亚马逊云科技

2021 Security Day

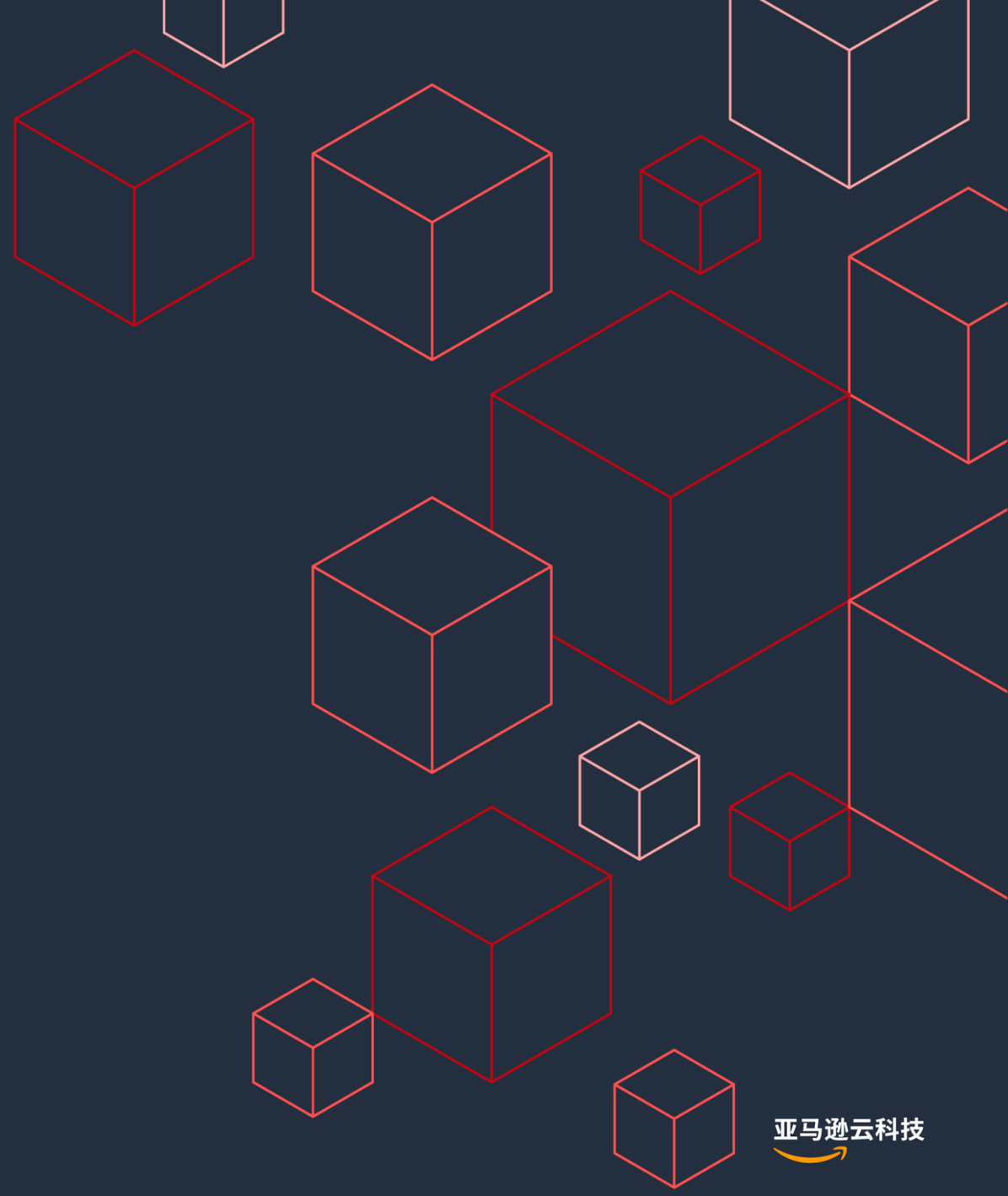
事件响应—云端生产环境安全设置自动恢复

安全服务和能力框架

Agenda

- 安全事件
- 事件响应模型
- Event-Driven事件响应
    - Lambda
    - Security Hub
    - Config rule
- 常见场景
- Demo

安全事件



亚马逊云科技

什么是安全事件?

- 任何违反安全策略的事件，未影响到服务的错误配置也是安全事件

  示例:

  - 试图访问未授权的系统或数据（无论成功与否）
  - 服务被破坏或拒绝访问
  - 未经授权使用系统来处理数据
  - 在所有者未知的情况下修改系统硬件，固件，或者软件功能

基于云的安全事件示例

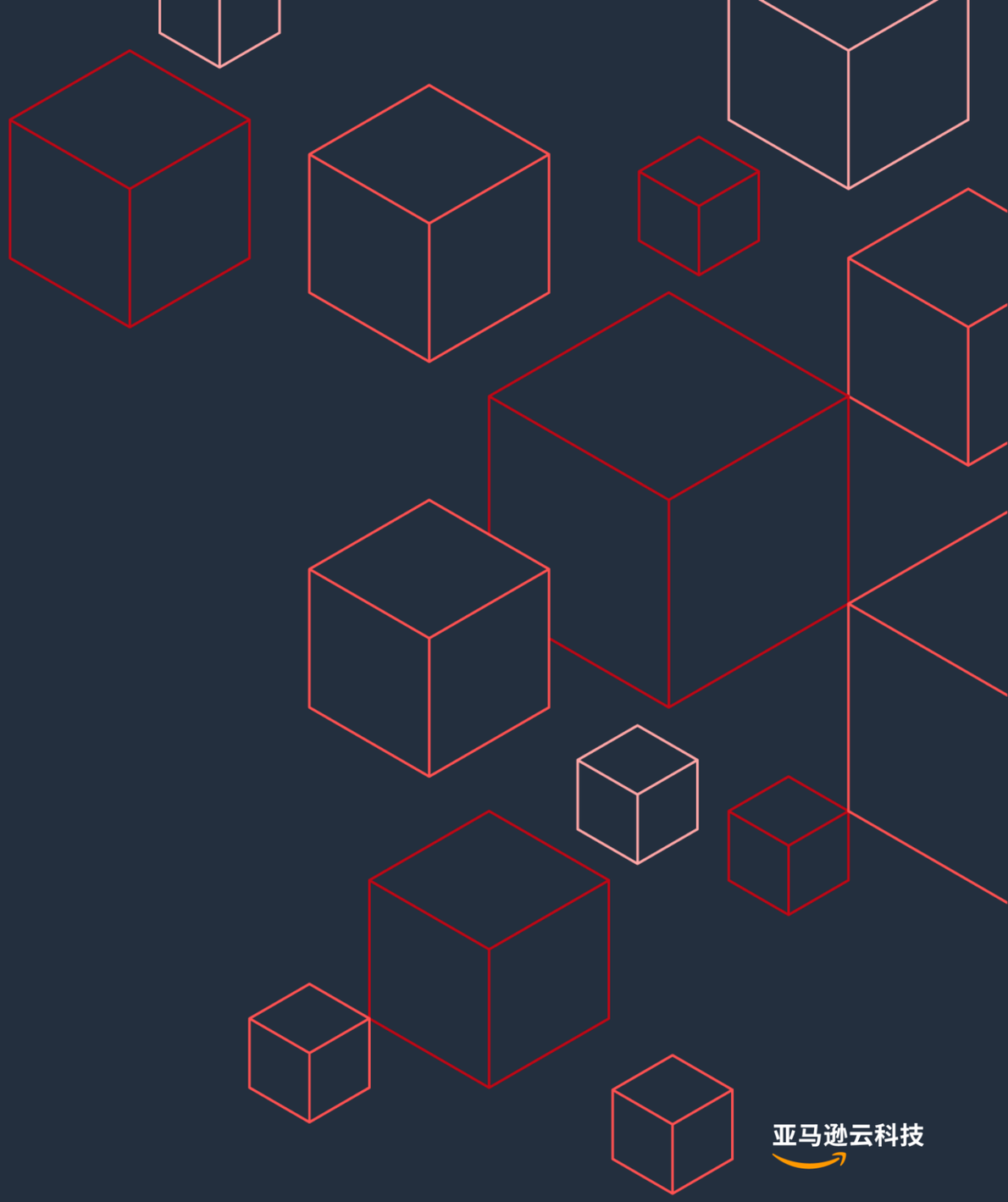
计算&基础设施	身份&权限控制	应用，存储 & 数据库
DDOS	Account Id Leak	Data Exposure
Cryptojacking	Session Token Hijacking	Website Defacement
Key Material Compromise	STS Token Replay Attack	Subdomain Takeovers
Pivot Attack	IAM Role Enumeration	Malicious File Hosting
AMI Poisoning	IAM User Brute Force Attack	Data Spillage
Account Jumping		

事件响应标准

- 作为事件响应者，需要实施的事件响应方案有以下特点：

  - ✓ 需要人能够掌控事件响应的全局
  - ✓ 使用自动化手段来简化响应流程和减少处理错误
  - ✓ 支持高可用的应用和遗留的应用
  - ✓ 聚焦在与本次事件相关的事件和入侵

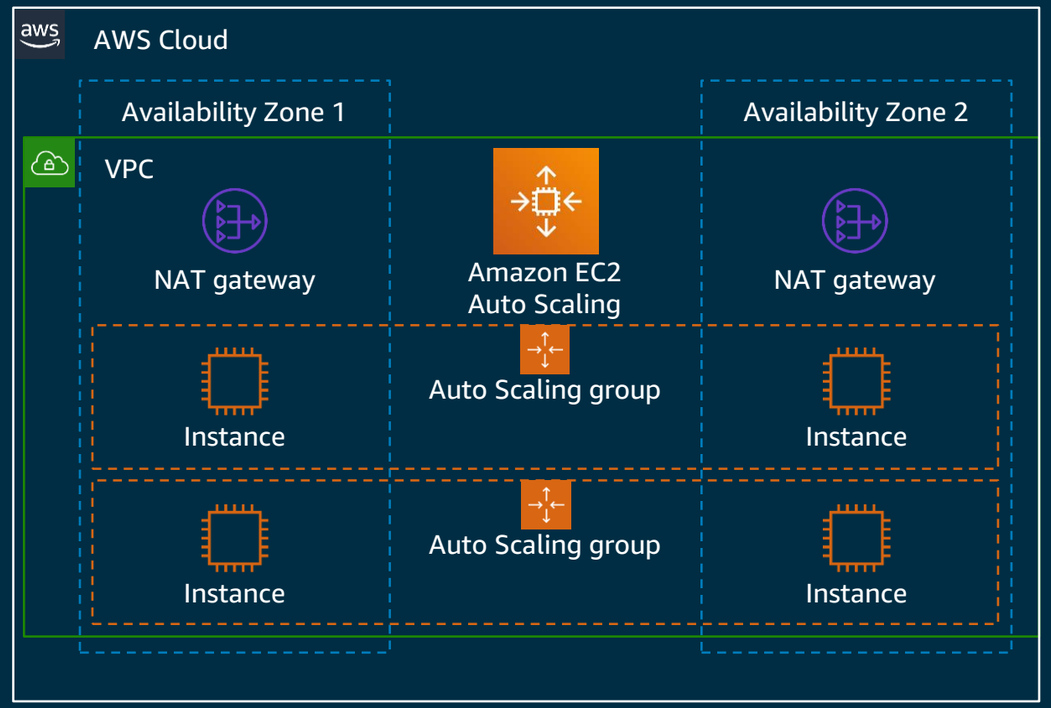
事件响应模型



亚马逊云科技

事件响应模型

- 行动者的行为被日志记录下来
- 有意或无意的行为



- 响应者收到警报，从日志中找出行动者的行为，并使用合适的工具去响应
- 在找出行动者的随机行为中花费更少的精力

行动者

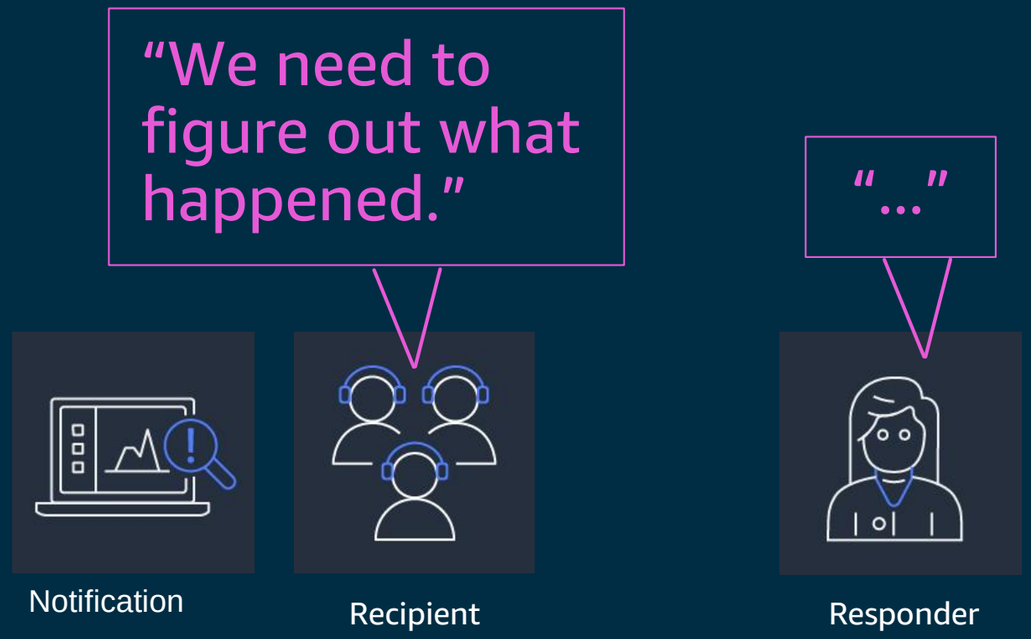
业务

响应者

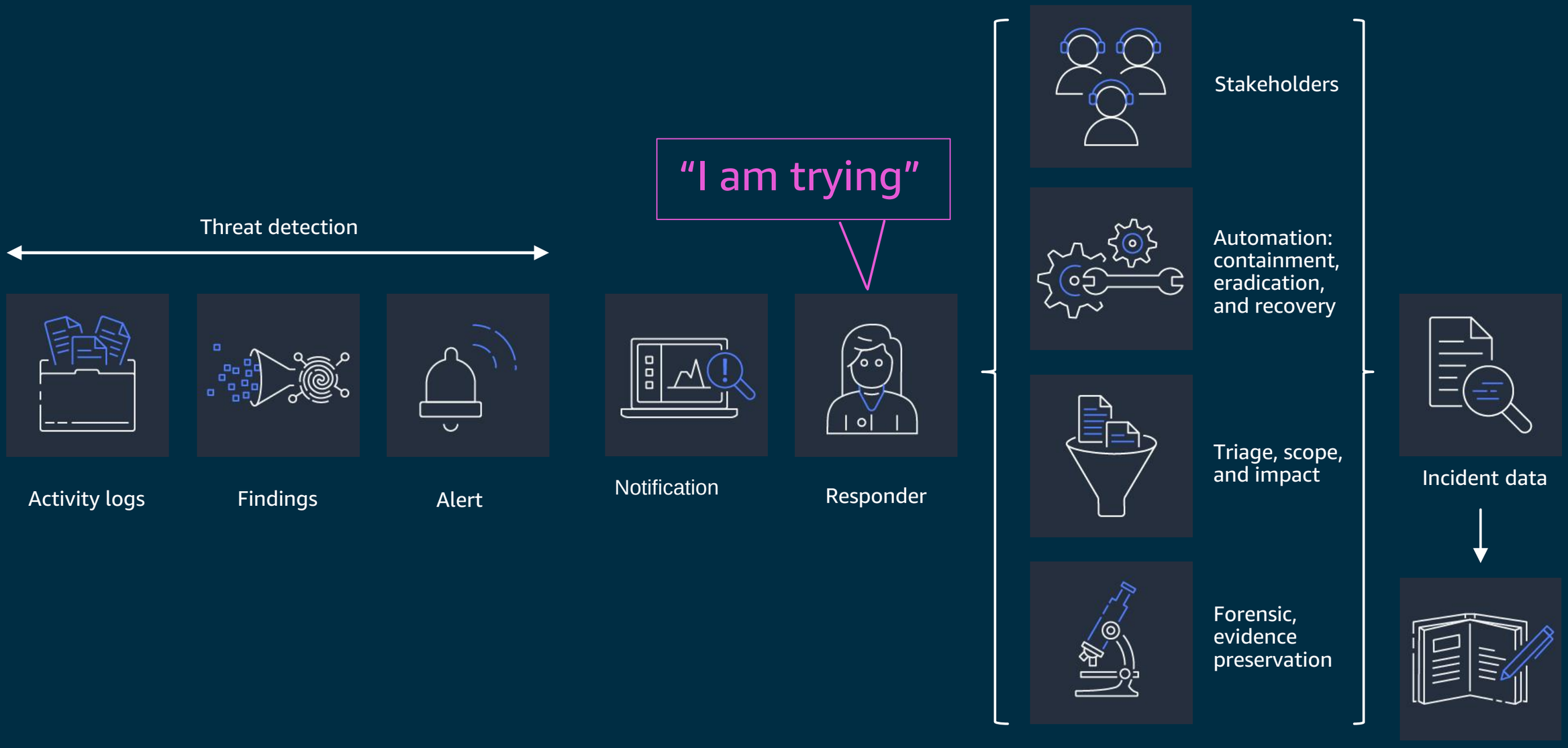
事件响应模型

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

1. “Zero playbook”



2. “Classic playbook”



为什么会这样?

太多警报或者没有警报

缺乏威胁检测和事件响应的技能

缺乏或不合适自动化措施

不足的playbooks

3. “Playbook as code”

IR repo

“I got this!”

pull / push

Threat detection

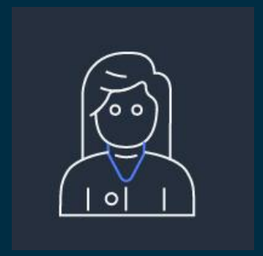
Activity logs

Indicators

Alert

Threat modeling

Notification



Responders

as needed

Automation: data for triage, containment, and eradication

Stakeholders

Incident data

Post-incident activity

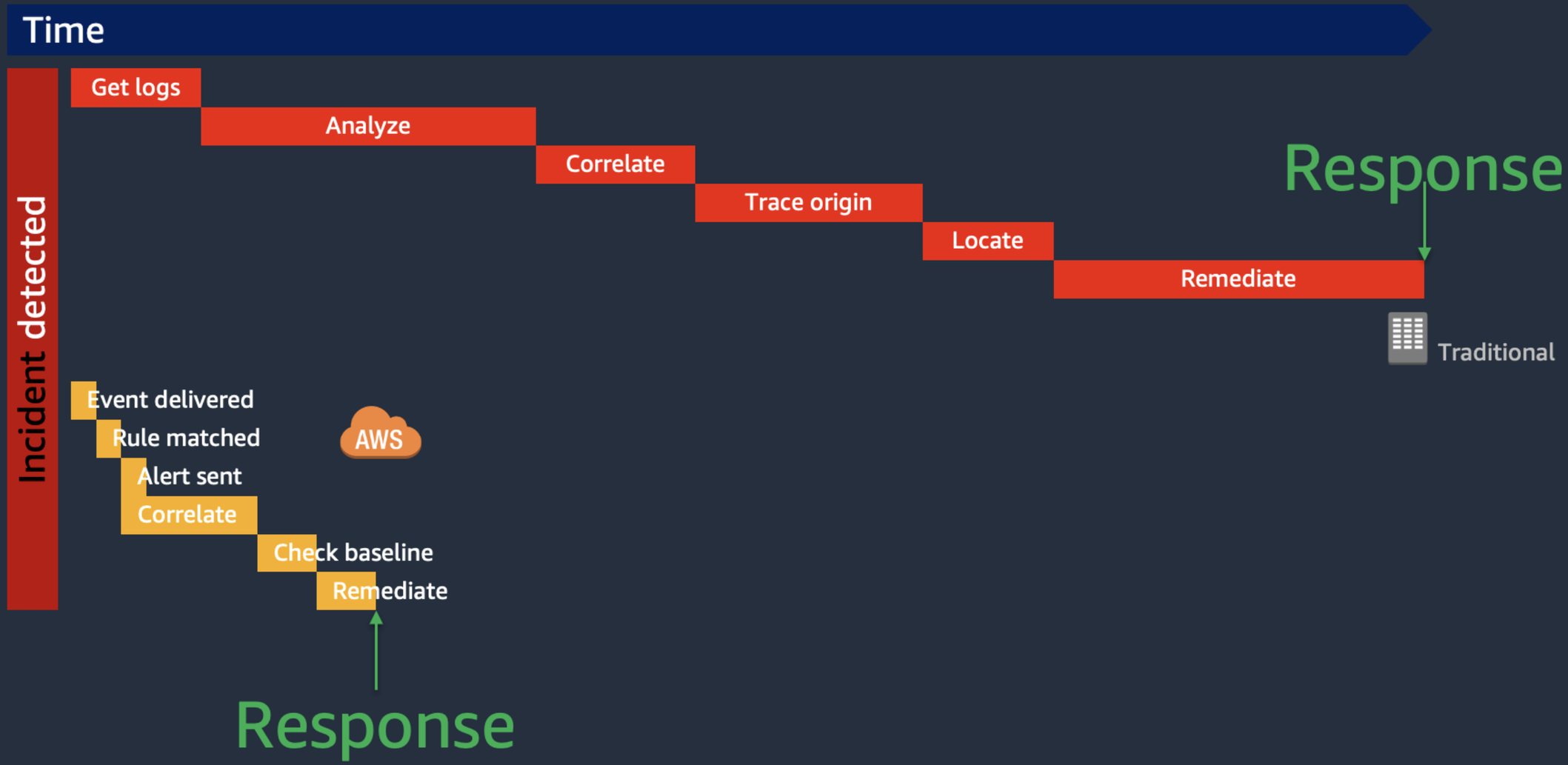
Data for triage, scope, and impact

Evidence preservation for forensics

Event-Driven Response

亚马逊云科技

响应时间对比(示例)



使用Lambda运行代码以响应事件

EVENT SOURCE

FUNCTION

SERVICES (ANYTHING)

Changes in data state

Requests to endpoints

Changes in resource state

Node
Python
Java
C#

Lambda的优势

在云中创建模块化的、动态的应用程序的高效计算服务

1

无需维护基础设施

专注于业务逻辑

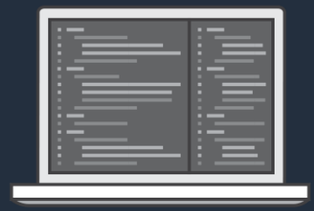
2

经济有效

按使用计费

3

自定义代码



运行标准语言的代码

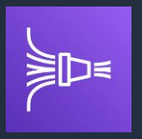
Amazon CloudWatch Events

Amazon CloudWatch

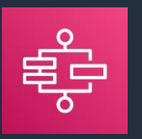
- 近实时的云资源状态改变事件流
- 和云资源集成（源和目标）

rule

```
{
  "source": [
    "aws.trustedadvisor"
  ],
  "detail-type": [
    "Trusted Advisor Check Item Refresh Notification"
  ],
  "detail": {
    "status": [
      "ERROR",
      "WARN"
    ]
  }
}
```



Amazon Kinesis Data Firehose



Step Functions

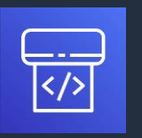
Amazon SQS

Amazon EC2

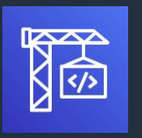
Lambda

Amazon Inspector

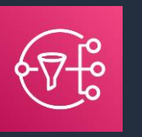
Systems Manager



CodePipeline



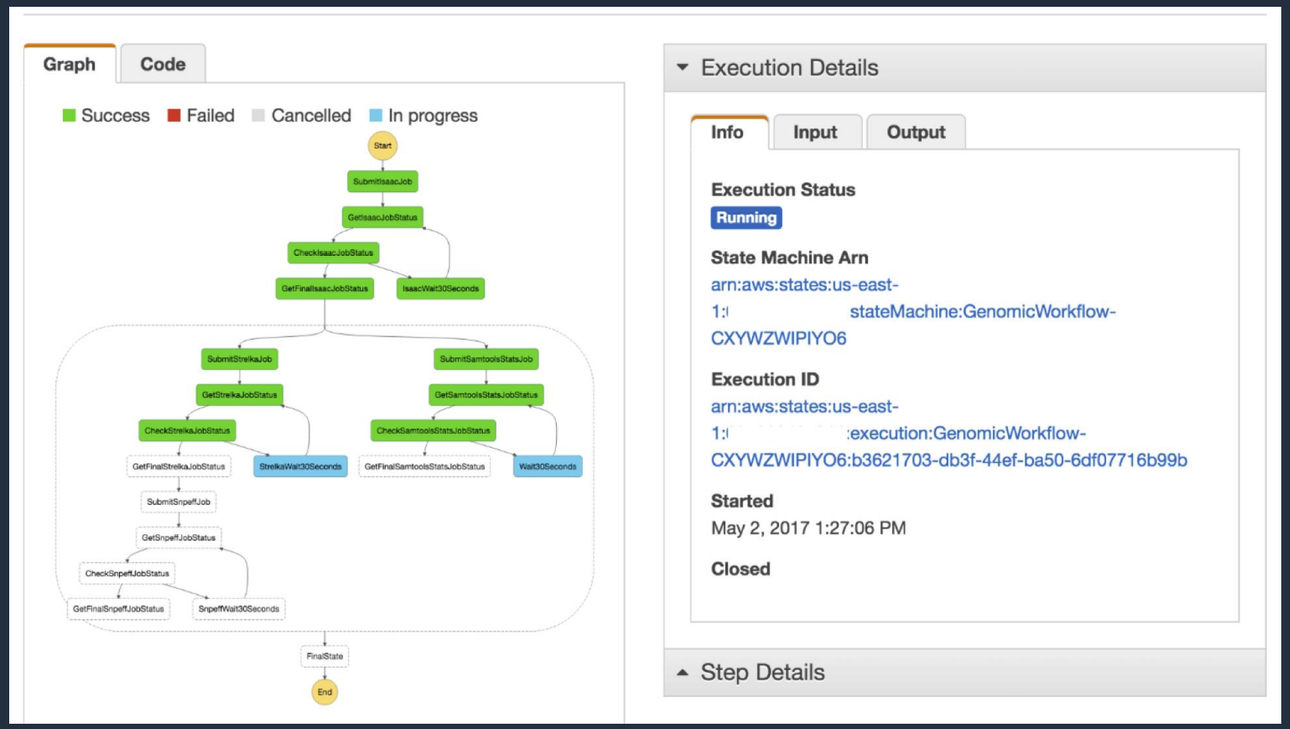
CodeBuild



Amazon Simple Notification Service

如果一个Lambda函数不够用?

Step Functions

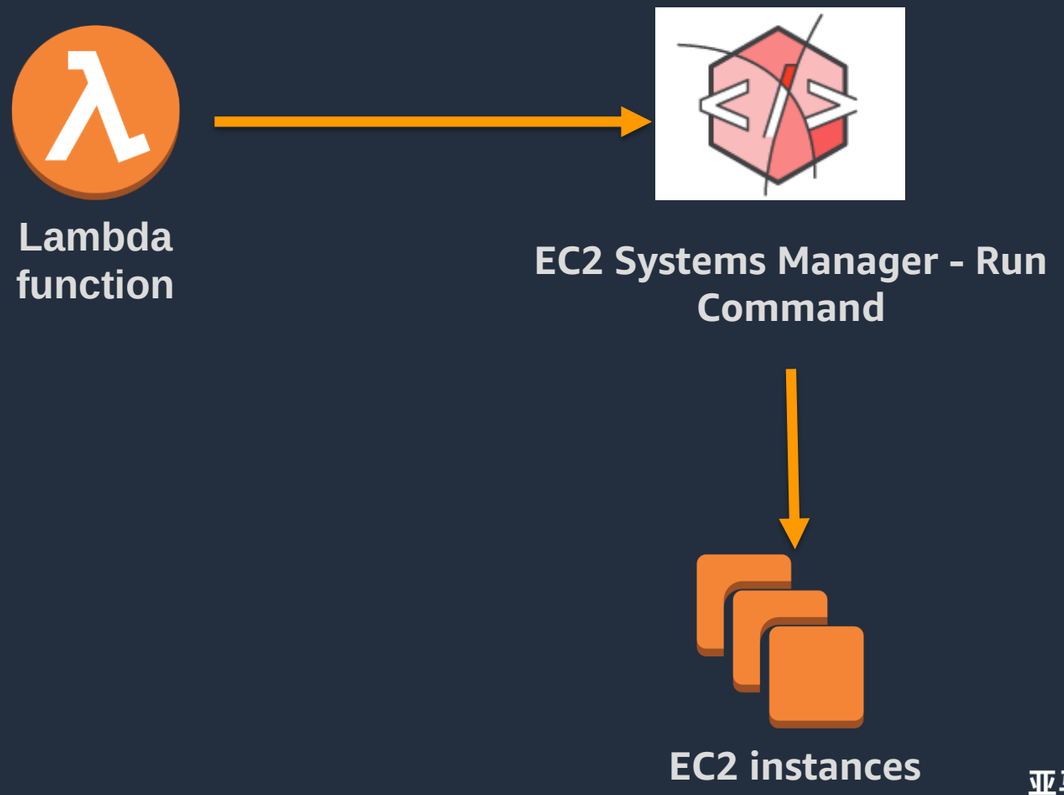


工作流
协调多个Lambda函数
将执行过程可视化

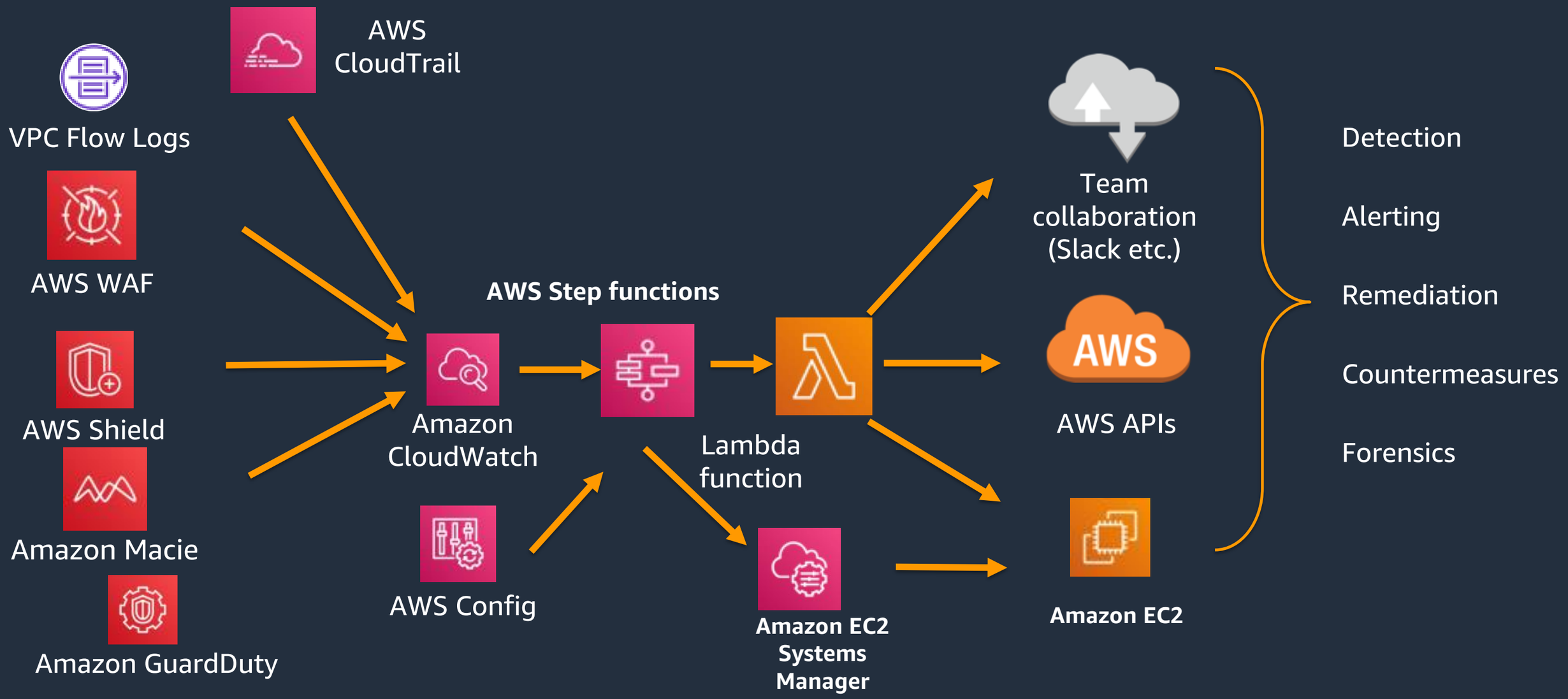
无需手工!

如果问题出在EC2内部?

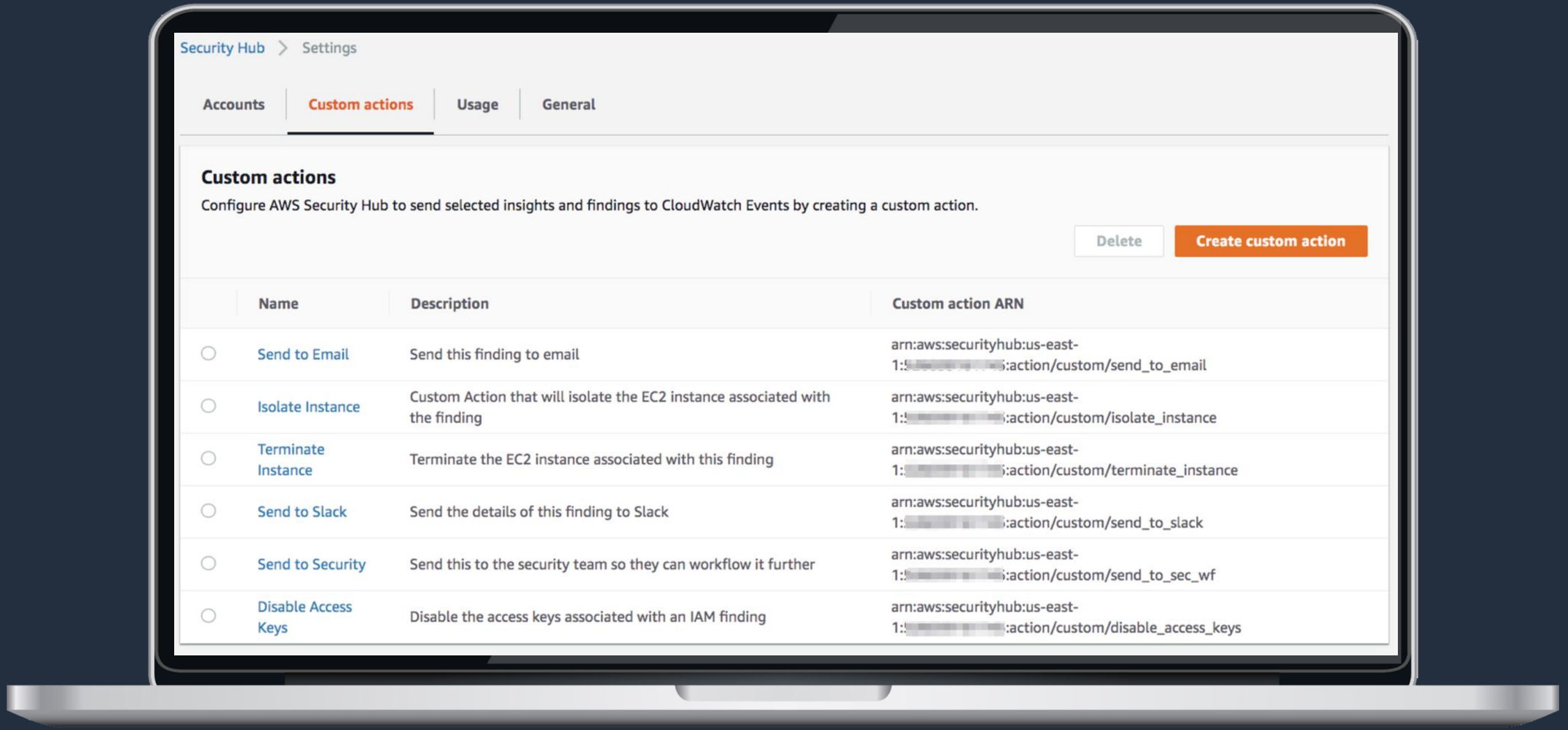
- 异步执行命令
- 无需SSH/RDP
- 命令和输出都被记录



事件驱动的安全响应架构

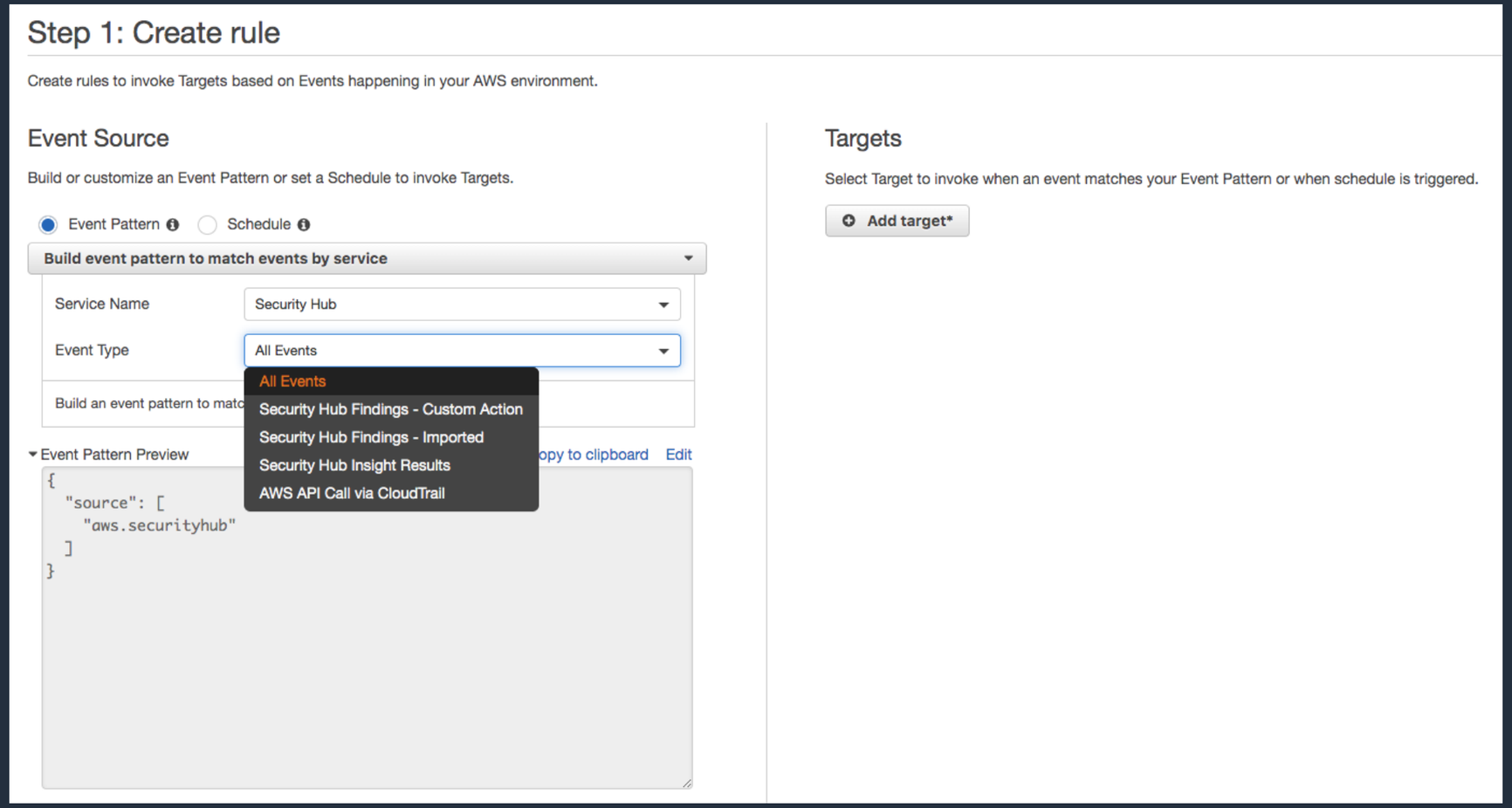


AWS Security Hub中的自定义操作



Taking action 对所有发现

每个新的AWS Security Hub发现都会发送到Amazon CloudWatch Events



事件模式示例

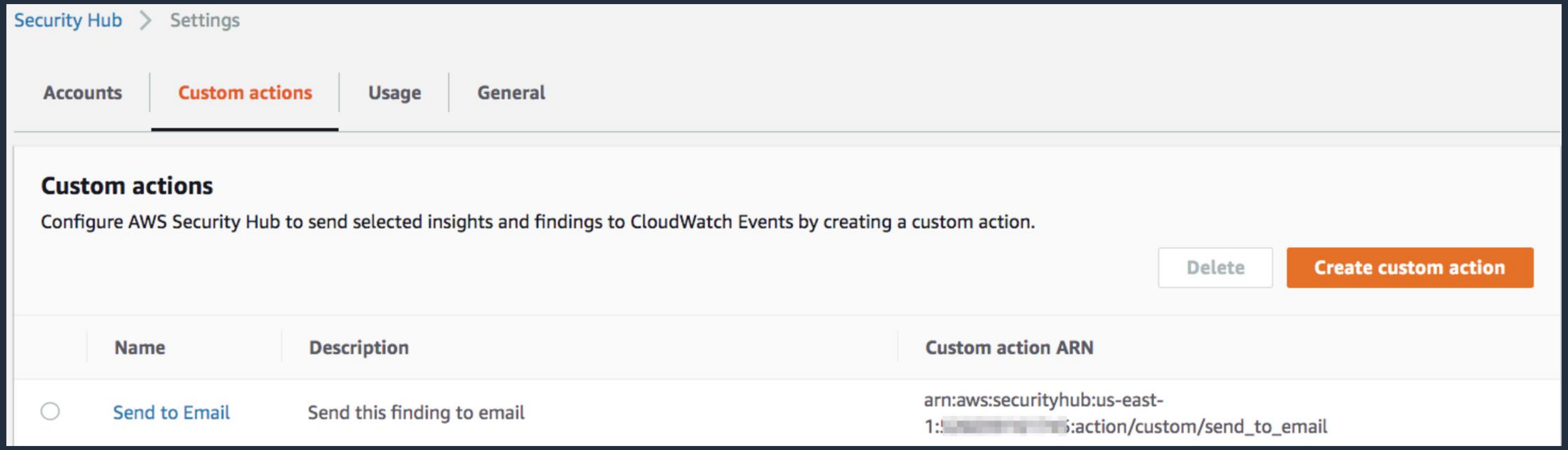
按标签过滤

```
{
  “source”: [
    “aws.securityhub”
  ],
  “detail-type”: [
    “Security Hub Findings”
  ],
  “detail”: {
    “findings”: {
      “Resources”: {
        “Tags”: {
          “Environment”: [
            “PCI”
          ]
        }
      }
    }
  }
```

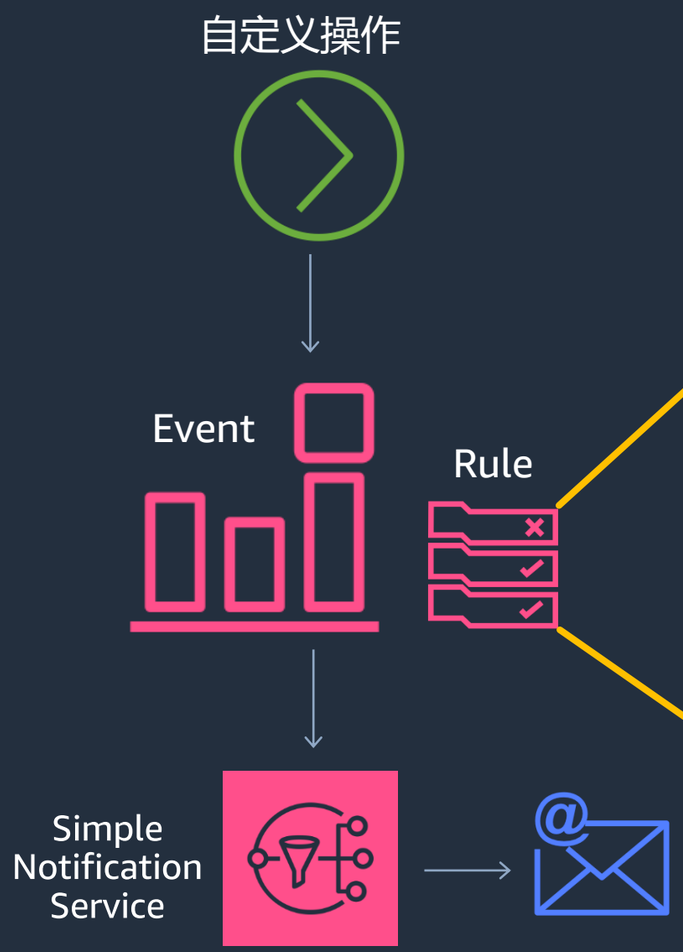
按严重性过滤

```
{
  “source”: [
    “aws.securityhub”
  ],
  “detail-type”: [
    “Security Hub Findings”
  ],
  “detail”: {
    “findings”: {
      “Severity”: {
        “Normalized”: [
          95,
          96,
          97,
          98,
          99,
          100
        ]
      }}}}
```

AWS Security Hub中的自定义操作

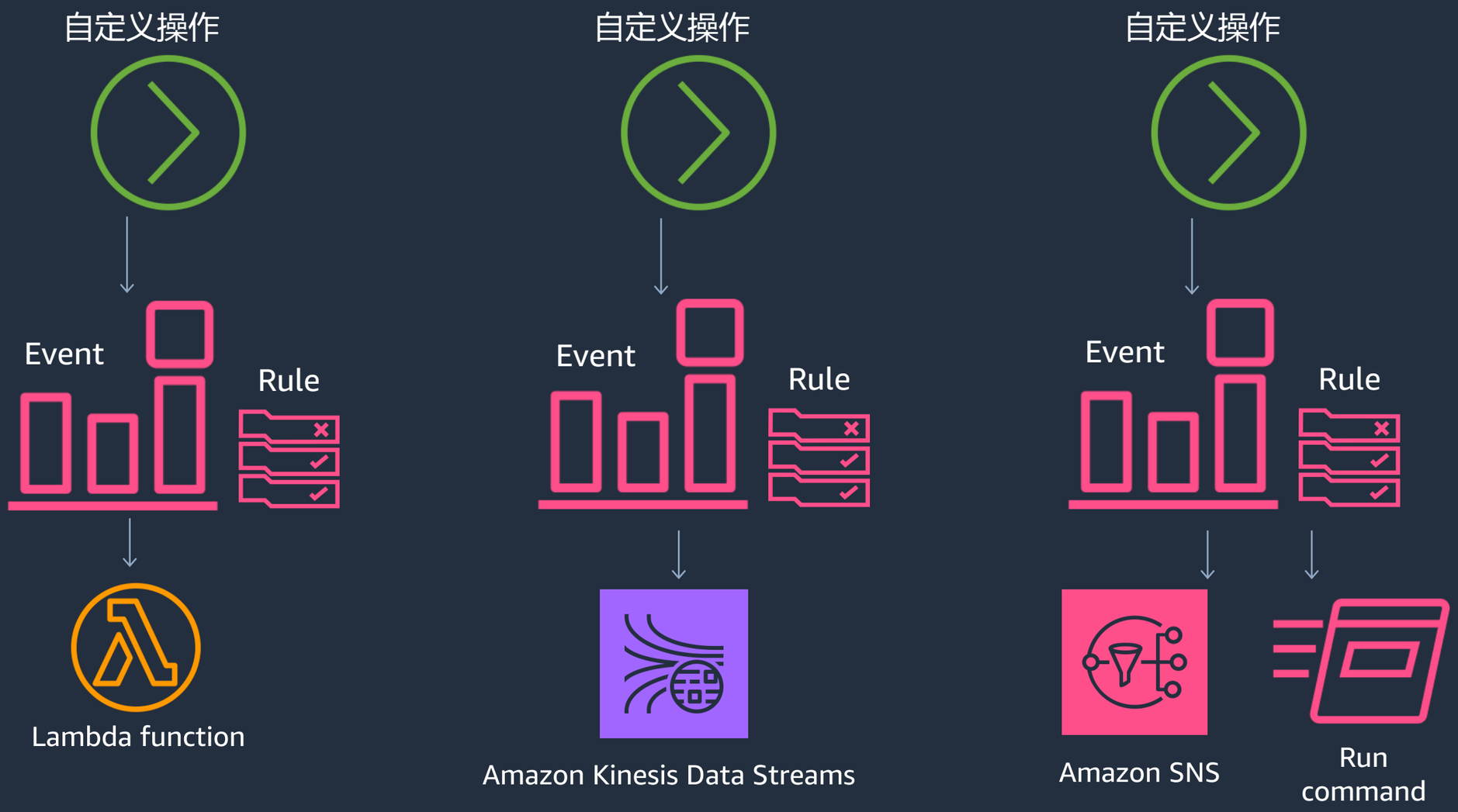


AWS Security Hub中的自定义操作




```
{
  "source": [
    "aws.securityhub"
  ],
  "resources": [
    "arn:aws:securityhub:us-west-
2:xxxxxxxxxxxx:action/custom/send_to_email"
  ]
}
```

Security Hub中的自定义操作



Config rules

分析配置的变化

和90+服务集成的预配置规则

用Lambda自定义规则

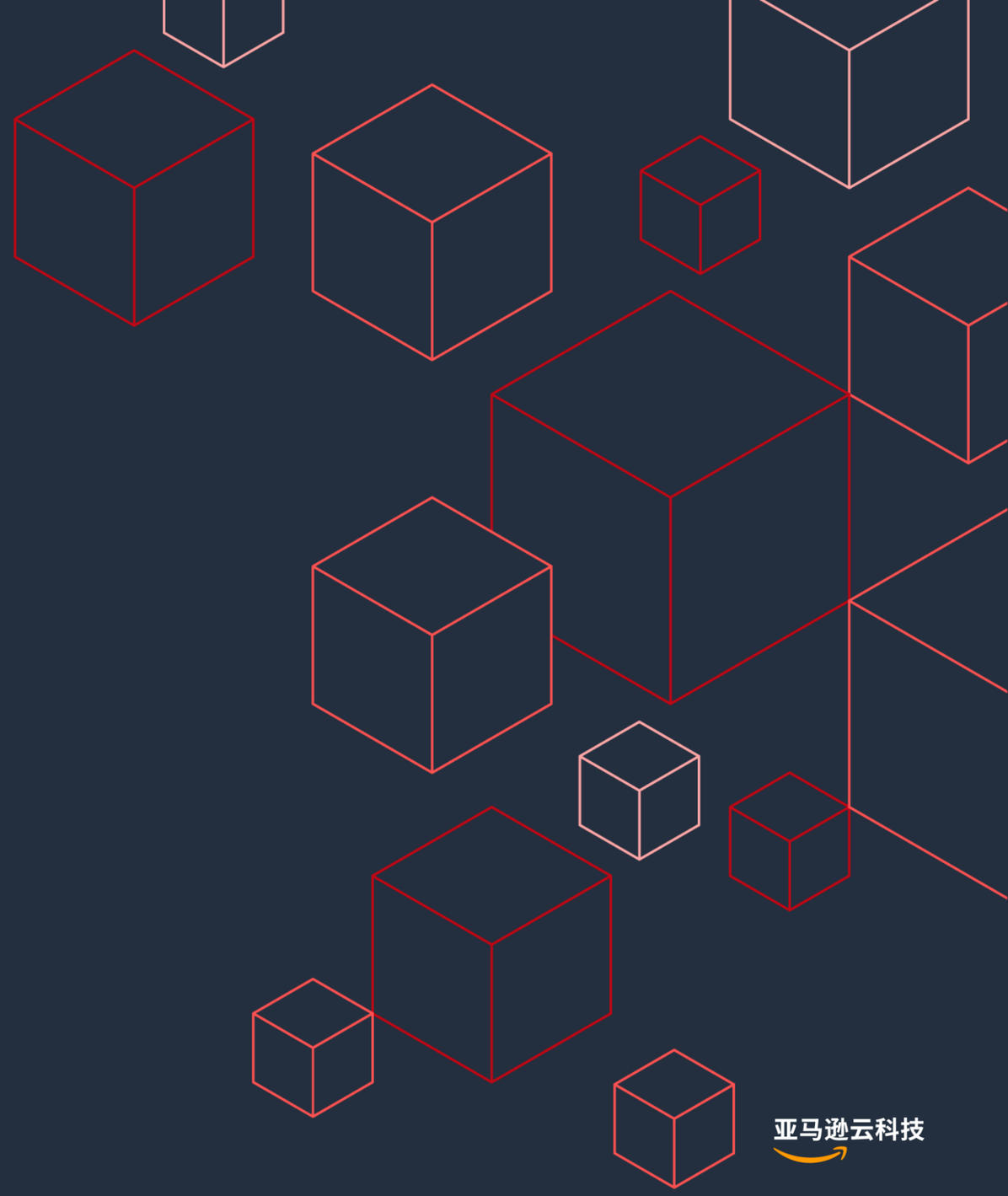
GitHub repo: 社区规则

跨账号管理

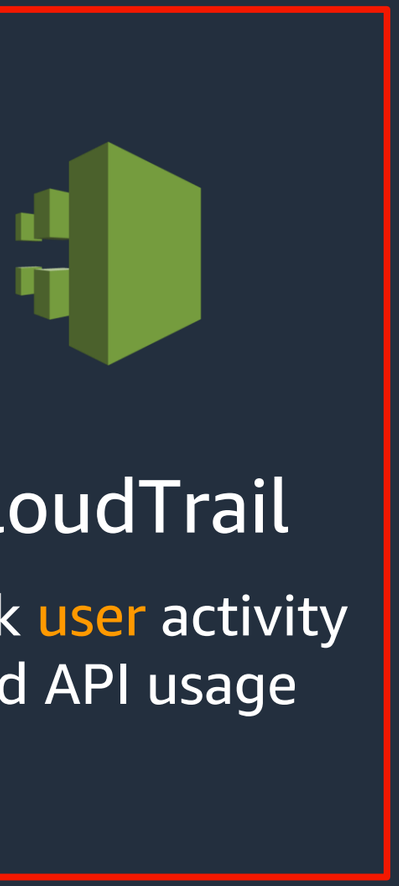
合规历史

Config Rule Demo

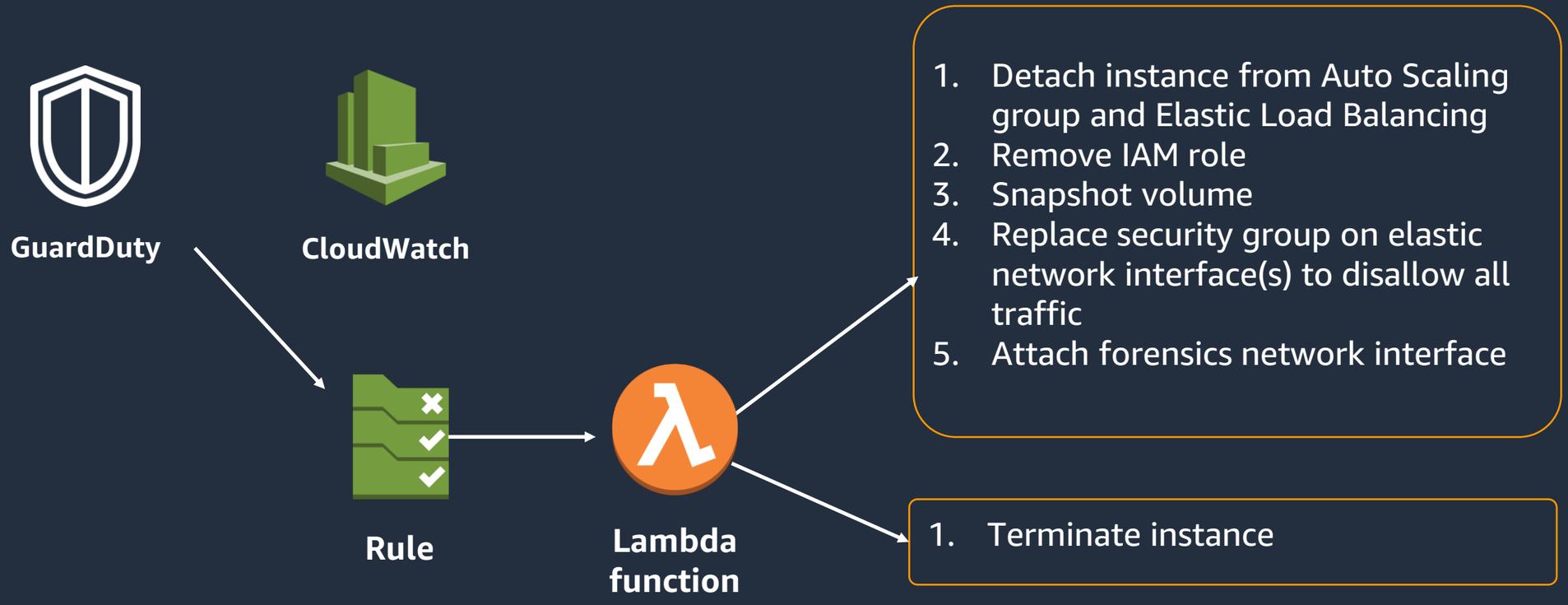
常见场景



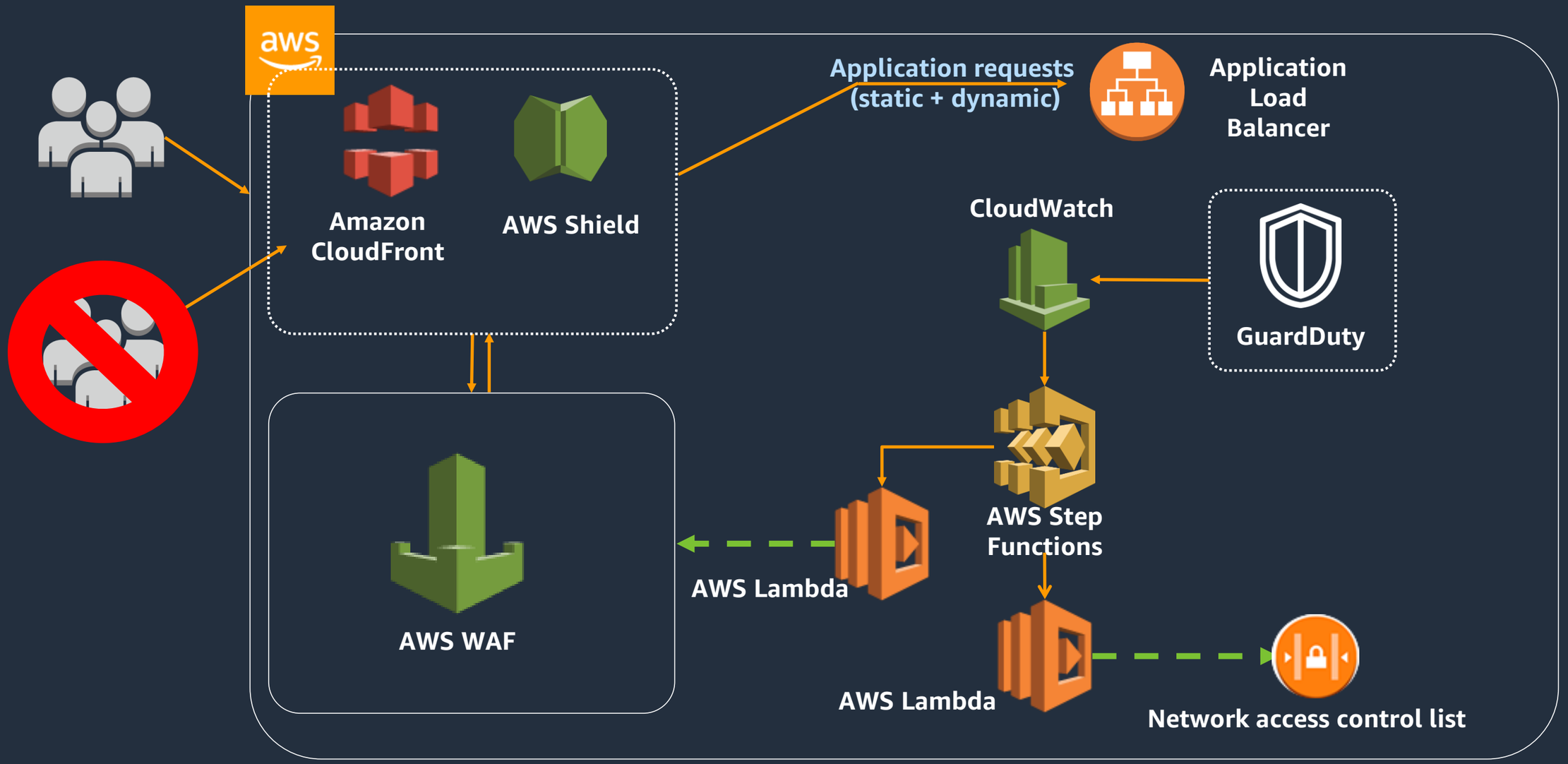
安全运维



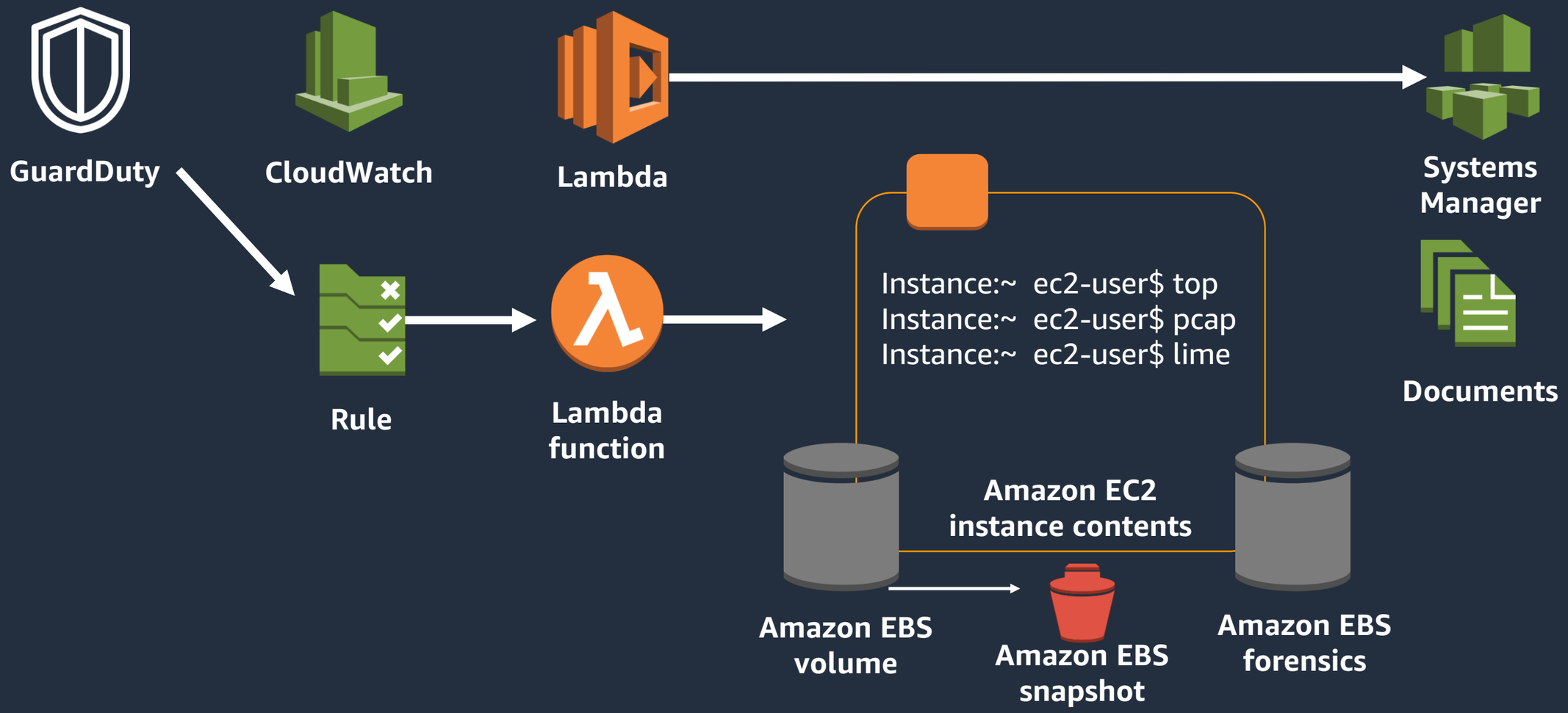
自动修复示例



事件响应：网络ACL和AWS WAF规则



自动化数据收集： Lambda + AWS Systems Manager



威胁检测与自动响应 - Demo

亚马逊云科技

Demo 架构

1. 受感染的实例连接到恶意主机，并且端口会扫描内部服务器。 恶意主机上的EIP在自定义威胁列表中。此流量记录在VPC流日志中。

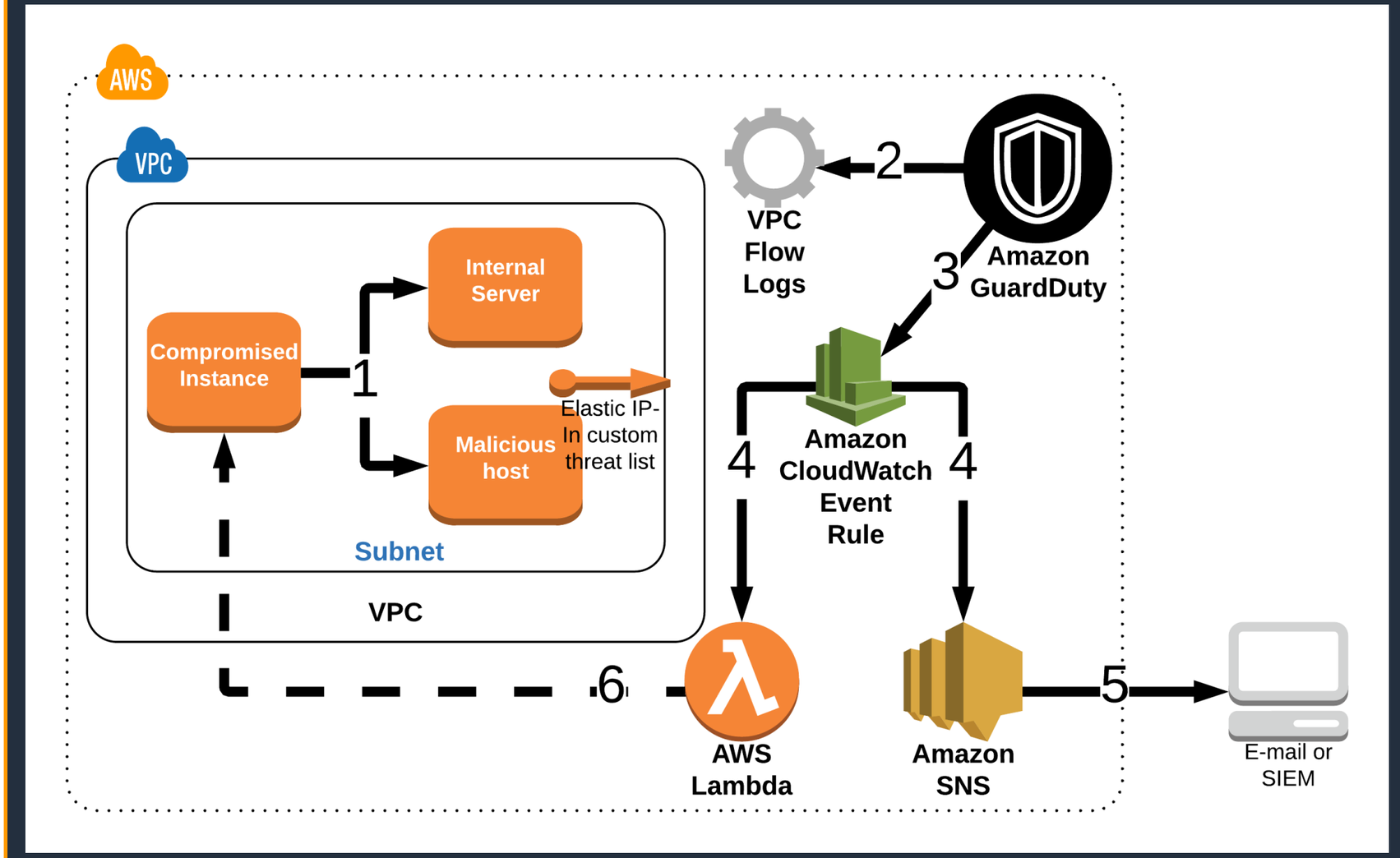
2. GuardDuty正在监视VPC流日志（除CloudTrail日志和DNS日志外），并根据威胁列表，机器学习，基准等对其进行分析。

3. GuardDuty会生成关于此活动的两个发现，并将这些发现发送到GuardDuty控制台和CloudWatch Events。 结果为：侦听：EC2 / Portscan和未经授权的访问：EC2 / MaliciousIPCaller.Custom

4. CloudWatch Event规则触发SNS主题和Lambda函数

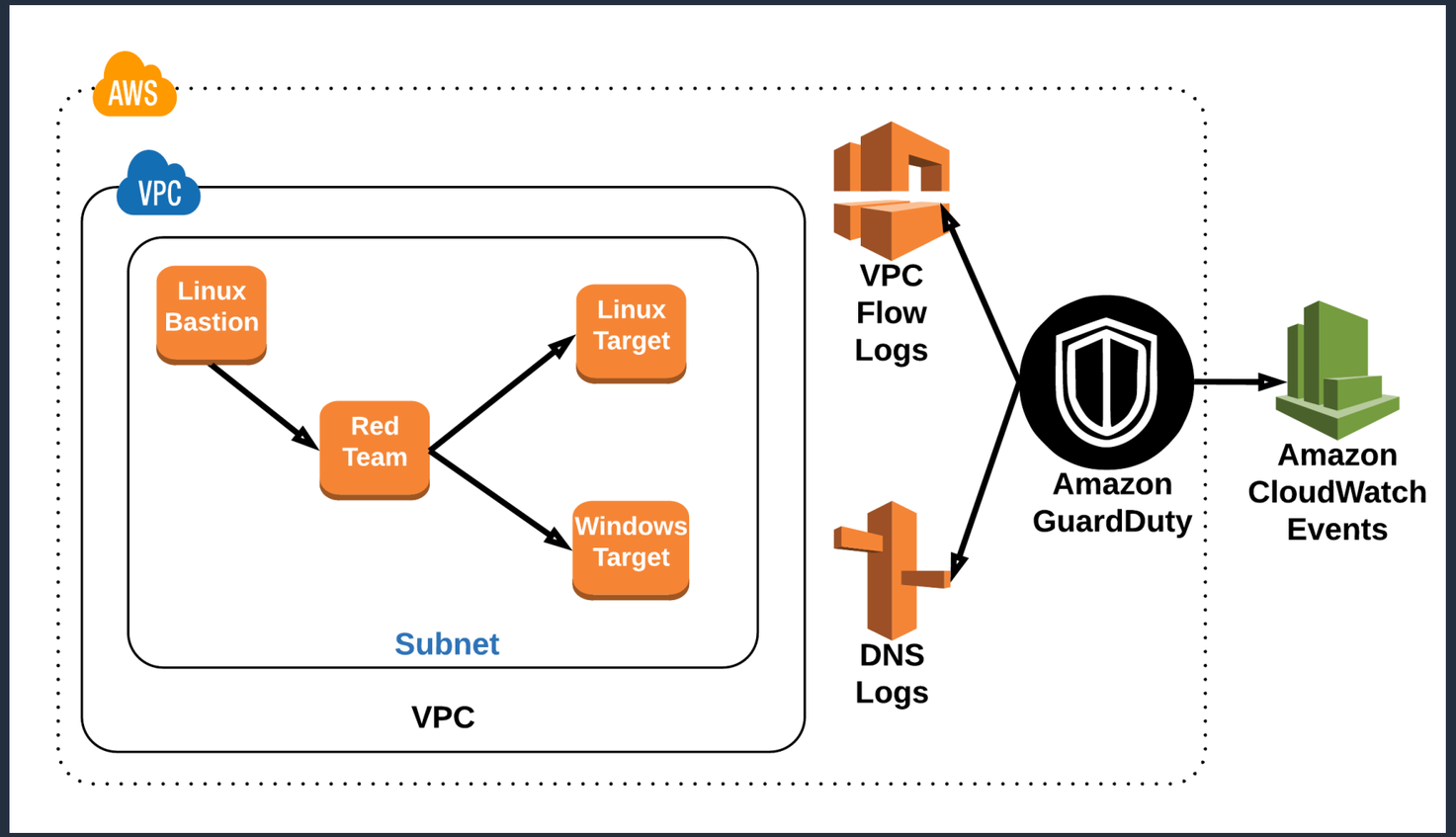
5. SNS发送带有发现信息的电子邮件和/或将发现传递给SIEM

6. 自动修复：Lambda对受感染实例执行操作



Demo 架构

1. 在Red Team实例上运行的脚本会同时调用Linux和Windows实例进行蛮力攻击
2. 该脚本还使DNS查询其他发现。
3. GuardDuty正在监视VPC流日志（除CloudTrail日志和DNS日志外），并根据威胁列表，机器学习，基准等对其进行分析。
4. GuardDuty会生成有关此活动的许多发现，并将这些发现发送到GuardDuty控制台和CloudWatch Events。



Q&A

Name of presenter

亚马逊云科技

亚马逊云科技