Part 2

AWS Workshop Series

Day 6: Security Hub

Taking Enterprise Beyond the Cloud by TrueIDC

Mr. Athiwat Itthiwatana

Cloud & Solution Consultant

Presented by

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

trueIDC

Agenda

- A least privilege
- Security at Scale
- Security Hub

Source: AWS Immersion day

Who can access what

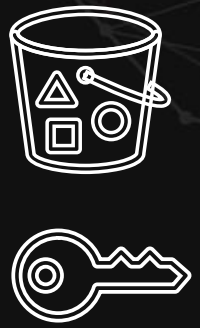
Who

People and applications

Can access

Permissions

What



Resources

Source: AWS Immersion day

Inspecting overly permissive access

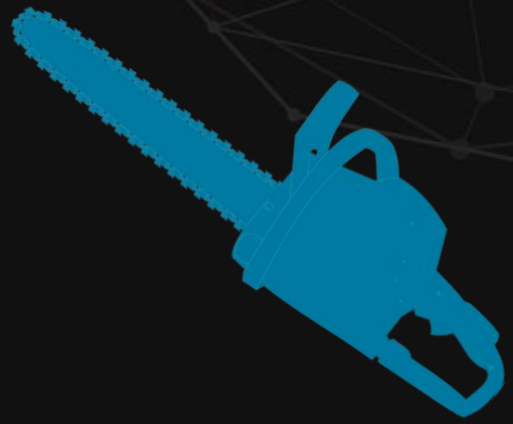
Public and cross-account access

Findings using IAM Access Analyzer

PassRole access

Security warnings using policy validation with IAM Access Analyzer

Powerful permissions

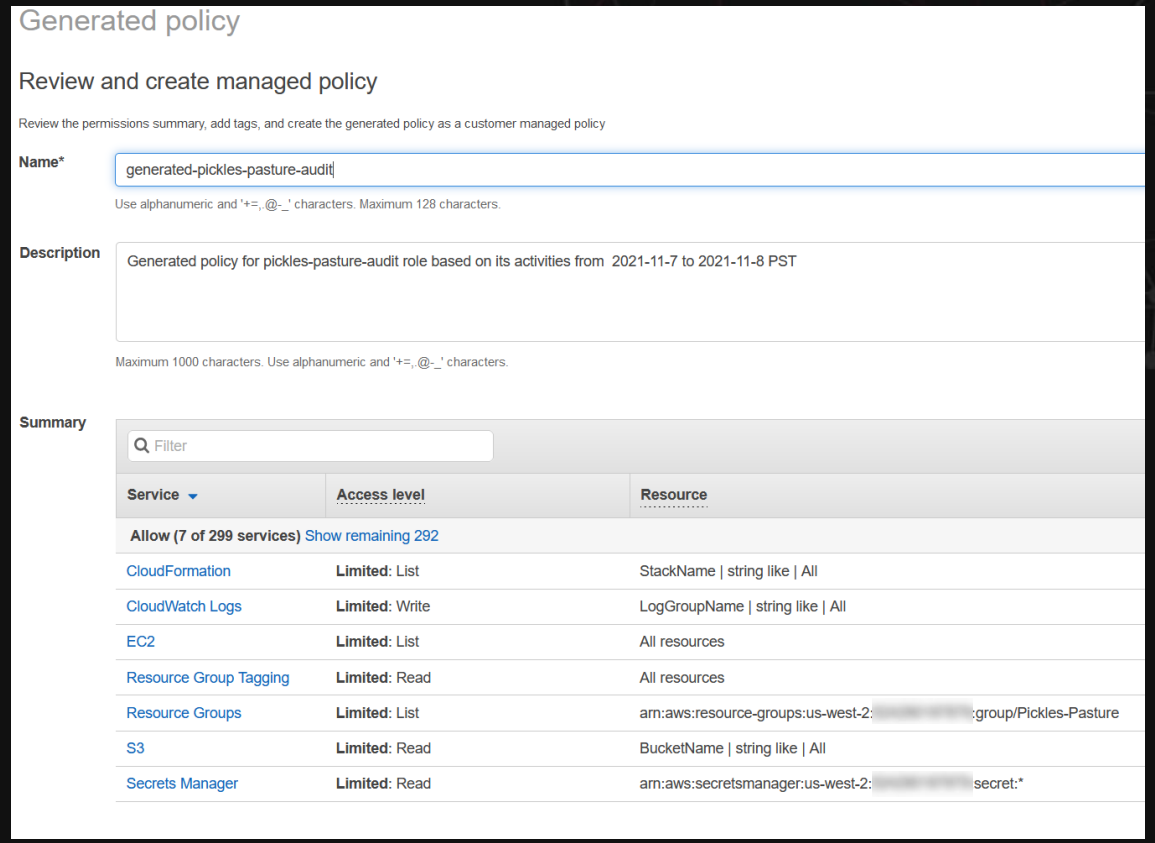


Service and action last accessed

Source: AWS Immersion day

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



Source: AWS Immersion day

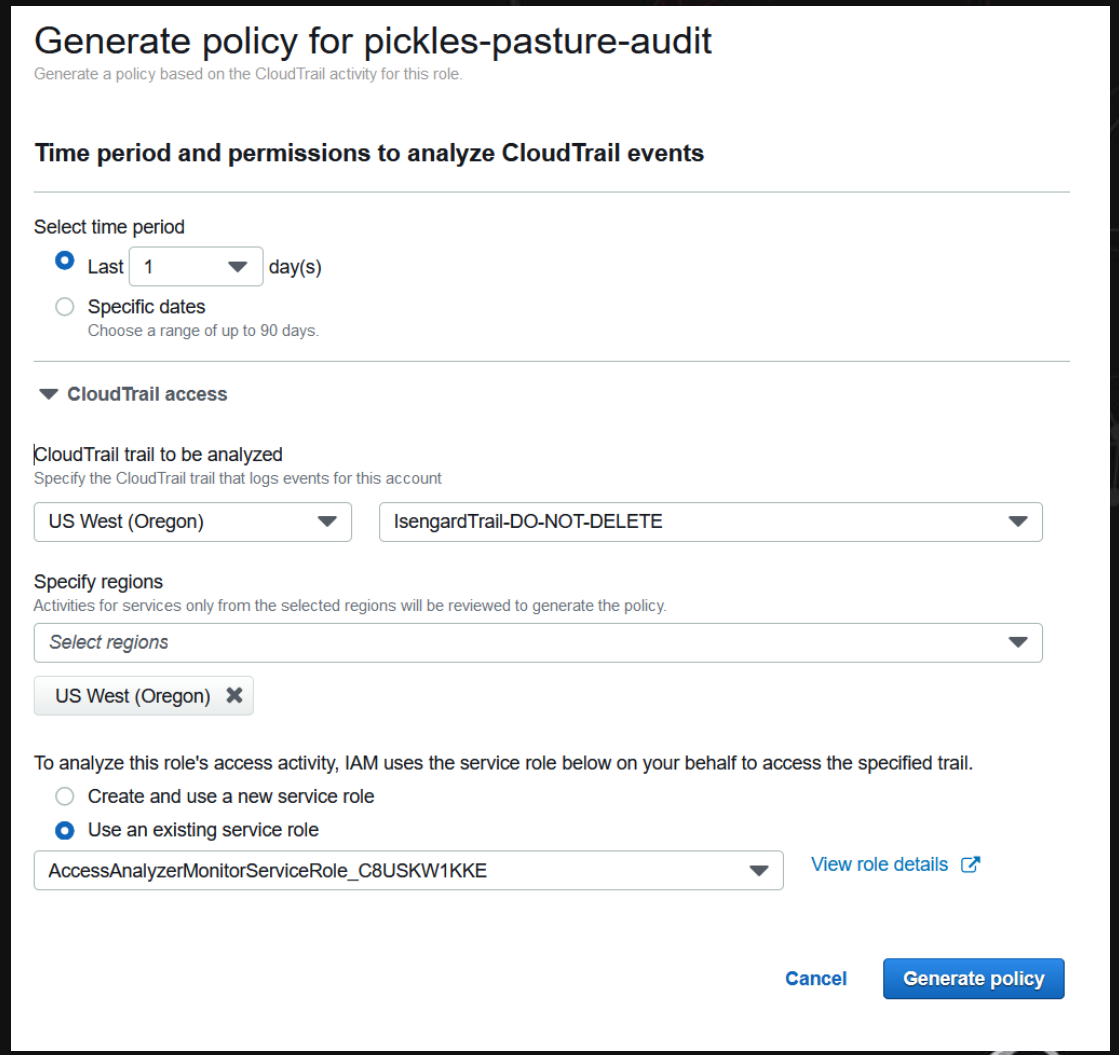
Policy generation inputs

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



Source: AWS Immersion day

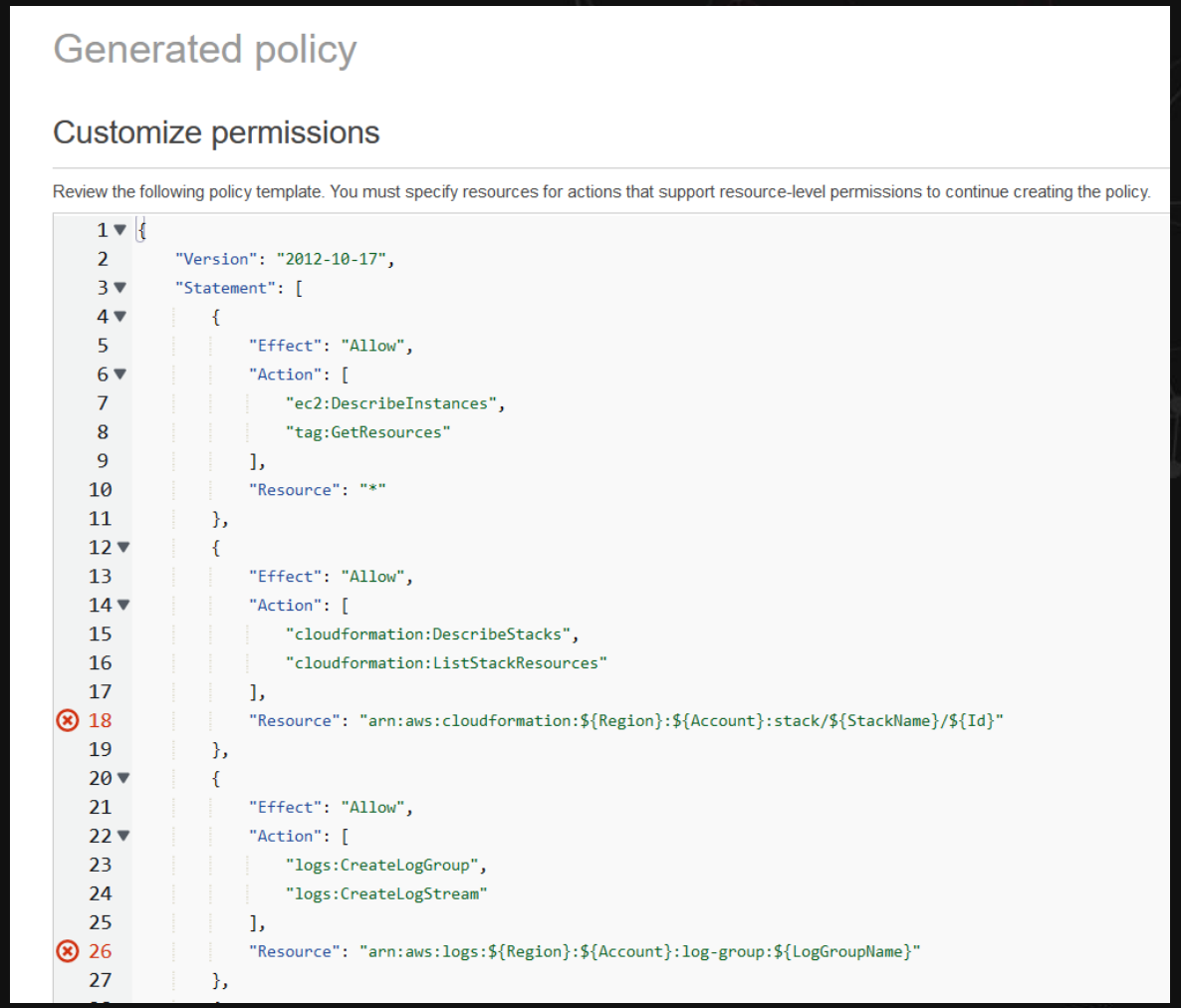
Policy generation analysis

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



Source: AWS Immersion day

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"}
            }
```

aws

Source: AWS Immersion day

trueIDC

Security at Scale

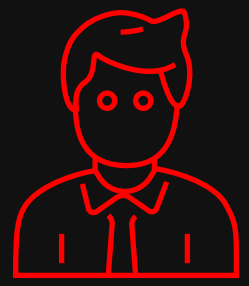
A Is for “Alice” and B Is for “Bob”

Alice follows best practices

Bob does NOT follow best practices

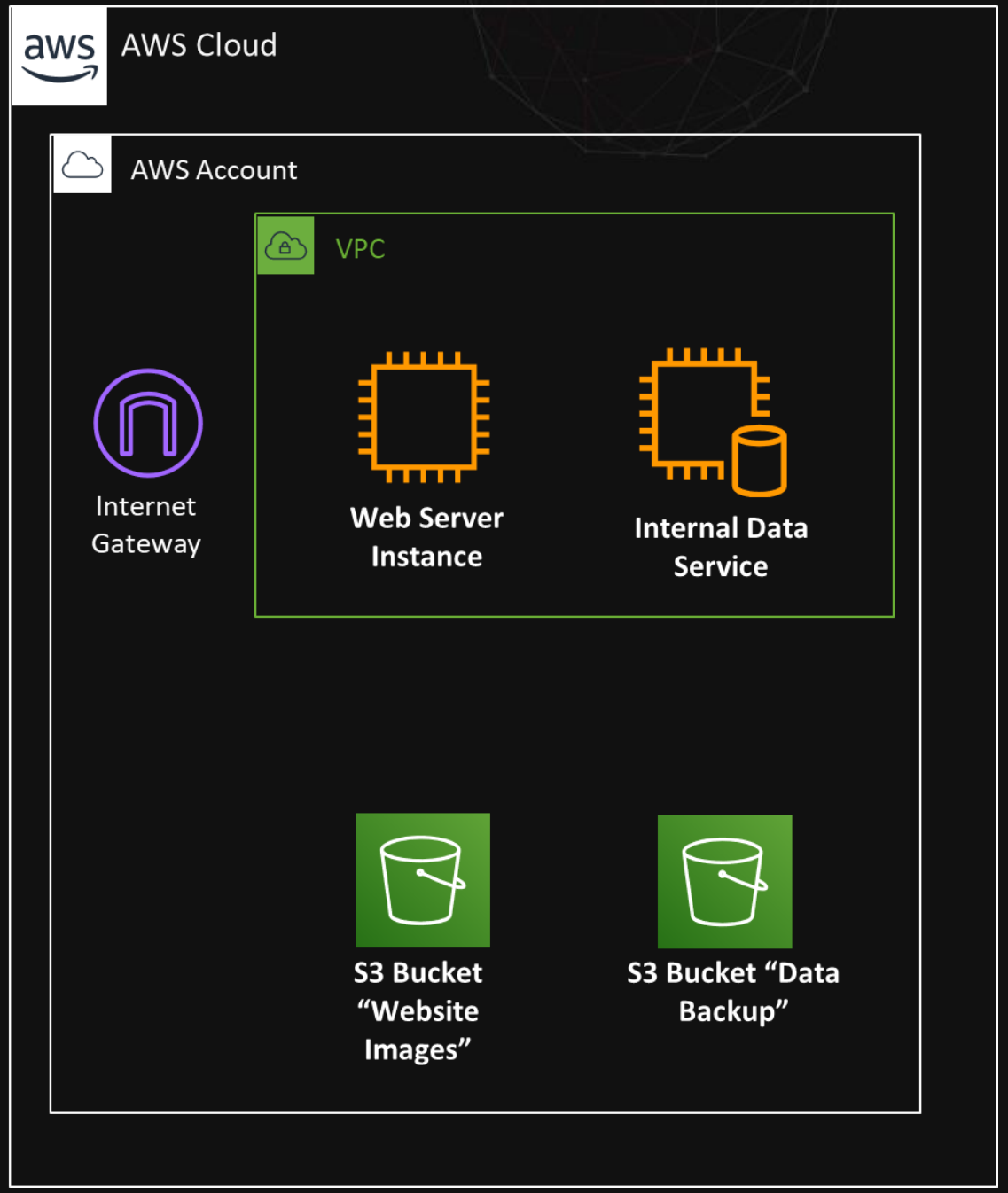
Source: AWS Immersion day

Bob's Bad Day



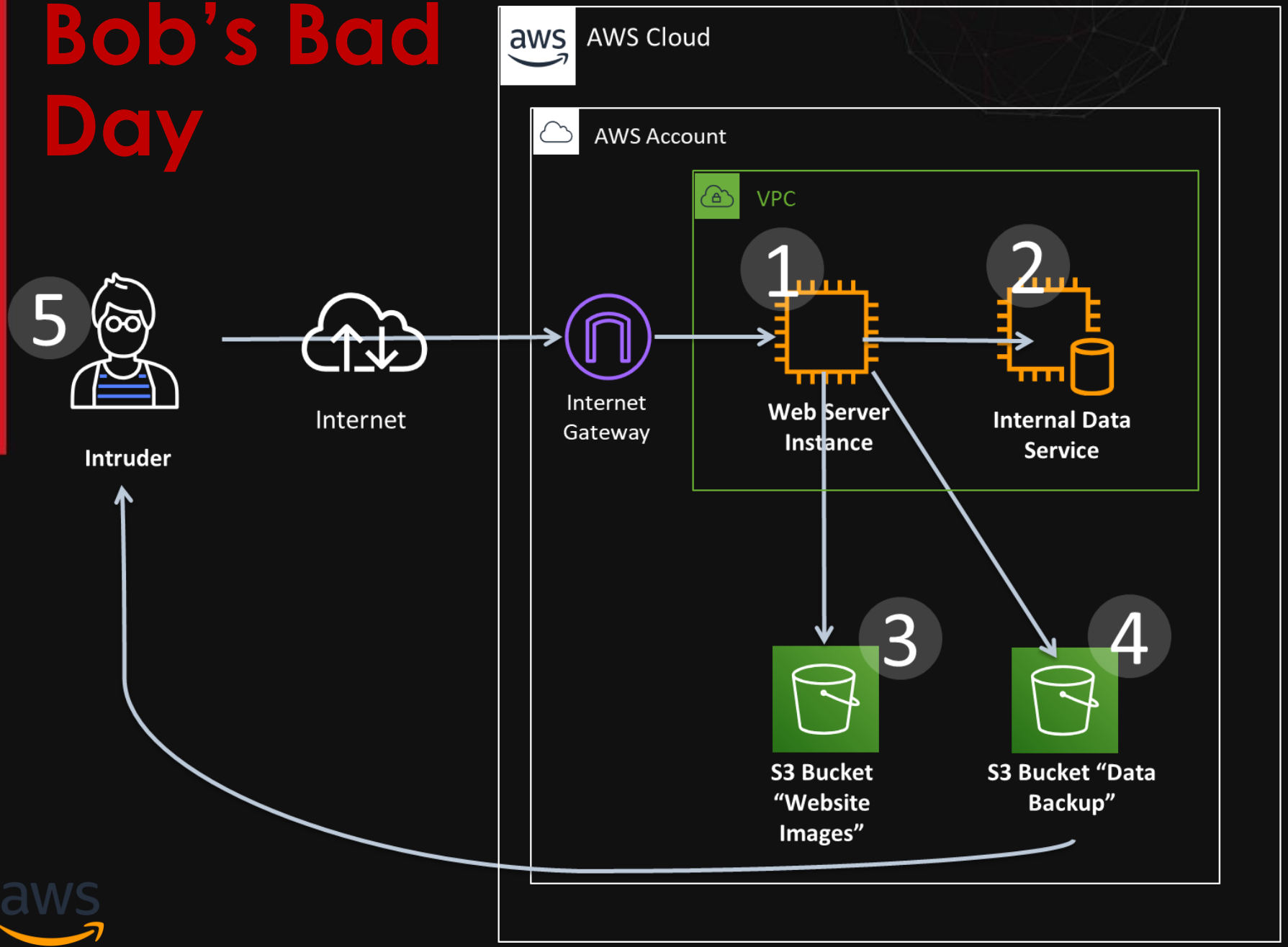
Bob

Internet



Source: AWS Immersion day

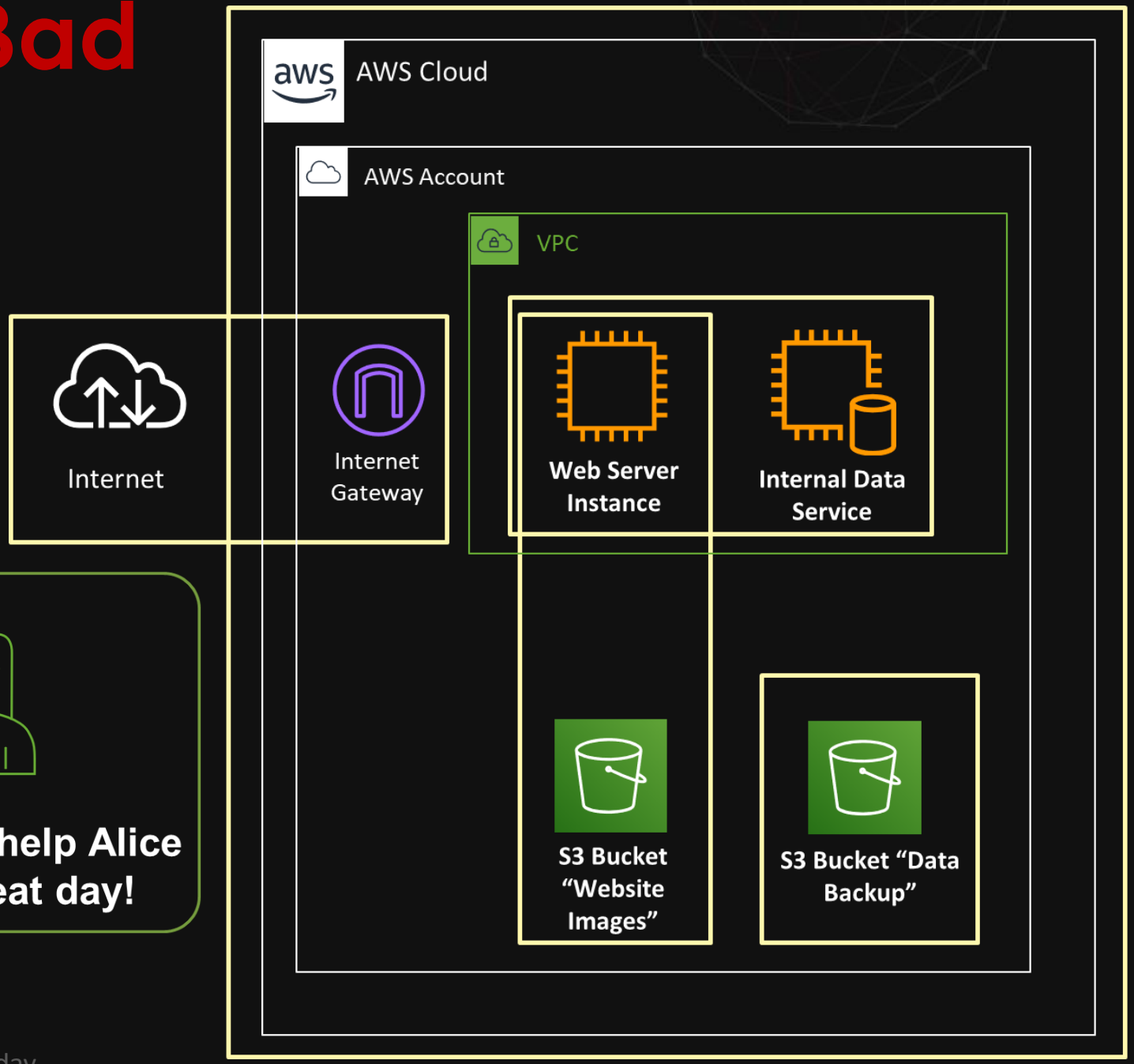
Bob's Bad Day



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



Alice

… now let's help Alice have a great 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

Source: AWS Immersion day

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

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

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 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

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

Source: AWS Immersion day

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

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

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

AWS Security Hub

AWS Config

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**

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

Source: AWS Immersion day

Best-of-the-Best Practices: Infrastructure Security

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

Amazon CloudFront

AWS Shield

AWS WAF

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.

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

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

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

Amazon Inspector

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

Source: AWS Immersion day

Best-of-the-Best Practices: Data Protection

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

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

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

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.

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

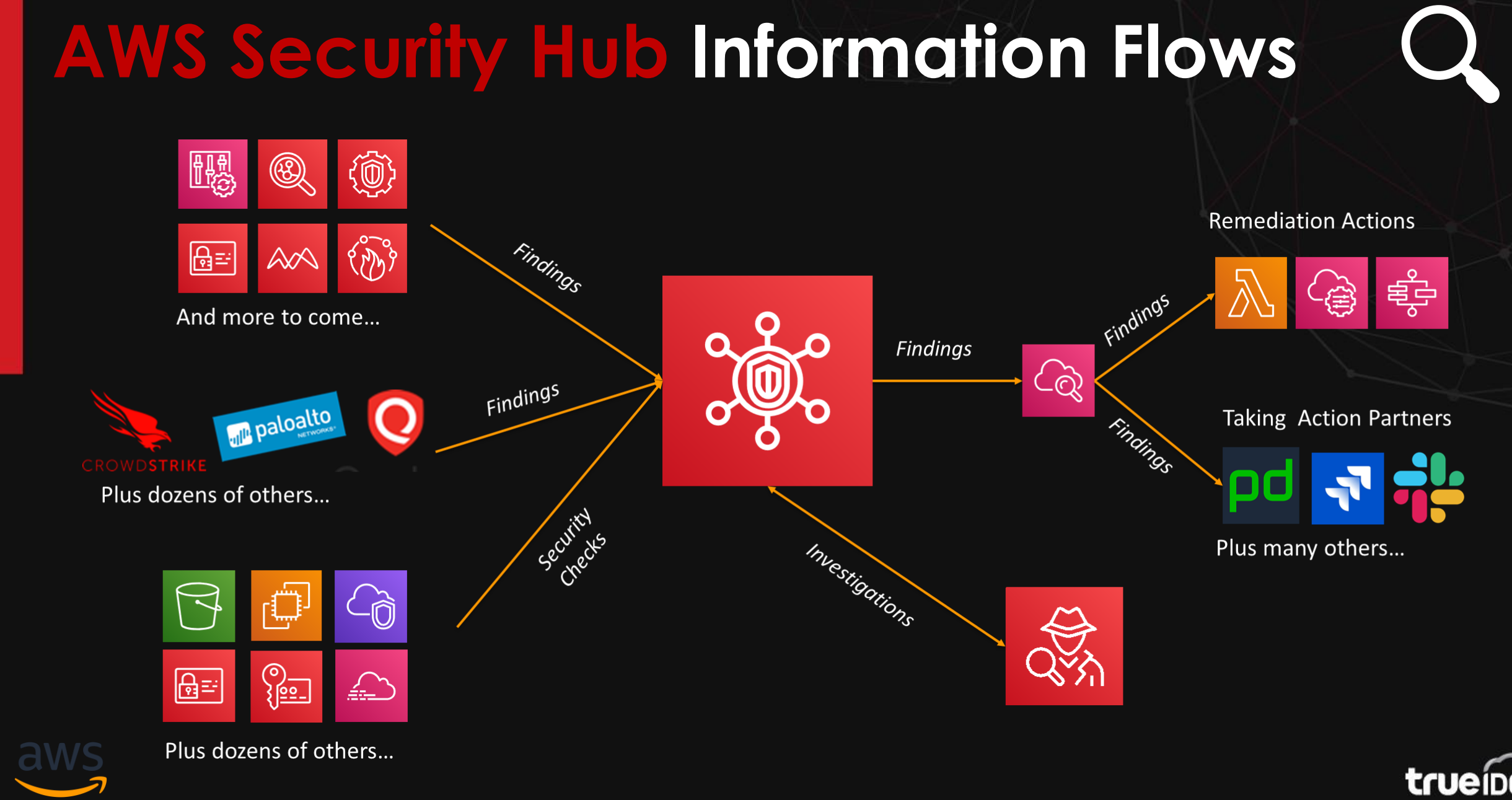
Encryption of data in transit provides protection from accidental disclosure, verifies the integrity of the data, and can be used to validate the remote connection.

Source: AWS Immersion day

Security Hub

Source: AWS Immersion day

AWS Security Hub Information Flows



Source: AWS Immersion day

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

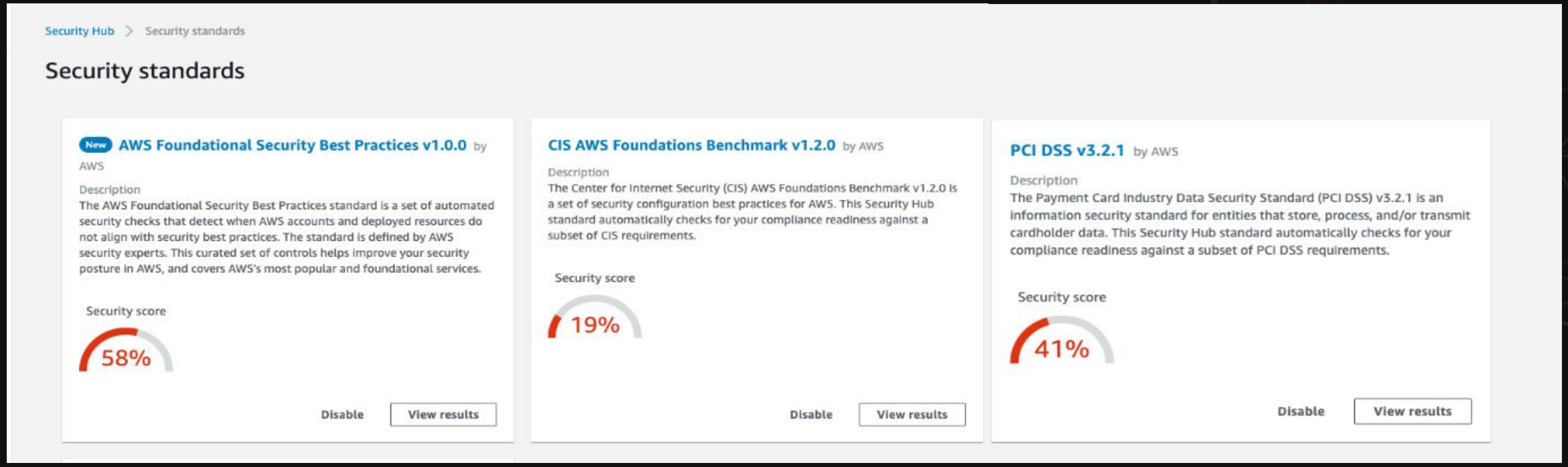
Curated security best practices

Seamless integration w/ standardized findings format

Multi-account support

Source: AWS Immersion day

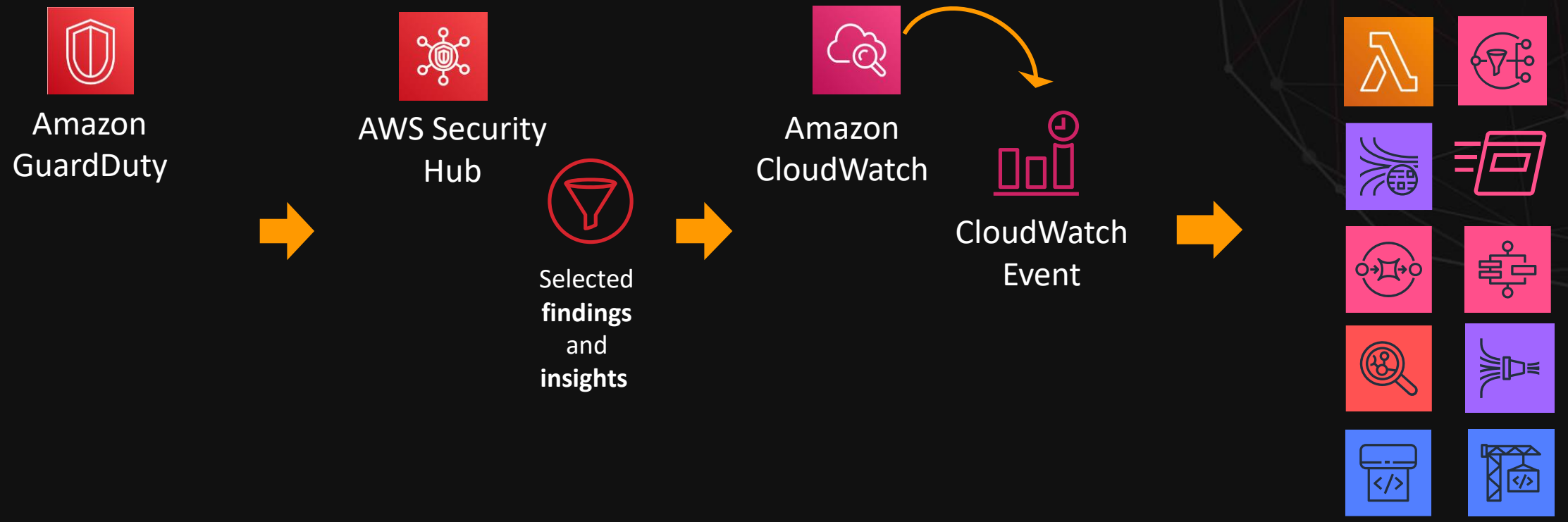
Automated security & compliance checks



- 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.

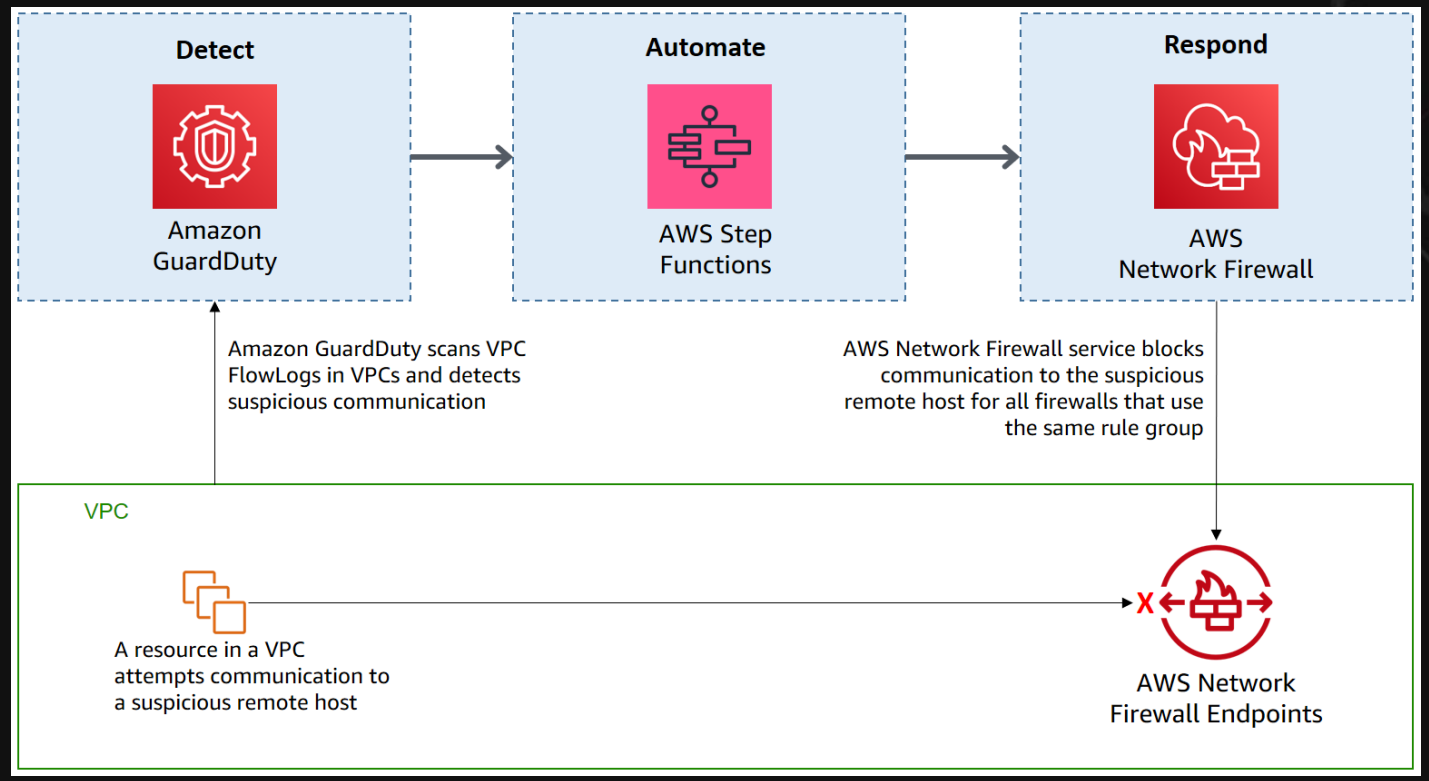
Source: AWS Immersion day

How do I automate response & remediation?



Source: AWS Immersion day

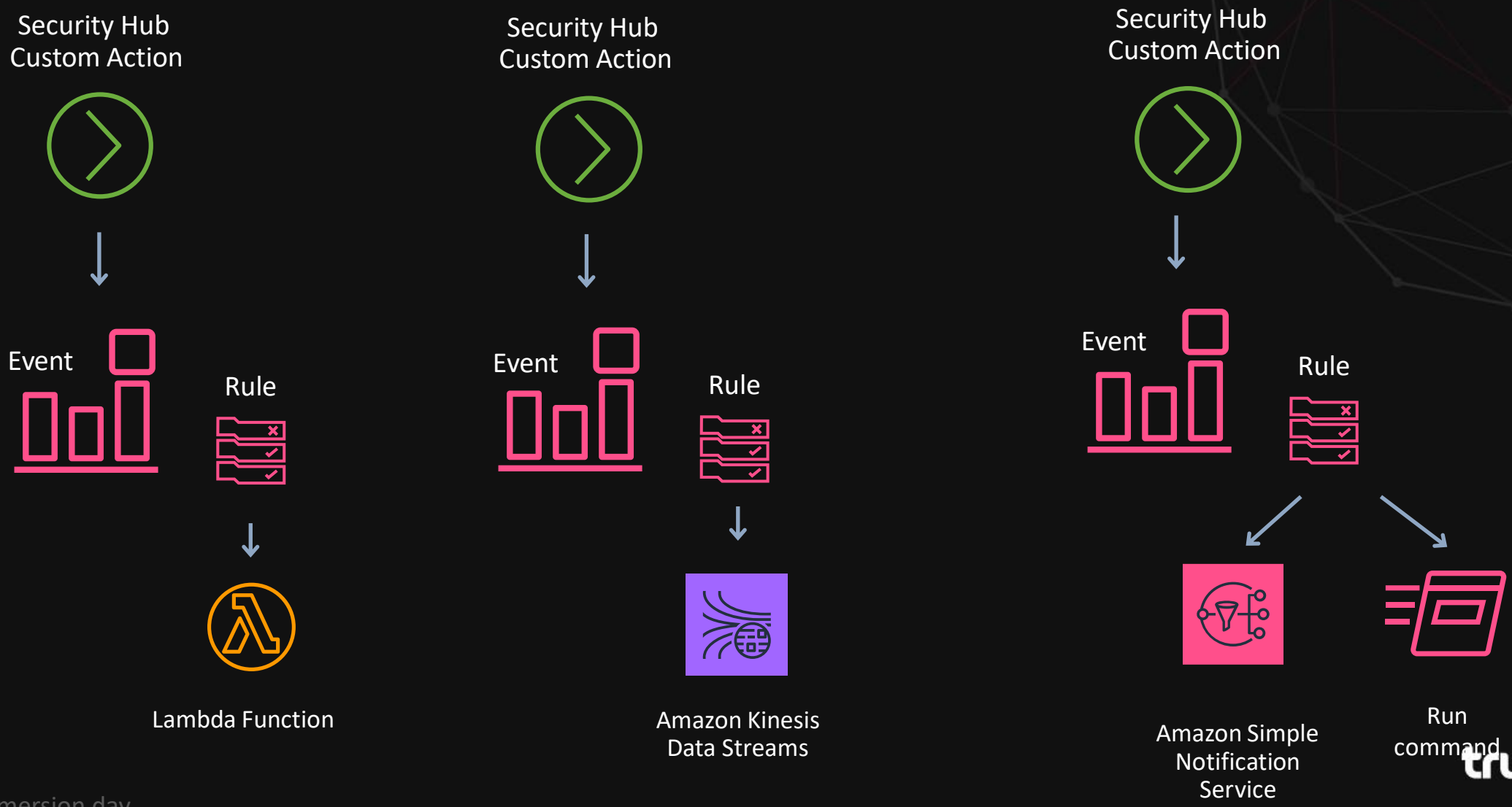
Automated detection & response



- 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.

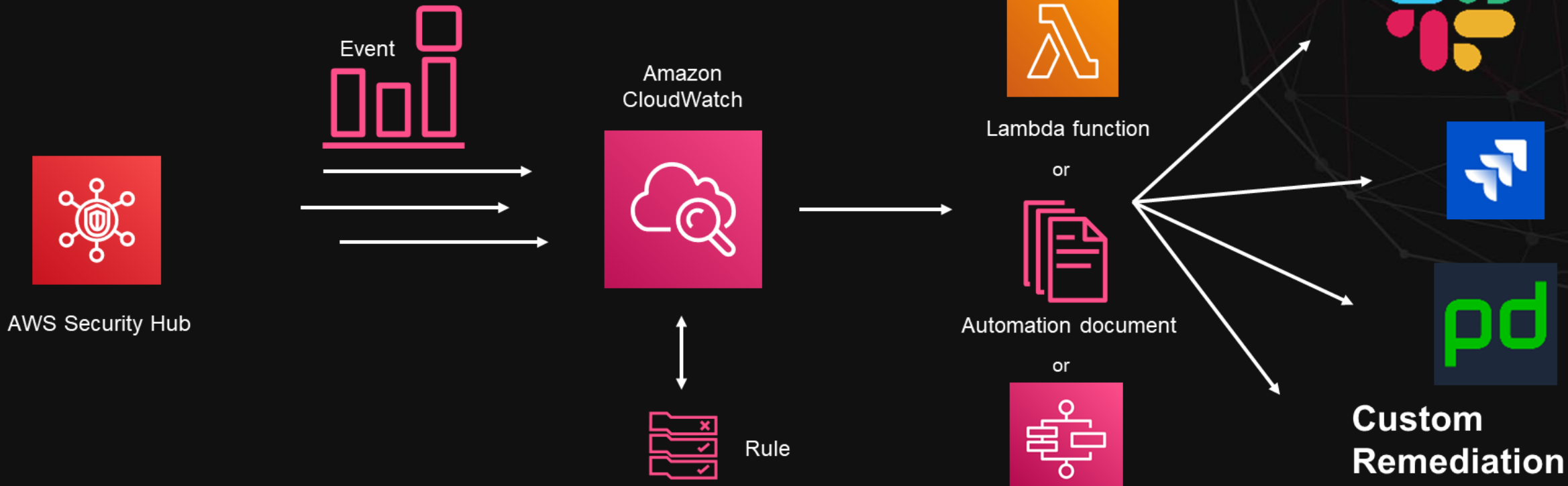
Source: AWS Immersion day

Use Security Hub Custom Actions to trigger automation



Source: AWS Immersion day

Customizable response and remediation actions



1. All findings automatically send to CloudWatch events, **and**

2. Security Hub user can select findings in the console and take a custom action on them. These findings are sent to CloudWatch decorated with a custom action ID

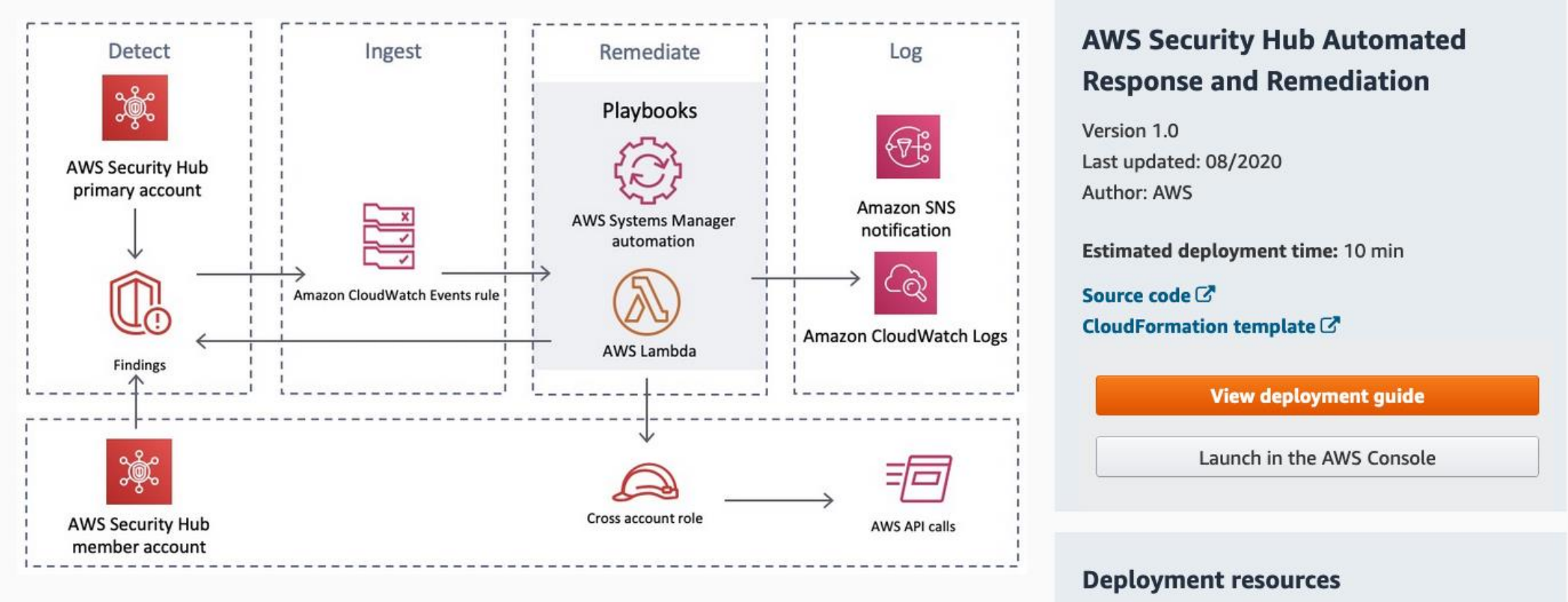
3. User creates Amazon CloudWatch Events rules to look for certain findings associated with a custom action ID or findings with specific characteristics.

4. The rule defines a target, typically a Lambda function, Step Function, or Automation document

5. The target could be things like a chat, ticketing, on-call management, SOAR platform, or custom remediation playbook

Source: AWS Immersion day

AWS Security Hub Automated Response and Remediation solution architecture



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

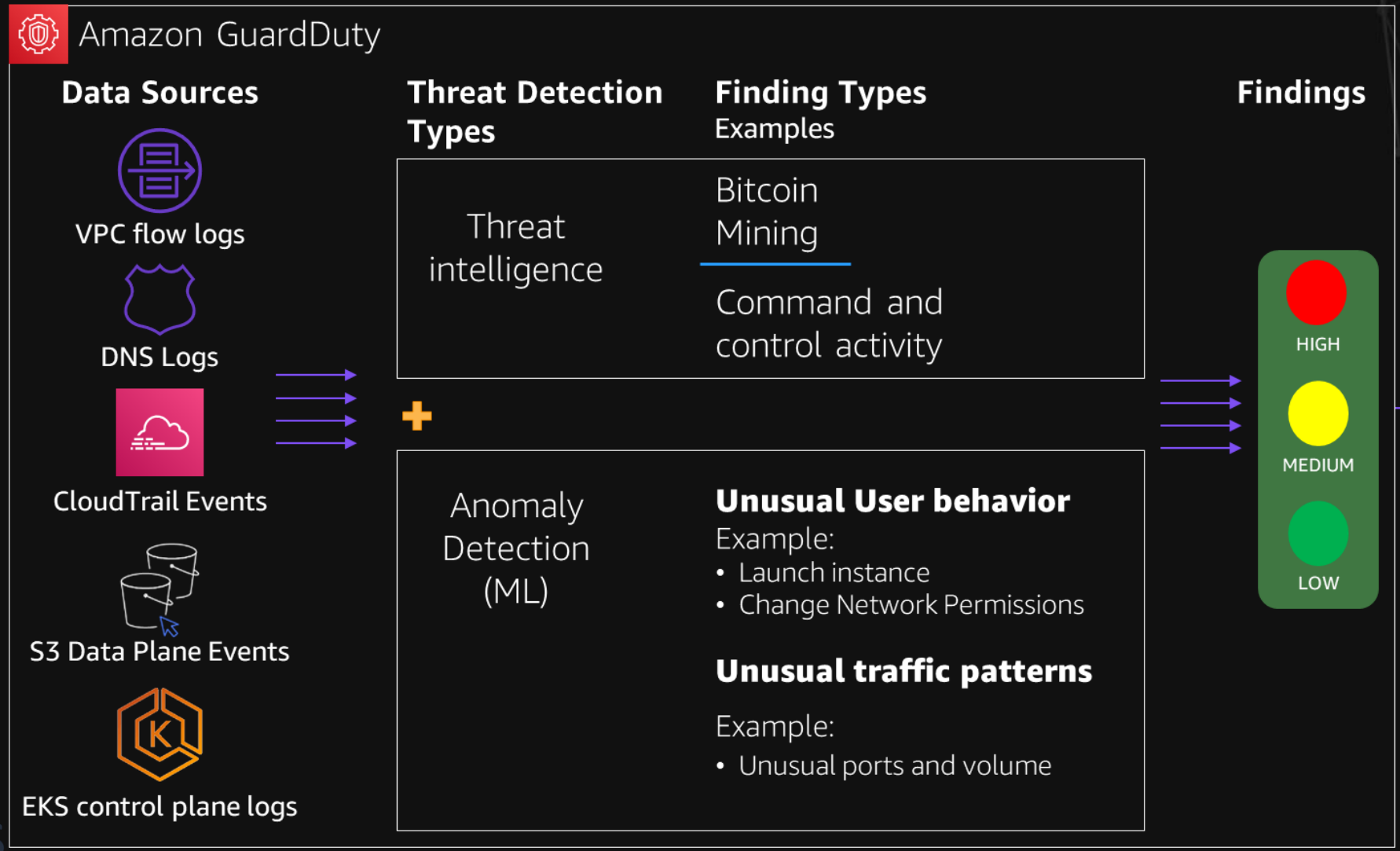
Appendix

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

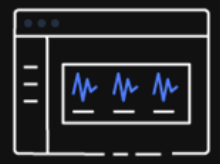
Source: AWS Immersion day

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

Source: AWS Immersion day

Amazon Detective

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

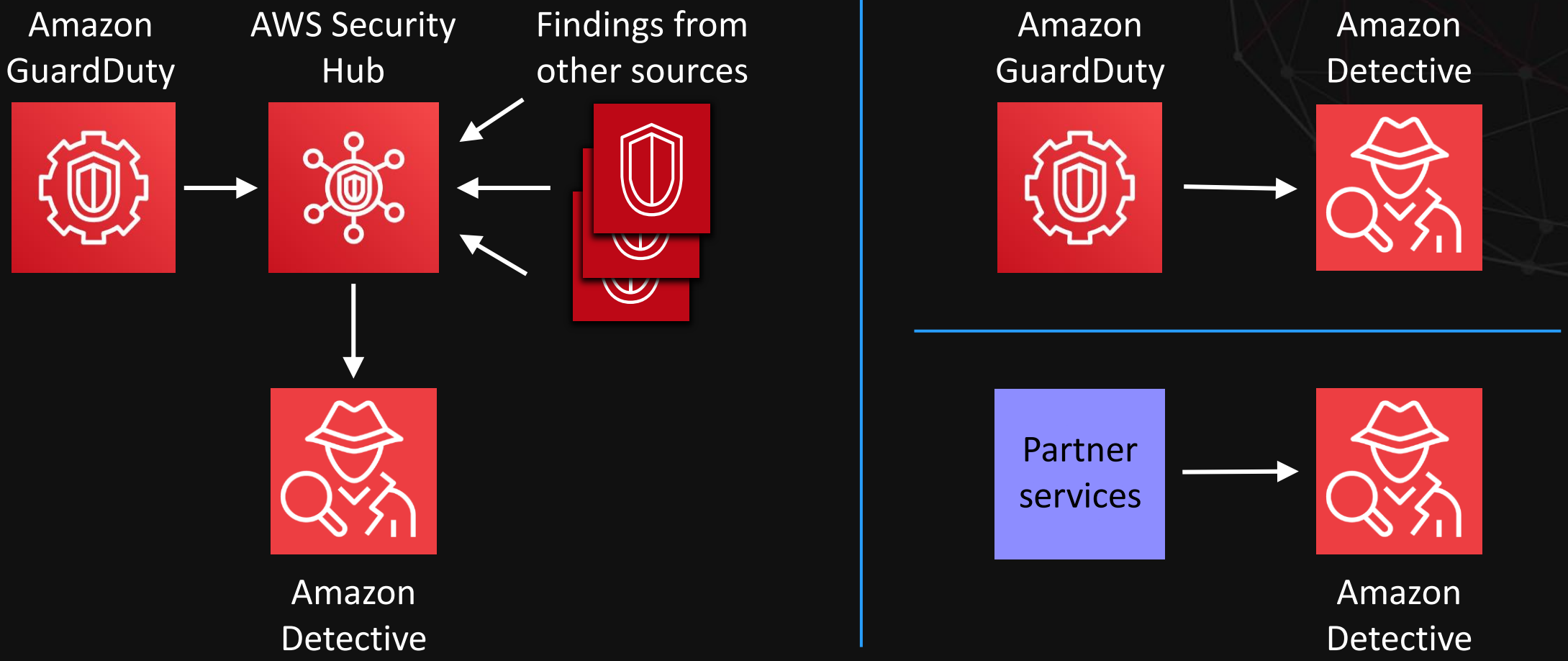
Built-in data collection

Automated analysis

Visual insights

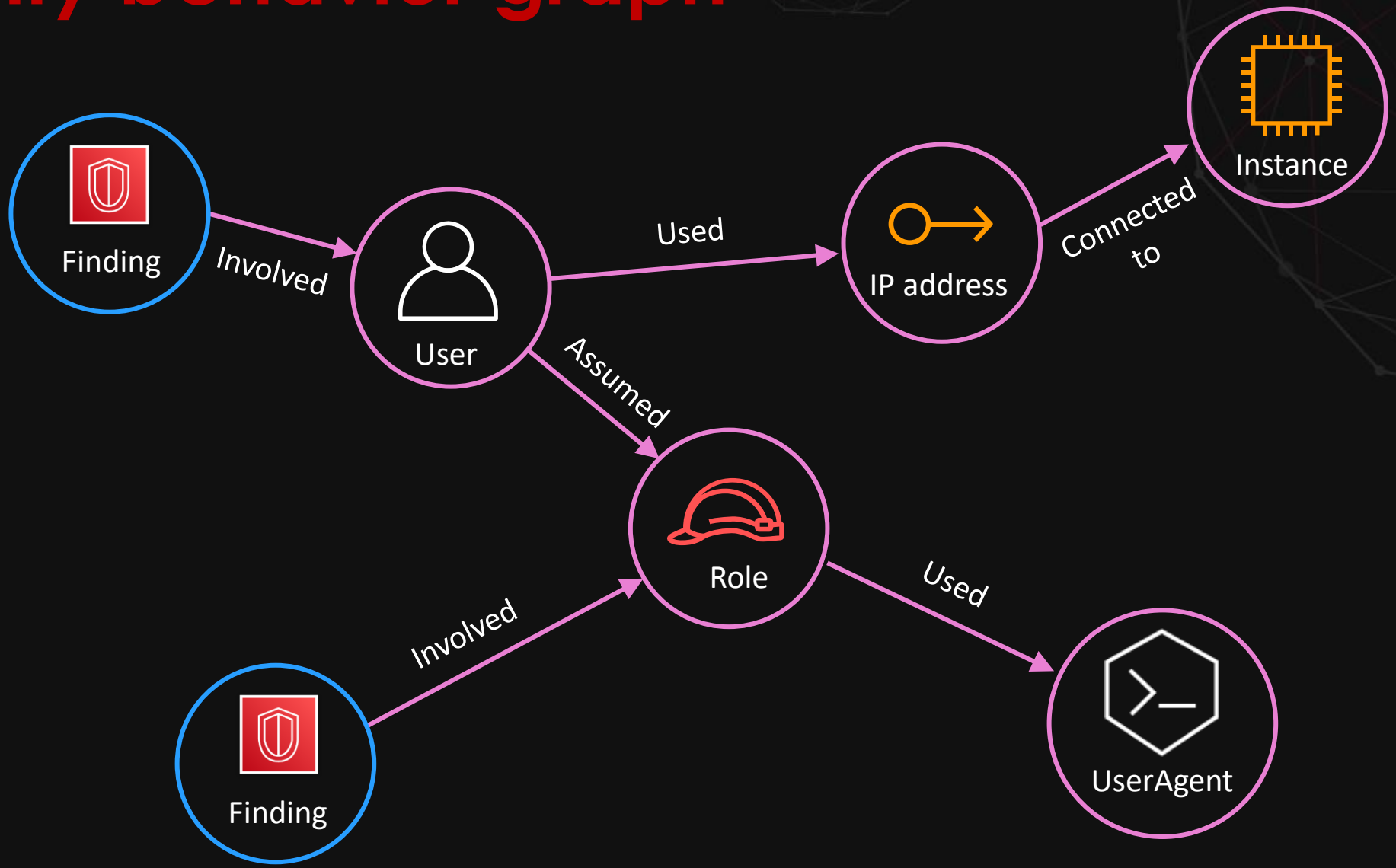
Source: AWS Immersion day

Amazon Detective usage flow



Source: AWS Immersion day

Security behavior graph



Source: AWS Immersion day

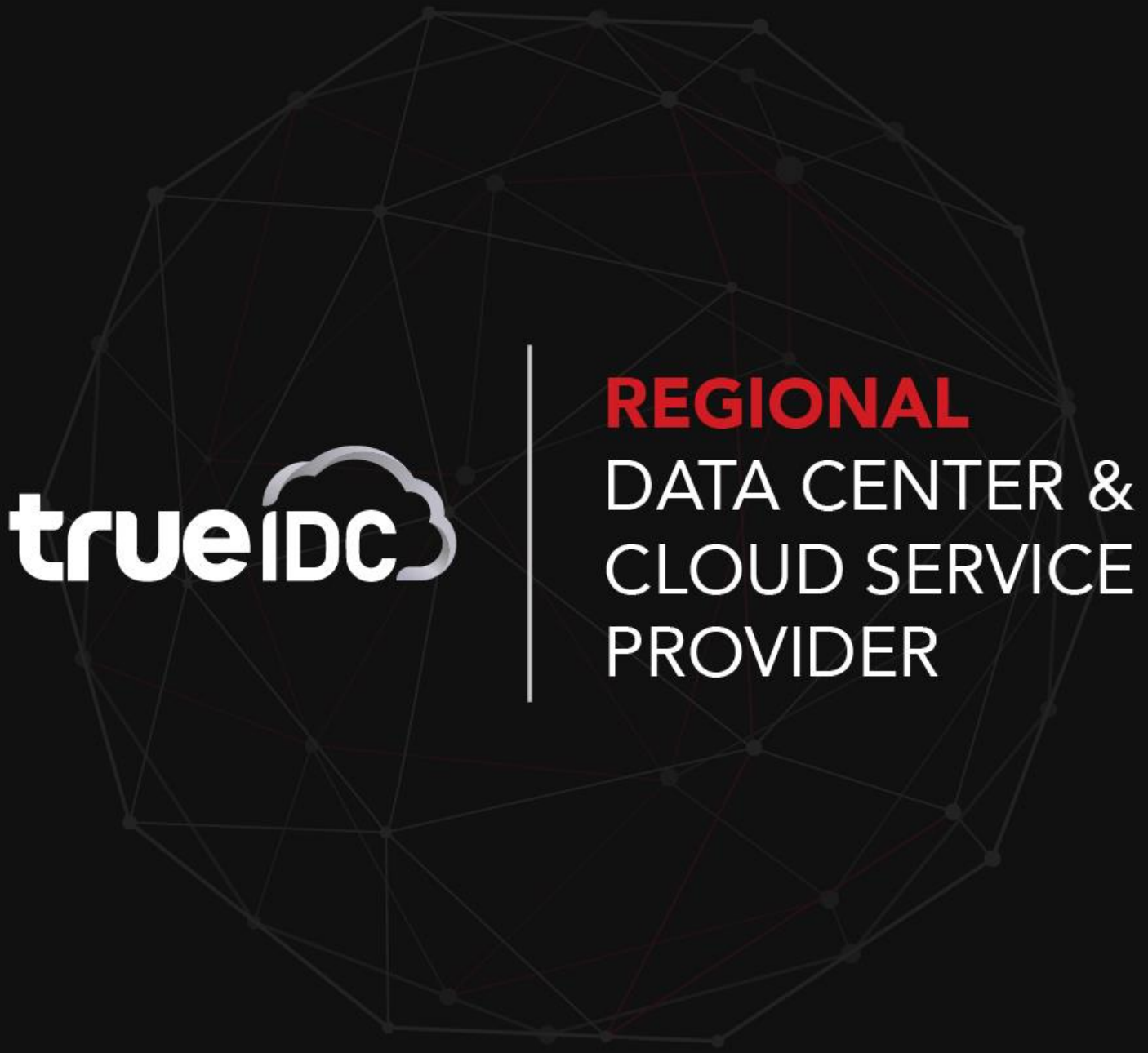
Amazon Inspector

Source: AWS Immersion day

Lab: Security Hub

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

trueIDC


trueIDC
REGIONAL
DATA CENTER &
CLOUD SERVICE
PROVIDER