
AWS
re:Invent

SEC321

Get ahead of the curve with Shield Response Team Escalations

Fola Bolodeoku

Security Engineer

AWS Shield Response Team (SRT, aka DRT)

AWS re:Invent

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

Agenda

- Preparing for Shield Advanced Escalations
- Lessons learned from Shield Advanced Escalations
- Avoiding common mistakes
- Discover simple yet effective ways to remain resilient to DDoS events



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

What is AWS Shield

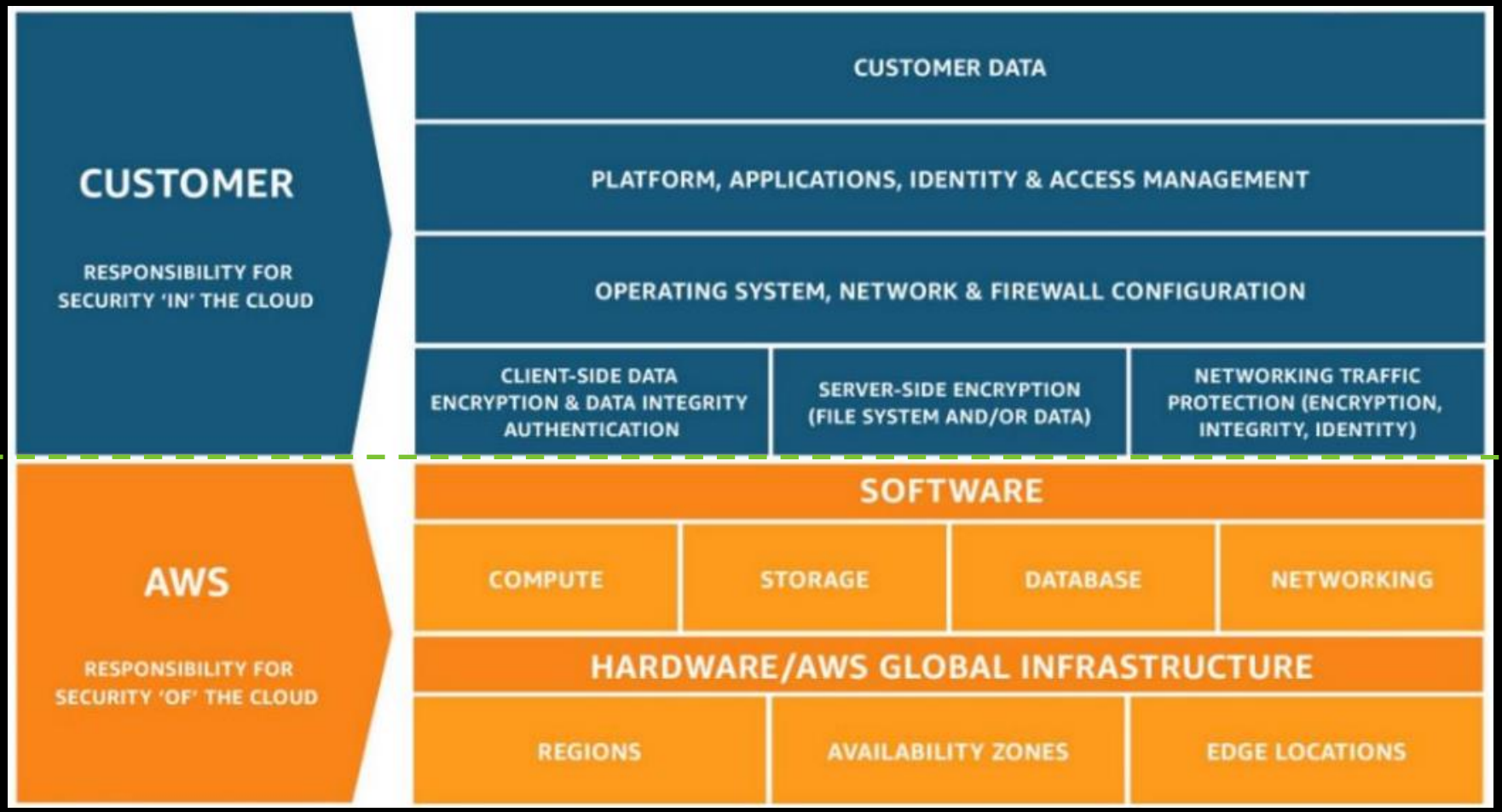
MANAGED APPLICATION SECURITY AND DDOS PROTECTION SERVICE WITH TWO TIERS:



- AWS Shield Standard
  - *Primarily* Protects Availability of AWS Infrastructure (L3 -4).
    - Protects all AWS customers from “noisy neighbor”
- AWS Shield **Advanced**
  - Designed to offer comprehensive protection for your application (L3–7)
    - Access to AWS WAF, and AWS Firewall Manage at no additional cost, for automated policy enforcement.
    - Access to Shield Response Team Support

AWS Shared Responsibility Model

AWS SHIELD DDOS PROTECTION

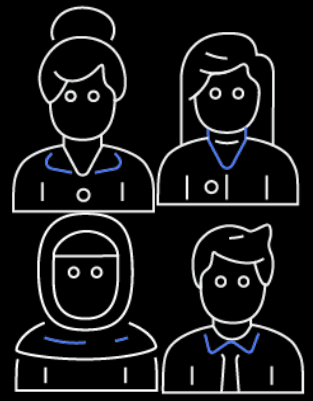


Shield Advanced

Shield Standard

"Noisy neighbor" Protection

Who are the Shield Response Team (SRT)?



Security Engineers available 24/7 to customers before, during, and after an event



DDoS mitigation specialists that deal with these issues on a daily basis, and can apply custom mitigations to ensure application availability

Before the event: Preparing for Shield Advanced Escalations



AWS re:Invent

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

First things first: How to prepare for an event before the event

- AWS Best Practices for DDoS Resiliency Whitepaper
  - https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/welcome.html
- Reduce your risk surface to a minimum:
  - Security Groups and Network Access Control Lists
  - Protecting Your Origin
  - Protecting API Endpoints
- Ensure your team is prepared, and are receiving critical DDoS event notifications

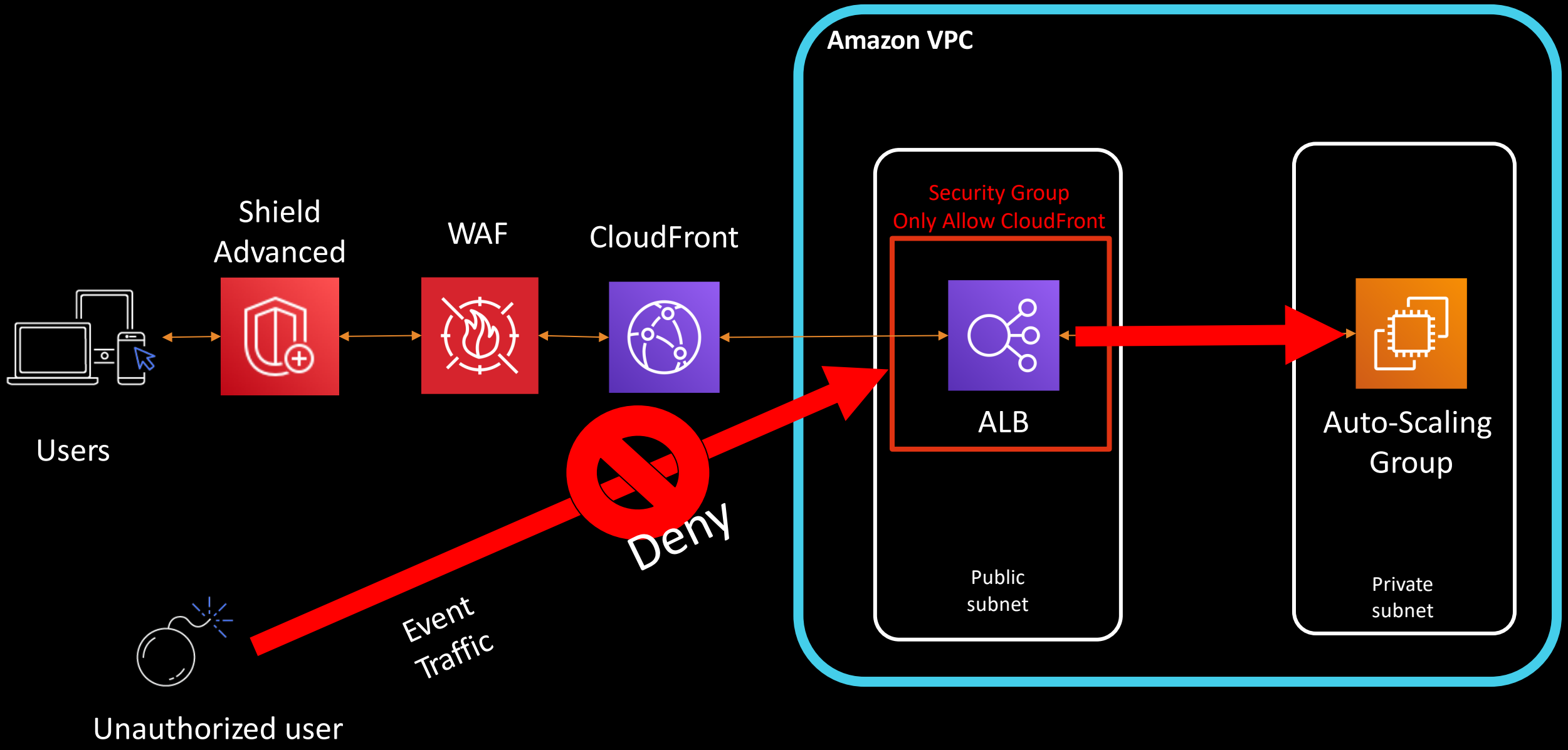
Customer stories from Shield Advanced Escalations



AWS re:Invent

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

Customer A, Life Science Manufacturer



Protecting Your Origin

- Protect your Cloudfront Origin:
  a) Automatically Update ALB Security Groups with CloudFront IPs Using AWS Lambda.

  b) Configure CloudFront to Add Custom Headers to Origin Requests.

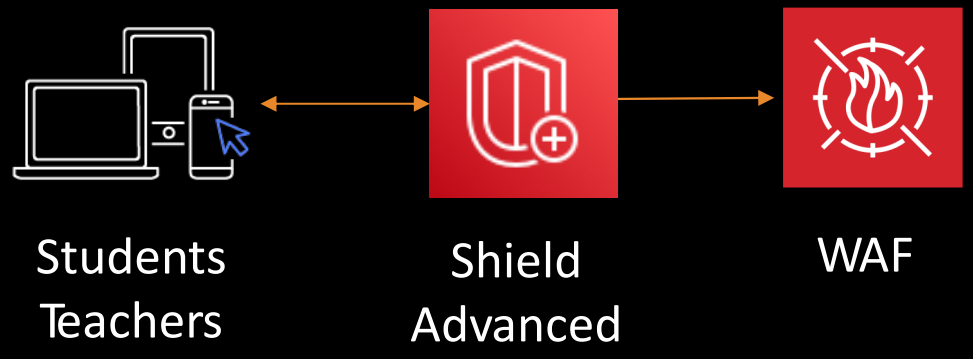
  c) For S3 origins, use Origin Access Identity (OAI)

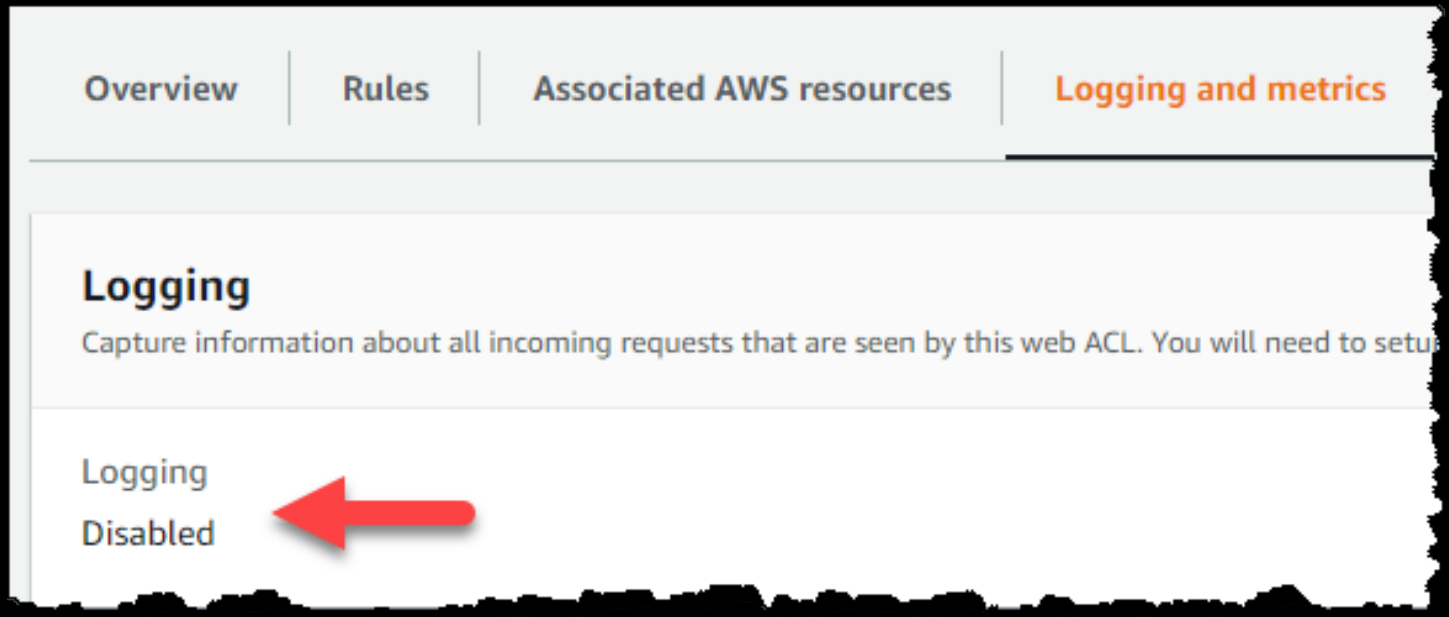
CloudFront

Inbound rules

Type	Protocol	Port range	Source
HTTPS	TCP	443	18.216.170.128/25
HTTPS	TCP	443	34.223.80.192/26
HTTPS	TCP	443	99.79.169.0/24
HTTPS	TCP	443	3.11.53.0/24
HTTPS	TCP	443	52.212.248.0/26
HTTPS	TCP	443	35.162.63.192/26
HTTPS	TCP	443	18.229.220.192/26
HTTPS	TCP	443	18.200.212.0/23
HTTPS	TCP	443	34.226.14.0/24
HTTPS	TCP	443	52.78.247.128/26
HTTPS	TCP	443	13.59.250.0/26
HTTPS	TCP	443	52.220.191.0/26
HTTPS	TCP	443	35.167.191.128/26

Customer B, eLearning Platform





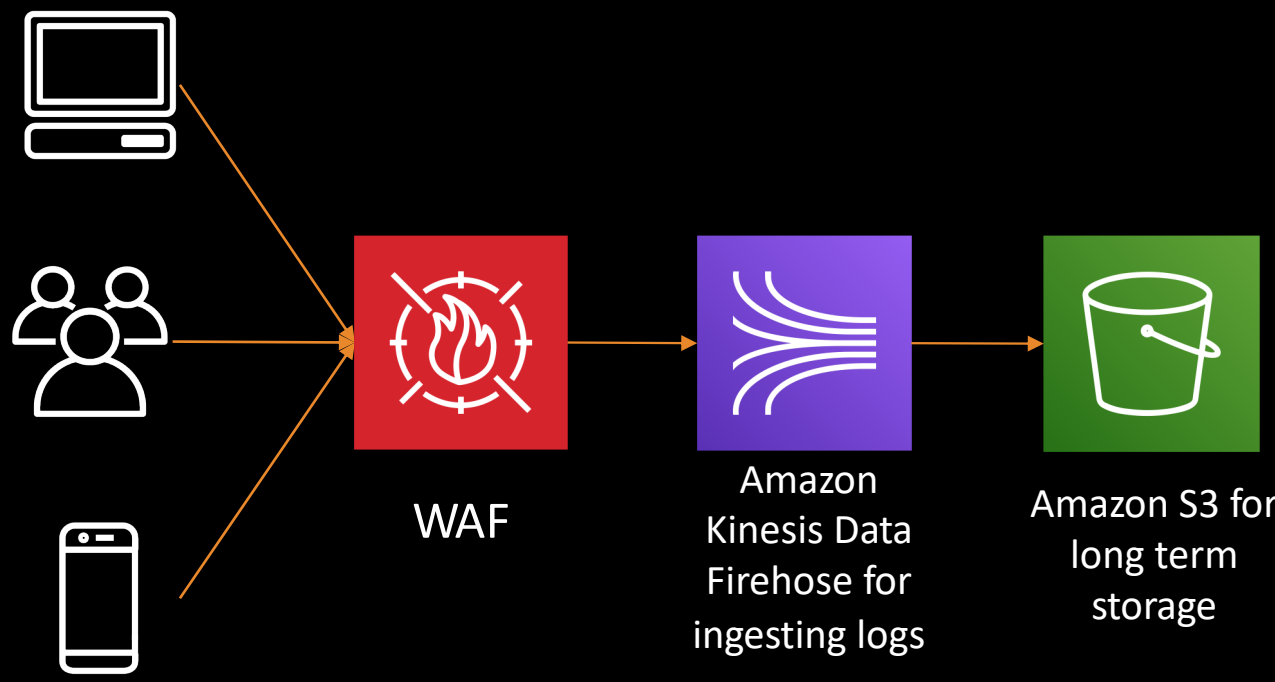
Custom rate-based rule to Block Request Flood

- Snippet of the rate based rule for the targeted URI.
  - (protect-web-sites-services-using-rate-based-rules-for-aws-waf/)

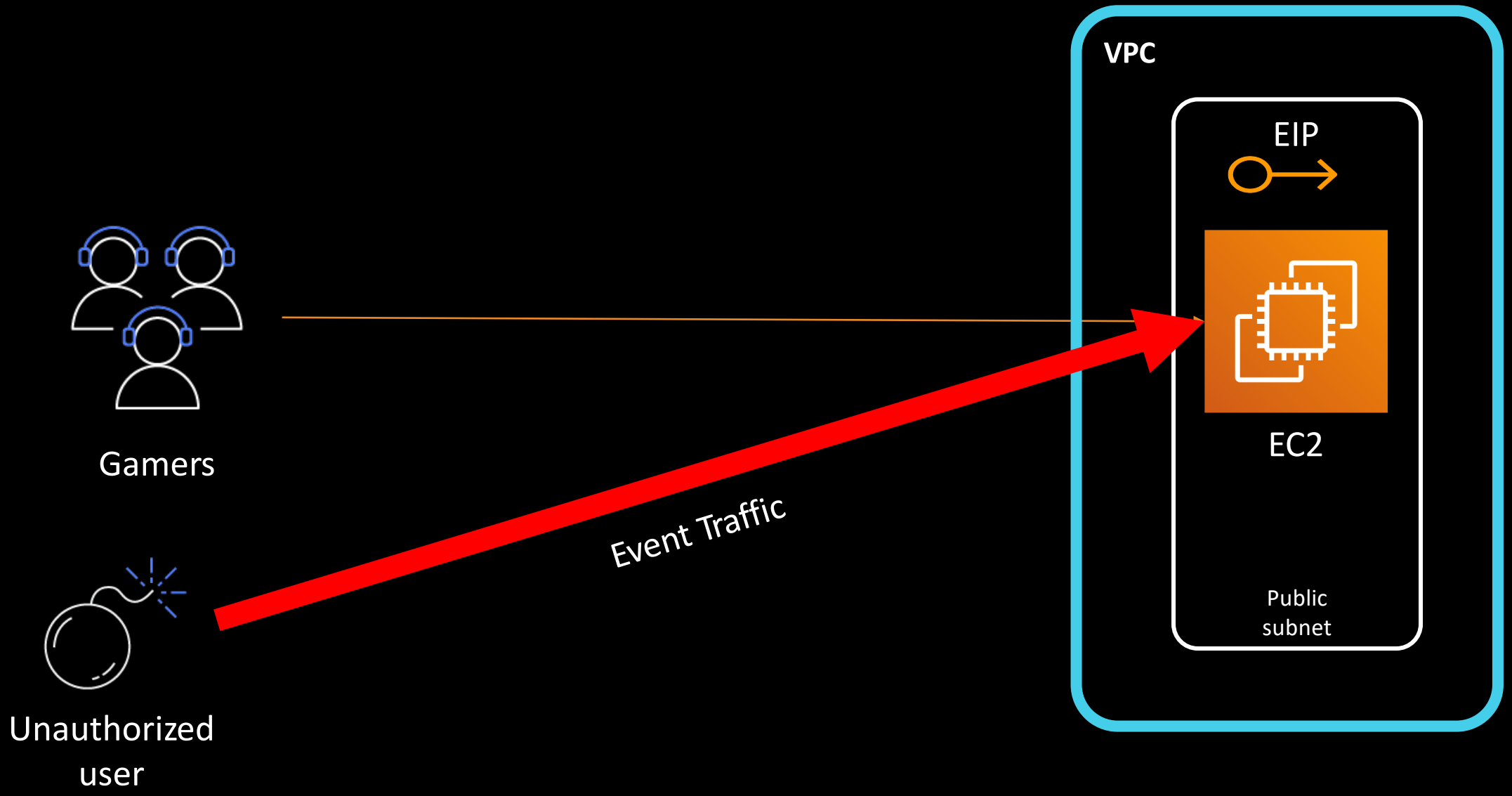


Enable WAF Full Logging

- Enable WAF Full Logging, and authorize DRT Access to write WAF Rules
- Centralize logs for multiple Accounts using Firewall Manager
- Enforce Application Compliance with WAF Rules using Firewall Manager.



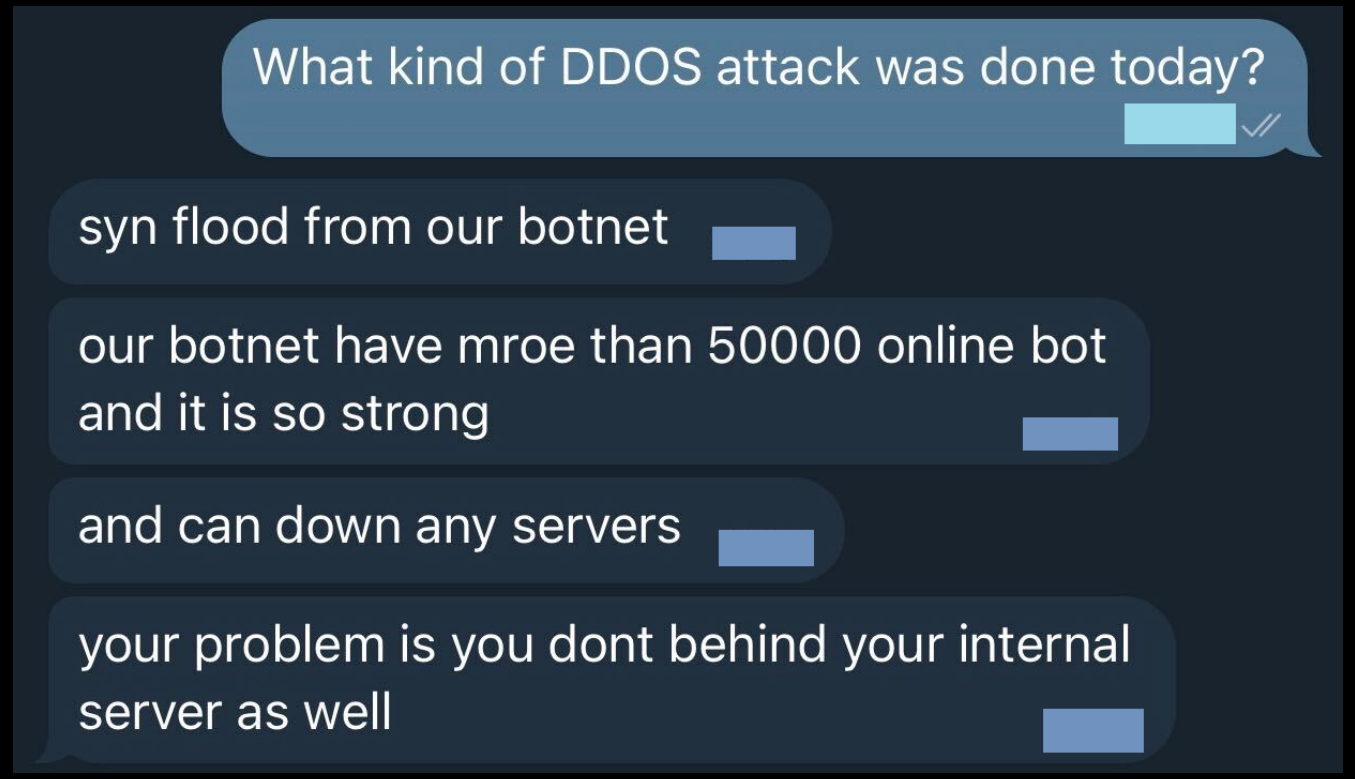
Customer C, Online gaming Company and DDoS extortion



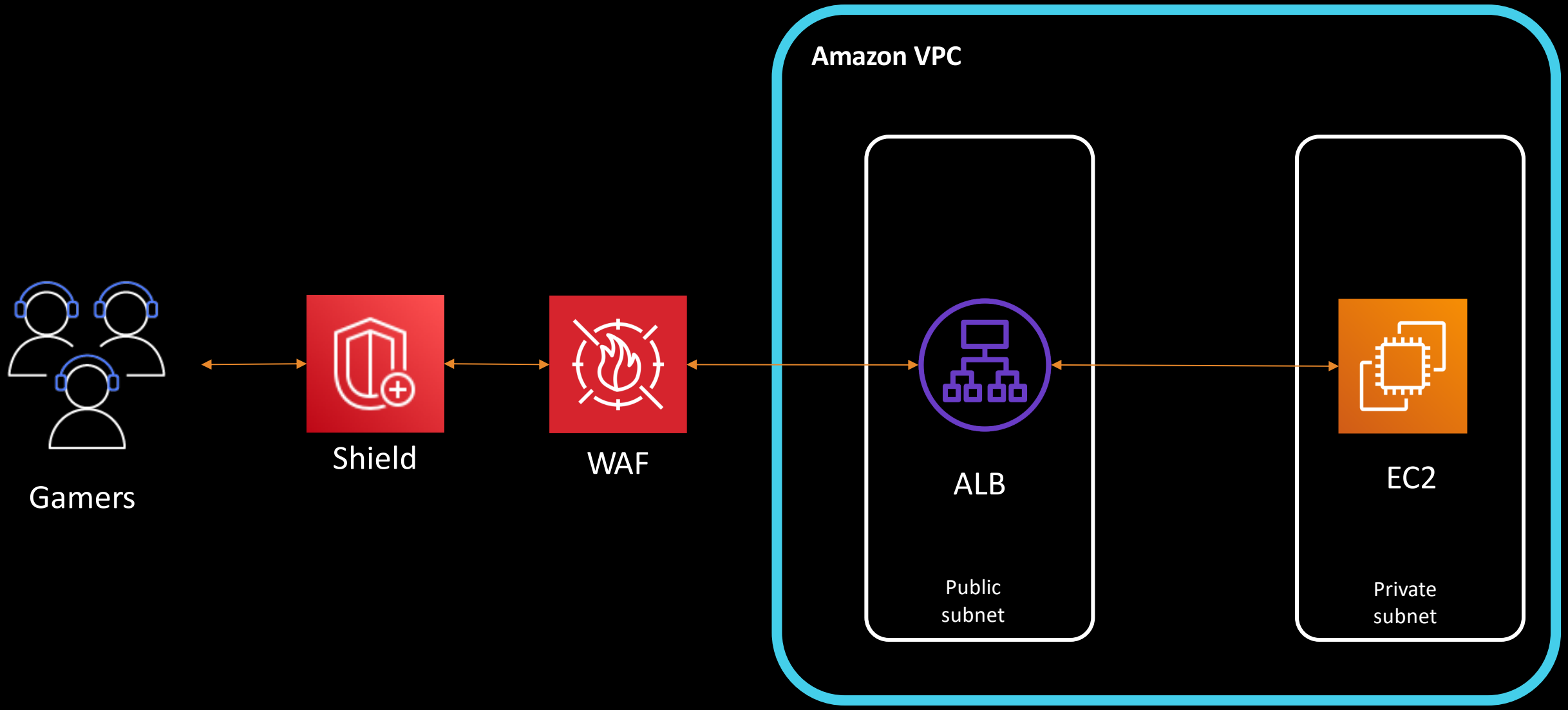
Application Layer Defence & Proactive Response

Customer

Attacker



Application Layer Defence



Custom Rate-Based Rule to Block Request Flood

JSON

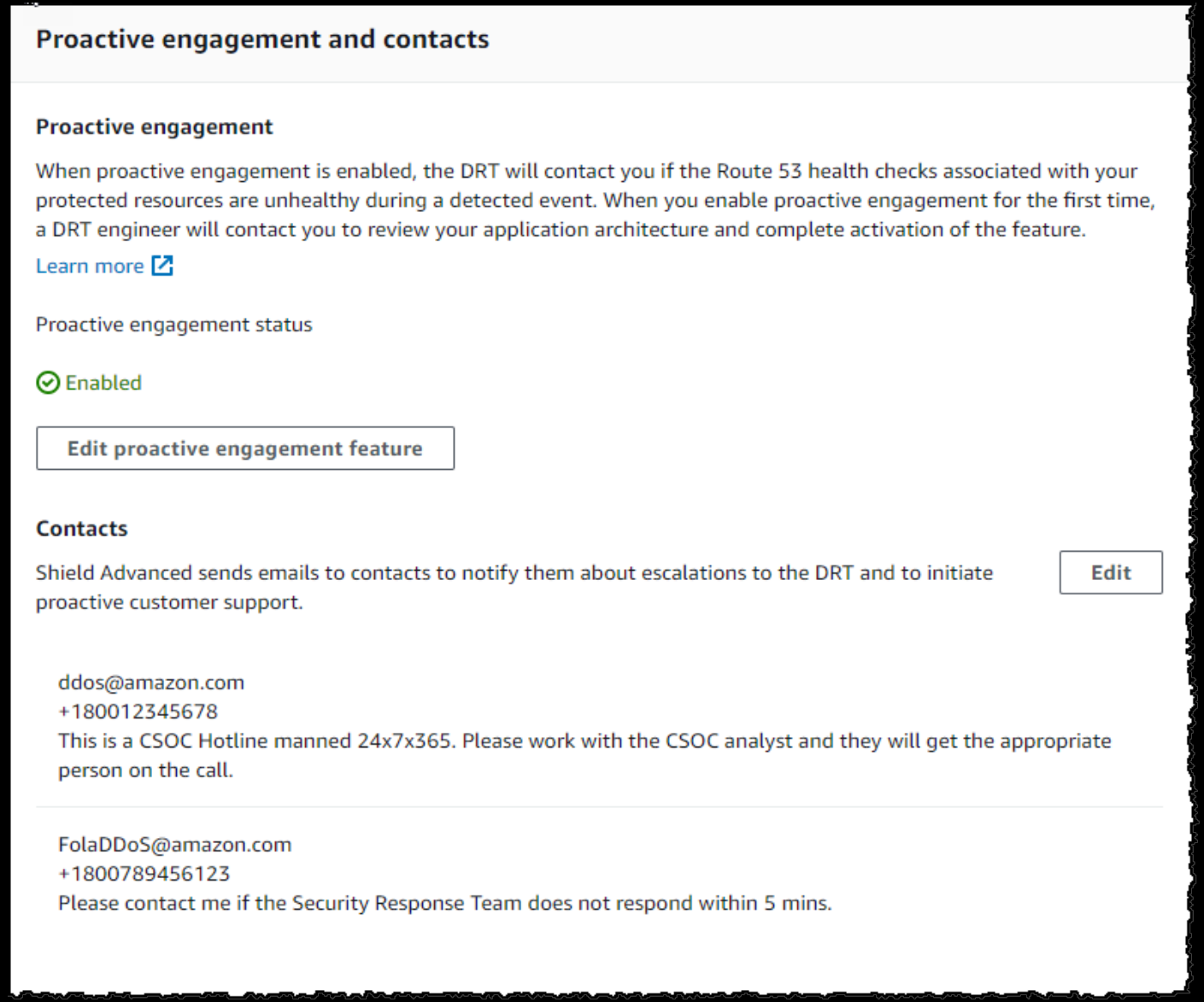
```
{
  "Name": "block_user-agent",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "block-user-agent"
  },
  "Statement": {
    "ByteMatchStatement": {
      "FieldToMatch": {
        "SingleHeader": {
          "Name": "user-agent"
        }
      },
      "PositionalConstraint": "CONTAINS",
      "SearchString": "user-agent-name-here",
      "TextTransformations": [
        {
          "Type": "LOWERCASE",
          "Priority": 0
```

JSON

```
{
  "Name": "block_cookie",
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "block_cookie"
  },
  "Statement": {
    "ByteMatchStatement": {
      "FieldToMatch": {
        "SingleHeader": {
          "Name": "cookie"
        }
      },
      "PositionalConstraint": "CONTAINS",
      "SearchString": "cookie-string-here",
      "TextTransformations": [
        {
          "Type": "LOWERCASE",
          "Priority": 0
        }
```

Shield Advanced Proactive Response

- Create Health Checks for SRT to monitor
- Associate them to Protected Resources
- Specify emergency contacts



Next actions from lessons learned



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

Items you need to become/remain resilient

- Enable AWS WAF for Layer 7 (Application Layer) event detections
- Enable AWS WAF logging, authorize SRT access to AWS WAF APIs and AWS WAF S3 log buckets
- Add custom rate-based rules
  - General rule, expensive page rule (e.g., login page/weakest link), geo rate-limiting
- Reduce risk surface & protect your origin
  - NACLs, SGs, Custom Origin header, geo blocking/IP reputation where possible
- Trigger the Shield Engagement Lambda for rapid SRT escalation
- Enable Shield Proactive Response for SRT to monitor your application's health

Thank you!

Fola Bolodeoku

Security Engineer
AWS Shield Response Team

© 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.