RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **CSV-R07**

Using Automation for Proactive Cloud Incident Response

Ben Potter

Global Security Lead, Well-Architected
Amazon Web Services
@benji_potter

#RSAC

Agenda

- Your Adversary
- Preparation
- Detection & Analysis
- Containment, Eradication & Recovery
- Summary & Application

NO MORE RANSOM!

www.nomoreransom.org

Your Adversary

Motivation

Insider | Outsider | Collaboration

- Entertainment
- Social group
- Ego
- Status
- Cause

Kilger, Stutzman, & Arkin, 2004

Knowledge

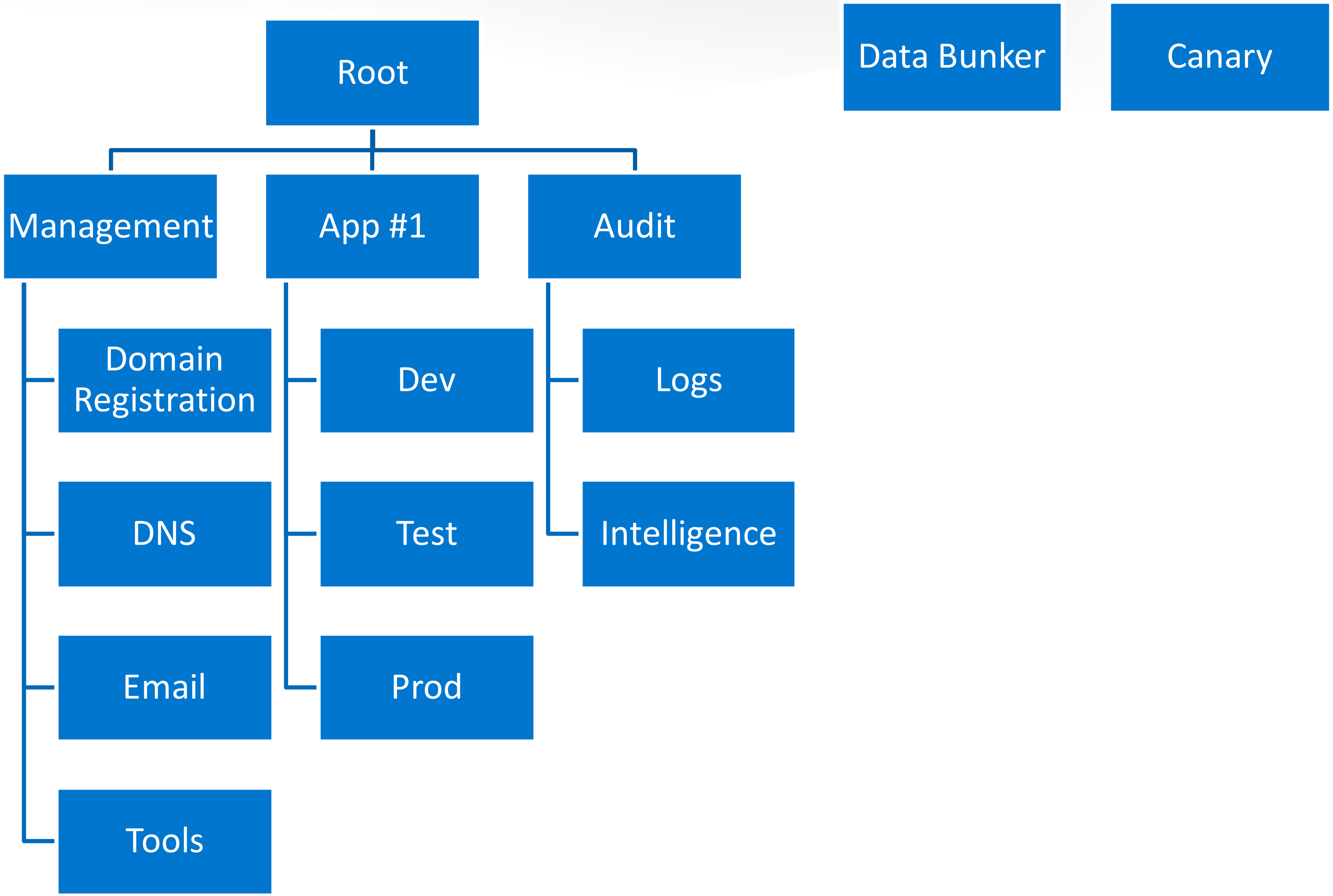
- Insider
  - Knows specifics e.g. storage buckets
  - Goes direct to resources
  - Covers tracks
- Outsider
  - Reconnaissance
  - Fingerprinting
  - May be easily deceived

Preparation

Requirements & Frameworks

- Local, federal laws
- Data breach notification
- Compliance e.g. PCI, HIPAA, GDPR
- Best practices https://aws.amazon.com/well-architected
- Threat model

Cloud account structure



Root

Management

Domain Registration

DNS

Email

Tools

App #1

Dev

Test

Prod

Audit

Logs

Intelligence

Data Bunker

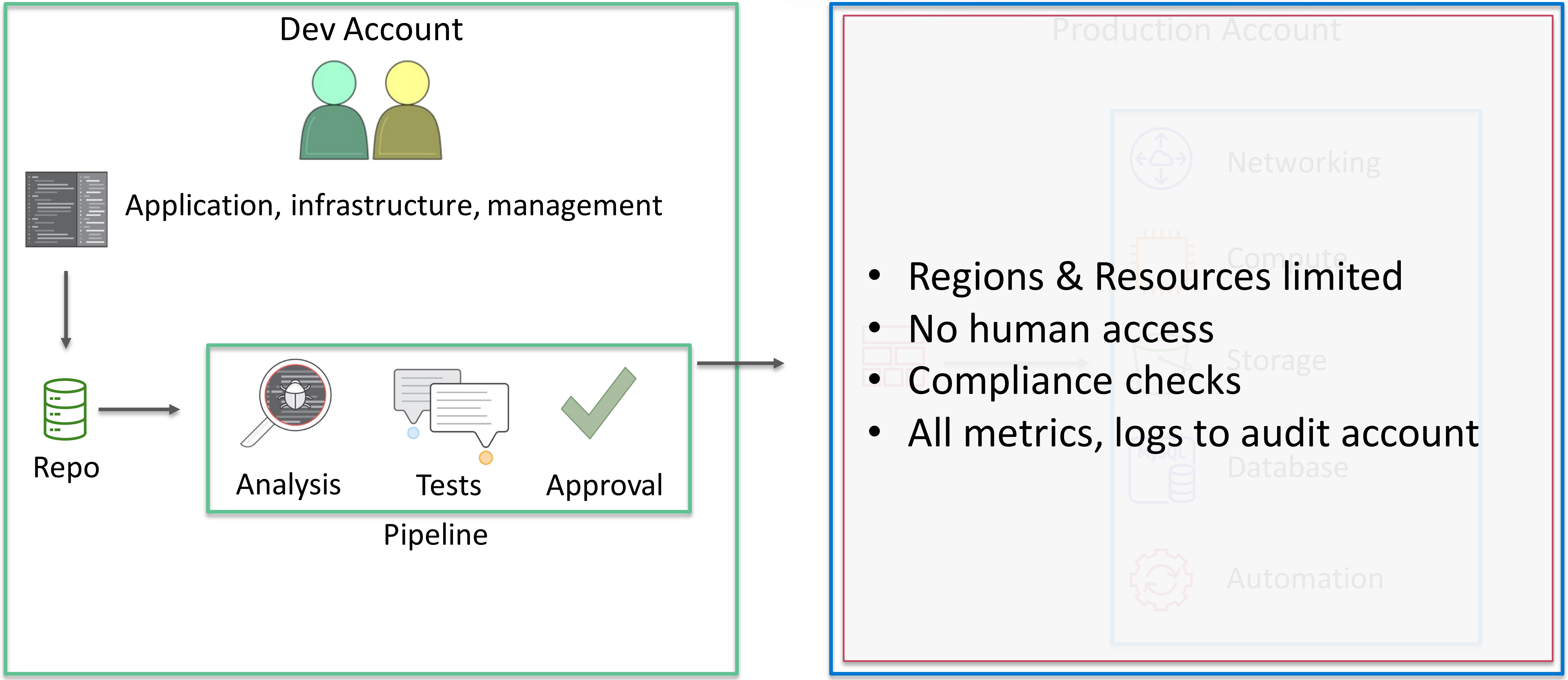
Canary

Access & Credential Management

All Users

- 2FA
- Least privilege
- Dynamic credentials
- Federation

Everything Is Code



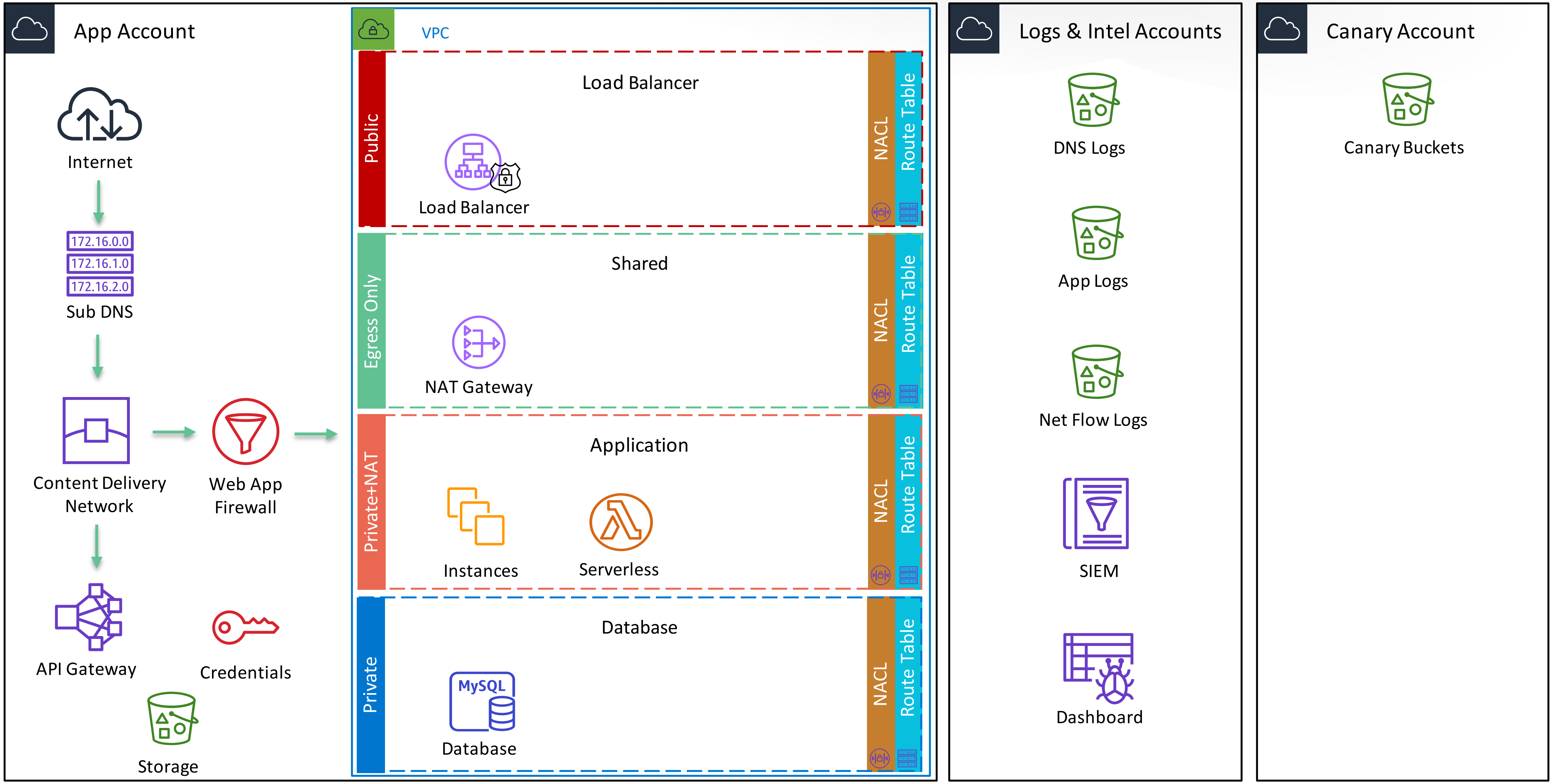
- Regions & Resources limited
- No human access
- Compliance checks
- All metrics, logs to audit account

AWS DevSecOps Blog: https://go.aws/2Fxw89t

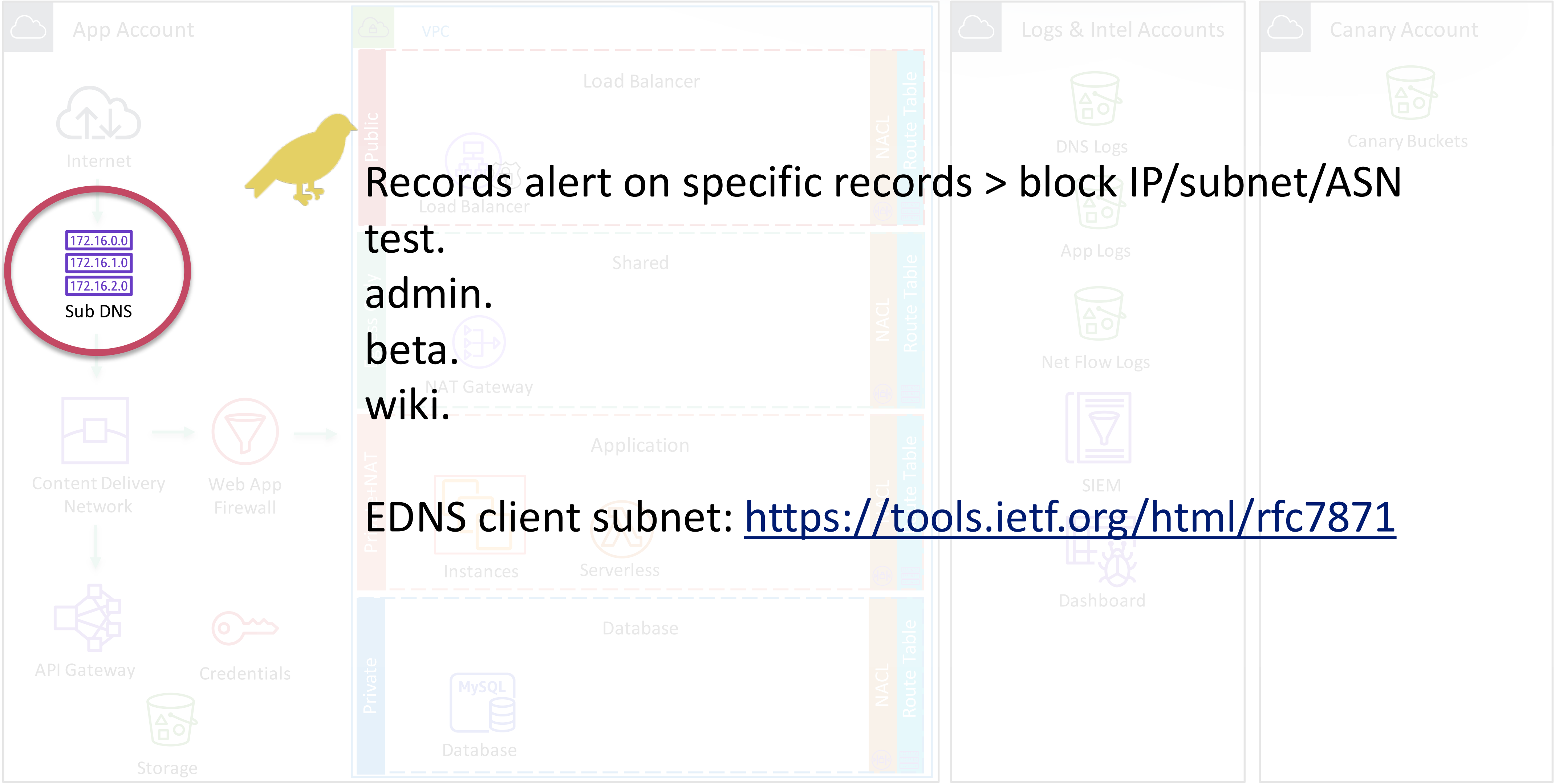
RSAConference2020

Detection & Analysis

Example Application Architecture



DNS Reconnaissance



Records alert on specific records > block IP/subnet/ASN

test.

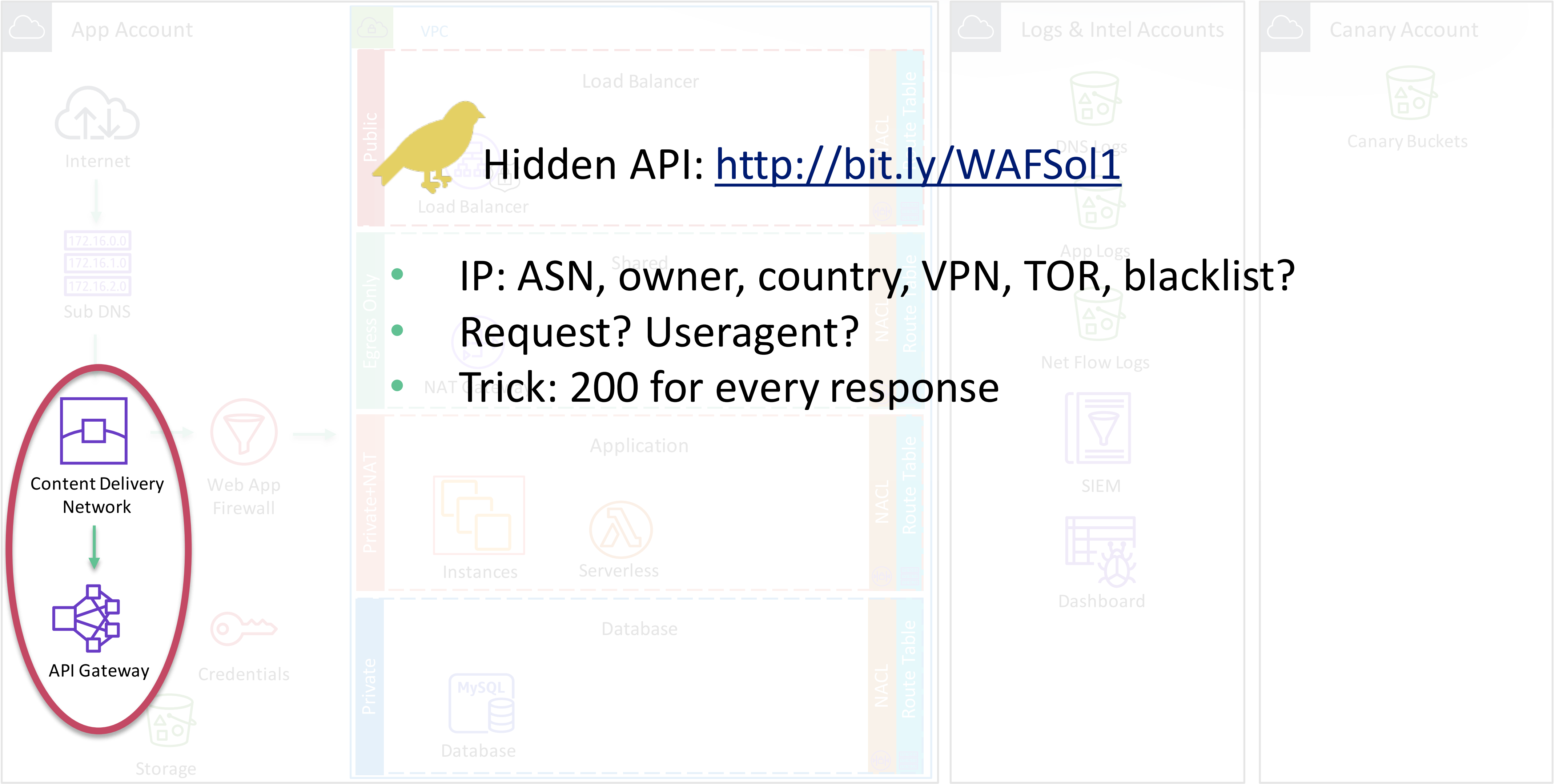
admin.

beta.

wiki.

EDNS client subnet: https://tools.ietf.org/html/rfc7871

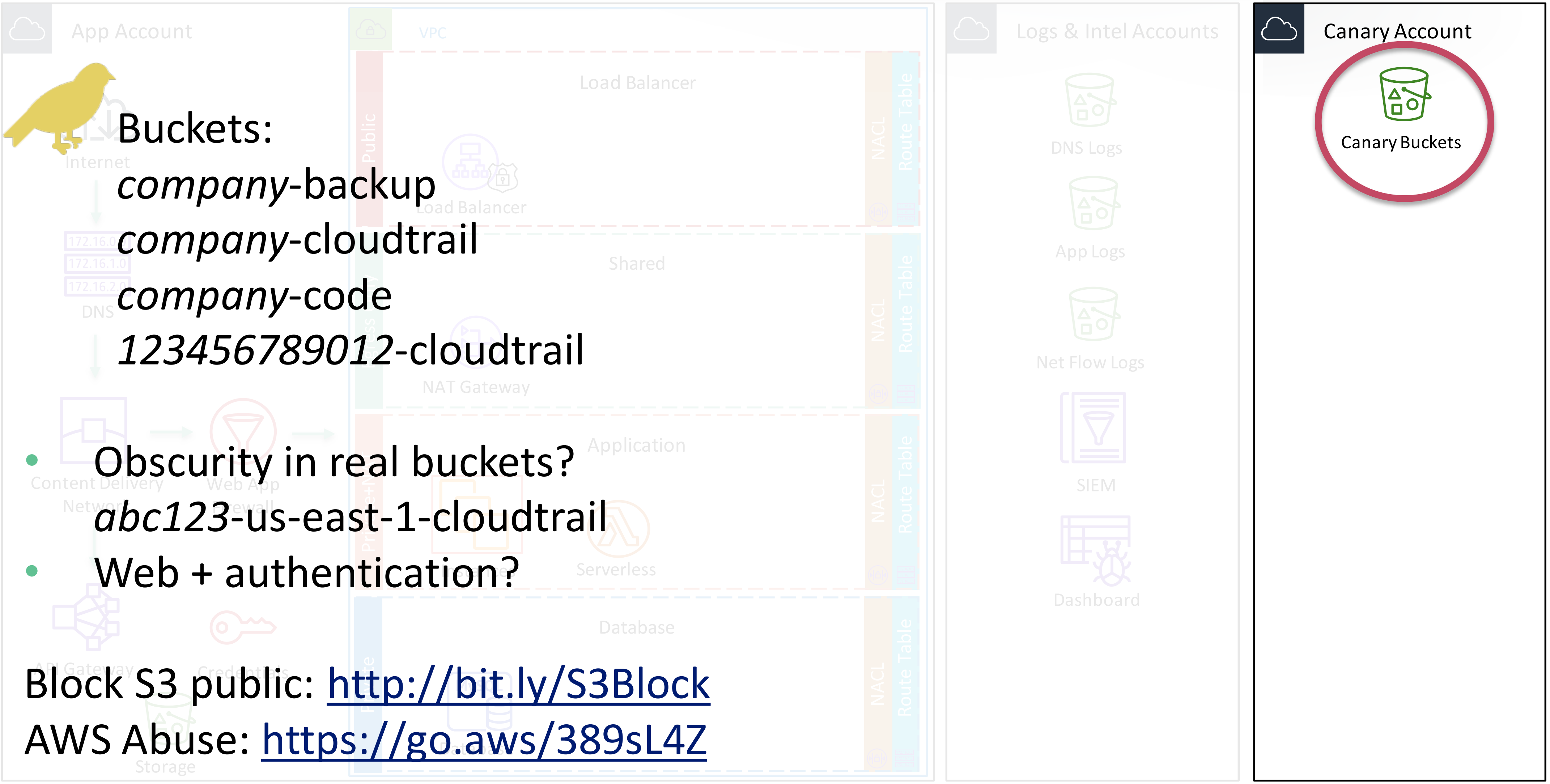
Hidden Honeypot API



Hidden API: http://bit.ly/WAFSol1

- IP: ASN, owner, country, VPN, TOR, blacklist?
- Request? Useragent?
- Trick: 200 for every response

Storage Canaries

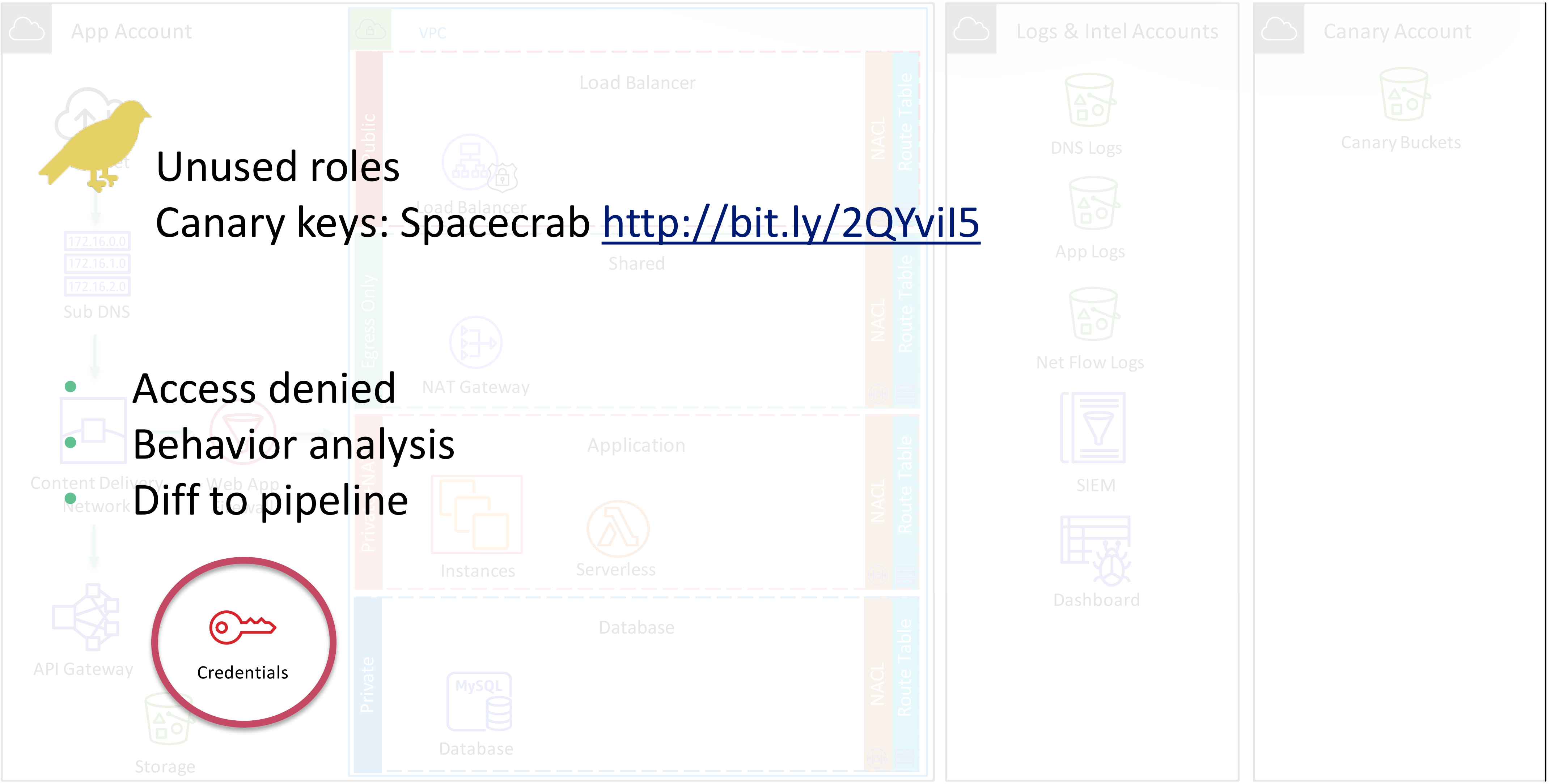


Buckets:
company-backup
company-cloudtrail
company-code
123456789012-cloudtrail

- Obscurity in real buckets?
  abc123-us-east-1-cloudtrail
- Web + authentication?

Block S3 public: http://bit.ly/S3Block
AWS Abuse: https://go.aws/389sL4Z

Identity Canary Tokens

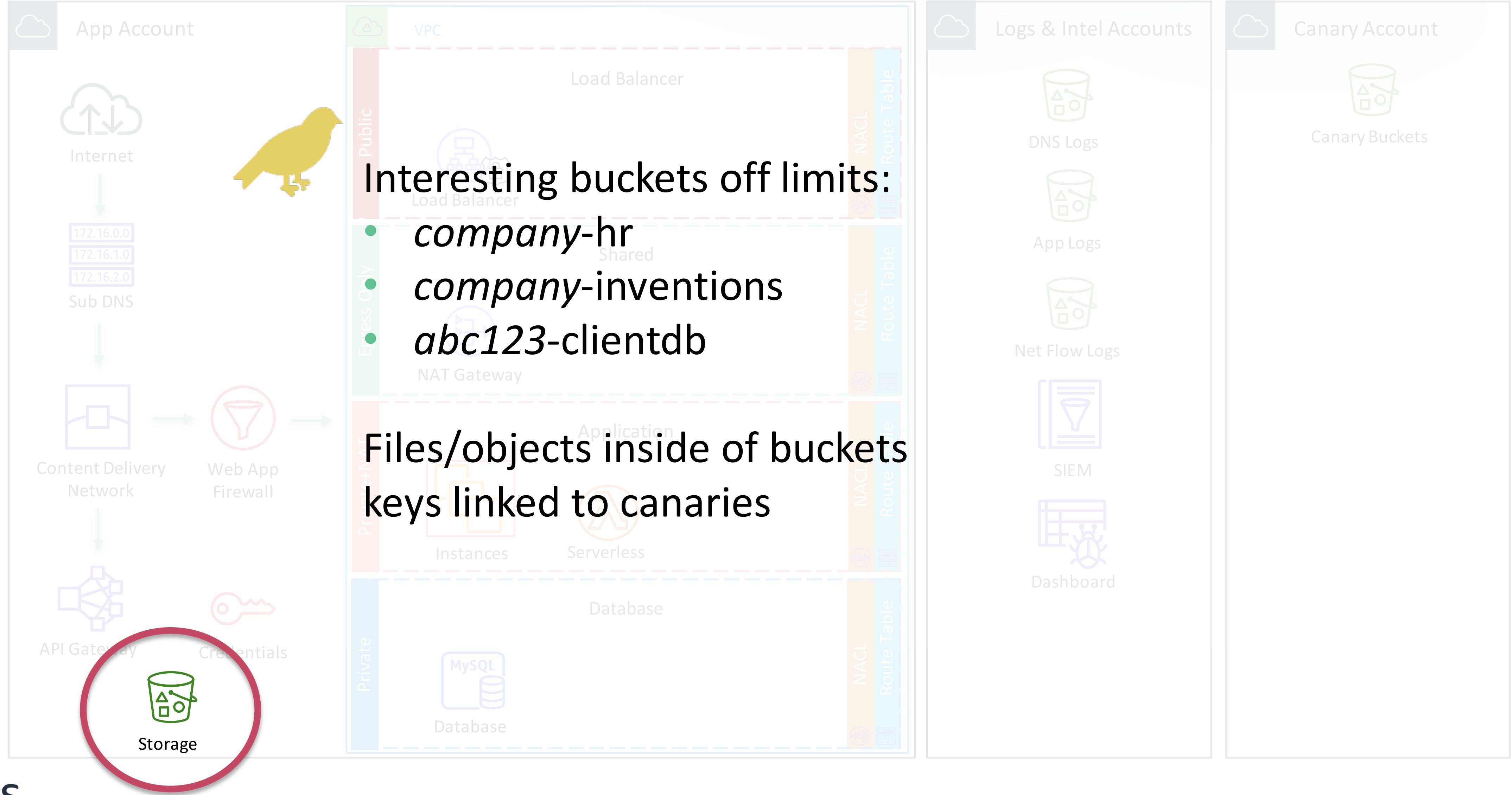


Unused roles

Canary keys: Spacecrab http://bit.ly/2QYviI5

- Access denied
- Behavior analysis
- Diff to pipeline

Storage Detection for Insiders

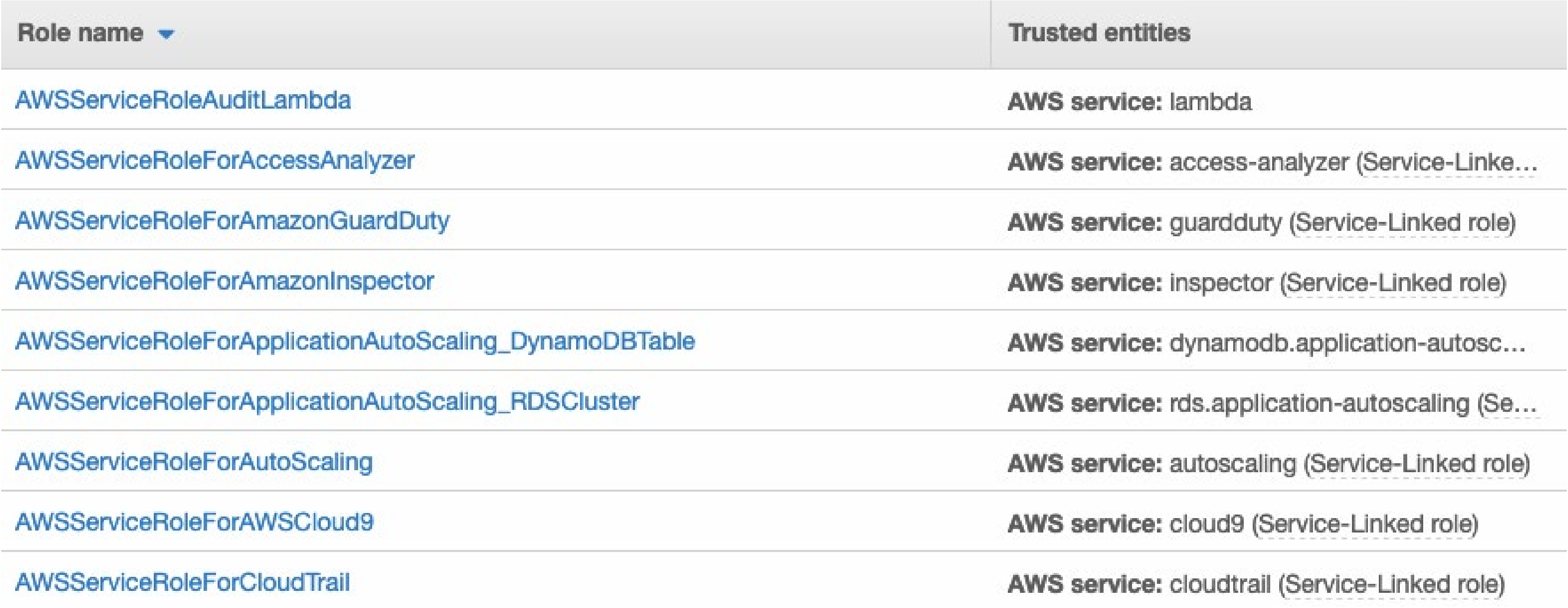


Interesting buckets off limits:

- *company*-hr
- *company*-inventions
- *abc123*-clientdb

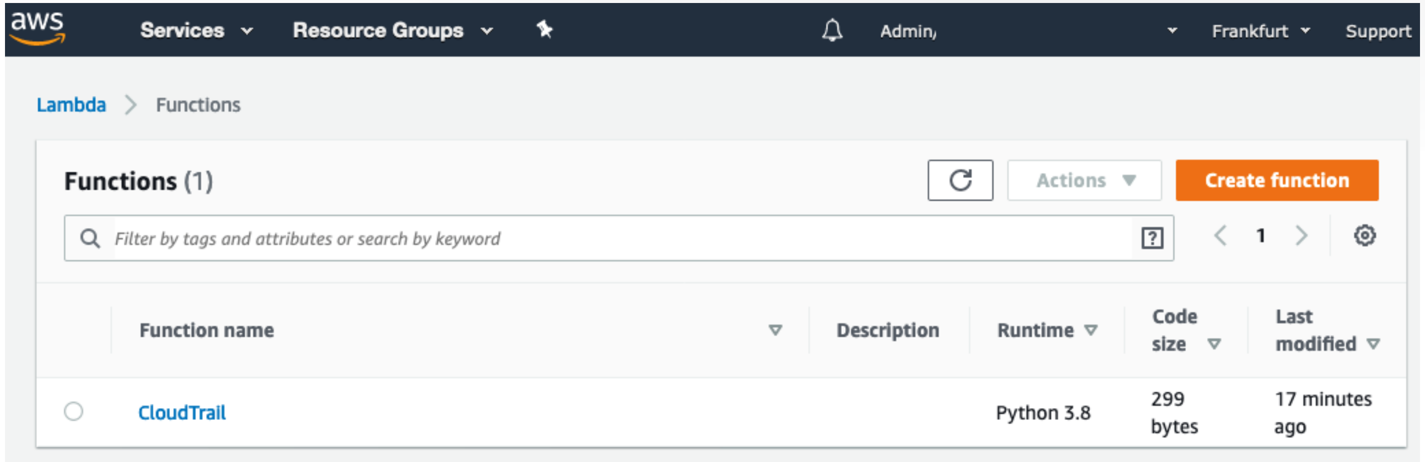
Files/objects inside of buckets keys linked to canaries

Concealed Adversary Roles



Role name ▾	Trusted entities
AWSServiceRoleAuditLambda	**AWS service:** lambda
AWSServiceRoleForAccessAnalyzer	**AWS service:** access-analyzer (Service-Linke...
AWSServiceRoleForAmazonGuardDuty	**AWS service:** guardduty (Service-Linked role)
AWSServiceRoleForAmazonInspector	**AWS service:** inspector (Service-Linked role)
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	**AWS service:** dynamodb.application-autosc...
AWSServiceRoleForApplicationAutoScaling_RDSCluster	**AWS service:** rds.application-autoscaling (Se...
AWSServiceRoleForAutoScaling	**AWS service:** autoscaling (Service-Linked role)
AWSServiceRoleForAWSCloud9	**AWS service:** cloud9 (Service-Linked role)
AWSServiceRoleForCloudTrail	**AWS service:** cloudtrail (Service-Linked role)

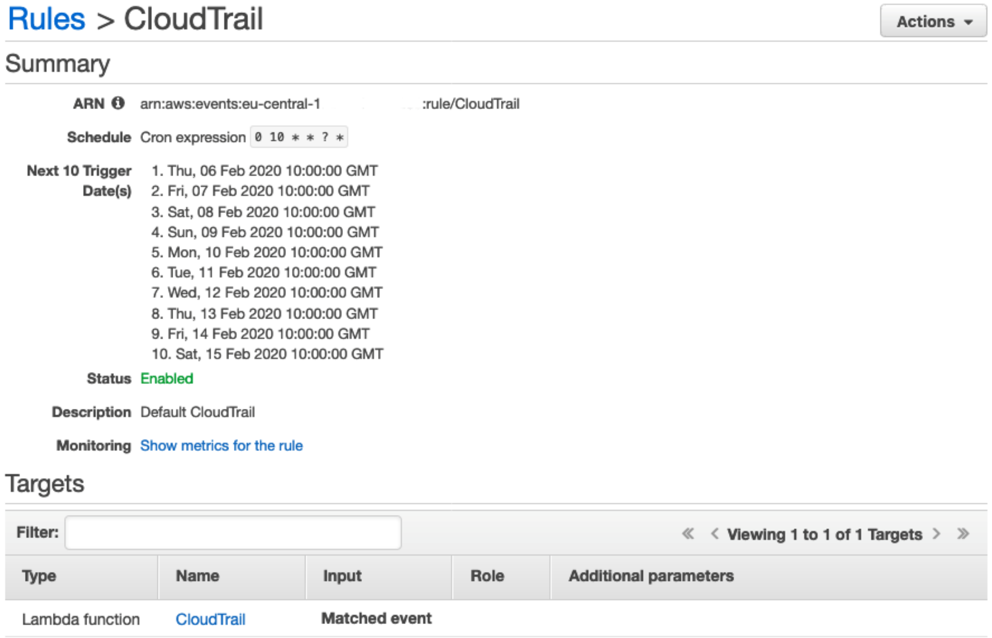
Concealed Resources - Serverless Functions



Lambda > Functions

Functions (1)

	Function name	Description	Runtime	Code size	Last modified
○	CloudTrail		Python 3.8	299 bytes	17 minutes ago



Rules > CloudTrail

Summary

ARN arn:aws:events:eu-central-1 [redacted] :rule/CloudTrail

Schedule Cron expression `0 10 * * ? *`

Next 10 Trigger Date(s)
1. Thu, 06 Feb 2020 10:00:00 GMT
2. Fri, 07 Feb 2020 10:00:00 GMT
3. Sat, 08 Feb 2020 10:00:00 GMT
4. Sun, 09 Feb 2020 10:00:00 GMT
5. Mon, 10 Feb 2020 10:00:00 GMT
6. Tue, 11 Feb 2020 10:00:00 GMT
7. Wed, 12 Feb 2020 10:00:00 GMT
8. Thu, 13 Feb 2020 10:00:00 GMT
9. Fri, 14 Feb 2020 10:00:00 GMT
10. Sat, 15 Feb 2020 10:00:00 GMT

Status Enabled

Description Default CloudTrail

Monitoring Show metrics for the rule

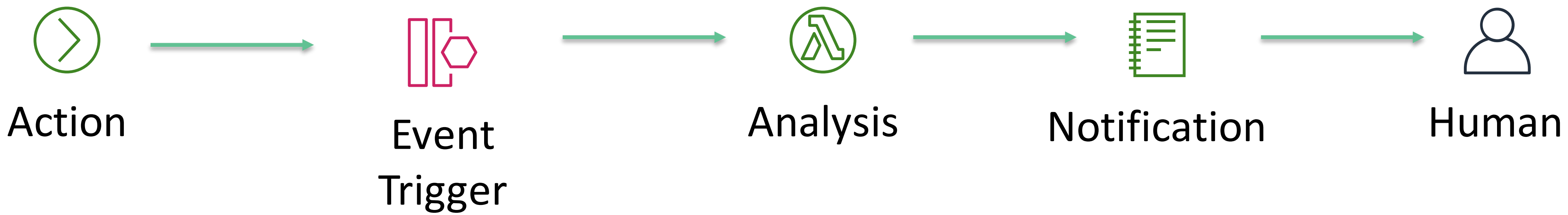
Targets

Filter:

Viewing 1 to 1 of 1 Targets

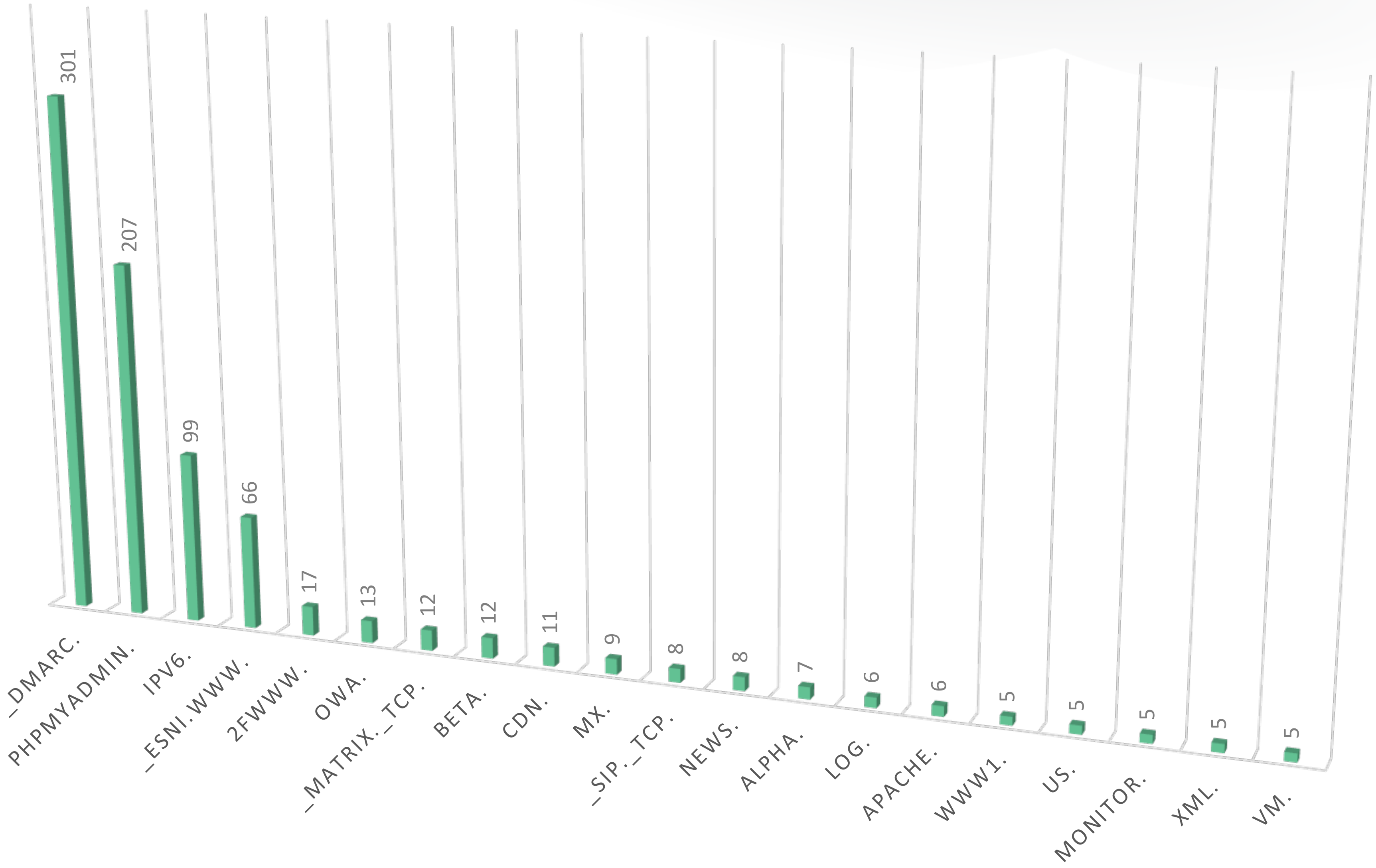
Type	Name	Input	Role	Additional parameters
Lambda function	CloudTrail	Matched event		

Automate Detection & Analysis

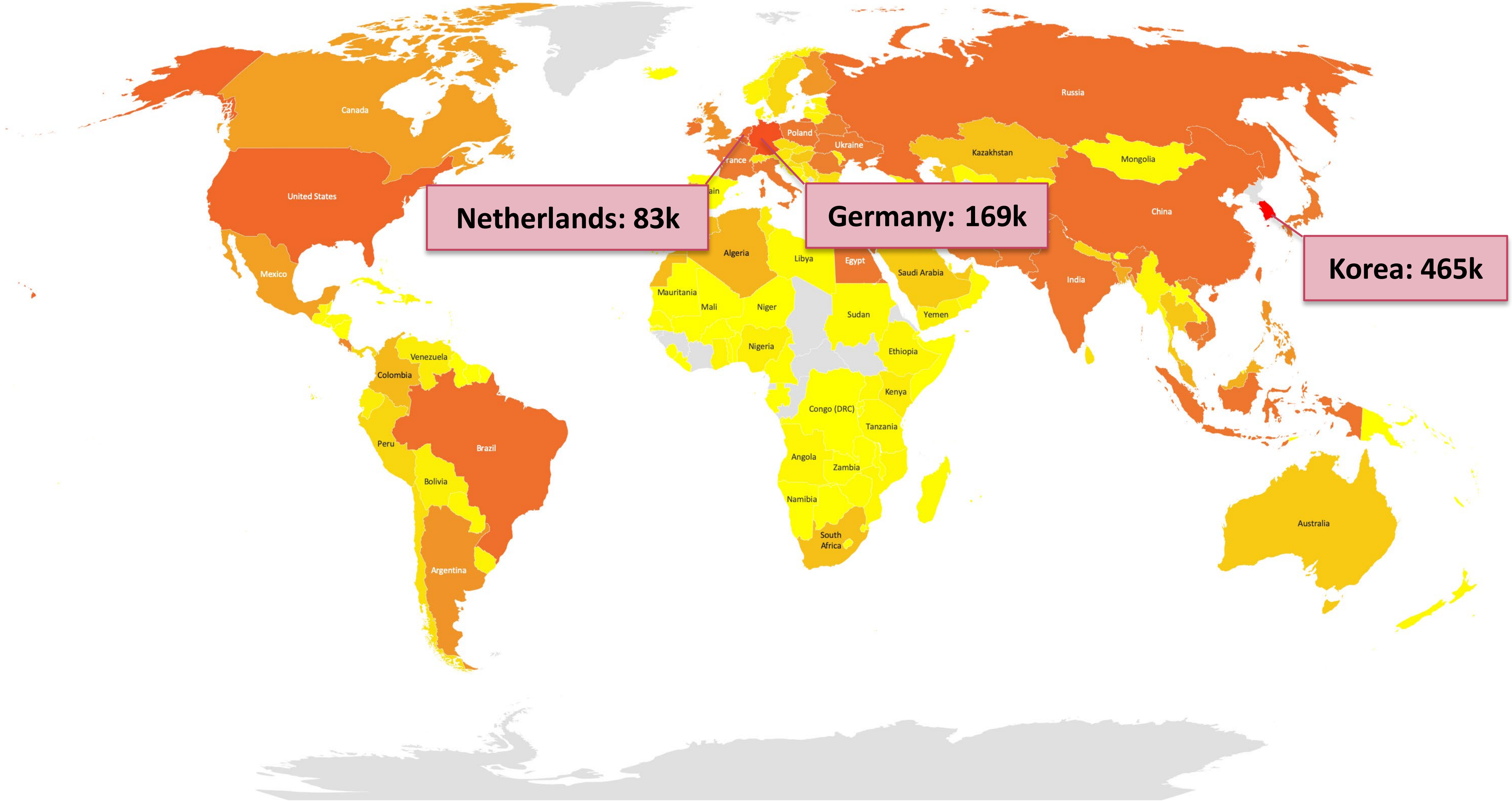


- Beware of noise
- Beware of multiple concurrent events
- Auto escalate

NoMoreRansom Findings - DNS



NoMoreRansom Findings - WAF Block

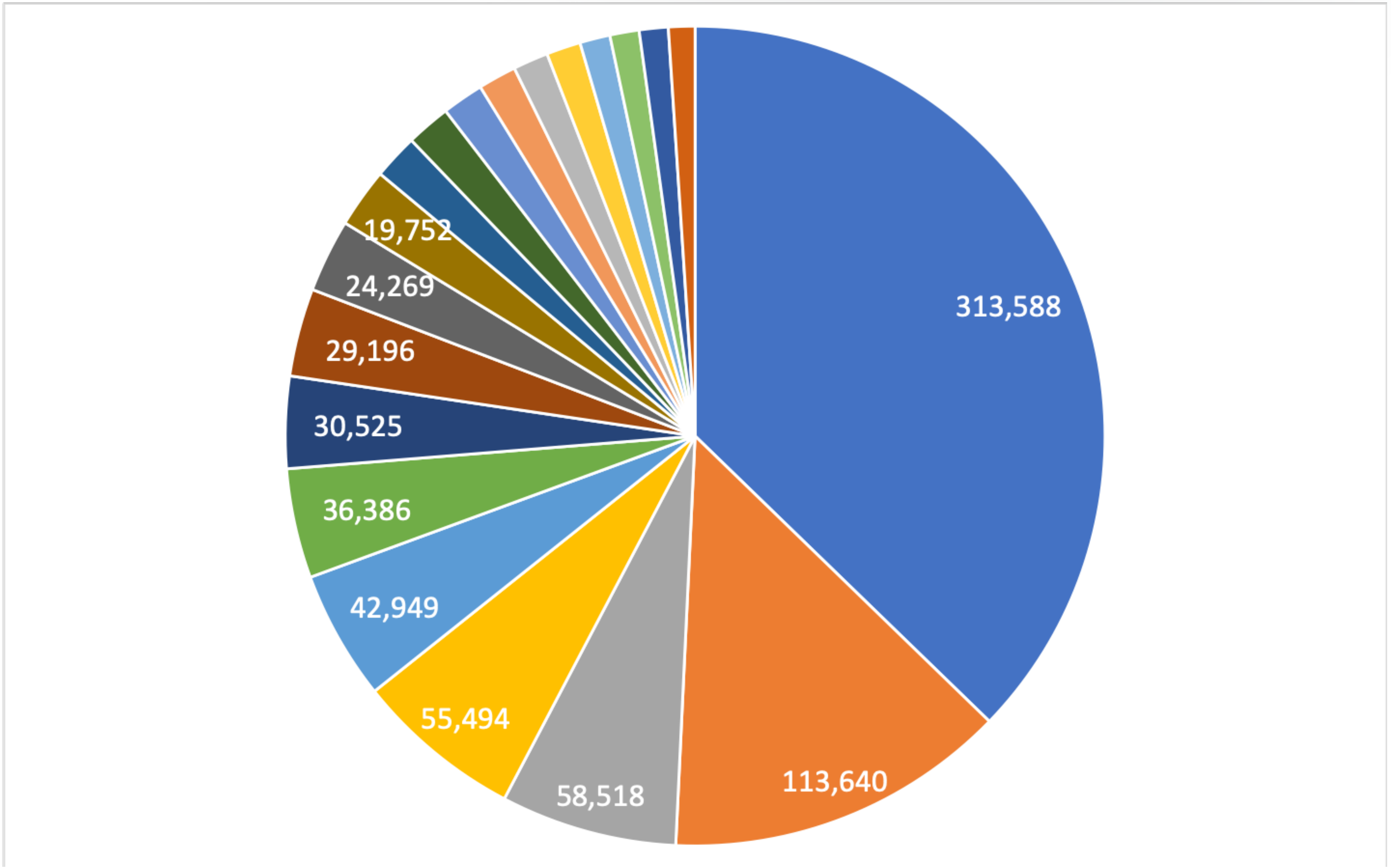


Netherlands: 83k

Germany: 169k

Korea: 465k

NoMoreRansom Findings - Top 20 IP Blocked Requests

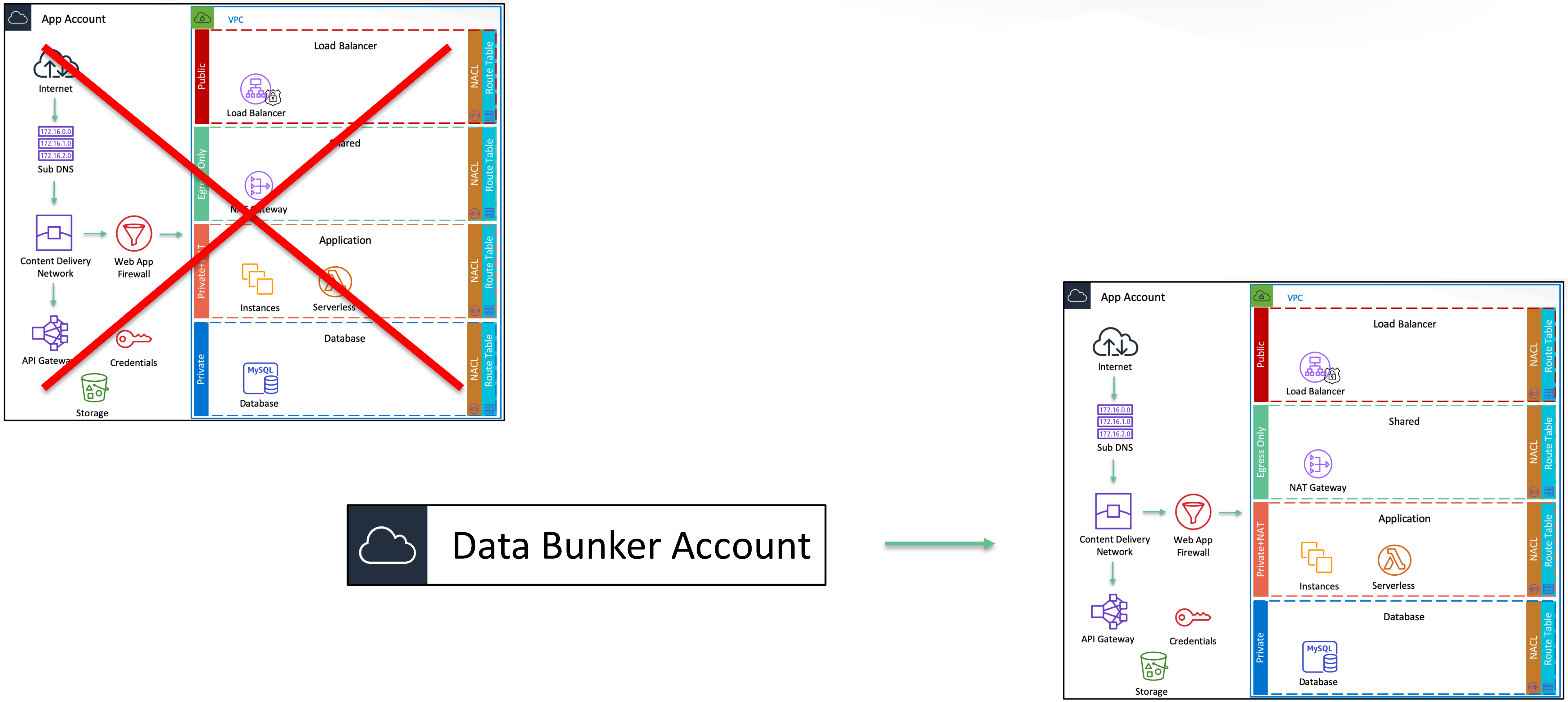


Containment, Eradication & Recovery

Considerations

- Response measured in seconds
- Record actions taken
- What has been touched? Drift: https://go.aws/2FA5e0v
- Is adversary really gone?
- Comms safe?

Containment, Eradication, & Recovery: Complete Replacement



Data Bunker Account

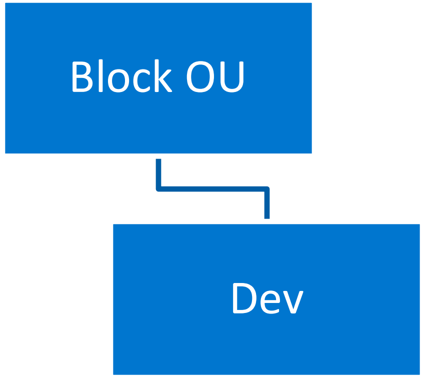
Containment: Identity & Access

- Explicit deny policy – individual principle

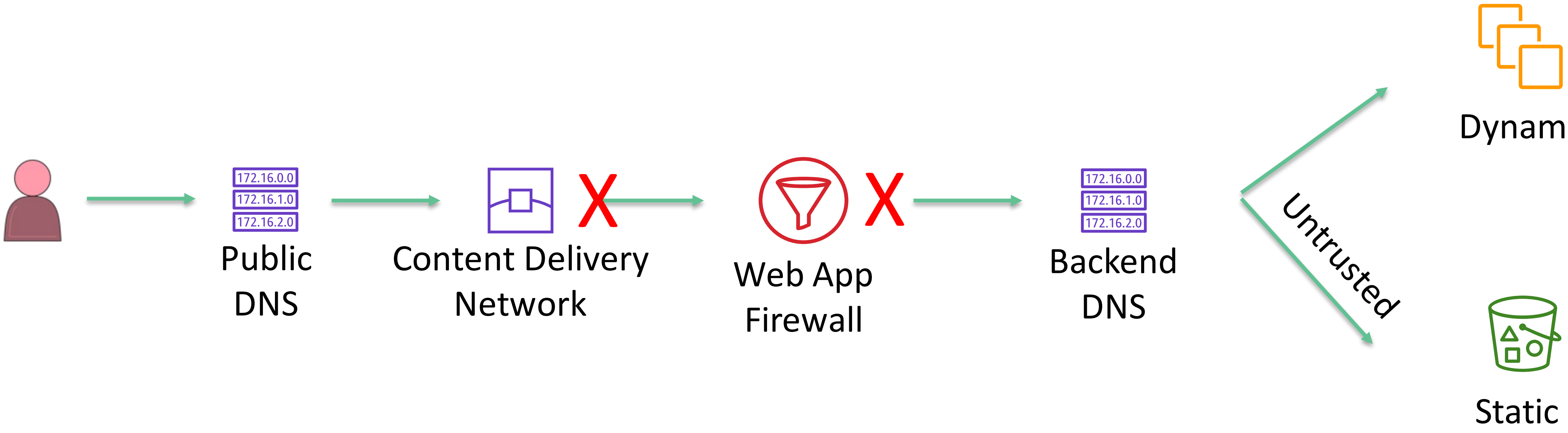
  { "Statement": [{ "Effect": "Deny", "Action": "*", "Resource": "*" }] }

- Explicit deny policy – account level

  { "Statement": [{ "Effect": "Deny", "Action": "*", "Resource": "*" }] }

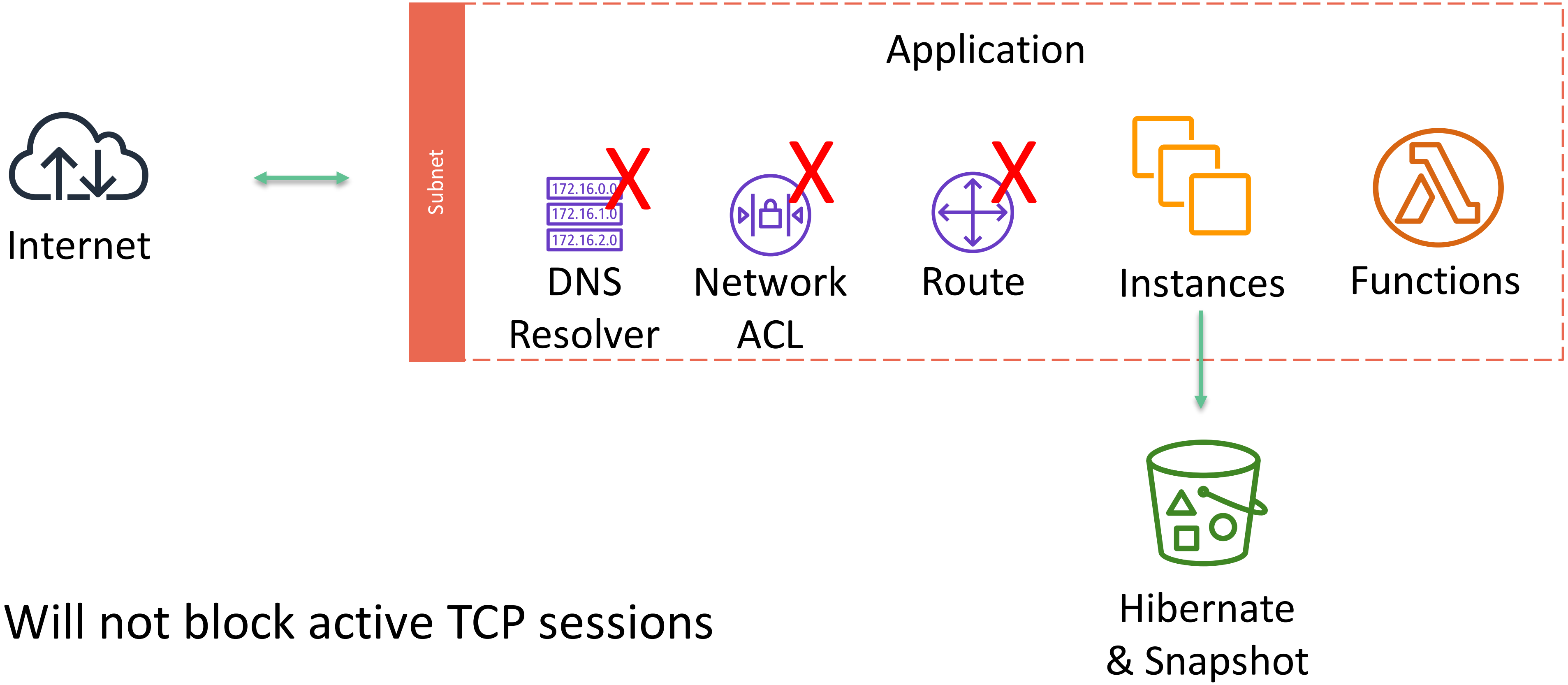


Containment & Recovery: Web Application



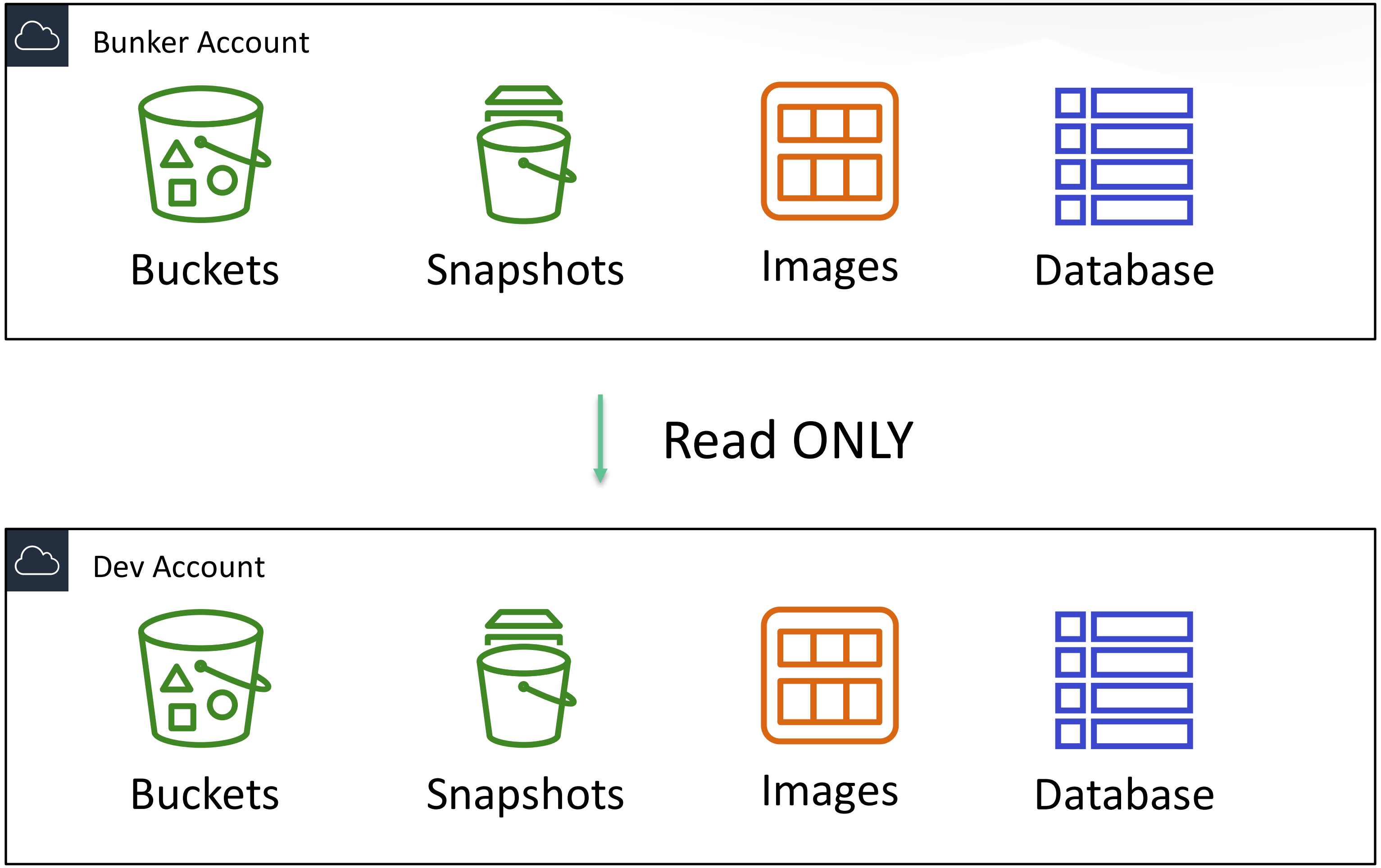
Content based routing: https://amzn.to/2tEdNF0

Containment: Instance & Function Network

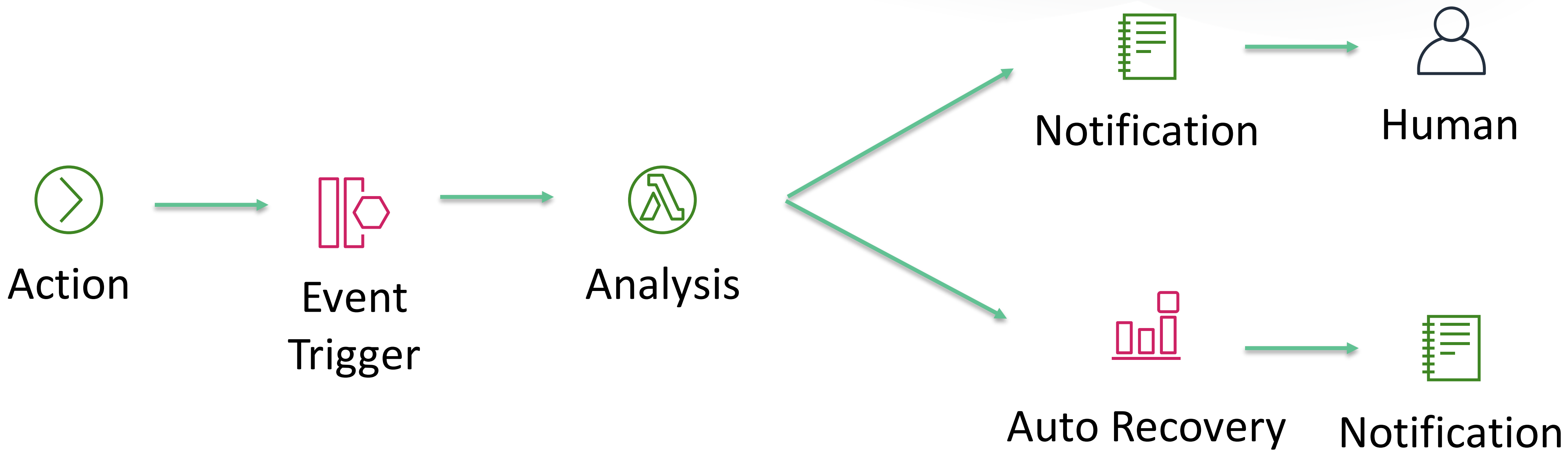


Note: Will not block active TCP sessions

Recovery: Storage



Automate Detection, Analysis, & Recovery



- Beware of noise
- Beware of multiple concurrent events
- Auto escalate

http://bit.ly/CRuleRem

Demo

TAKE ACTION!

Focus On…

- 3P’s: Patching, Preparation, Practice
- Small improvements & iterate
- Ask for help
- Automate as much as possible

Apply What You Have Learned Today

- Next week you should:
  - Identify critical risks & remediate
  - Start an IR plan based on pragmatic threat modelling
- In the first three months following this presentation you should:
  - Iterate on plans & threat model
  - Implement tools and practice using them
- Within six months you should:
  - Actions at a distance - hands off data and systems
  - Implement canaries

Links

www.nomoreransom.org

Best practices: https://aws.amazon.com/well-architected

AWS DevSecOps Blog: https://go.aws/2Fxw89t

EDNS client subnet: https://tools.ietf.org/html/rfc7871

Hidden API: http://bit.ly/WAFSol1

Block S3 public: http://bit.ly/S3Block

AWS Abuse: https://go.aws/389sL4Z

Spacecrab http://bit.ly/2QYvil5

Drift: https://go.aws/2FA5e0v

Content based routing: https://amzn.to/2tEdNF0

Auto remediation: http://bit.ly/CRuleRem

Demo: https://wellarchitectedlabs.com/