
AWS
re:Invent

SEC306

Automated forensic artifact collection on AWS with Goldman Sachs

Ryan Tick
Cloud Security Architect
Goldman Sachs

Vaishnav Murthy
Cloud Security Architect
Goldman Sachs

Logan Bair
Cloud Security Architect,
WWPS Professional Services
AWS

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

Agenda

Learning objectives

Problem space

Goldman Sachs's solution

Additional resources



AWS re:Invent

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

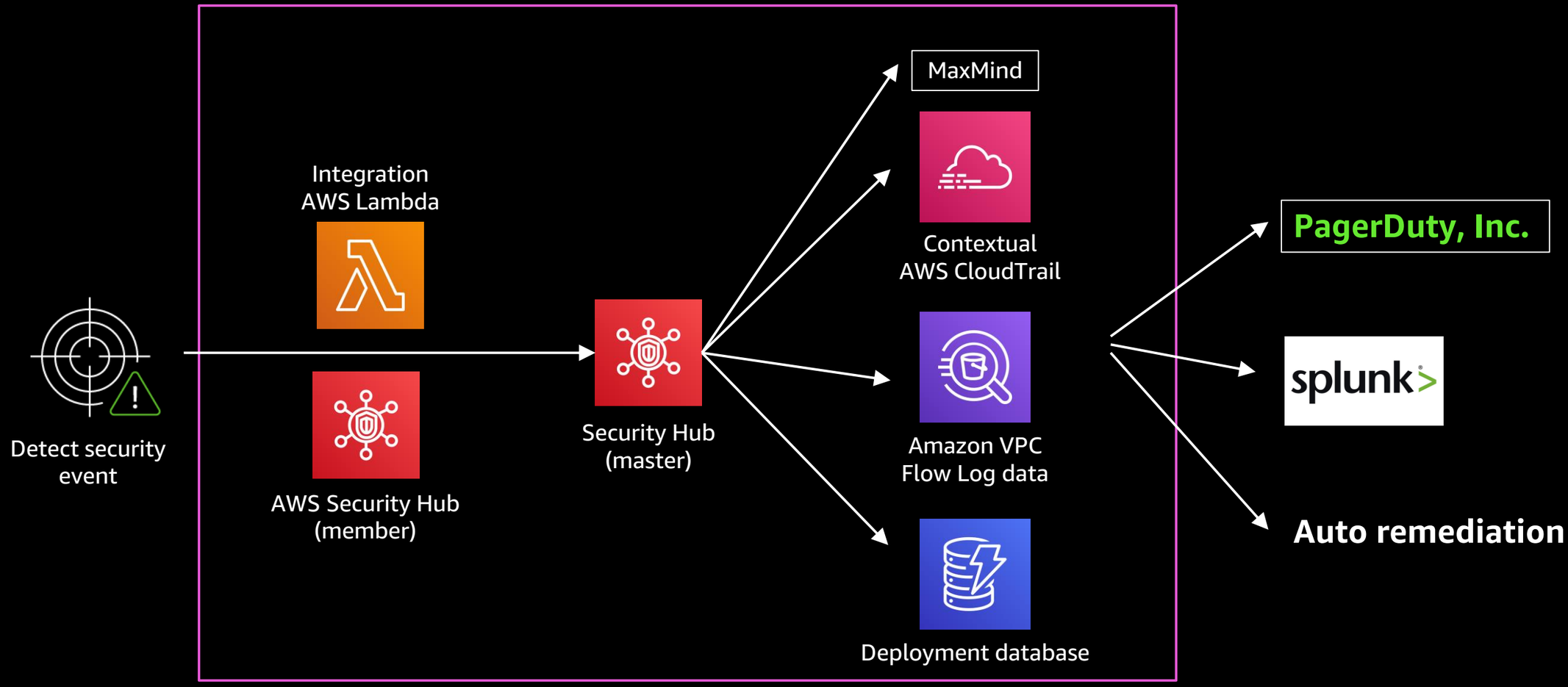
Learning objectives



AWS re:Invent

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

Q3 Tech Talk recap



1

Leverage AWS Security Hub

to centralize findings and automate security checks



AWS re:Invent

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

2

Enrich findings and tune detections

to provide contextual data and account for varied configurations



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

3

Trigger remediation actions

to quickly and consistently resolve security events



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

Problem space



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

Why is threat detection so difficult?



Large, varied datasets

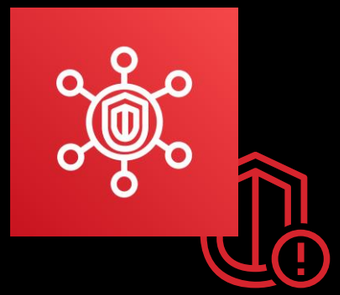


High rate of false-positives

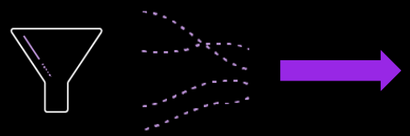


Limited resources

Goldman Sachs's solution



AWS Security Finding Format (ASFF)



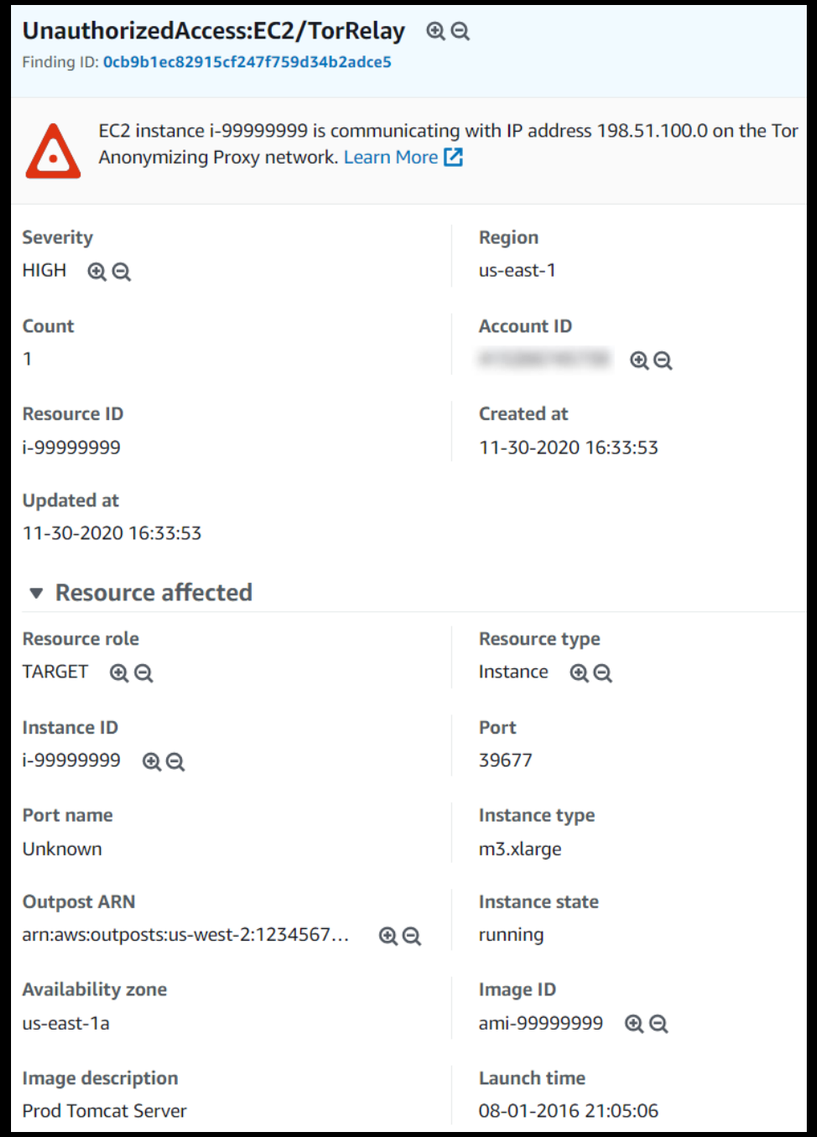
Enrichment and filtering



Automated detection and response

Set the scene

EXAMPLE GUARDDUTY FINDING



Set the scene

EXAMPLE INSPECTOR FINDING

Finding for assessment target 'Assessment-Target-All-Instances-All-Rules' and template 'Assessment-Template-Default-All-Rules'

ARN	[redacted]
Run name	Run - Assessment-Template-Default-All-Rules
Target name	Assessment-Target-All-Instances-All-Rules
Template name	Assessment-Template-Default-All-Rules
Start	Today at 5:33 PM (GMT-5) (an hour ago)
End	Today at 6:35 PM (GMT-5) (17 minutes ago)
Status	Analysis complete
Rules package	CIS Operating System Security Configuration Benchmarks-1.0
AWS agent ID	i-99999999
Finding	Instance i-99999999 is not compliant with rule 1.6.1.2 Ensure the SELinux state is enforcing, 1.0.0 CIS Amazon Linux 2 Benchmark. Applicable profiles: Level 2.
Severity	High
Description	Description Set SELinux to enable when the system is booted. Rationale SELinux must be enabled at boot time in to ensure that the controls it provides are in effect at all times.
Recommendation	Edit the /etc/selinux/config file to set the SELINUX parameter: SELINUX=enforcing

Show Details

What happens next?

- How does SOC analyst get notified about and access this finding?
- What is the purpose of the AWS account?
- What other API calls happened around the time of the event?
- Is the EC2 instance communicating with a known-bad IP address?
- Has someone made a change to the EC2 instance or any of its related resources?

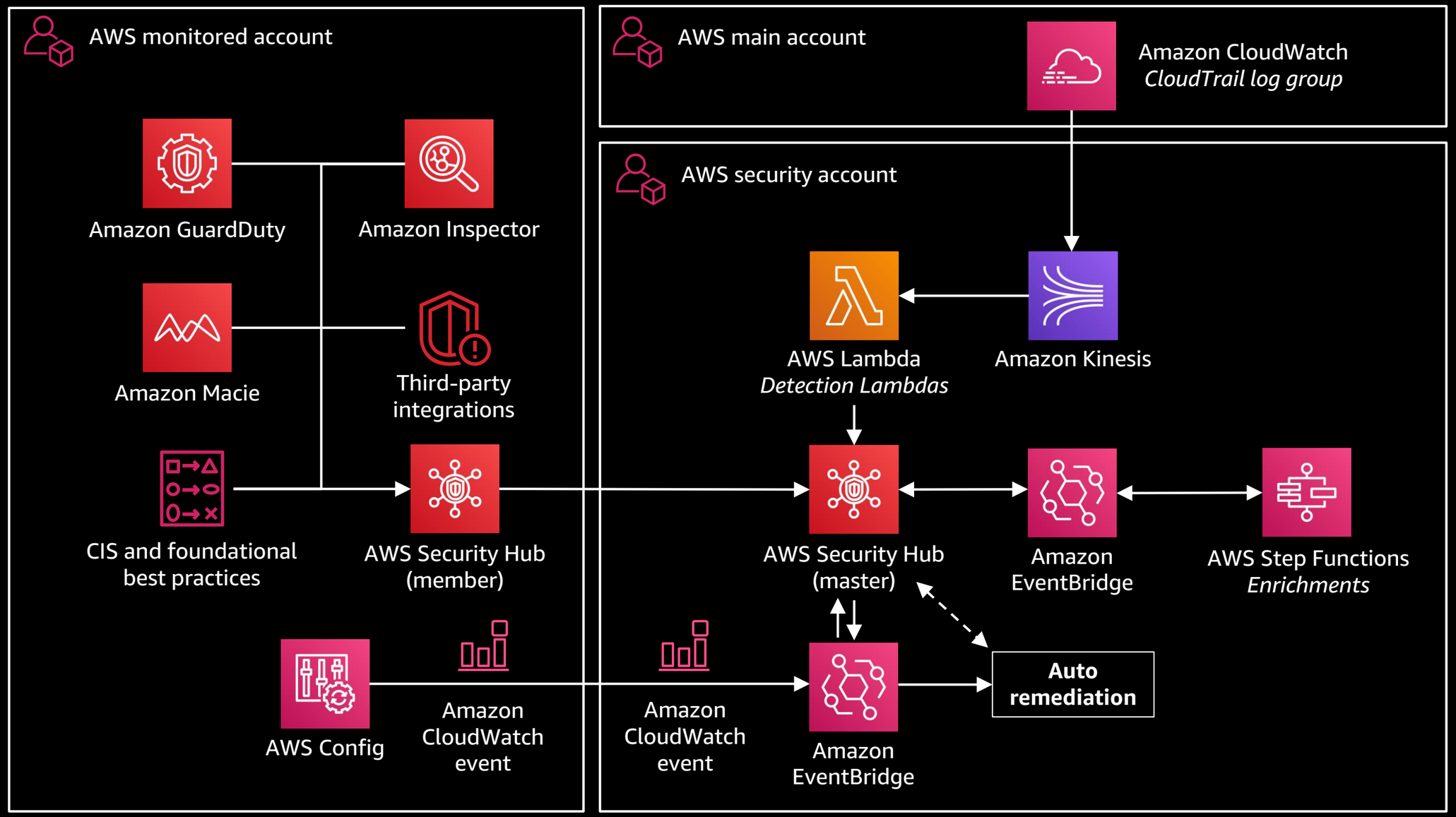
Sky Watch



AWS re:Invent

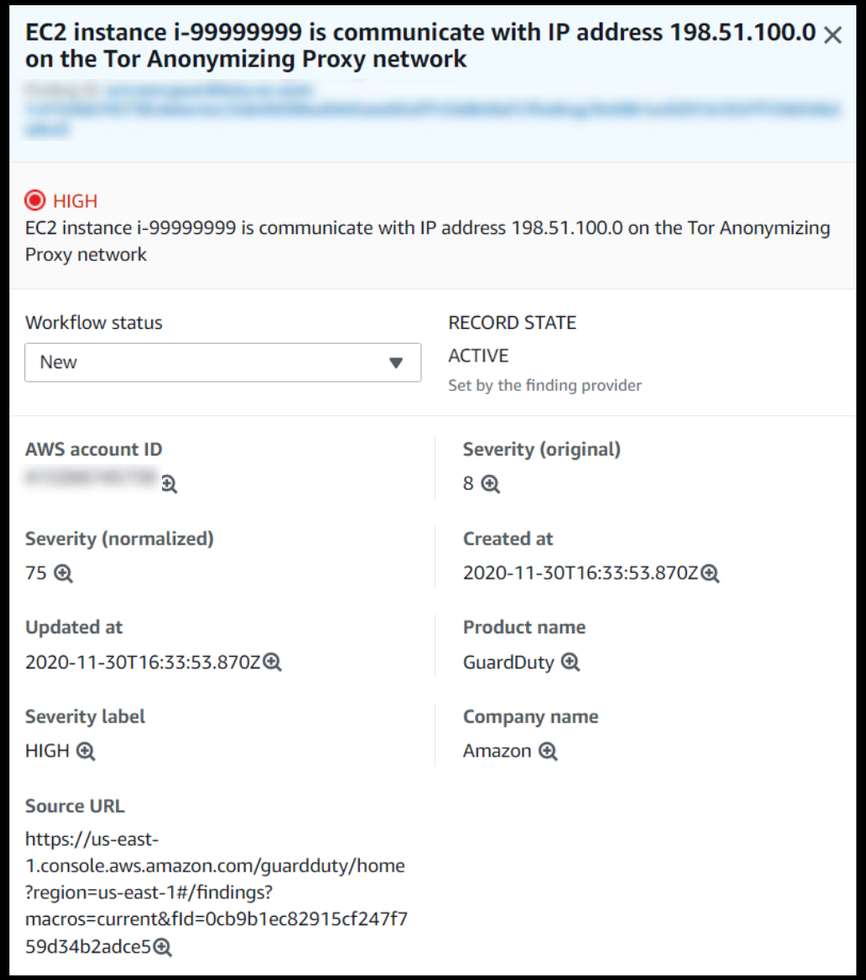
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

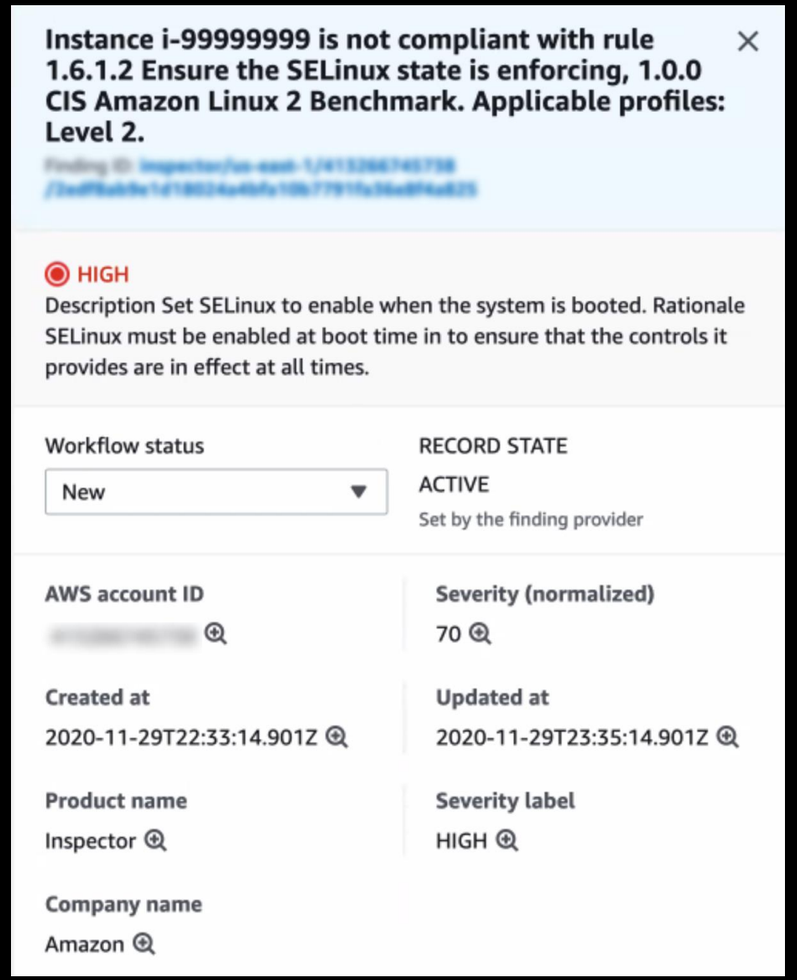
Sky Watch – 1,000-foot view



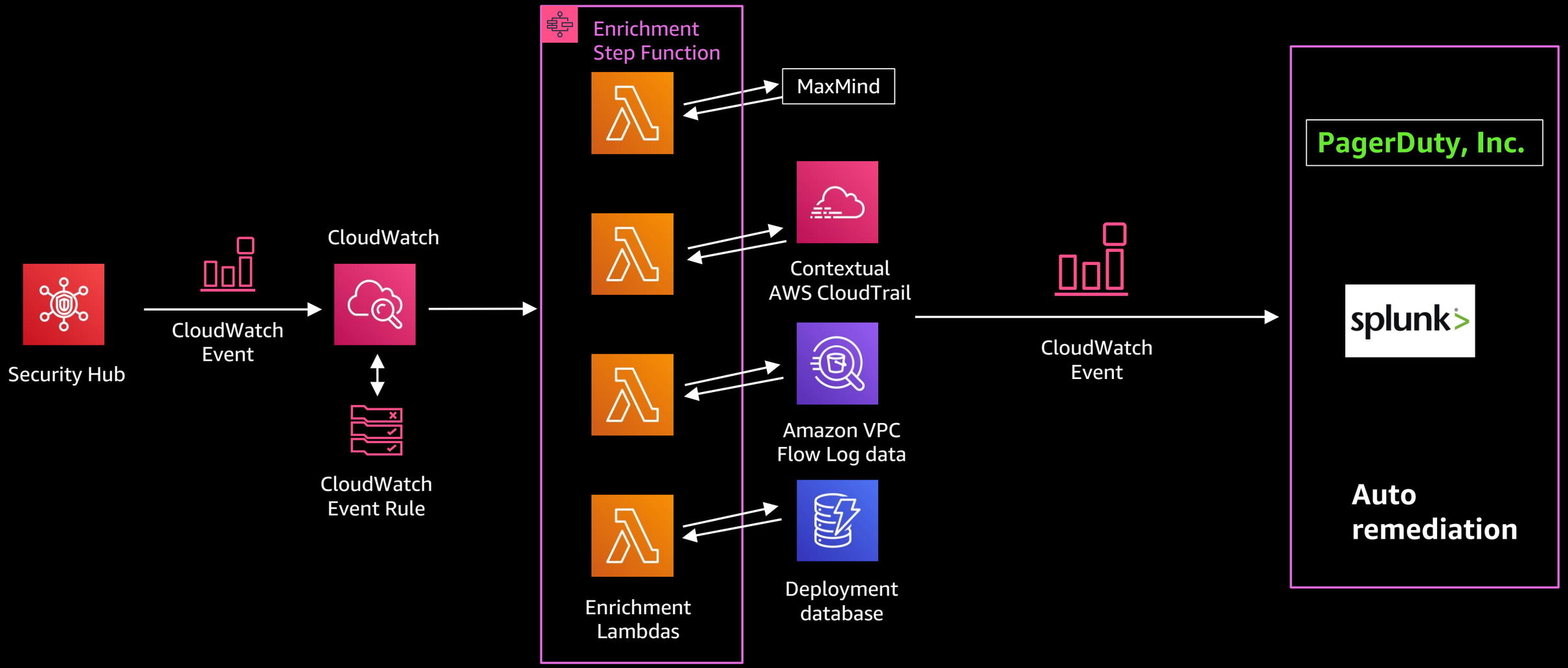
AWS Security Hub finding

ORIGINAL FINDING





Enrichment and auto remediation architecture



AWS Security Hub finding

ENRICHED FINDING


```
"USERDEFINEDFIELDS": {
  "Business_Unit": "Web Server Architecture",
  "Account_Name": "Prod Tomcat Account",
  "Account_Type": "Prod",
  "VPC_Flow_Location": "s3://vpcflow-
  bucket/0cb9b1ec82915cf247f759d34b2adce5",
  "Contextual_CloudTrail_Location": "s3://contextual-cloudtrail-
  bucket/0cb9b1ec82915cf247f759d34b2adce5",
  "Enriched_IP_City": "Moscow",
  "Enriched_IP_Country": "Russia",
  "Enriched_IP_ASN": "AS60804"
}
```

AWS CloudTrail and Amazon VPC Flow evidence



Contextual evidence from CloudTrail

Timestamp	UserIdentity.ARN	Event name	Error code
2020-11-27T14:30:35	arn:aws:iam::XXXXXXXXXXXX:role/TomcatServerRole	ListBuckets	AccessDenied
2020-11-27T14:30:37	arn:aws:iam::XXXXXXXXXXXX:role/TomcatServerRole	DescribeInstances	
2020-11-27T14:30:41	arn:aws:iam::XXXXXXXXXXXX:role/TomcatServerRole	RunInstances	AccessDenied



Contextual evidence from VPC Flow

Timestamp	Instance ID	Port	Packet source address	Packet destination address	Action
2020-11-30T16:33:53	i-99999999	443	198.51.100.0	192.168.1.45	ALLOW
2020-11-30T16:30:55	i-99999999	2057	192.168.1.45	198.51.100.0	ALLOW
2020-11-30T16:31:01	i-99999999	9001	198.51.100.0	192.168.1.45	ALLOW

Are we done?



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

Digital forensic evidence

Disk forensic evidence

What

Point in time copy of all volumes attached to compromised instance

Why

- When and how did the malware get installed on the instance?
- How many times has the malware been run on the instance?
- How was the malware configured to run? (e.g., scheduled task or on boot)
- Were any other suspicious files (e.g., other malware, worms, or large encrypted archives) created on the instance?

Memory forensic evidence

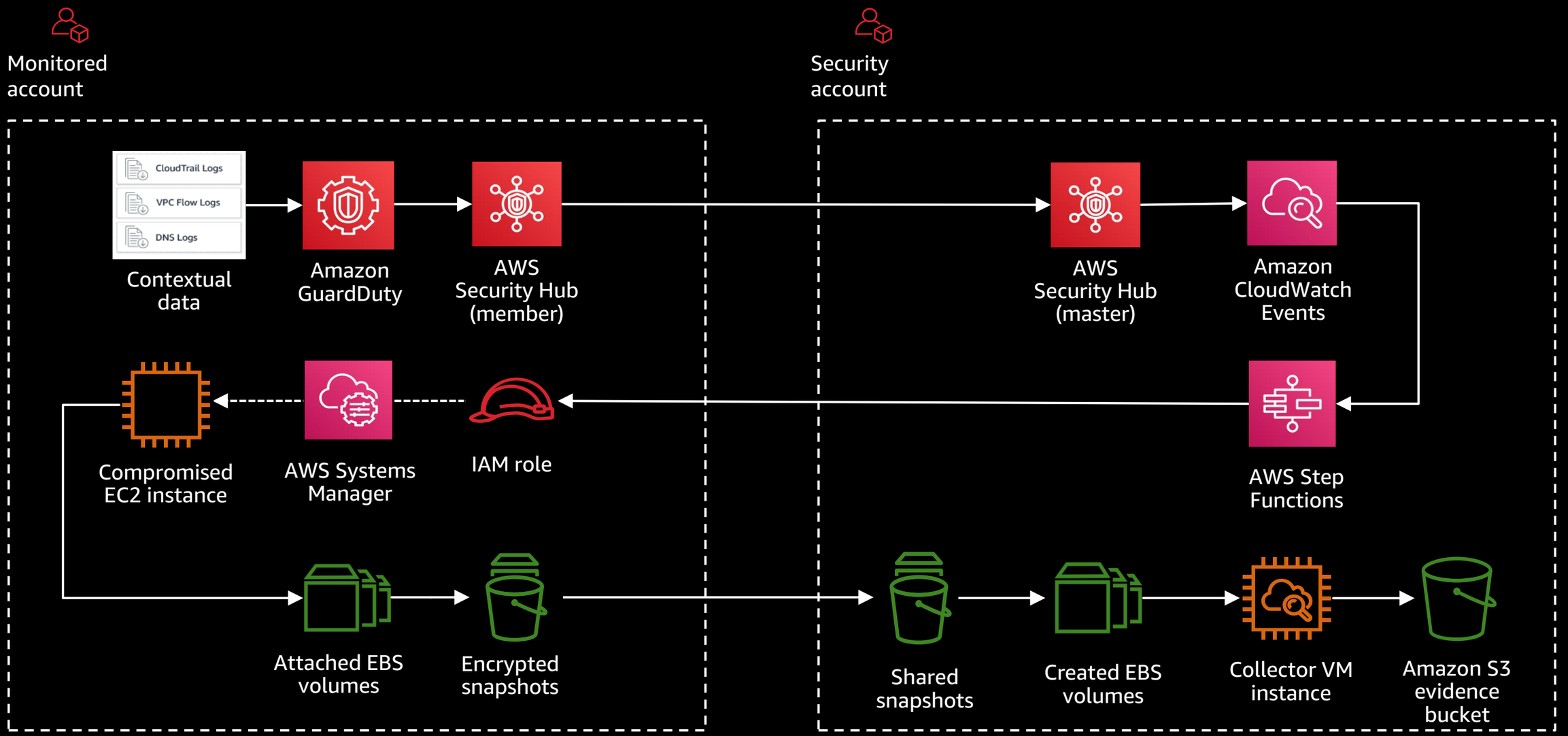
What

Point in time copy of memory (RAM) associated with compromised instance

Why

- What process is running the malware?
- What network connections has been established?
- What parent process executed the malware?
- What evasion techniques (if any) have been employed by the malware?

Sky Collect


Monitored account
Security account
CloudTrail Logs
VPC Flow Logs
DNS Logs
Contextual data
Amazon GuardDuty
AWS Security Hub (member)
AWS Security Hub (master)
Amazon CloudWatch Events
Compromised EC2 instance
AWS Systems Manager
IAM role
AWS Step Functions
Attached EBS volumes
Encrypted snapshots
Shared snapshots
Created EBS volumes
Collector VM instance
Amazon S3 evidence bucket

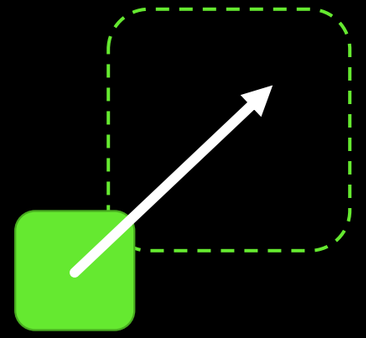
Benefits of Sky Watch



Near real-time response



Cost-effective, serverless workflows



Scalable, auditable and event driven

Metrics on Sky Watch and Sky Collect



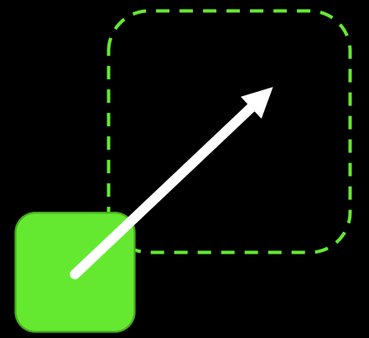
12 hours → 70 seconds

Mean detection to remediation time



63%

Average monthly cost savings



80 minutes → 11 minutes*

Disk evidence collection time savings

Summary

- Discussed challenges of aggregating multiple, disparate sources across a large number of accounts
- Reviewed Sky Watch and Sky Collect solutions built by Goldman Sachs
- Demonstrated cost and time savings achieved using Sky Watch / Sky Collect solutions

Appendices



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

Resources

APPENDIX A

AWS Q3 Tech Talk: Disk and Memory Evidence Collection

AWS re:Invent 2019

- SEC301 – Automating threat detection and response in AWS
- SEC318 – DIY guide to runbooks, incident reports, and incident response

---

AWS re:Invent 2020

- SEC301 – Security investigations with Amazon Detective
- SEC307 – Use Amazon GuardDuty and AWS Security Hub to secure multiple accounts
- SEC313 – A security operator's guide to practical AWS CloudTrail analysis
- **And many more!**

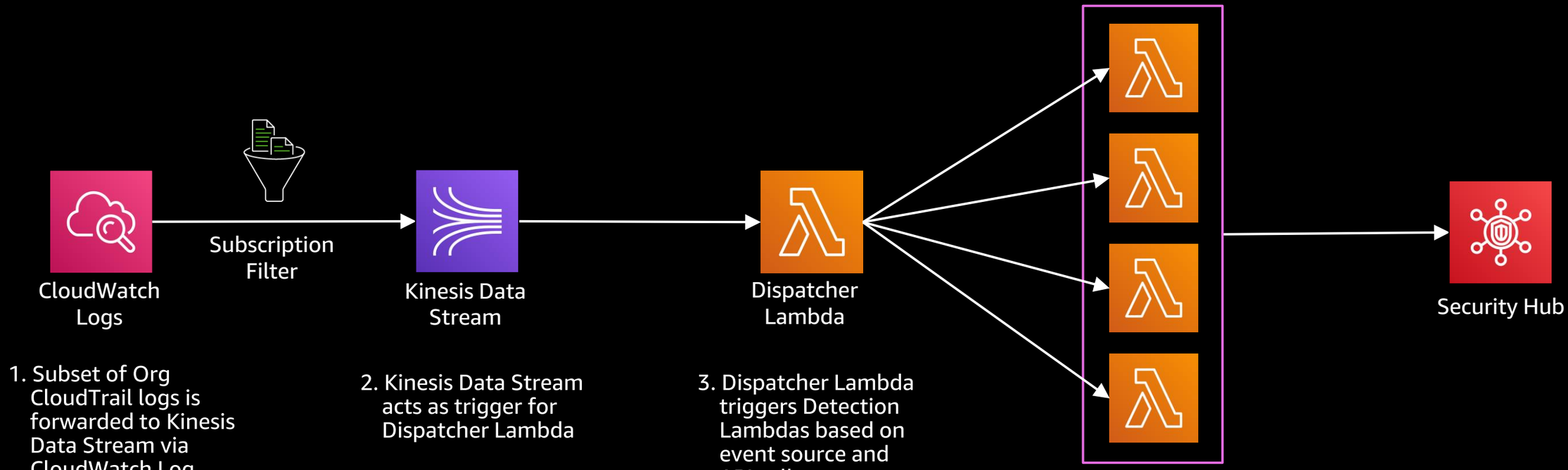
Pro tips

APPENDIX B

- Consider deploying in phases
  1) **Native integrations** – Security Hub has many useful native integrations with services (e.g., GuardDuty, Macie, and Inspector); integrations are enabled by default on initial Security Hub configuration
  2) **Custom Integrations** – For services that do not yet support native Security Hub integration, bespoke solutions must be created to import findings as custom findings
  3) **Enrichments** – Leverage UserDefinedFields and BatchUpdateFindings API to provide and store contextual enrichment data in the finding
- Evaluate business impact before turning on auto remediations
- Design to be fault tolerant, enable monitoring, and establish SLAs to minimize downtime – anything could fail at any time

CloudTrail detection architecture

APPENDIX C



1. Subset of Org CloudTrail logs is forwarded to Kinesis Data Stream via CloudWatch Log Subscription Filter

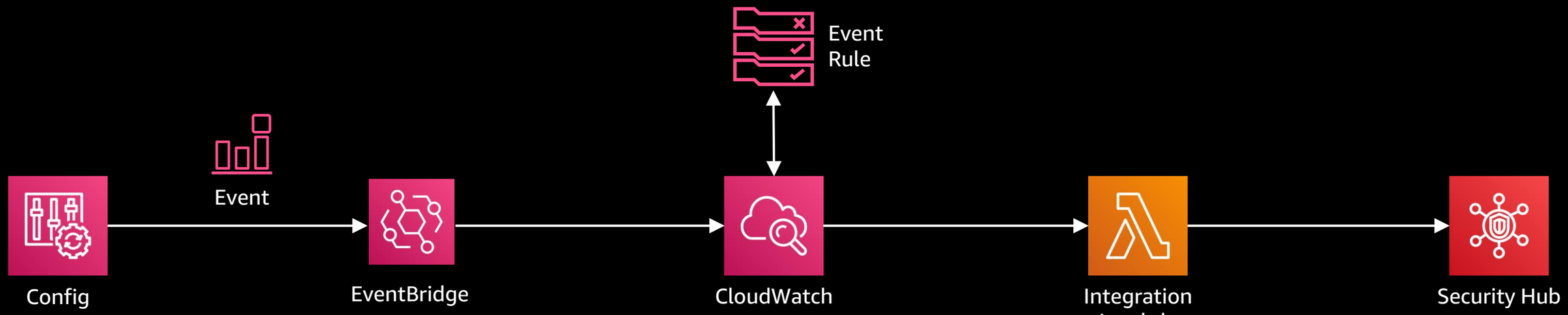
2. Kinesis Data Stream acts as trigger for Dispatcher Lambda

3. Dispatcher Lambda triggers Detection Lambdas based on event source and API call

4. Detection Lambdas evaluate API call and import true positives into Security Hub

Config detection architecture

APPENDIX D



1. Config evaluates resource for compliance change

2. Compliance change notification forwarded to Security account Event Bridge as CloudWatch Event

3. CloudWatch Event Rule picks up event and triggers Integration Lambda

4. Integration Lambda extracts relevant fields and imports finding into Security Hub

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.