AWS re:Invent

SEC357

Turner's Journey to Scale Securely on a Lean Budget

Chris Farris
Cloud Security Architect
Turner Broadcasting, Inc.

Suman Koduri
Sr. Technical Account Manager
AWS Enterprise Support

Damindra Bandara
Security Consultant
AWS Professional Services

AWS re:Invent

aws

Chalktalk repeats

Tuesday, November 27th

Turner’s Journey to Scale Securely on a Lean Budget

3:15pm | Aria East, Level 2, Mariposa 8, T2

Wednesday, November 28th

Turner’s Journey to Scale Securely on a Lean Budget

4pm | Bellagio, Level 1, Grand Ballroom 1, T1

Related breakouts

Thursday, November 29

SEC319 - Meeting Enterprise Security Requirements with AWS Native Security Services

1-2 | Venetian, Level 2, Titian 2204

Tuesday, November 27

SEC303 - Architecting Security & Governance across a Multi-Account Strategy

4:00 – 5:00 | Aria East, Mariposa 5

Thursday, November 29

SEC349 - Governance at Scale

1:45 – 2:45 | MGM Level 3

Survey time

AWS re:Invent

aws

Turner

tbs · TNT · CNN · Boomerang · Cartoon Network · [adult swim] · HLN · truTV · TCM Turner Classic Movies · Turner Sports · b/r

WB Now That's Hollywood! · TCM · Tabi Channel · CHV · WB TV · glitz* · TCM · Toonami · TNT Film · Space · Boing

Much · cartoonito · h2o · Mondo TV · Esporte Interativo · TNT Serie · tooncast · pogo · INF · TNT Comedy · TCM Turner Classic Movies

ohk · CISAT · HBO · TCM cinéma · Eleague · Super Deluxe · Great Big Story · FilmStruck

WarnerMedia

Turner's story

Then

Executive-driven migration
- Lift-and-shift

Limited AWS experience

Automation wasn't our thing

Fewer, bigger accounts

Security was an after-thought

Now

Lots of higher-order services
- Optimization matters

Still varying experience levels

Automation is king

Many AWS Accounts
- Every Account has an accountable VP

Security Standards & Scorecards

Security Challenges

Inventory, Inventory, Inventory

- Who owns what, where is it?

Logging

Threat Detection & Response

Open buckets, open security groups, not a CloudTrail in sight

Tools are really expensive

Tools are hard to deploy

Tools are focused on basic services

Solution?

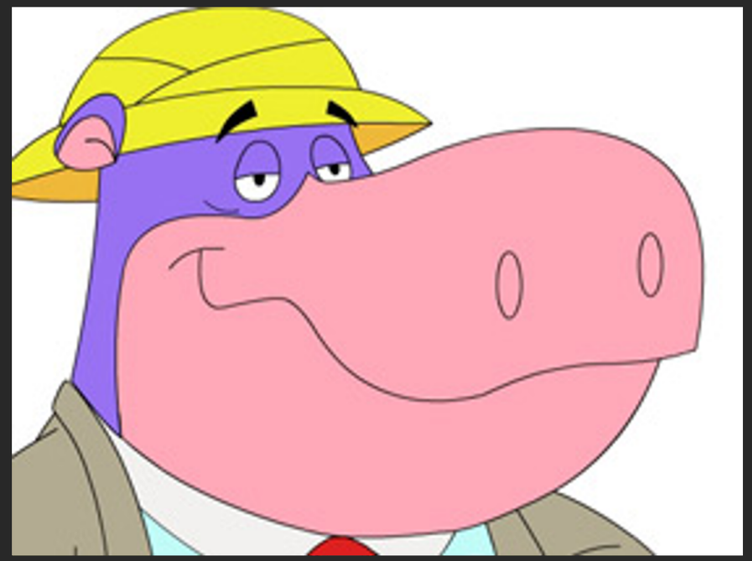
Building Blocks

Organizations
Security Account
CloudFormation
Cross-account role
Lambda & boto3
Step-Functions, SNS, SQS
DynamoDB & S3
Elastic Search

… and a little later
GuardDuty
Cloudwatch Dashboards
CloudSploit
Trusted Advisor

Accountability

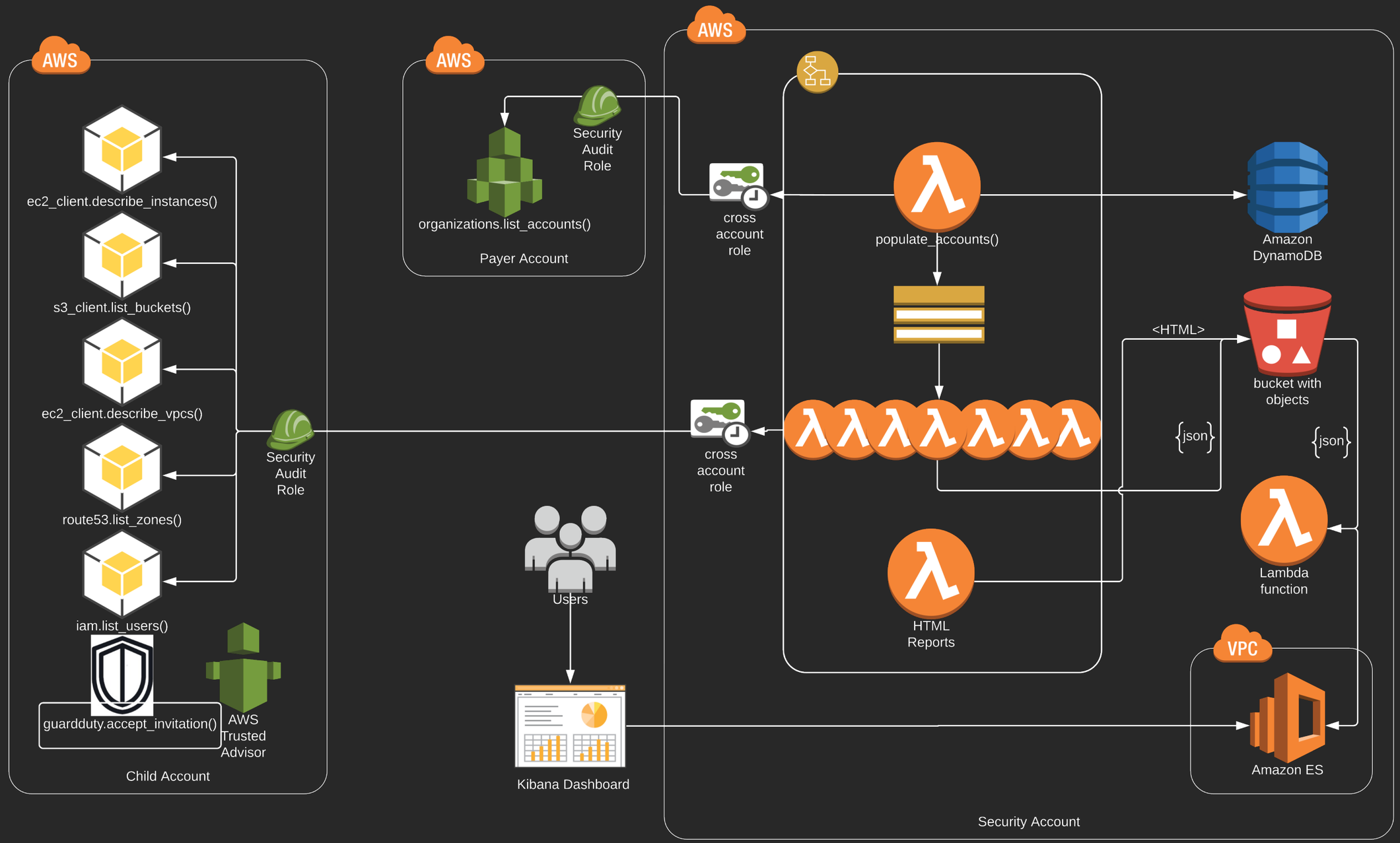
Did ya get that open Security Group I sent you?



Executive Sponsor	Score	Total Spend
Alan Probe	61%	$44,571.21
Carl Brutananadilewski	96%	$46,822.29
Frylock	99%	$1,672.02
Harvey Birdman	99%	$78.89
Ignignokt	83%	$2,114.55
Master Shake	97%	$22,505.57
Meatwad	95%	$93,151.77
Mentok	93%	$1,132,425.64
Peter Potamus	96%	$999.93
Phil Ken Sebben	81%	$4,157.52
Ryu	91%	$10,786.92
Dr. Blake Downs	96%	$27,752.35
Brak	99%	$28,651.99
Space Ghost	100%	$1,554.53
Huey Freeman	90%	$8,602.14
Morty Smith	100%	$97.45
Rick Sanchez	92%	$8,992.38
Summer Smith	93%	$77,998.17
Mr. Meeseeks	84%	$7,436.16
Pickle Rick	91%	$9,659.12
MC Pee Pants	51%	$3,537.44
Peter Potamus	39%	$183,250.56

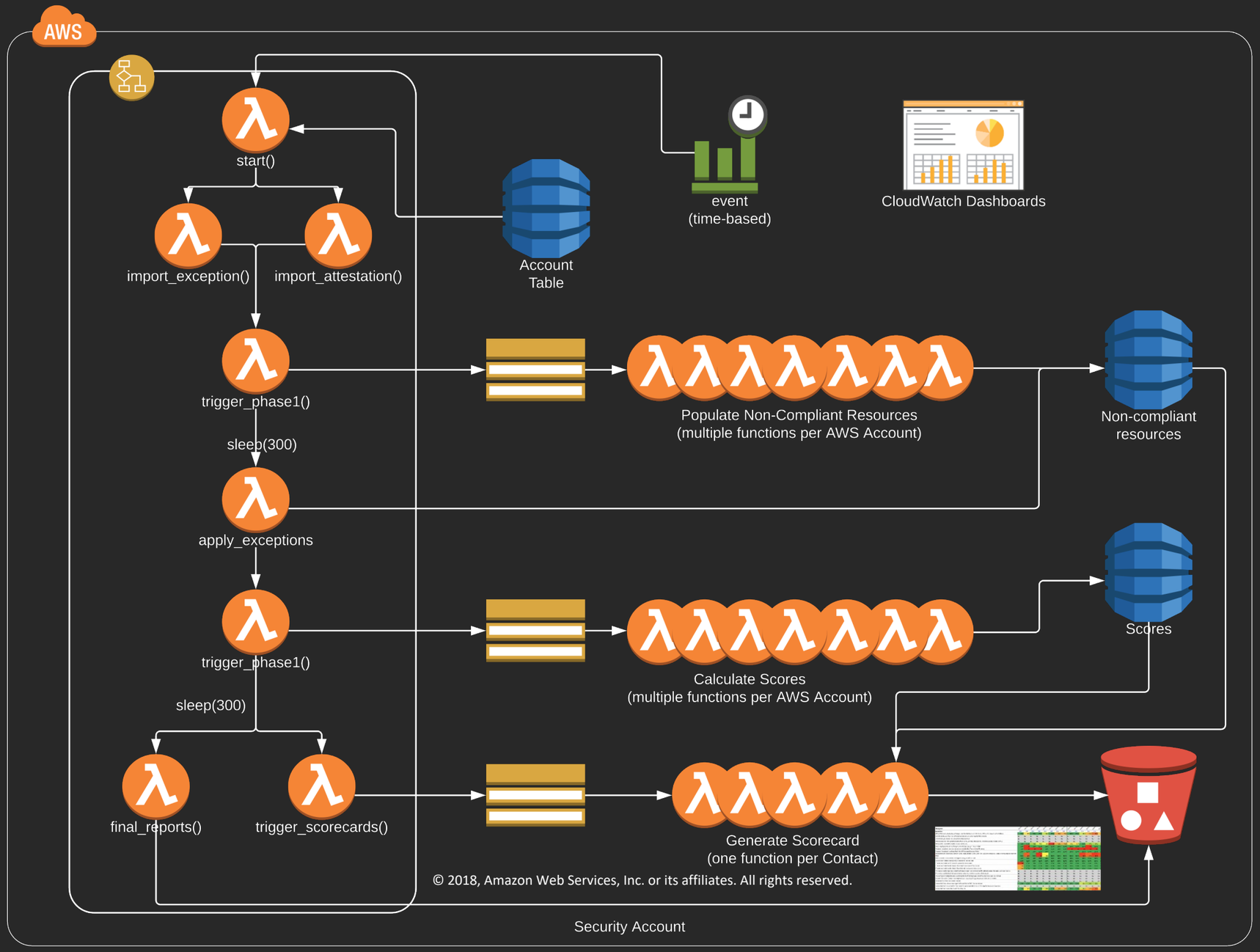
aws

99%	100%	88%	93%	100%	90%	88%	99%	94%	73%	75%	95%	86%	89%	87%	86%	95%	99%	86%	53%	99%	99%	93%	98%	100%	99%	80%	92%	86%	90%	96%	94%	98%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	77%	100%	100%	100%	100%	100%	100%	100%	100%	80%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	0%	100%	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%	100%	100%	75%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	71%	100%	100%	100%	50%	100%	89%	43%	20%	56%	26%	100%	100%	0%	0%	100%	100%	36%	100%	100%	100%	100%	43%	100%	100%	100%	100%	92%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	0%	0%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	0%	0%	100%
100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	QNA	100%	100%	100%	100%	100%	100%	QNA	100%	QNA	100%	100%	100%	100%	100%	100%	QNA	0%	0%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	77%	100%	100%	100%	100%	100%	100%	100%	100%	80%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
0%	75%	50%	83%	96%	88%	88%	0%	67%	33%	0%	94%	79%	11%	89%	56%	96%	80%	70%	8%	91%	90%	87%	0%	75%	0%	83%	85%	60%	50%	80%	75%	90%
100%	100%	100%	100%	100%	100%	100%	100%	100%	50%	100%	95%	47%	50%	56%	41%	100%	100%	67%	0%	100%	100%	49%	100%	100%	100%	100%	64%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	95%	100%	86%	100%	100%	100%	100%	90%	99%	82%	100%	79%	78%	99%	100%	98%	41%	100%	100%	95%	100%	100%	100%	100%	100%	97%	81%	100%	100%	100%
100%	100%	100%	97%	99%	33%	95%	100%	100%	82%	85%	96%	93%	100%	69%	83%	100%	100%	77%	70%	100%	100%	95%	100%	100%	100%	97%	100%	87%	64%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	0%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	0%	50%	80%	60%	80%	0%	100%	100%	100%	100%	0%	0%	67%	100%	100%	100%	100%	100%	83%	100%	50%	100%	0%
100%	100%	0%	50%	100%	100%	0%	100%	100%	100%	100%	50%	20%	60%	20%	100%	100%	100%	100%	0%	100%	100%	33%	0%	100%	100%	100%	67%	50%	100%	100%	100%	100%
100%	100%	0%	50%	100%	100%	0%	100%	60%	100%	100%	76%	38%	69%	63%	65%	100%	100%	51%	0%	97%	100%	94%	100%	100%	100%	100%	71%	38%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	0%	0%	0%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	QNA	100%	100%	0%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	0%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	QNA	100%	100%	0%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	0%	100%	0%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	QNA	100%	100%	0%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	0%	100%	0%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	99%	100%	100%	98%	100%	100%	100%	95%	100%	100%	98%	100%	100%	100%	100%	100%	93%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	QNA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	QNA	100%	100%	100%	100%	100%	100%



COMPLIANCE SCORECARDS

Chris Farris | October 11, 2018



Business Impact

Searchable inventory across 218 accounts in 4 Organizations

Trivial on-boarding of acquired company

100% compliant on MFA

Permissive Security groups locked down

Public S3 buckets identified & tagged

AWS Account creation process nearly 100% automated

Cost: $1k /mo

- Lambda invocations and DynamoDB
- 30min execution frequency

Lessons Learned

API Limits

- AWS was much better than our vendors

~~5 minute timeouts~~

DDB Autoscaling

Lambda sizing

Trusted Advisor is the best open bucket check

CloudTrail Encryption

Remember what is regional

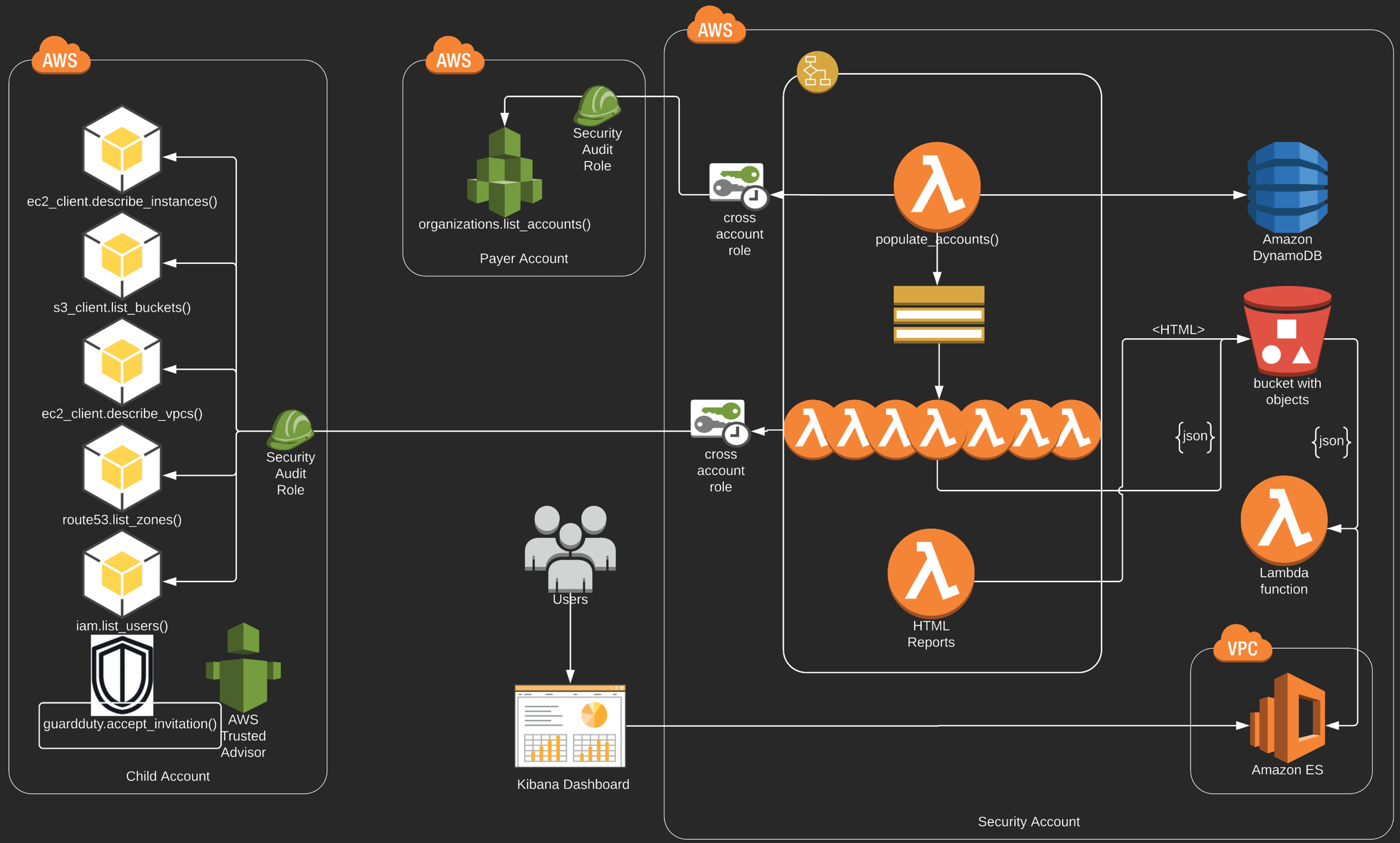
Where we're going next

Opensource all this as Antiope

https://github.com/turnerlabs/antiope

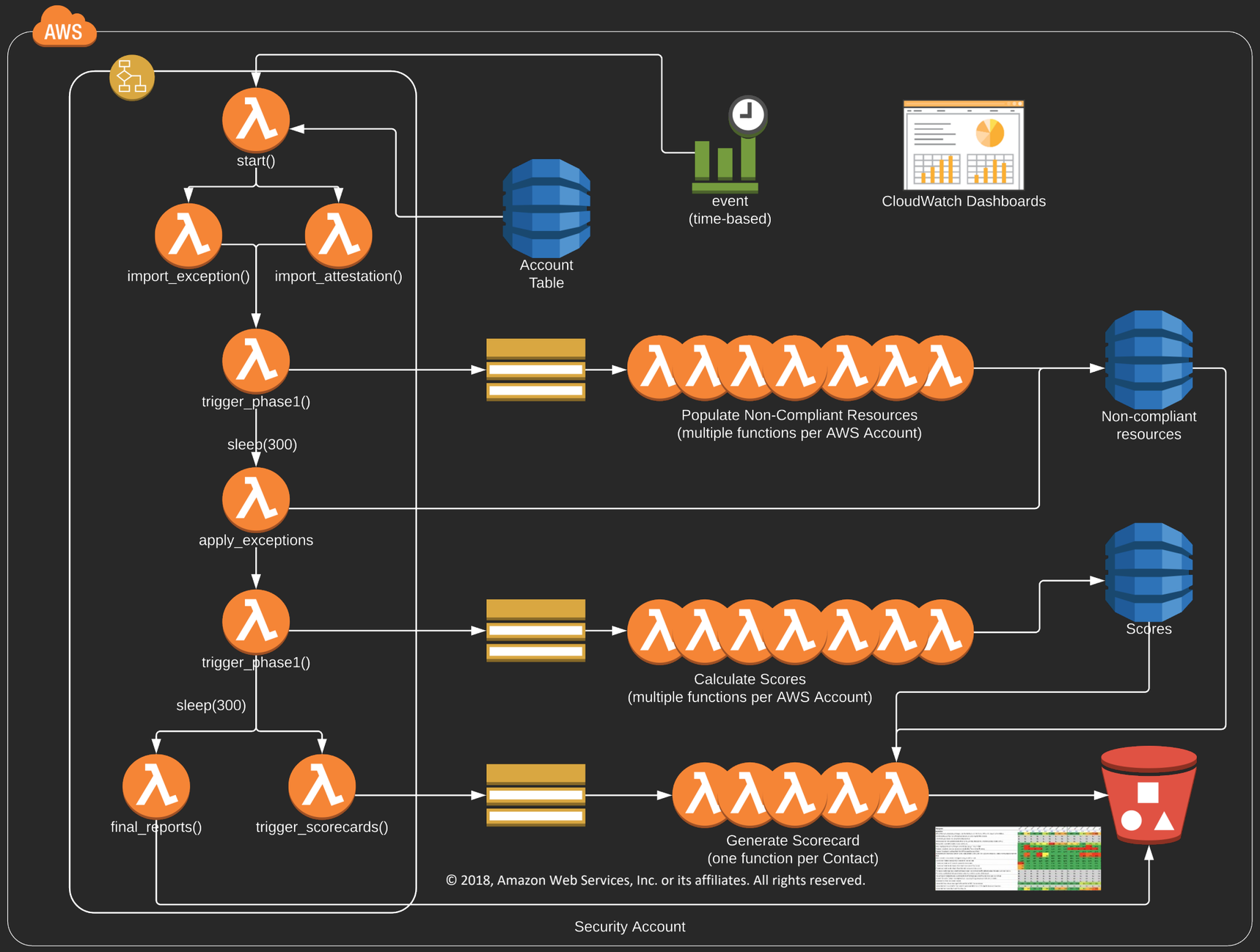
Focus on services that have Resource Policies

Whatever Andy & Werner announce this week!



COMPLIANCE SCORECARDS

Chris Farris | October 11, 2018



Please complete the session survey in the mobile app.

AWS re:Invent

aws

Thank you!

Chris Farris (chris.farris@turner.com)

 @jcfarris

 https://github.com/jchrisfarris

 https://www.linkedin.com/in/jcfarris

 http://www.chrisfarris.com

Suman Koduri (skkoduri@amazon.com)

 @sumankoduri

 https://www.linkedin.com/in/sumankoduri

Damindra Bandara (kbband@amazon.com)

 @Damindra5

 https://www.linkedin.com/in/damindra-bandara-74618a16/

AWS re:Invent

aws

Reference Slides

AWS re:Invent

aws

Spray & Pray

```
my_AccountList = AWSAccountList(inventory_config=config)

for a in my_AccountList.get_active_accounts():
    logger.info("Account: {} ({}) is {}".format(a.account_name, a.account_id, a.account_status))
    if a.account_status == "ACTIVE":
        a.create_contact_record()
        try:
            a.test_cross_account_role(os.environ['DEFAULT_ROLE_NAME'])
        except AssumeRoleError as e:
            logger.error(e)
            continue

        # Now trigger the parallel collection of data
        client = boto3.client('sns')
        message = {}
        message['account_id'] = a.account_id
        response = client.publish(
          TopicArn=os.environ['TRIGGER_ACCOUNT_INVENTORY_ARN'],
          Message=json.dumps(message)
        )

return(event)
```

Spray & Pray

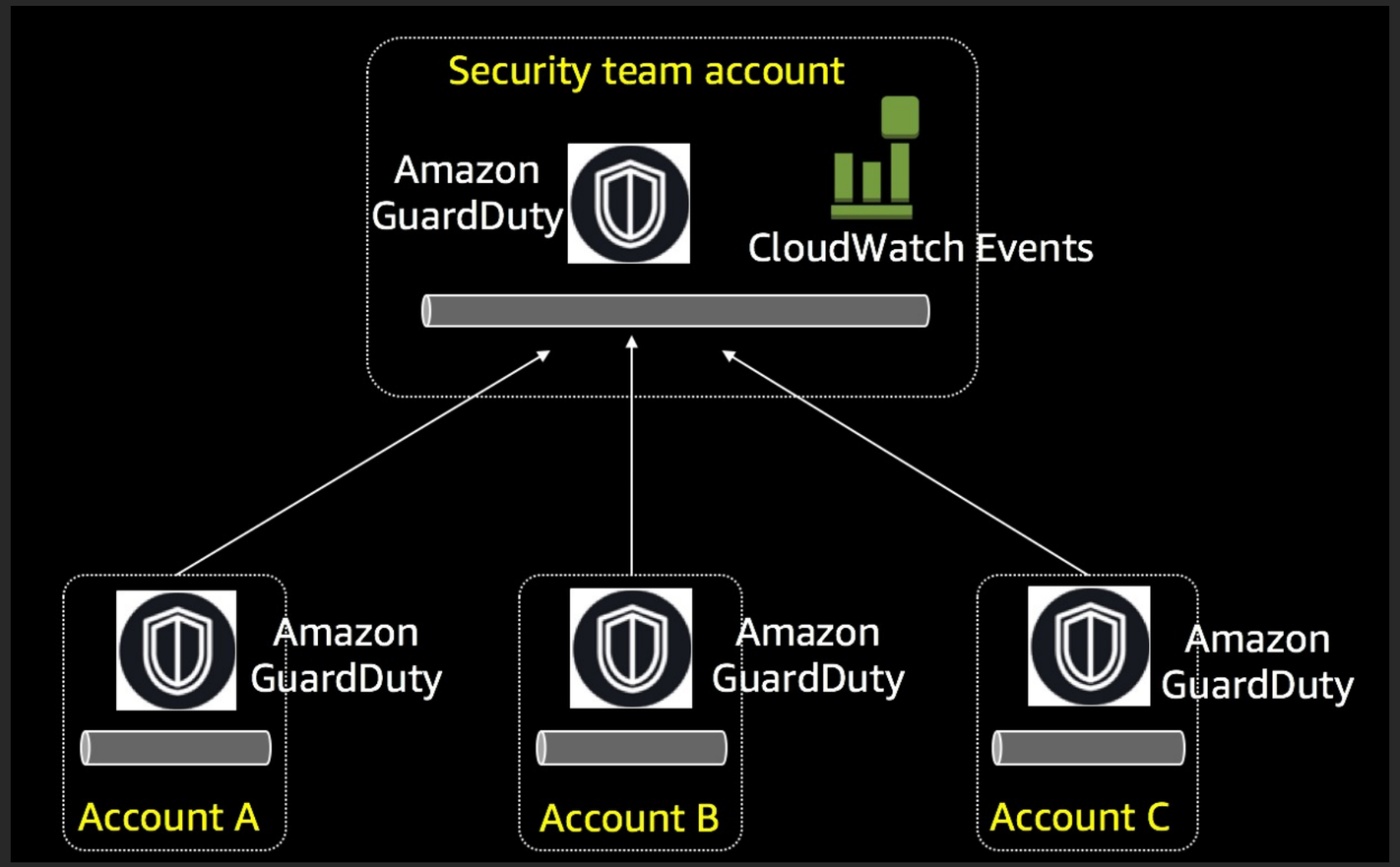
```yaml
TriggerAccountInventoryFunctionTopic:
  Type: AWS::SNS::Topic
  Properties:
    DisplayName: !Sub "Triggers the Inventory of each Account for ${AWS::Sta

EIPInventoryLambdaFunction:
  Type: AWS::Lambda::Function
  Properties:
    FunctionName: !Sub "${AWS::StackName}-eip-inventory"
    Description: AWS Lamdba to to inventory all public IPs in an account
    Handler: inventory_public_ip.lambda_handler
    Runtime: python3.6
    Role: !GetAtt InventoryLambdaRole.Arn
    Code:
      S3Bucket: !Ref pDeployBucket
      S3Key: !Sub ${pLambdaZipFile}

EIPInventoryLambdaFunctionPermission:
  Type: AWS::Lambda::Permission
  Properties:
    FunctionName: !GetAtt EIPInventoryLambdaFunction.Arn
    Principal: sns.amazonaws.com
    SourceArn: !Ref TriggerAccountInventoryFunctionTopic
    Action: lambda:invokeFunction

EIPInventoryTopicToLambdaSubscription:
  Type: AWS::SNS::Subscription
  Properties:
    Endpoint: !GetAtt [EIPInventoryLambdaFunction, Arn]
    Protocol: lambda
    TopicArn: !Ref 'TriggerAccountInventoryFunctionTopic'
```

Cloud Security Standard

```
IAMConsoleMFA:
  description: All IAM Users have MFA enabled for Console Access
  human_section_id: 5.01(b)(i)
  knowledge_source: CloudSploit
  requirement: true
  weight: 100
  CloudSploit:
    Finding: "Users MFA Enabled"
RootAccountUsage:
  description: Root account is not used after initial provisioning of AWS account
  human_section_id: 5.03(a)
  knowledge_source: CloudSploit
  requirement: true
  weight: 10
  CloudSploit:
    PassFail: true
    Finding:
      - "Root Account In Use"
      - "Root Access Keys"
```

Multi Accounts

GuardDuty Multi Account Structure



GuardDuty Findings

Recon
Port probe on unprotected port
Outbound port scans
Callers from anonymizing proxies

Backdoor
Spambot or C&C activity
Exfiltration over DNS channel
Suspicious domain request

Trojan
Domain generation algorithm (DGA) domain request
Blackhole traffic
Drop point

Unauthorized Access
Unusual ISP caller
SSH/RDP brute force

Stealth
Password policy change
AWS CloudTrail logging disabled
Amazon GuardDuty disabled in member account

Cryptocurrency
Communication with bitcoin DNS pools
Cryptocurrency related DNS calls
Connections to bitcoin mining pool

GuardDuty service role permission

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    }
  ]
}
```

Macie

PII and personal data

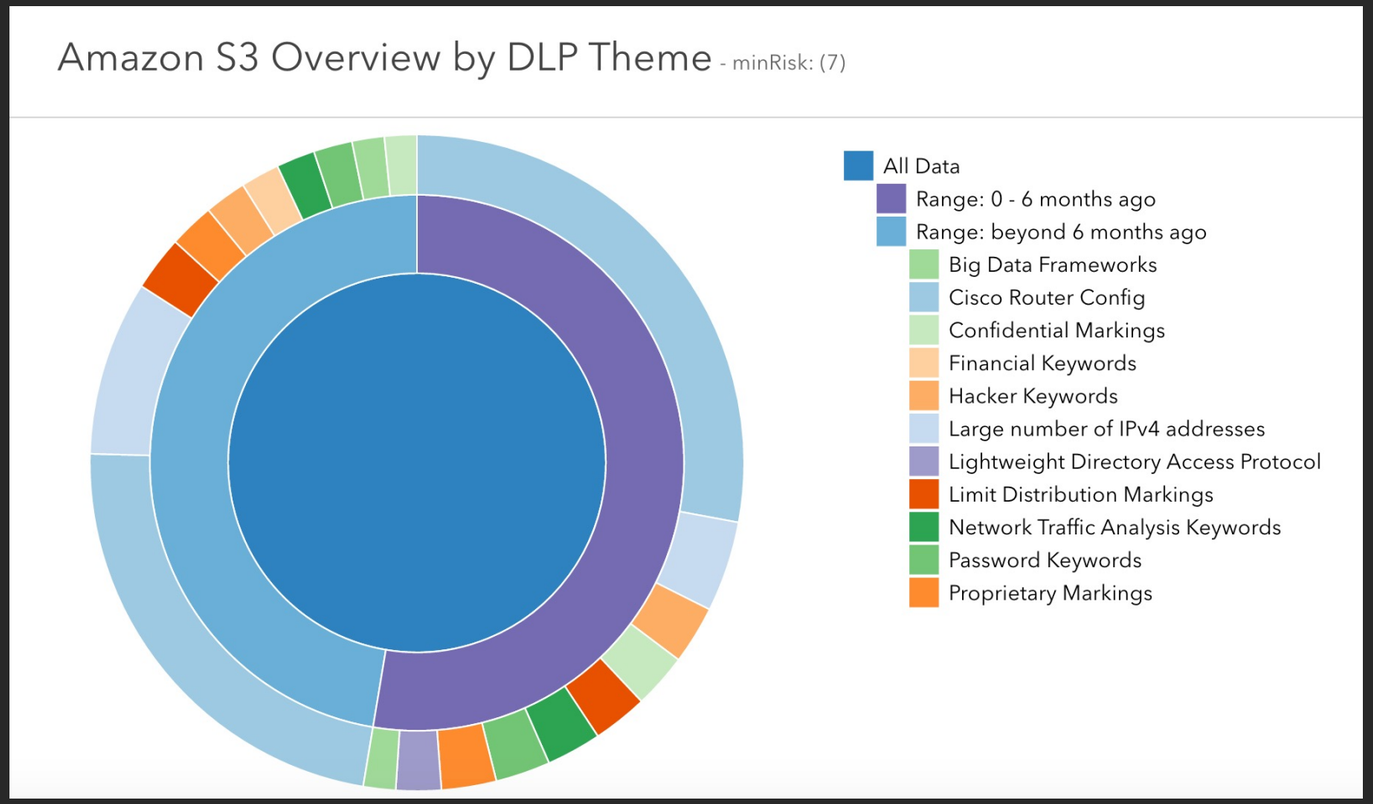
Source code

SSL certificates, private keys

iOS and Android app signing keys

Database backups

OAuth and cloud SaaS API Keys



Enterprise Support

SMEs Cloud Support Engineers, Solutions Architects, and product teams are available for guidance

TECHNICAL ACCOUNT MANAGER (TAM) Designated technical point of contact to all necessary AWS expertise

SUPPORT CONCIERGE Dedicated team of enterprise account specialists to help with billing and account subjects

TRUSTED ADVISOR (TA) Online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment

PERSONAL HEALTH DASHBOARD (PHD) Delivers alerts and remediation guidance when AWS is experience events that may impact your environment

INFRASTRUCTURE EVENT MANAGEMENT (IEM) Focused planning and support business-critical events (e.g. launches or migrations)

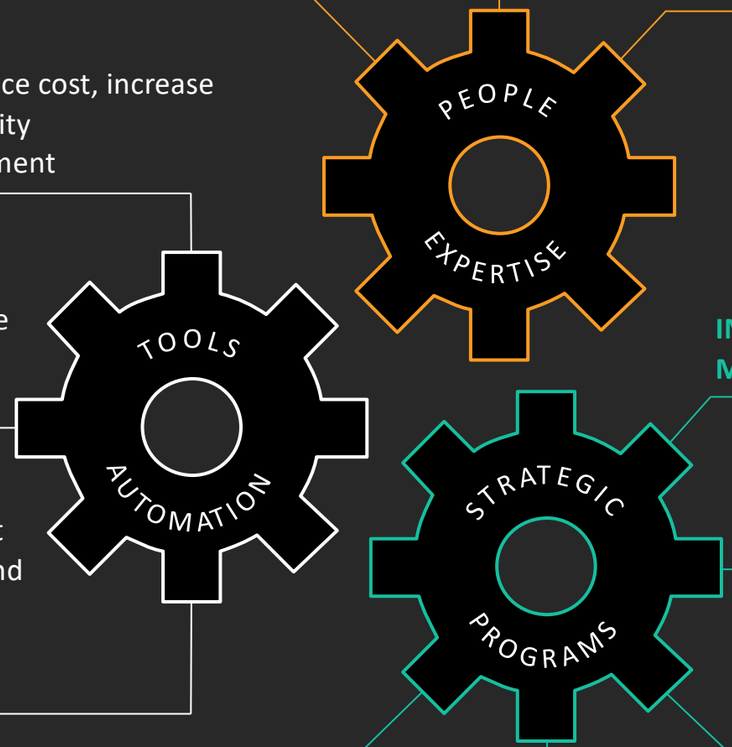
WELL-ARCHITECTED REVIEW Detailed review of your architecture guidance on how to best design your systems

SUPPORT API Programmatic access to AWS Support Center features to create, manage, and close your support cases, and operationally manage your TA check requests and status

ARCHITECTURE SUPPORT Consultative reviews of your application architecture and how to align it with AWS

TRAINING Credits for online self-paced labs provided through an AWS training provider

OPERATIONS SUPPORT Consultative reviews of your cloud operations and advice for optimization



AWS re:Invent

aws