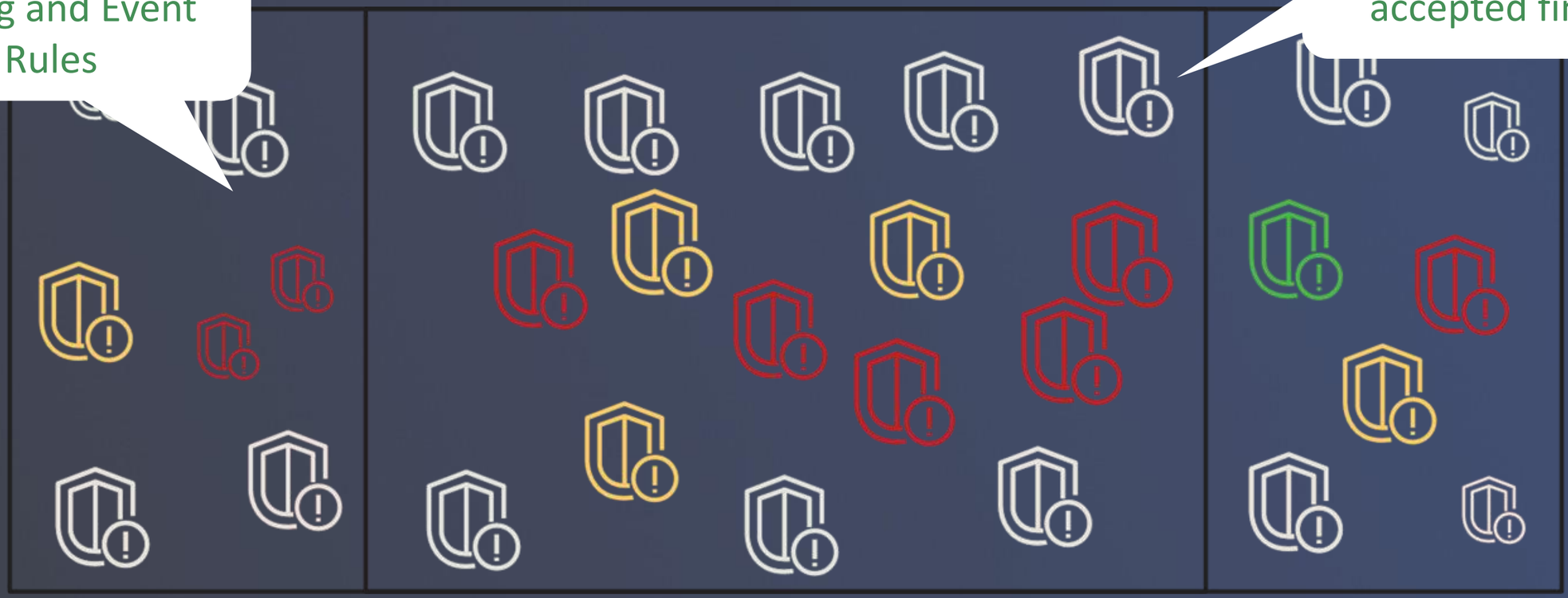

nuvibit cloud foundation

# ...but there is still a lot of room for improvement!

# ...but there is still a lot of room for improvement!

Close gaps with Config and Event Rules

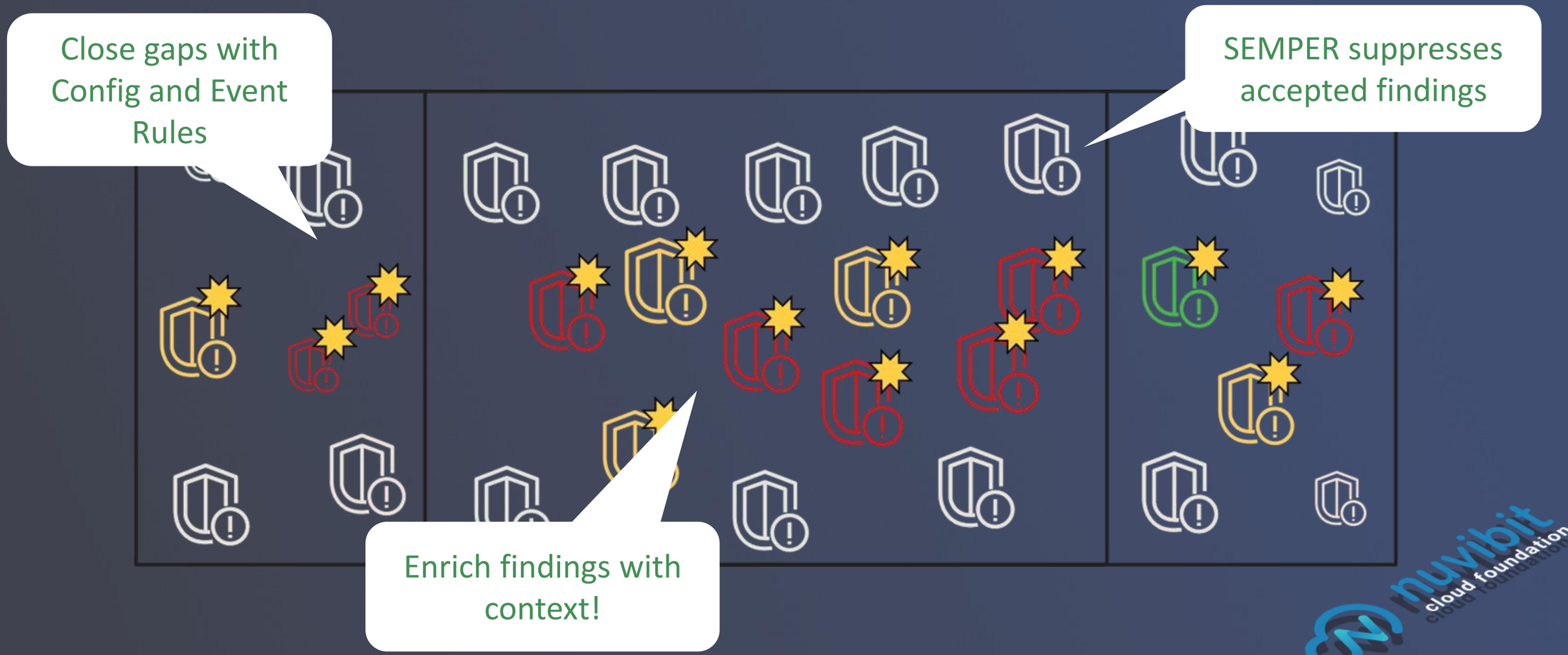
SEMPER suppresses accepted findings



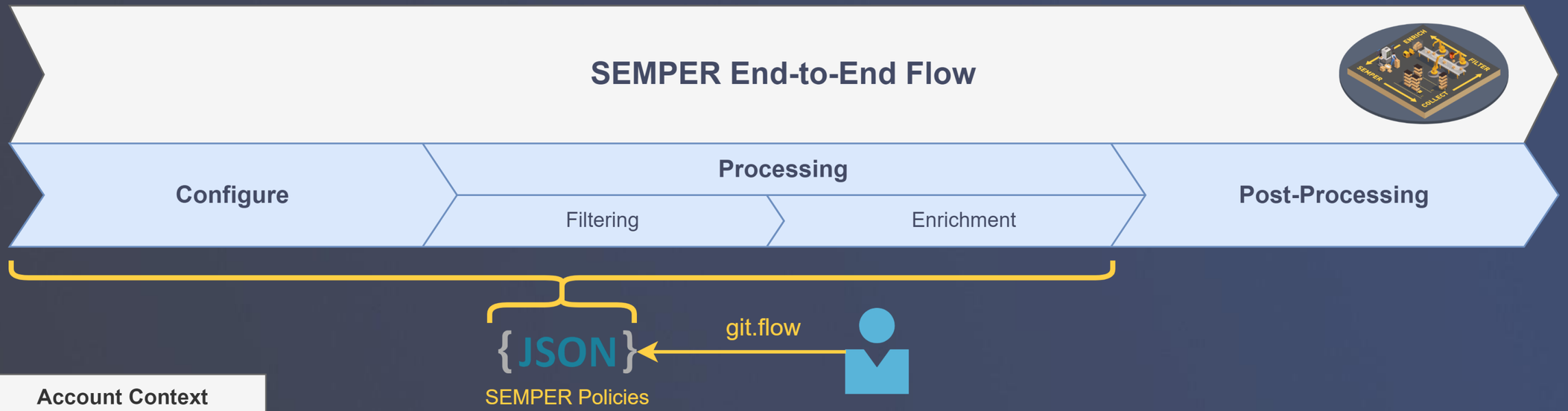
nuvibit cloud foundation

# ...but there is still a lot of room for improvement!

# Now your Cloud SOC loves you!



# Your Success Factor: Security / Policy as Code




**Account Context**
ID, OU-ID, Account-Tags

**AWS Region Context**

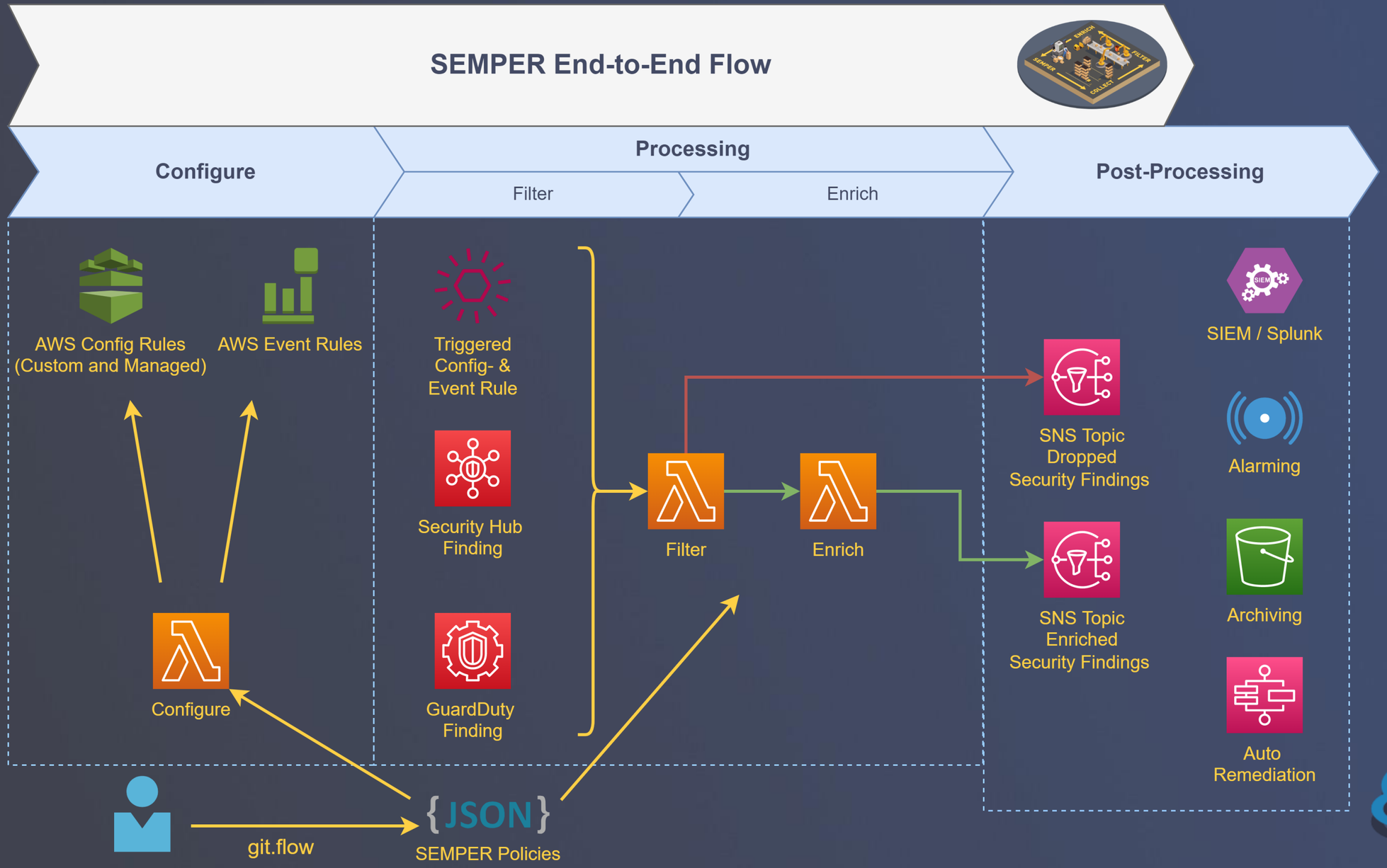
Context-Driven Configuration and Processing

[Nuvibit SEMPER Policy Documentation]

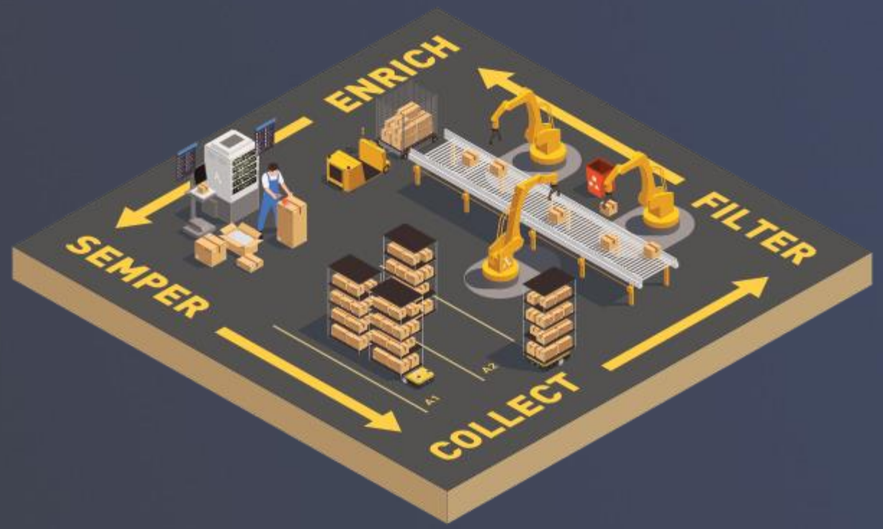
Because it is the most effective approach to securing cloud workloads with speed and agility!

1. McKinsey - Security as code: The best (and maybe only) path to securing cloud applications and systems
2. Gartner - Using Cloud-Native 'Policy as Code' to Secure Deployments at Scale

# Let’s dive slightly deeper



# SEMPER in a nutshell




1. **Collect** findings for your blind spots
2. **Filter** unnecessary findings
3. **Enrich** your findings with context

**Manage everything in a single central Policy as a Code repository!**

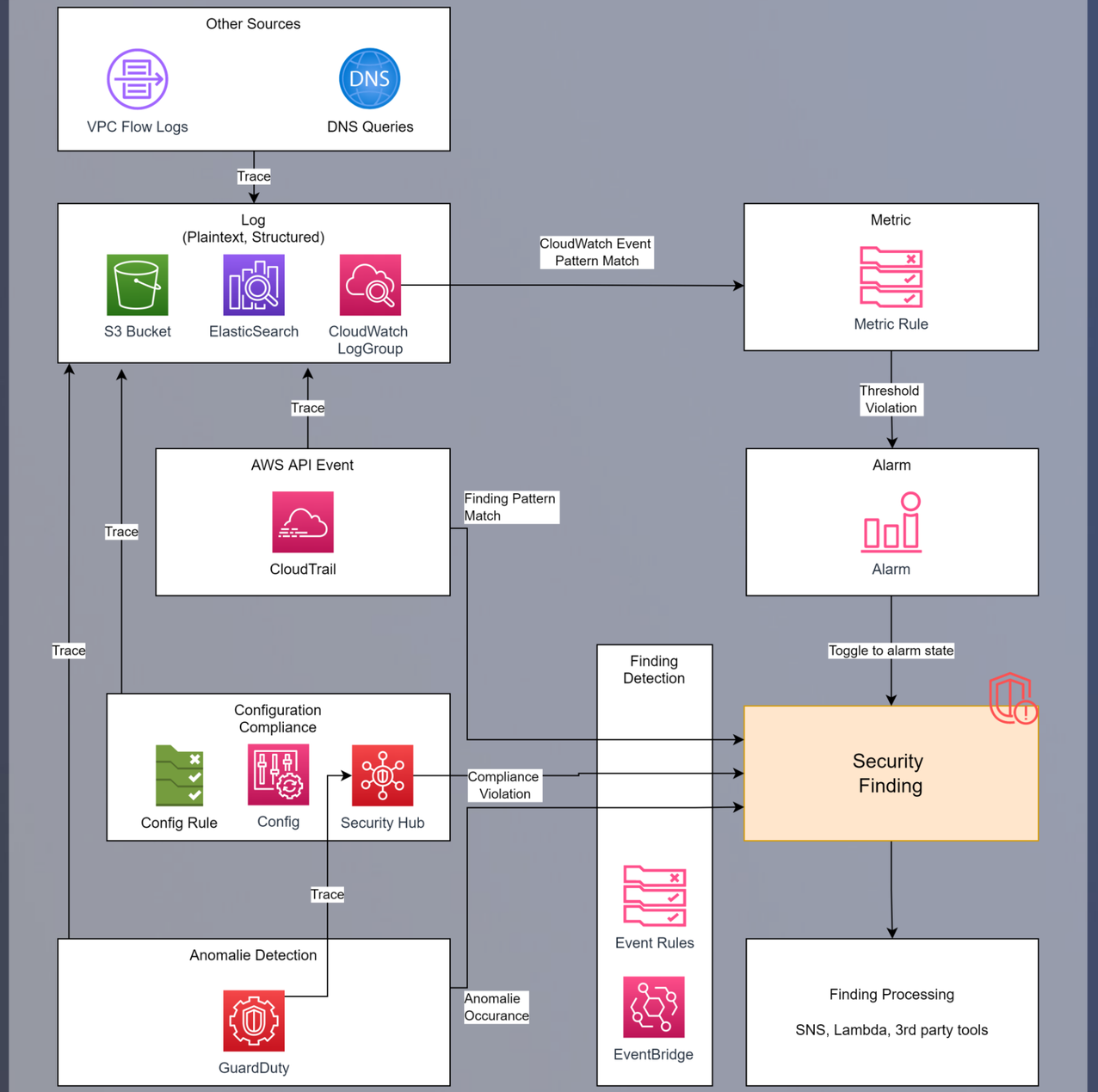
nuvibit cloud foundation

# Thank You!

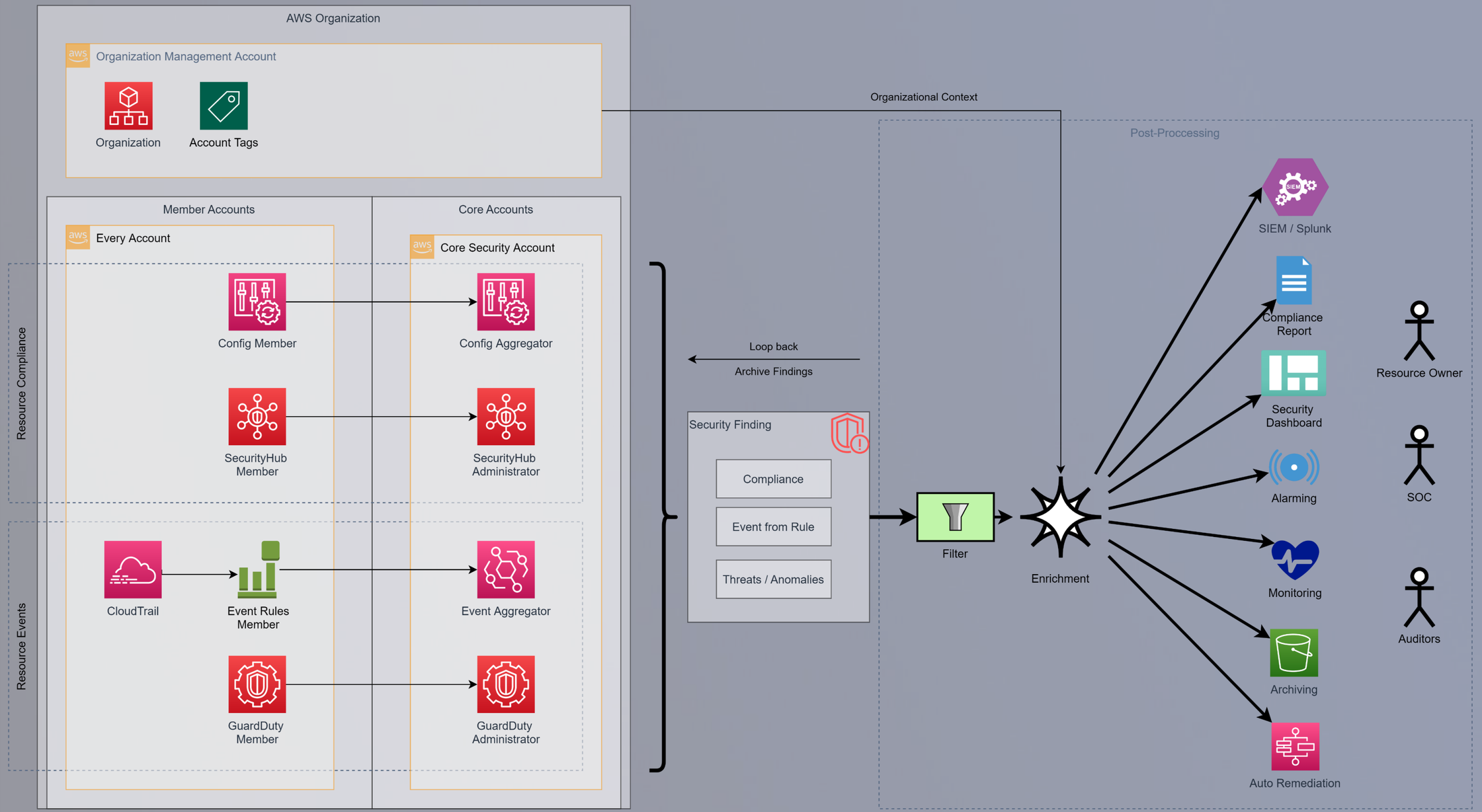

nuvibit
cloud foundation

# Appendix

# Security Finding Model



# Security Finding Management Reference Architecture




Author: Nuvibit AG
Version: 0.1

# CIS AWS 3.x Controls

- 3.1 Monitor for unauthorized API calls
- 3.2 Monitor for AWS Management Console sign-in without MFA
- 3.3 Monitor for usage of root account
- 3.5 Monitor for CloudTrail configuration changes
- 3.6 Monitor for AWS Management Console authentication failures
- 3.7 Monitor for disabling or scheduled deletion of customer created CMKs
- 3.8 Monitor for S3 bucket policy changes
- 3.9 Monitor for AWS Config configuration changes
- 3.10 Monitor for security group changes
- 3.11 Monitor for changes to Network Access Control Lists (NACL)
- 3.12 Monitor for changes to network gateways
- 3.13 Monitor for route table changes
- 3.14 Monitor for VPC changes

Control Details

Nuvibit Blog Post

```
{
    "finding": {
        "sourceService": "AwsCloudTrail",
        "time": "2022-01-20T20:46:26Z",
        "raw": {
            "version": "0",
            "id": "e67b423d-11fe-3cdd-5f3e-996100e39e36",
            "detail-type": "AWS API Call via CloudTrail",
            "source": "aws.kms",
            "account": "626708301729",
            "time": "2022-01-20T20:46:26Z",
            "region": "eu-central-1",
            "resources": [],
            "detail": {
                "eventVersion": "1.08",
                "userIdentity": {
                    "type": "AssumedRole",
                    "principalId": "AROAZD2VZY6QQWB4D7CX6:semper@nuvibit.com",
                    "arn": "arn:aws:sts::626708301729:assumed-role/AWSReservedSSO_AdministratorAccess_1f51a532758ff888/semp
                    "accountId": "626708301729",
                    "accessKeyId": "ASIAZD2VZY6QSRIMENEC",
                    "sessionContext": {
                        "sessionIssuer": {
                            "type": "Role",
                            "principalId": "AROAZD2VZY6QQWB4D7CX6",
                            "arn": "arn:aws:iam::626708301729:role/aws-reserved/sso.amazonaws.com/eu-central-1/AWSReservedS
                            "accountId": "626708301729",
                            "userName": "AWSReservedSSO_AdministratorAccess_1f51a532758ff888"
                        },
                        "webIdFederationData": {},
                        "attributes": {
                            "creationDate": "2022-01-20T20:13:01Z",
                            "mfaAuthenticated": "false"
                        }
                    }
                },
                "eventTime": "2022-01-20T20:46:26Z",
                "eventSource": "kms.amazonaws.com",
                "eventName": "DisableKey",
                "awsRegion": "eu-central-1",
                "sourceIPAddress": "1.2.3.4",
                "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.
                "errorCode": "KMSInvalidStateException",
                "errorMessage": "arn:aws:kms:eu-central-1:626708301729:key/ab9508d2-1f91-4090-945a-5894b1a082eb is pending
                "requestParameters": {
                    "keyId": "ab9508d2-1f91-4090-945a-5894b1a082eb"
                },
                "responseElements": null,
                "requestID": "a19215dc-e53d-49d2-a359-2f9a7962a22d",
                "eventID": "c228fa45-174c-4624-ac73-363530327457",
                "readOnly": false,
                "resources": [
                    {
                        "accountId": "626708301729",
                        "type": "AWS::KMS::Key",
                        "ARN": "arn:aws:kms:eu-central-1:626708301729:key/ab9508d2-1f91-4090-945a-5894b1a082eb"
                    }
                ],
                "eventType": "AwsApiCall",
                "managementEvent": true,
                "recipientAccountId": "626708301729",
                "eventCategory": "Management",
                "tlsDetails": {
                    "tlsVersion": "TLSv1.2",
                    "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
                    "clientProvidedHostHeader": "kms.eu-central-1.amazonaws.com"
                },
                "sessionCredentialFromConsole": "true"
            }
        }
    },
    "accountContext": {
        "accountId": "626708301729",
        "ouId": "ou-srnr-lwyhsa9c",
        "accountTags": {
            "account_email": "accounts+aws-c1-security@nuvibit.com",
            "environment": "nonprod",
            "recycled": "false",
            "account_name": "aws-c1-security",
            "share_remote_state": "false",
            "title": "security account - customer1 stage",
            "account_owner": "semper@nuvibit.com",
            "tenant": "customer1",
            "tfc_execution_mode": "remote"
        }
    }
}
```



```
{
  "finding": {
    "sourceService": "AwsSecurityHub",
    "time": "2022-01-19T09:20:46Z",
    "raw": {
      "version": "0",
      "id": "3af15e19-19c3-3a4c-5e77-c64e4ba49d42",
      "detail-type": "Security Hub Findings - Imported",
      "source": "aws.securityhub",
      "account": "626708301729",
      "time": "2022-01-19T09:20:46Z",
      "region": "eu-central-1",
      "resources": [
        "arn:aws:securityhub:eu-central-1::product/aws/securityhub/arn:aws:securityhub:eu-central-1:626708301729:subscri
      ],
      "detail": {
        "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
        "Types": [
          "Software and Configuration Checks/Industry and Regulatory Standards/AWS-Foundational-Security-Best-Practice
        ],
        "Description": "This AWS control checks whether your AWS account is enabled to use hardware multi-factor authent
        "Compliance": {
          "Status": "FAILED"
        },
        "ProductName": "Security Hub",
        "FirstObservedAt": "2022-01-14T21:20:14.018Z",
        "CreatedAt": "2022-01-14T21:20:14.018Z",
        "LastObservedAt": "2022-01-19T09:20:42.632Z",
        "CompanyName": "AWS",
        "FindingProviderFields": {
          "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards/AWS-Foundational-Security-Best-Prac
          ],
          "Severity": {
            "Normalized": 90,
            "Label": "CRITICAL",
            "Product": 90,
            "Original": "CRITICAL"
          }
        },
        "ProductFields": {
          "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0",
          "StandardsSubscriptionArn": "arn:aws:securityhub:eu-central-1:626708301729:subscription/aws-foundational-sec
          "ControlId": "IAM.6",
          "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/IAM.6/remediation",
          "RelatedAWSResources:0/name": "securityhub-root-account-hardware-mfa-enabled-a8ad20fb",
          "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
          "StandardsControlArn": "arn:aws:securityhub:eu-central-1:626708301729:control/aws-foundational-security-best
          "aws/securityhub/ProductName": "Security Hub",
          "aws/securityhub/CompanyName": "AWS",
          "Resources:0/Id": "arn:aws:iam::626708301729:root",
          "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/securityhub/arn:aws:securityhub:
        },
        "Remediation": {
          "Recommendation": {
            "Text": "For directions on how to fix this issue, consult the AWS Security Hub Foundational Security Bes
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.6/remediation"
          }
        },
        "SchemaVersion": "2018-10-08",
        "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/IAM.6",
        "RecordState": "ACTIVE",
        "Title": "IAM.6 Hardware MFA should be enabled for the root user",
        "Workflow": {
          "Status": "NEW"
        },
        "Severity": {
          "Normalized": 90,
          "Label": "CRITICAL",
          "Product": 90,
          "Original": "CRITICAL"
        },
        "UpdatedAt": "2022-01-19T09:20:38.543Z",
        "WorkflowState": "NEW",
        "AwsAccountId": "626708301729",
        "Region": "eu-central-1",
        "Id": "arn:aws:securityhub:eu-central-1:626708301729:subscription/aws-foundational-security-best-practices/v/1.0
        "Resources": [
          {
            "Partition": "aws",
            "Type": "AwsAccount",
            "Region": "eu-central-1",
            "Id": "AWS:::Account:626708301729"
          }
        ]
      }
    }
  },
  "accountContext": {
    "accountId": "626708301729",
    "ouId": "ou-srnr-lwyhsa9c",
    "accountTags": {
      "account_email": "accounts+aws-c1-security@nuvibit.com",
      "environment": "nonprod",
      "recycled": "false",
      "account_name": "aws-c1-security",
      "share_remote_state": "false",
      "title": "security account - customer1 stage",
      "account_owner": "semper@nuvibit.com",
      "tenant": "customer1",
      "tfc_execution_mode": "remote"
    }
  }
}
```


# Examples of raw Security Finding Messages