

Part 2

AWS Workshop Series Day 6: Security Hub

Taking Enterprise Beyond the Cloud by TruelDC

Mr. Athiwat Itthiwatana

Cloud & Solution Consultant



Presented by



- Athiwat Itthiwatana (HAM)
- Cloud & Solution Consultant, TrueIDC
- AWS Specialist
- SAP Basis Specialist
- athiwat.itt@ascendcorp.com



Agenda

- A least privilege
- Security at Scale
- Security Hub



Source: AWS Immersion day



A wide-angle photograph of a winding asphalt road leading through a dense forest of tall evergreen trees towards a range of rugged, light-colored mountains under a dramatic sky with scattered clouds.

Least privilege is a journey

Who can access what

Who



People and
applications

Can access



Permissions

What



Resources

Inspecting overly permissive access

Public and cross-account access



Findings using IAM Access Analyzer

PassRole access



Security warnings using policy validation with IAM Access Analyzer

Powerful permissions



Service and action last accessed



Policy generation with IAM Access Analyzer

1

Run your application or task

2

Request a policy from IAM Access Analyzer

3

IAM Access Analyzer gets to work

4

Customize further and apply

Generated policy

Review and create managed policy

Review the permissions summary, add tags, and create the generated policy as a customer managed policy

Name* Use alphanumeric and '+-_@-' characters. Maximum 128 characters.

Description Maximum 1000 characters. Use alphanumeric and '+-_@-' characters.

Summary

Service	Access level	Resource
CloudFormation	Limited: List	StackName string like All
CloudWatch Logs	Limited: Write	LogGroupName string like All
EC2	Limited: List	All resources
Resource Group Tagging	Limited: Read	All resources
Resource Groups	Limited: List	arn:aws:resource-groups:us-west-2: [REDACTED]:group/Pickles-Pasture
S3	Limited: Read	BucketName string like All
Secrets Manager	Limited: Read	arn:aws:secretsmanager:us-west-2: [REDACTED] secret:*



Policy generation inputs

1

Run your application or task

2

Request a policy from IAM Access Analyzer

Tell us the following inputs from Step 1:

- Application role used
- Time period
- CloudTrail trail and access
- AWS Regions

Generate policy for pickles-pasture-audit

Generate a policy based on the CloudTrail activity for this role.

Time period and permissions to analyze CloudTrail events

Select time period

Last 1 day(s)

Specific dates

Choose a range of up to 90 days.

CloudTrail access

CloudTrail trail to be analyzed

Specify the CloudTrail trail that logs events for this account

US West (Oregon)

IsengardTrail-DO-NOT-DELETE

Specify regions

Activities for services only from the selected regions will be reviewed to generate the policy.

Select regions

US West (Oregon) X

To analyze this role's access activity, IAM uses the service role below on your behalf to access the specified trail.

- Create and use a new service role
- Use an existing service role

AccessAnalyzerMonitorServiceRole_C8USKW1KKE

[View role details](#)

[Cancel](#)

[Generate policy](#)



Source: AWS Immersion day



Policy generation analysis

3

IAM Access Analyzer gets to work

- Looks for all unique AWS actions
- Maps CloudTrail activity to IAM actions for 50+ services
- Generates policy that adheres to IAM policy language

4

Customize and apply

- Specify additional actions
- Specify resource-level permissions with templates

Generated policy

Customize permissions

Review the following policy template. You must specify resources for actions that support resource-level permissions to continue creating the policy.

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Action": [  
7                 "ec2:DescribeInstances",  
8                 "tag:GetResources"  
9             ],  
10            "Resource": "*"  
11        },  
12        {  
13            "Effect": "Allow",  
14            "Action": [  
15                "cloudformation:DescribeStacks",  
16                "cloudformation>ListStackResources"  
17            ],  
18            "Resource": "arn:aws:cloudformation:${Region}:${Account}:stack/${StackName}/${Id}"  
19        },  
20        {  
21            "Effect": "Allow",  
22            "Action": [  
23                "logs>CreateLogGroup",  
24                "logs>CreateLogStream"  
25            ],  
26            "Resource": "arn:aws:logs:${Region}:${Account}:log-group:${LogGroupName}"  
27        }  
]
```



Pro tip: Become besties with conditions



Grant access to these actions, **but only if** these conditions are met

```
"Effect": "Allow",
"Action": [
    "ec2:StartInstances",
    "ec2:StopInstances"],
"Resource": "*",
"Condition": {
    "StringEquals": {"ec2:ResourceTag/project": "cloudmigration"}}
```



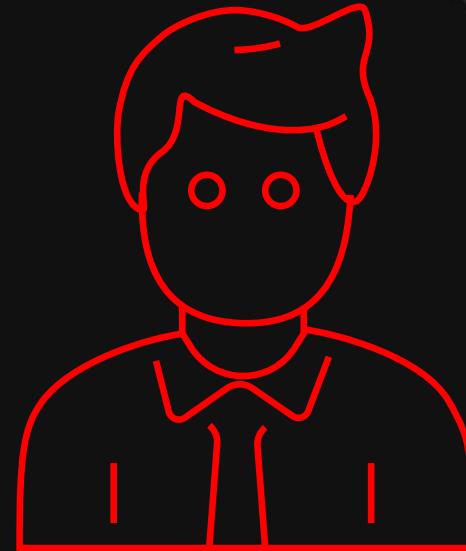
Security at Scale



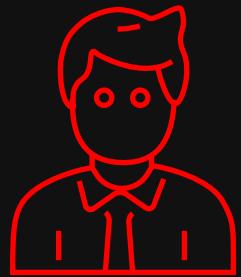
A Is for “Alice” and B Is for “Bob”

Alice follows best practices

Bob does NOT follow best practices



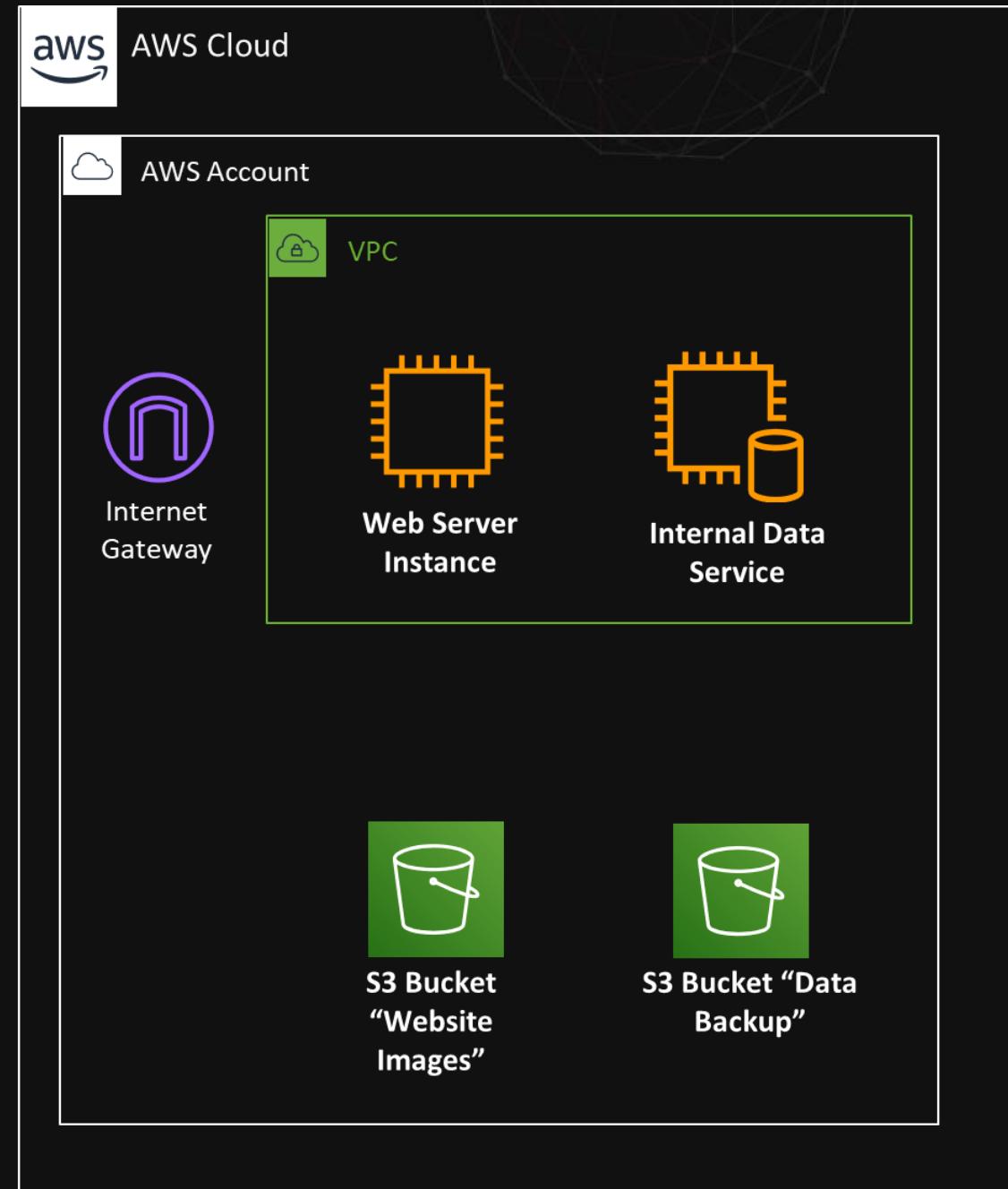
Bob's Bad Day



Bob



Internet



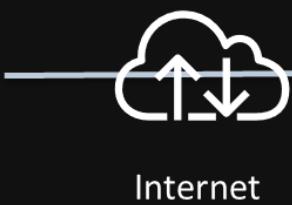
Source: AWS Immersion day



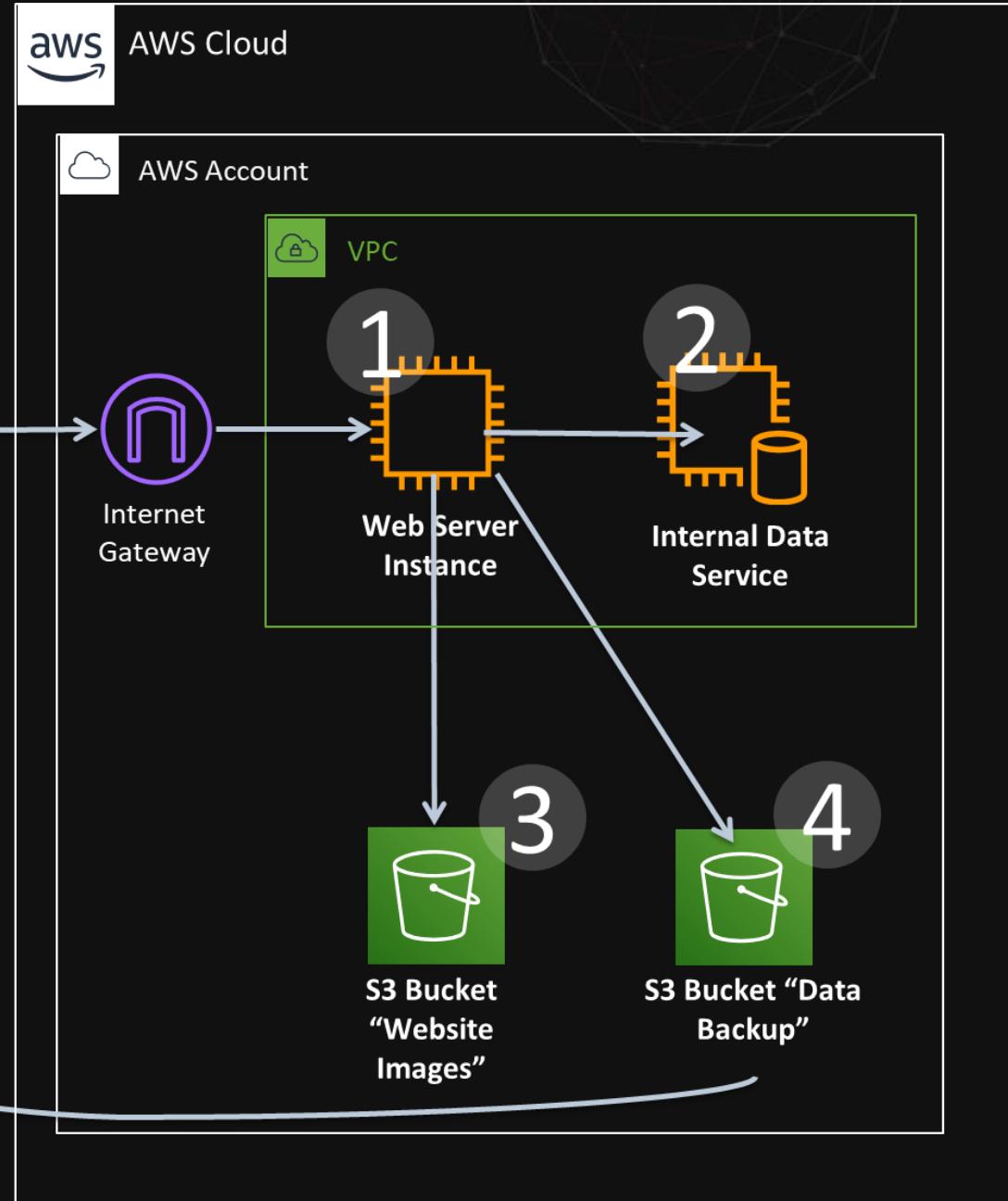
Bob's Bad Day



Intruder



Internet



1

Access the vulnerable web application

2

Pivot to the data service

3

Delete the website image files

4

Change permissions to the data backup

5

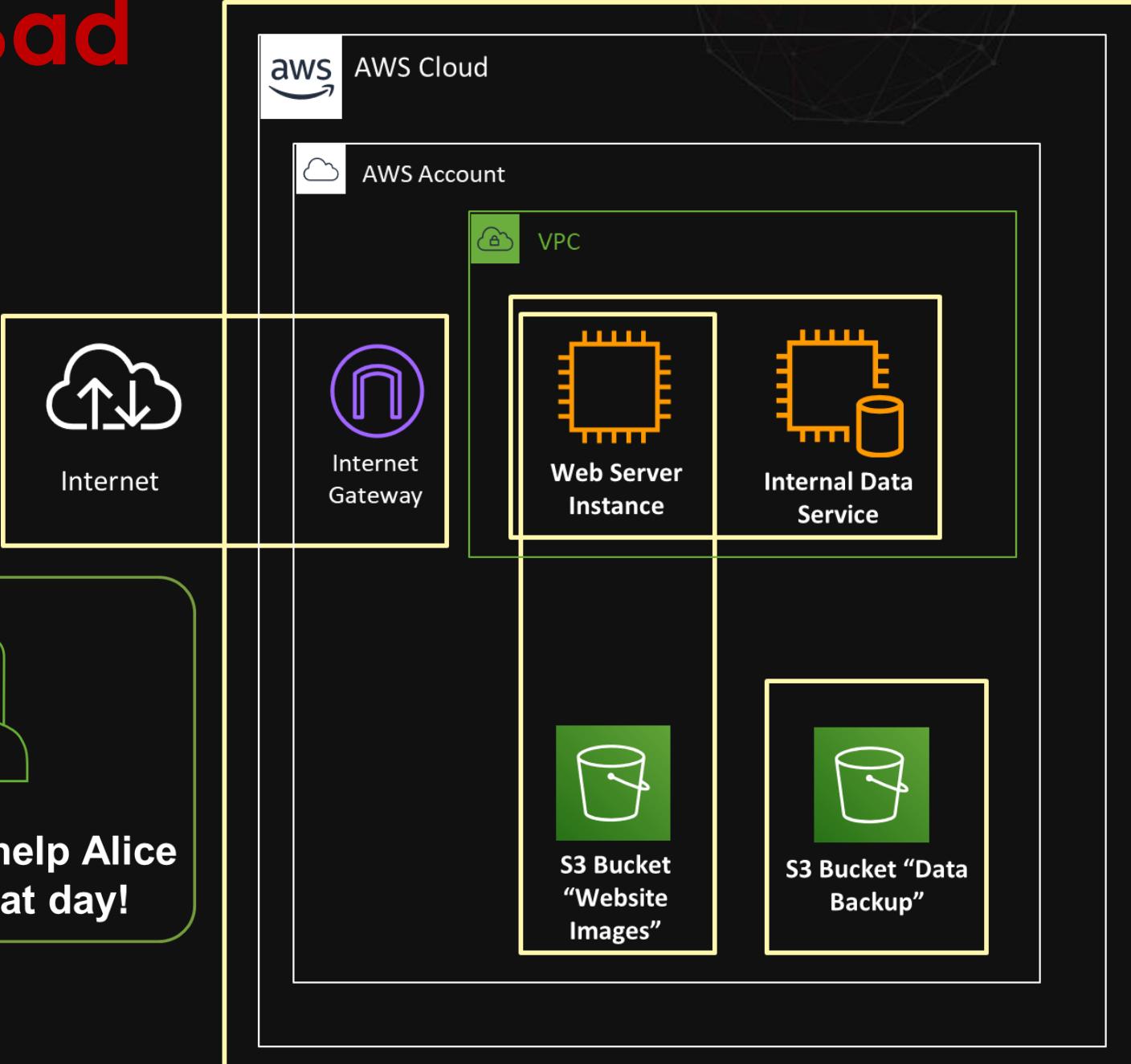
Download the data backup



Source: AWS Immersion day



Bill's Bad Day



- 1 No web application protection
- 2 No segmentation
- 3 One account
- 4 All permissions granted
- 5 Sensitive data not encrypted
- 6 No logging, monitoring, alerting

Best-of-the-Best Practices: Identity and Access Management

1) Use **multiple AWS accounts** to reduce scope of impact

Production



Staging



AWS accounts provide administrative isolation between workloads across different lines of business, regions, stages of production and classes of data.

2) Use **limited roles** and grant **temporary security credentials**



IAM



IAM Roles



Secrets Manager

IAM roles and temporary security credentials mean you don't always have to manage long-term credentials and IAM users for each entity that requires access to a resource.

3) **Federate** to an existing identity service



IAM



MFA token

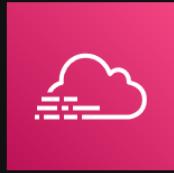


AWS SSO

Control access to AWS resources, and manage the authentication and authorization process without needing to recreate all your corporate users as IAM users.

Best-of-the-Best Practices: Logging and Monitoring

4) Turn on **logging** in all accounts, for all services, in all regions



AWS
CloudTrail



Amazon GuardDuty

5) Use the AWS platform's built-in **monitoring and alerting** features



AWS Security
Hub



AWS Config

The AWS API history in CloudTrail enables security analysis, resource change tracking, and compliance auditing. GuardDuty provides managed threat intelligence and findings.

Monitoring a broad range of sources will ensure that unexpected occurrences are detected. Establish alarms and notifications for anomalous or sensitive account activity.

6) Use a separate AWS account to fetch and **store copies of all logs**



Production



Security

Configuring a security account to copy logs to a separate bucket ensures access to information which can be useful in security incident response workflows.

Best-of-the-Best Practices: Infrastructure Security

7) Create a **threat prevention layer** using AWS edge services



Amazon
CloudFront

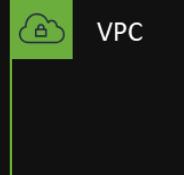


AWS Shield

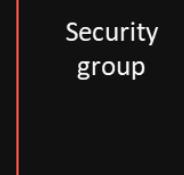


AWS WAF

8) Create **network zones** with Virtual Private Clouds (VPCs) and security groups

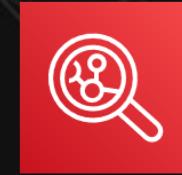


VPC



Security
group

9) Manage vulnerabilities through **patching and scanning**



Amazon Inspector

Use the hundreds of worldwide points of presence in the AWS edge network to provide scalability, protect from denial-of-service attacks, and protect from web application attacks.

Implement security controls at the boundaries of hosts and virtual networks within the cloud environment to enforce access policy.

Test virtual machine images and snapshots for operating system and application vulnerabilities throughout the build pipeline, and into the operational environment.



Best-of-the-Best Practices: Data Protection

10) Encrypt **data at rest** (with occasional exceptions)



AWS KMS



Amazon S3

11) Use **server-side encryption** with provider managed keys



AWS KMS



Data Encryption Key

12) Encrypt **data in transit** (with no exceptions)



Amazon CloudFront



Certificate Manager



SSL / TLS /
HTTPS

Enabling encryption at rest helps ensure the confidentiality and integrity of data. Consider encrypting everything that is not public.

AWS Key Management Service (KMS) is seamlessly integrated with multiple AWS services. You can use a default master key or select a custom master key, both managed by AWS.

Encryption of data in transit provides protection from accidental disclosure, verifies the integrity of the data, and can be used to validate the remote connection.



Security Hub



Source: AWS Immersion day

AWS Security Hub Information Flows



And more to come...



CROWDSTRIKE



Plus dozens of others...

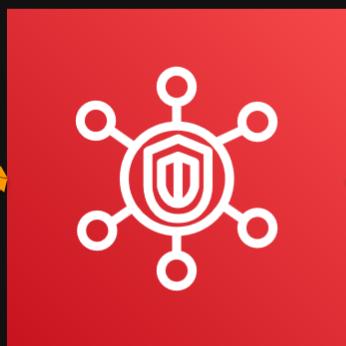


Plus dozens of others...

Findings

Findings

Security Checks



Findings



Findings

Findings



Investigations

Remediation Actions



Taking Action Partners



Plus many others...



AWS Security Hub

CONTINUOUS SECURITY ASSESSMENT & AUTOMATED RESPONSE LAYER

Centrally view & manage security alerts & automate security checks



Save time with aggregated findings



Improve security posture with automated checks



Curated security best practices



Seamless integration w/ standardized findings format



Account 1
Account 2
Account 3

Multi-account support



Source: AWS Immersion day



Automated security & compliance checks

Security Hub > Security standards

Security standards

New AWS Foundational Security Best Practices v1.0.0 by AWS

Description: The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve your security posture in AWS, and covers AWS's most popular and foundational services.

Security score: 58%



Disable View results

CIS AWS Foundations Benchmark v1.2.0 by AWS

Description: The Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.

Security score: 19%



Disable View results

PCI DSS v3.2.1 by AWS

Description: The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data. This Security Hub standard automatically checks for your compliance readiness against a subset of PCI DSS requirements.

Security score: 41%



Disable View results

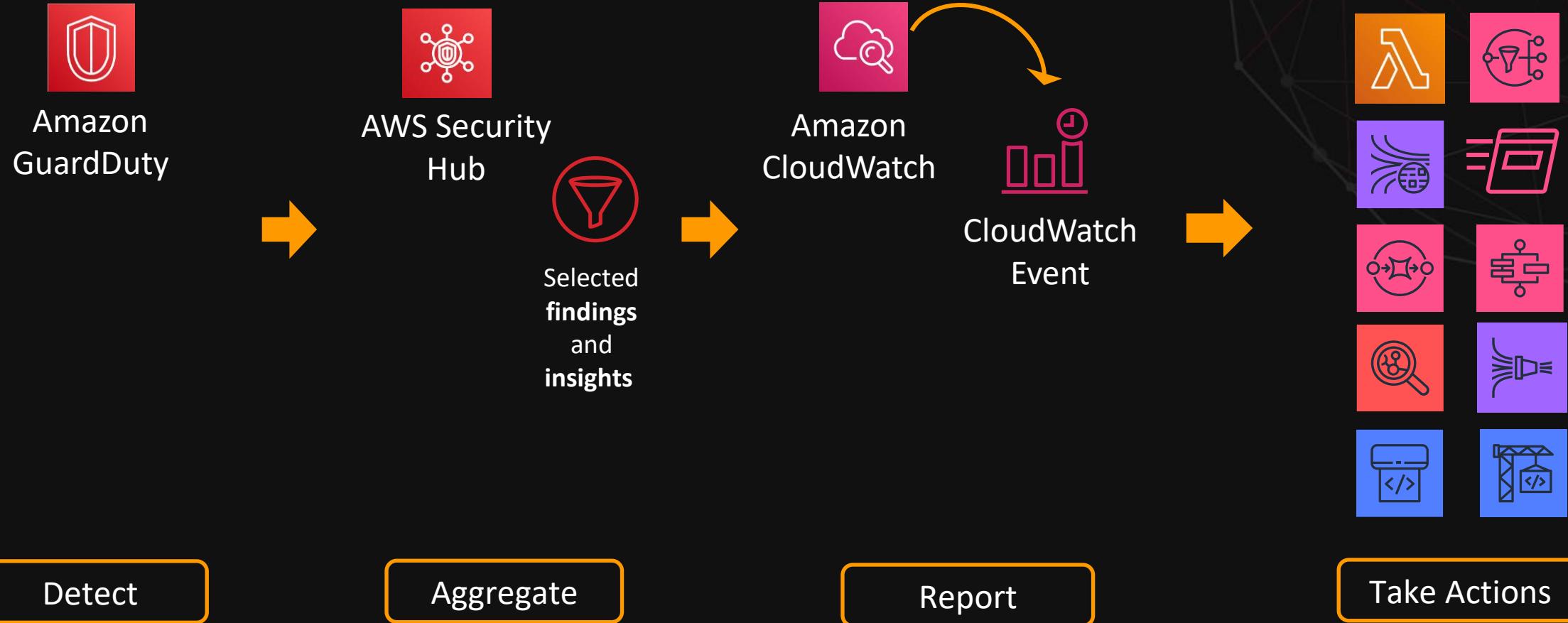
- 150+ fully automated, nearly continuous checks evaluated against pre-configured rules
- Findings are displayed on main dashboard for quick access.
- Best practices information is provided to help mitigate gaps to be in compliance.



Source: AWS Immersion day



How do I automate response & remediation?



Detect

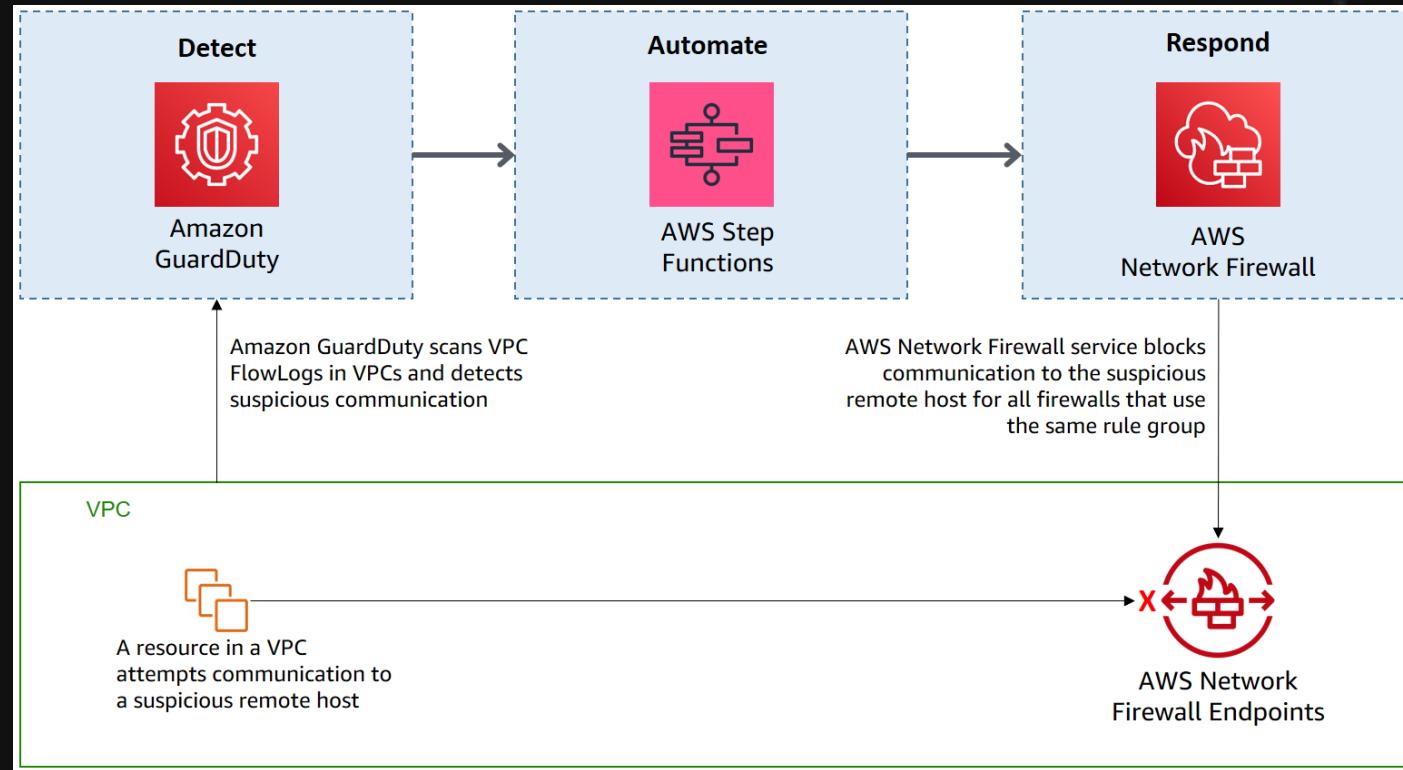
Aggregate

Report

Take Actions



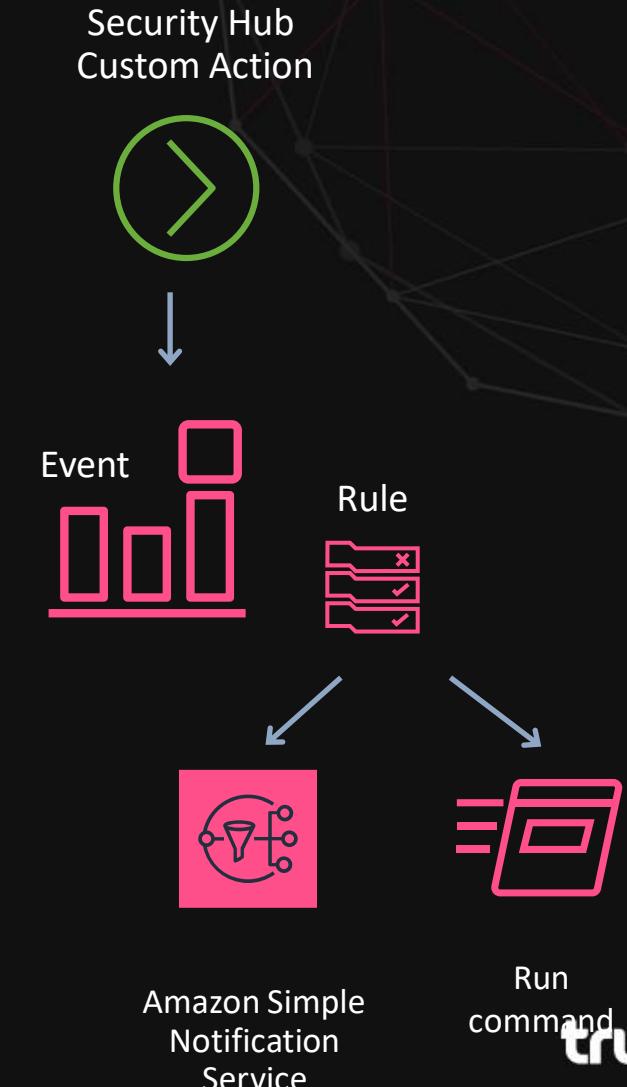
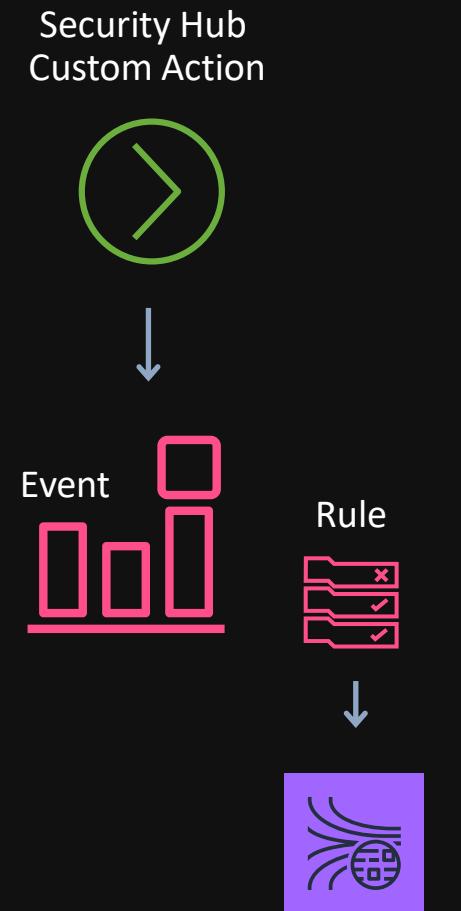
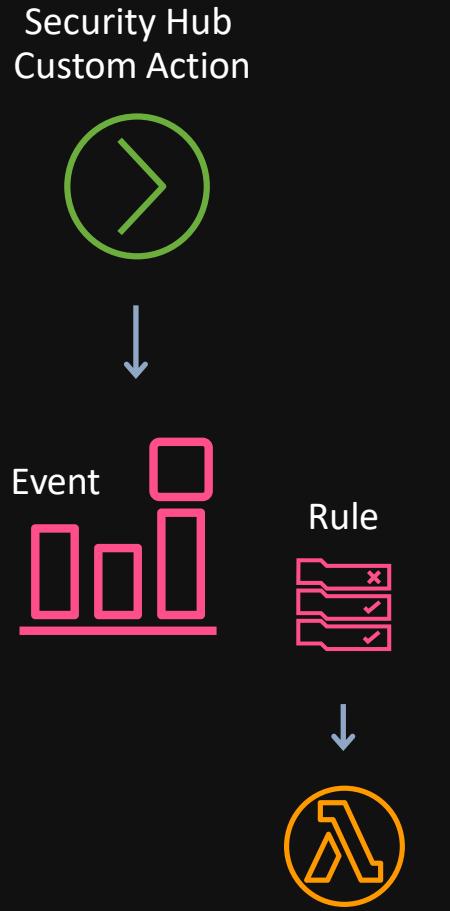
Automated detection & response



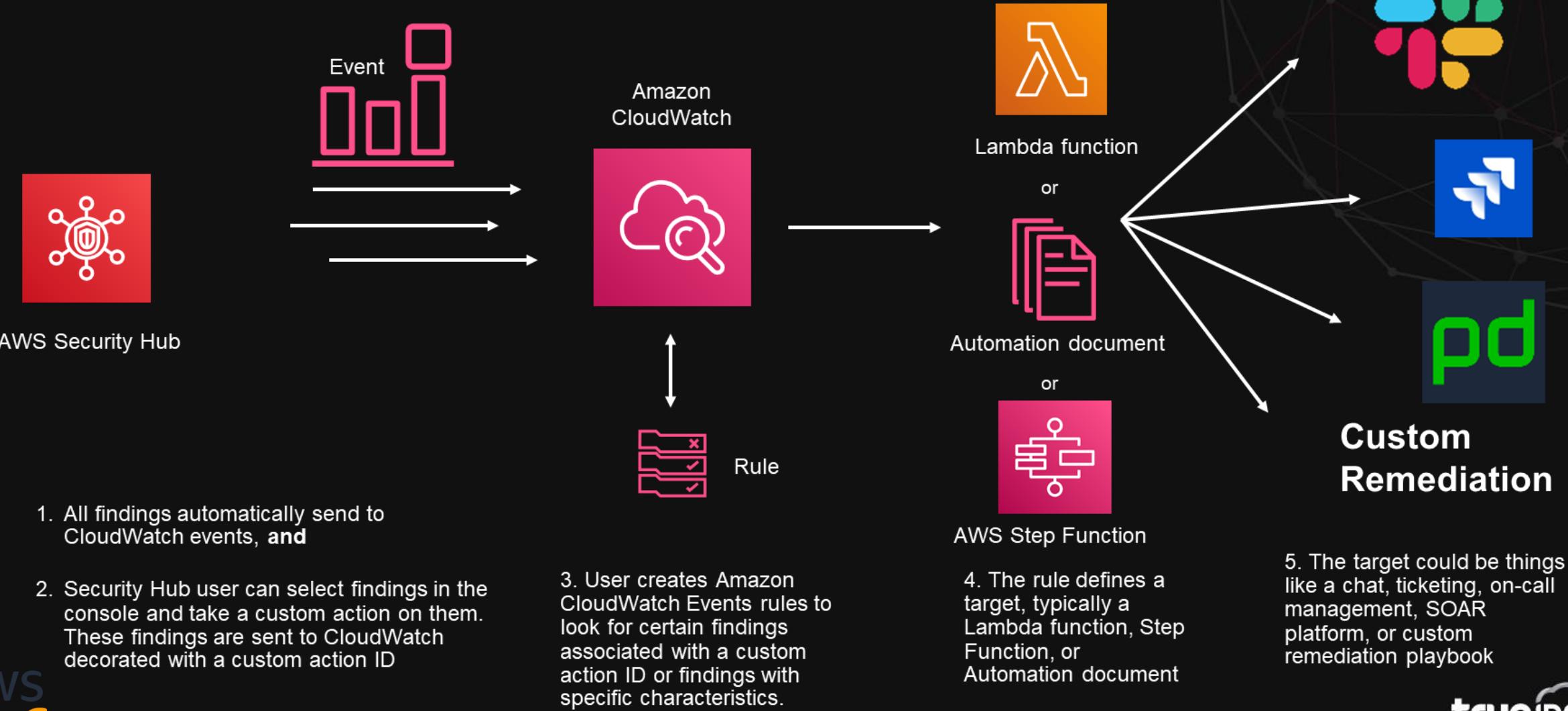
- Blocking traffic to and from suspicious remote hosts, for example to IP addresses associated with known command and control servers for botnets.
- GuardDuty detection of unintended communication with remote hosts triggers a series of steps, including blocking of network traffic to those hosts by using Network Firewall, and notification of security operators.



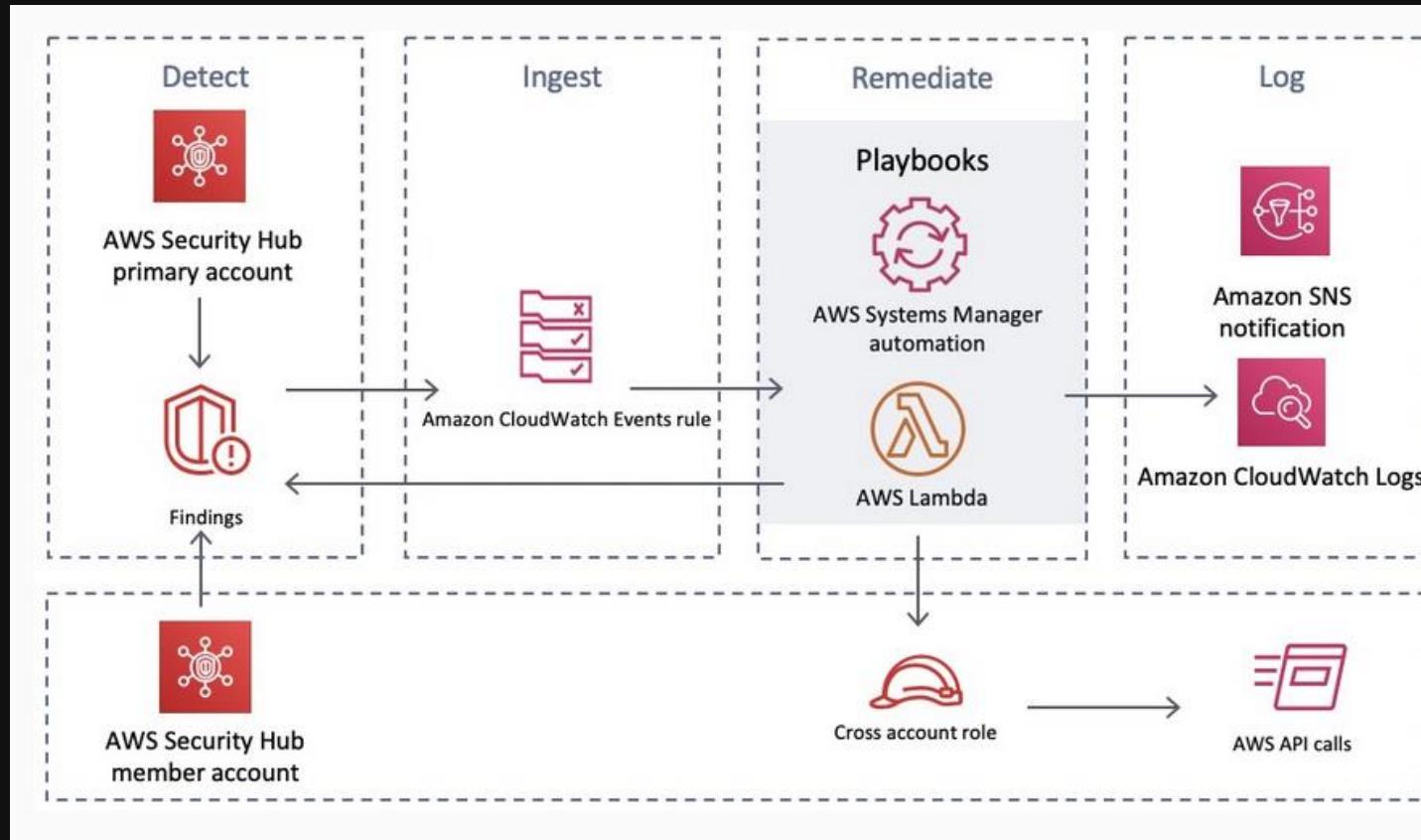
Use Security Hub Custom Actions to trigger automation



Customizable response and remediation actions



AWS Security Hub Automated Response and Remediation solution architecture



AWS Security Hub Automated Response and Remediation

Version 1.0

Last updated: 08/2020

Author: AWS

Estimated deployment time: 10 min

[Source code](#)

[CloudFormation template](#)

[View deployment guide](#)

[Launch in the AWS Console](#)

Deployment resources

<https://aws.amazon.com/solutions/implementations/aws-security-hub-automated-response-and-remediation/>



Source: AWS Immersion day



Layer Threat Detection and Response Services

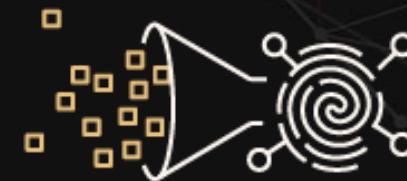
ADVANCED THREAT DETECTION AND RESPONSE ON AWS



Security tools natively available in AWS



Reduce the burden for the security team



Centralized & scalable deployment with a click of a button



Source: AWS Immersion day



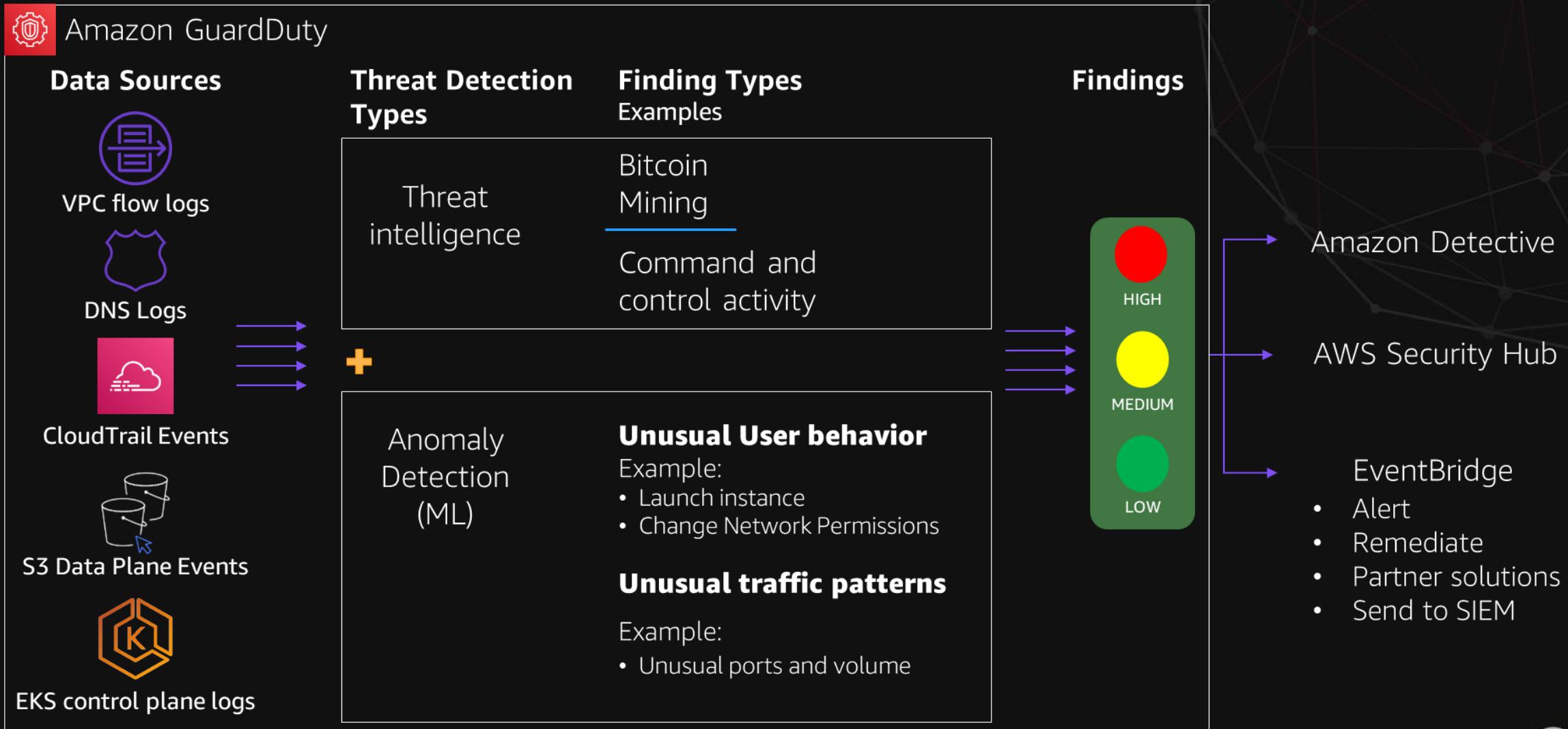
Appendix

AWS Config

- Logs resource configurations (changes) over time
 - What was created/changed
 - What was the state/details of the configuration
- Can also record (with instrumentation) Instance OS/Software configuration changes and updates
- Leverage these logs to discover, map, track (and alert on) AWS resource relationships and changes in your account



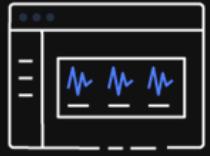
Amazon GuardDuty



Source: AWS Immersion day



Amazon Inspector



Gain centralized visibility

- Environment coverage
- High impact findings
- Resources by finding severity



One-click continuous monitoring

- Automatic discovery of resources
- Monitors throughout the resource life-cycle



Prioritize with contextualized scoring

- Inspector Risk score
- Security metrics
- Customized views



Centrally manage at scale

- AWS Organizations
- Package vulnerability, Network reachability
- Environment coverage



Automate and take actions

- Management APIs
- Detailed findings in Eventbridge
- Security Hub integration

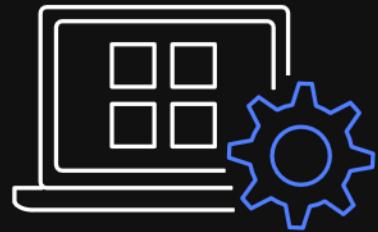


Amazon Detective

Quickly analyze, investigate, and identify root cause of security issues



Built-in data
collection

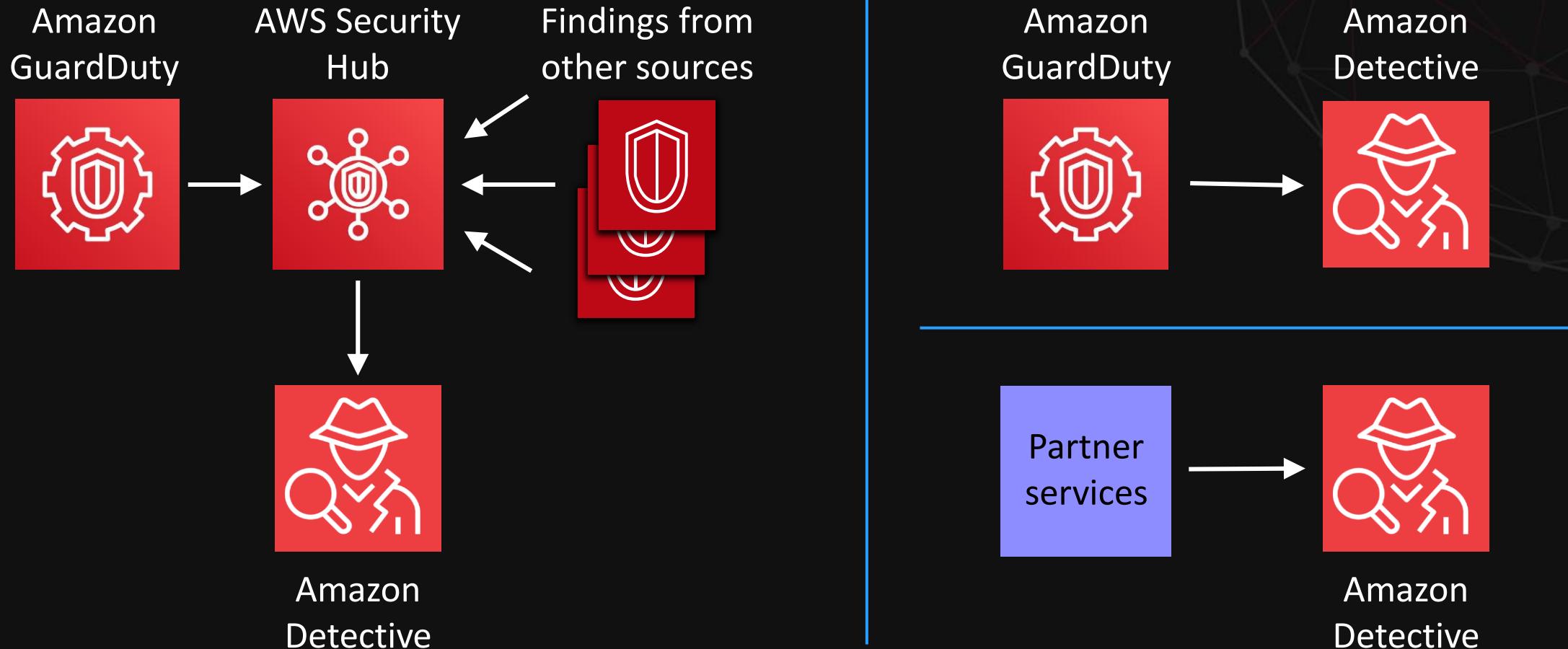


Automated analysis



Visual insights

Amazon Detective usage flow



Security behavior graph



Amazon Inspector



Source: AWS Immersion day



Lab: Security Hub



<https://github.com/TIDC-PS-Inter/AWS-Workshop>



REGIONAL
DATA CENTER &
CLOUD SERVICE
PROVIDER