
AWS
re:Invent

SEC323

Building your cloud incident response program

Freddy Kasprzykowski
Security Consultant
AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Fundamentals of AWS cloud security for IR

Incident response maturity model

Foundation of incident response



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Fundamentals of AWS cloud security for IR

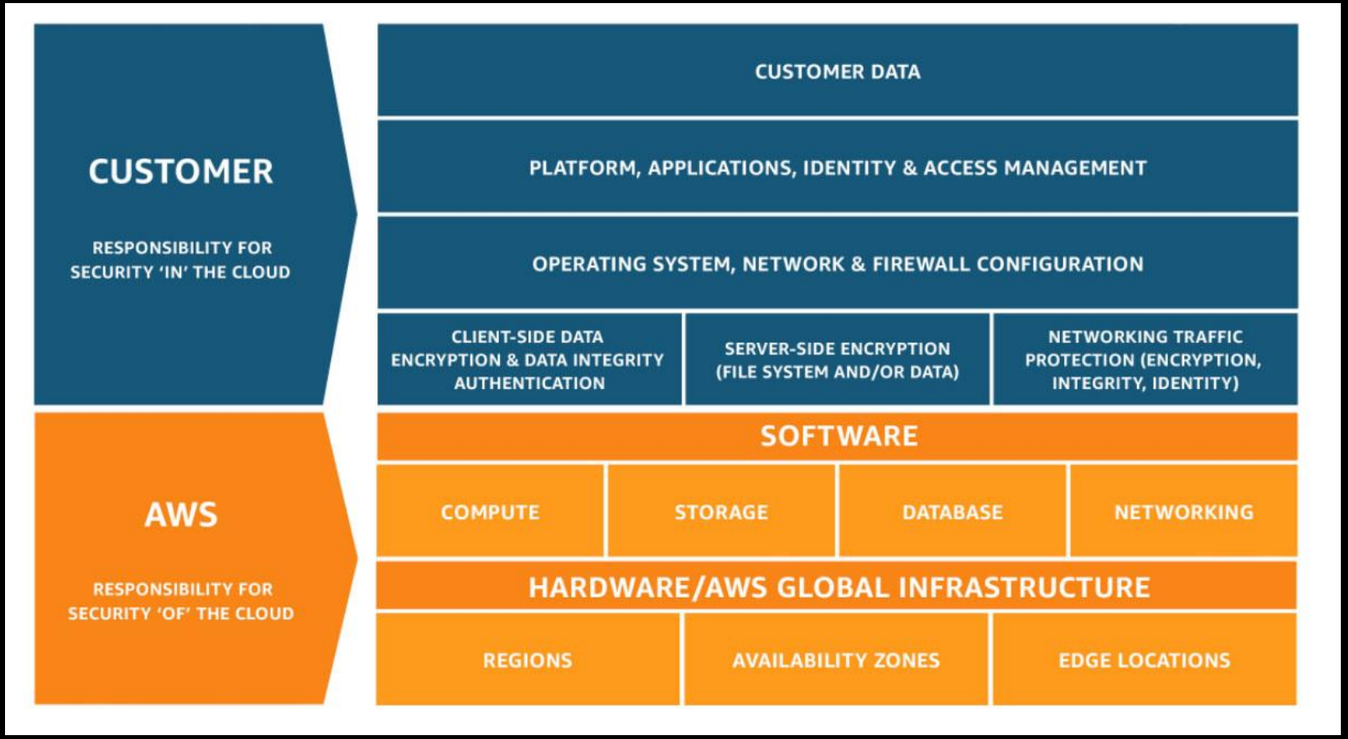


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS shared responsibility model

- Security **in** the cloud events
- Number of components in scope for incident response varies by service



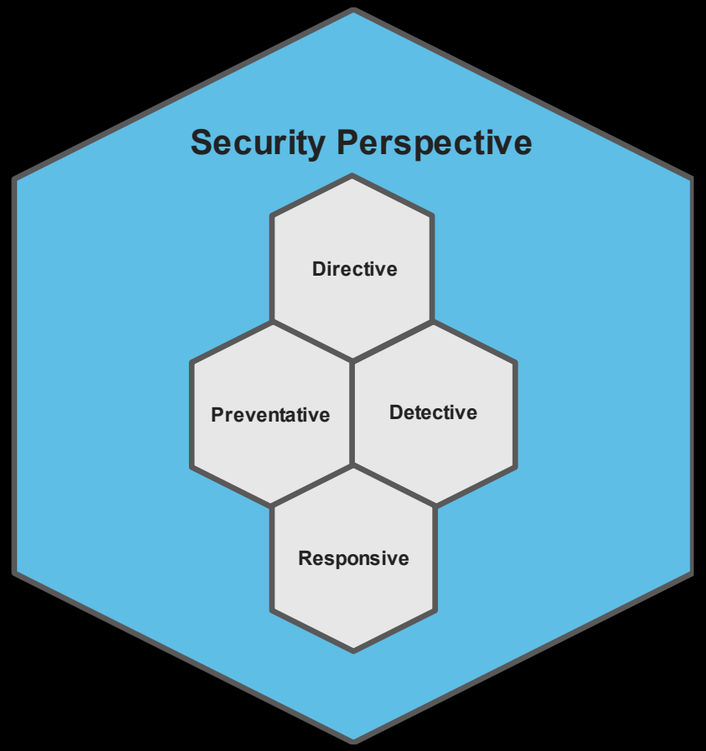
AWS Well-Architected Framework





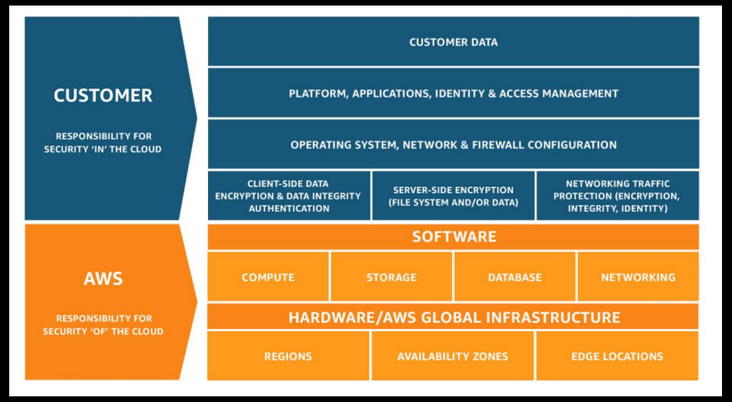
"Even with extremely mature preventive and detective controls, your organization should still implement mechanisms to respond to and mitigate the potential impact of security incidents."

AWS Cloud Adoption Framework



"Although incident response (IR) is generally viewed under the responsive controls component, these are dependent and influenced by the other components."

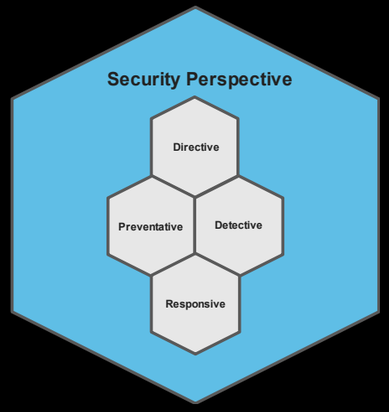
AWS incident response whitepaper

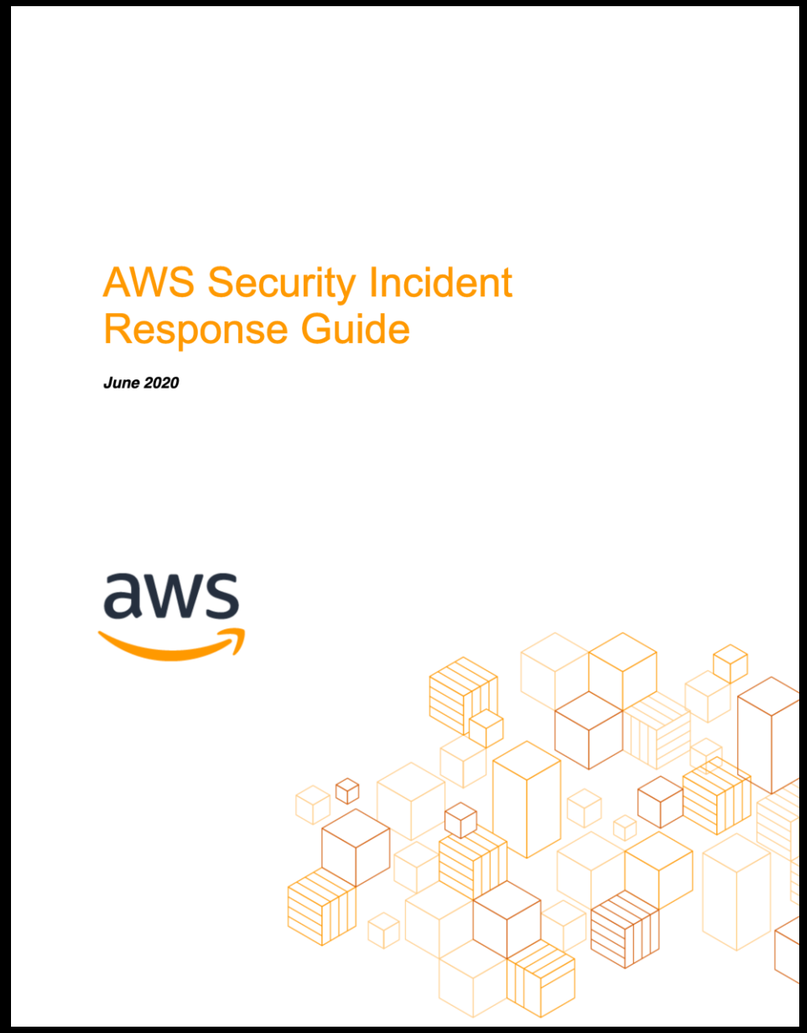


AWS Professional Services

Helping you achieve your desired business outcomes with AWS







Threat modeling

- What are we trying to protect?
- What are the threats?
- What alerts do we need?



The baseline

```
## Workload/Service component: example.com/S3
### Threat #7: Unauthorized Bucket change or deletion
#### Controls list:

* Directive:
    S3 Buckets and associated policy can only be deleted by the IAM Roles used by the
    account governance pipeline.
* Preventative:
    An SCP should be present including
      "s3:DeleteBucket", "s3:DeleteBucketPolicy"
      as a set of deny actions for any principal other than the ones used by the IAM Roles
      used by the account governance pipeline.
    For all S3 Buckets created in the Organization, the policy should state
      "s3:*" in allow statement for the IAM Roles used by the account governance pipeline
      "s3:DeleteBucket", "s3:DeleteBucketPolicy" in deny statement except for the IAM
      Roles used by the account governance pipeline
* Detective:
    Create a config rule to alert on changes to S3 Bucket policy circunventing preventive
    controls
    Create a config rule to alert on S3 Bucket deletion
    Create a CloudWatch Rule to alert on S3 Bucket deletion
    Enable GuardDuty and monitor finding "Impact:S3/PermissionsModification.Unusual"
* Responsive:
    Implement a process to revert changes made to a S3 Bucket policy deviating from
    preventative baseline
    Implement a process to recreate a deleted S3 Bucket
    Implement a process to restore the data from a deleted S3 Bucket
    Implement a process to notify S3 Bucket owner of deletion
    Implement a process to investigate the principals involved with the attempted or
    succesful deletion of a S3 Bucket

```

Alert:

“Attempted or successful S3 bucket deletion”

Threat detection requirements

Incident response requirements

The noise

```
fredski — ec2-user@ip-172-31-40-205:~ — ssh ec2-user@ec2-54-87-183-197.compute-1.amazonaws.com -i keys/ir-ssh-pair.pem — 174×10
06598,nop,wscale 7], length 0
22:26:46.736836 IP 157.230.212.33.33438 > 172.31.40.205.radan-http: Flags [.], ack 1, win 229, options [nop,nop,TS val 116706662 ecr 1643782720], length 0
22:26:46.776811 IP 157.230.212.33.33438 > 172.31.40.205.radan-http: Flags [P.], seq 1:250, ack 1, win 229, options [nop,nop,TS val 116706708 ecr 1643782720], length 249
22:26:46.776839 IP 172.31.40.205.radan-http > 157.230.212.33.33438: Flags [.], ack 250, win 219, options [nop,nop,TS val 1643782824 ecr 116706708], length 0
22:26:46.777333 IP 172.31.40.205.radan-http > 157.230.212.33.33438: Flags [P.], seq 1:43, ack 250, win 219, options [nop,nop,TS val 1643782824 ecr 116706708], length 42
22:26:46.777435 IP 172.31.40.205.radan-http > 157.230.212.33.33438: Flags [FP.], seq 43:381, ack 250, win 219, options [nop,nop,TS val 1643782824 ecr 116706708], length 338
22:26:46.791999 IP 157.230.212.33.33438 > 172.31.40.205.radan-http: Flags [.], ack 43, win 229, options [nop,nop,TS val 116706723 ecr 1643782824], length 0
22:26:46.794810 IP 157.230.212.33.33438 > 172.31.40.205.radan-http: Flags [F.], seq 250, ack 382, win 245, options [nop,nop,TS val 116706726 ecr 1643782824], length 0
22:26:46.794835 IP 172.31.40.205.radan-http > 157.230.212.33.33438: Flags [.], ack 251, win 219, options [nop,nop,TS val 1643782842 ecr 116706726], length 0
```

Packet capture

```
fredski — ec2-user@ip-172-31-40-205:~ — ssh ec2-user@ec2-54-87-183-197.compute-1.amazonaws.com -i keys/ir-ssh-pair.pem — 174×5
157.230.212.33 - - [31/Oct/2020 22:26:09] code 501, message Unsupported method ('POST')
157.230.212.33 - - [31/Oct/2020 22:26:09] "POST /ws/v1/cluster/apps/new-application HTTP/1.1" 501 -
157.230.212.33 - - [31/Oct/2020 22:26:46] code 501, message Unsupported method ('POST')
157.230.212.33 - - [31/Oct/2020 22:26:46] "POST /ws/v1/cluster/apps/new-application HTTP/1.1" 501 -
```

HTTP server

#	eventTime	eventSource	eventName
▶ 1	2020-10-31T22:14:13Z	ec2.amazonaws.com	ModifyInstanceAttribute



AWS CloudTrail

~1.5 minutes after opening the SG

#	start	srcAddr	dstAddr	action
▶ 1	1604182555	5.189.191.89	172.31.40.205	ACCEPT



Flow logs

Incident response maturity model

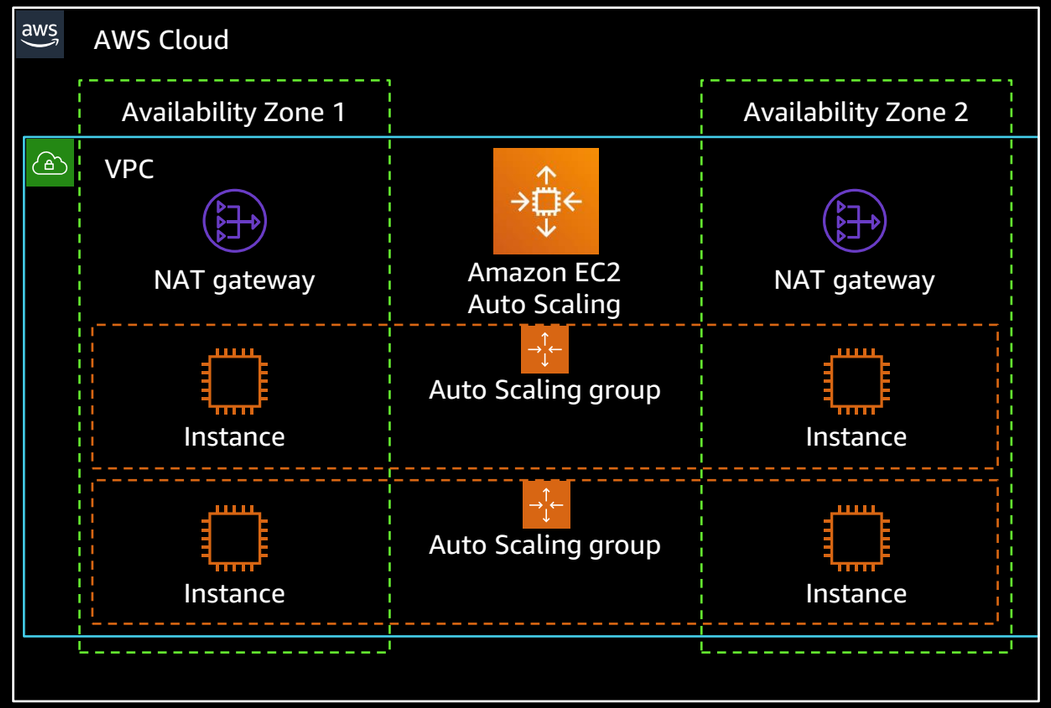


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of a security incident

- Actor's actions are translated into activity logs
- Targeted or opportunistic behavior



- Responder is alerted, translates activity logs into actor's behavior, and uses appropriate tools to respond
- Spend less effort in opportunistic behavior



Actor



Business

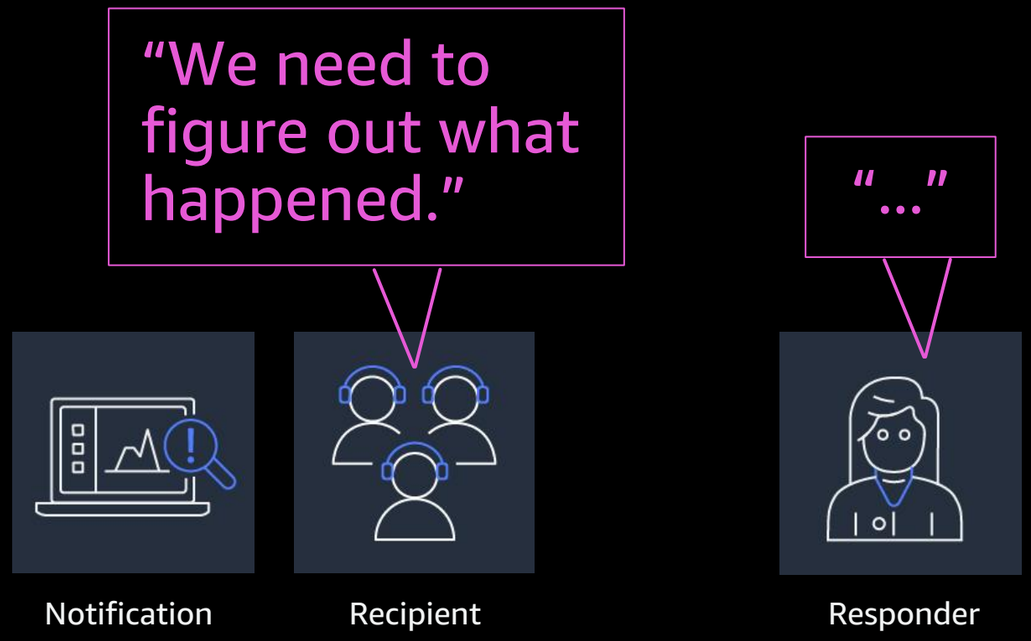


Responder

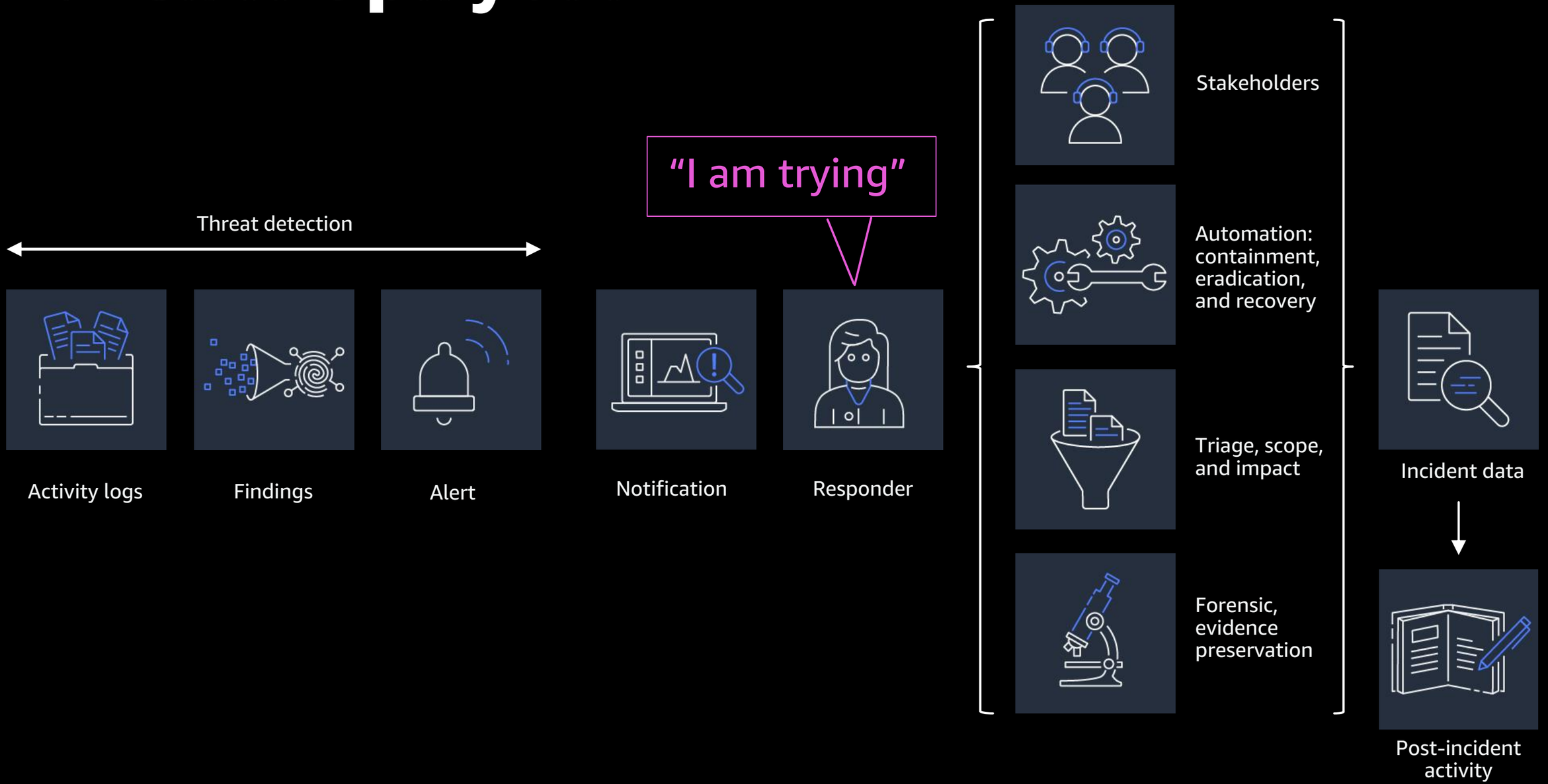
Incident response maturity model

1. “Zero playbook”
2. “Classic playbook”
3. “Playbook as code”

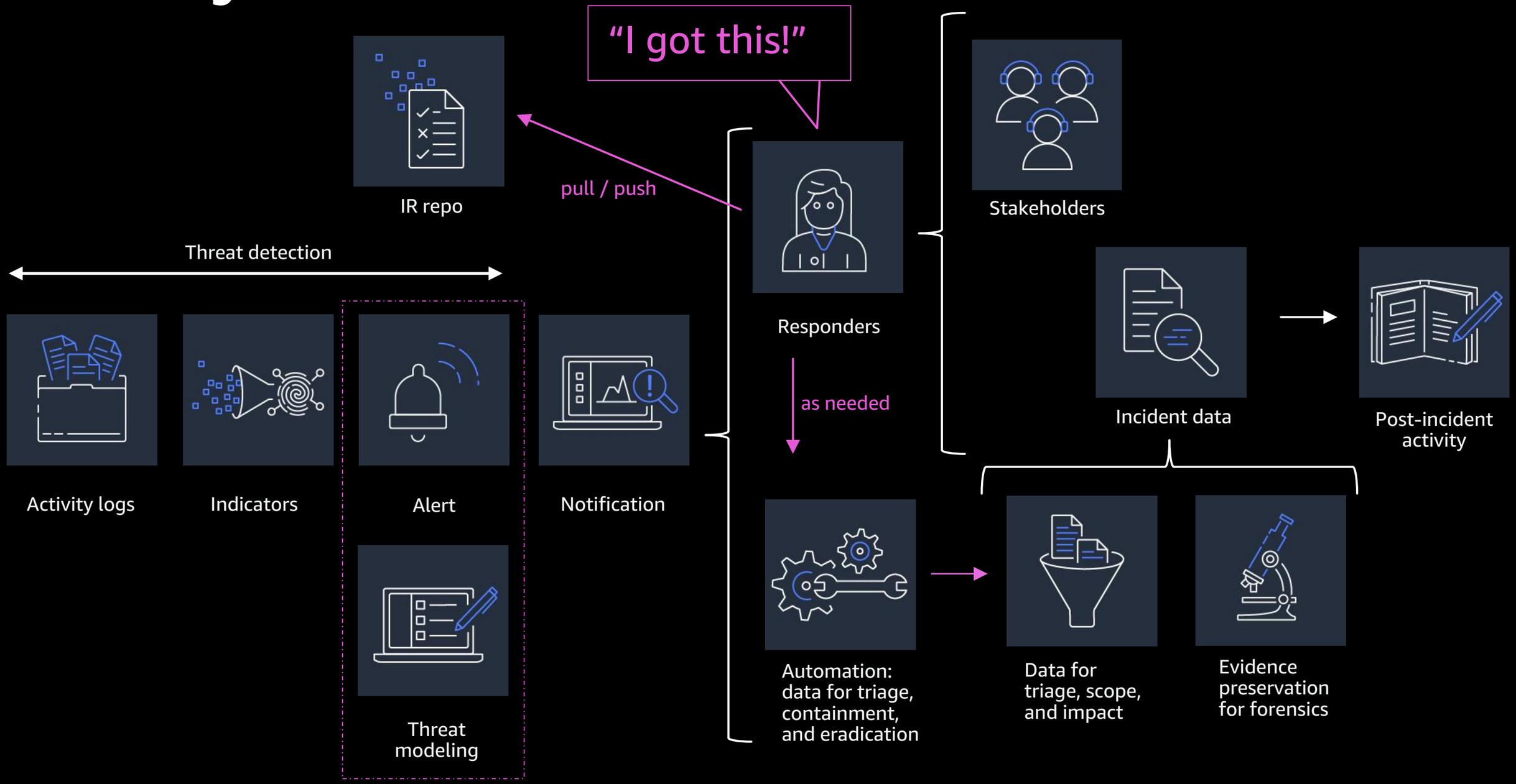
1. “Zero playbook”



2. “Classic playbook”



3. “Playbook as code”



What is getting in the way?



Too many alerts or no alerts



Inadequate threat detection and incident response skills



Lack of or wrong expectations about automation



Inadequate playbooks

The journey: Educate, prepare, simulate, iterate



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From workloads to alerts

Workloads



Services

aws

VPC

Amazon EC2

AWS Identity and Access Management

Amazon Simple Storage Service

Threats

Root user abused

Unauthorized access

IAM access keys abused

Sensitive data being made public

Alerts

“Root usage detected”

“Unauthorized access to EC2 instance detected”

“Long-term IAM access keys exposed”

“S3 bucket or object made public”

From alerts to log sources

Alerts

"Root usage detected"

"Unauthorized access to EC2 instance detected"

"Long-term IAM access keys exposed"

"S3 bucket or object made public"

Findings

Amazon GuardDuty:

- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/RDPBruteForce
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual

Custom solution:

- NETBIOS SMB NTLMSSP authentication brute force attempt
- INDICATOR-SCAN SSH brute force login attempt

Log sources



AWS CloudTrail



AWS Config



Amazon GuardDuty



Flow logs



AWS Security Hub



Custom solution

From logs to analysis

Log sources



AWS CloudTrail



AWS Config



Amazon GuardDuty



Flow logs



AWS Security Hub



Custom solution

Log storage



Amazon EventBridge



Amazon Simple Storage Service



Amazon S3 Glacier

Analytics



Amazon CloudWatch

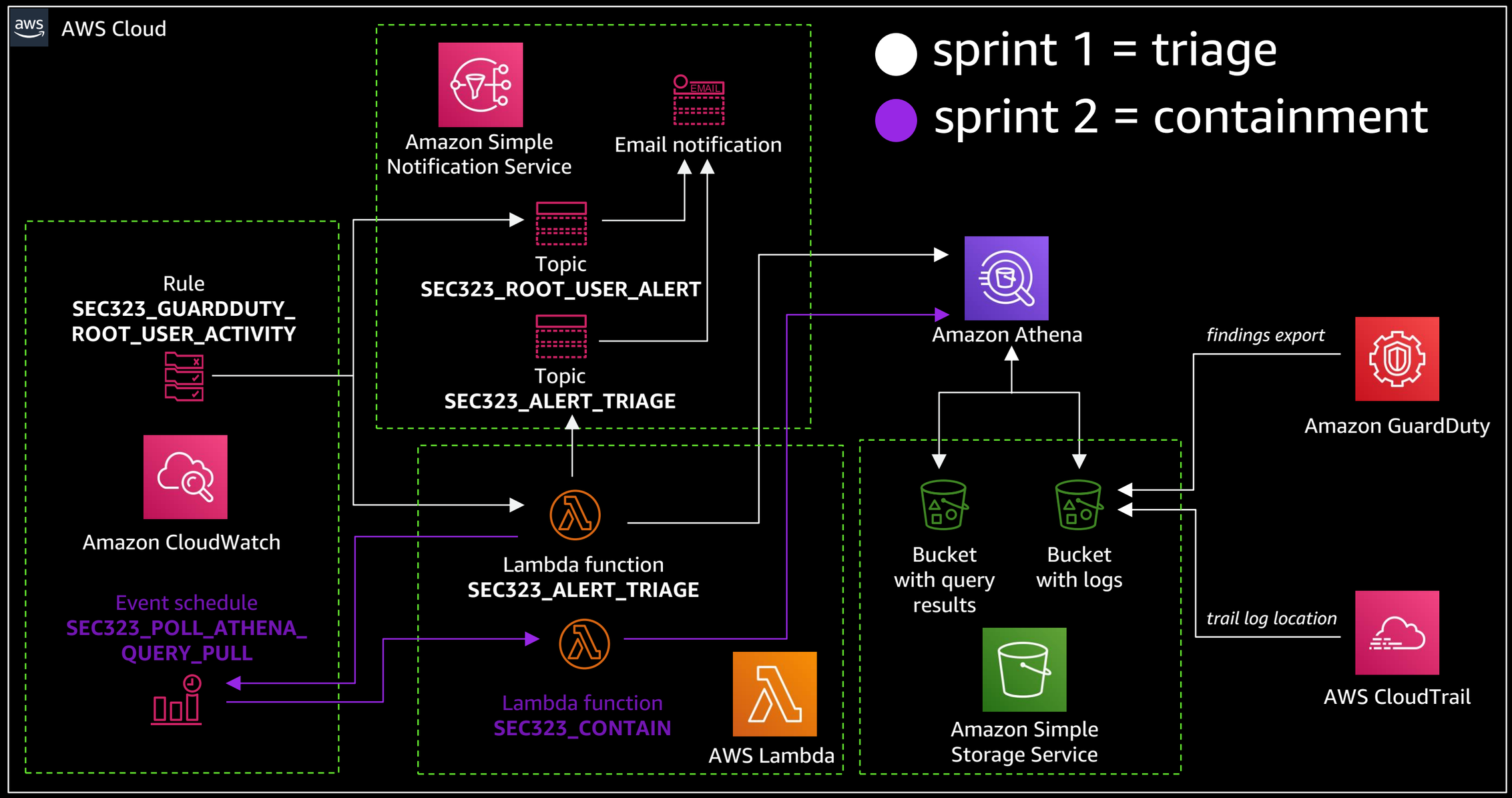


Amazon Athena



Amazon Detective

Automation


AWS Cloud
sprint 1 = triage
sprint 2 = containment
Amazon Simple Notification Service
Email notification
Topic
SEC323_ROOT_USER_ALERT
Topic
SEC323_ALERT_TRIAGE
Rule
SEC323_GUARDDUTY_ROOT_USER_ACTIVITY
Amazon CloudWatch
Event schedule
SEC323_POLL_ATHENA_QUERY_PULL
Lambda function
SEC323_ALERT_TRIAGE
Lambda function
SEC323_CONTAIN
AWS Lambda
Amazon Athena
Bucket with query results
Bucket with logs
Amazon Simple Storage Service
findings export
Amazon GuardDuty
trail log location
AWS CloudTrail

Educate, prepare, simulate, iterate

- Git-based repository for IR
- Expanded scope for automation
- Code + documents
- Playbooks as educational opportunity
- Leverage existing CI / CD pipeline

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.