
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT326

SPONSORED BY DATADOG

Security incident monitoring, mitigation, and metrics using feature flags

Andrew Krug

Engineering Manager &
Lead of Security Advocacy
Datadog

Alex Hardman

Technical Marketing Engineer
LaunchDarkly

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways

WHAT YOU'LL LEAVE WITH

Identify	Identify the evolution of the "incident" in the cloud
Learn	Learn about new methods of mitigating an incident
Demo	See a demonstration of a resilient system

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The world is changing



View of the Earth as seen by the Apollo 17 crew traveling toward the moon

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

And we must too



AWS CloudTrail AWS Lambda

2016
Security automation

AWS Systems Manager

2018
Forensics automation

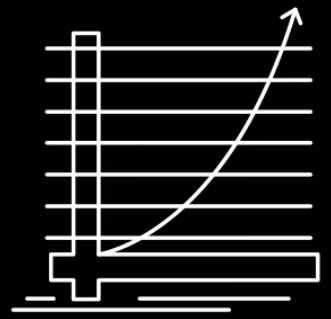
AWS Step Functions

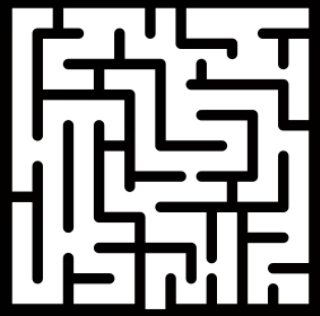
2019
Playbooks as code

View of the Earth as seen by the Apollo 17 crew traveling toward the moon

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Present day







Thousands of assets

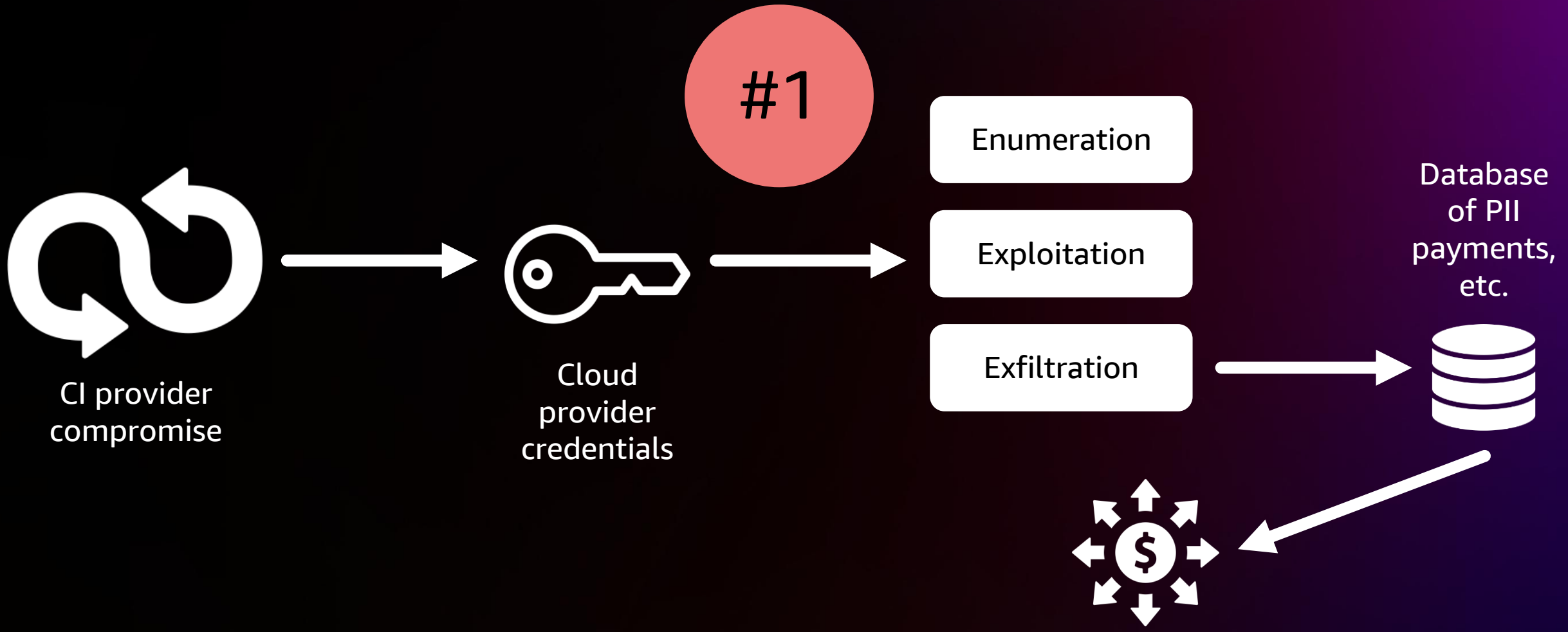
Increasing complexity

Increasing attack surface

aws

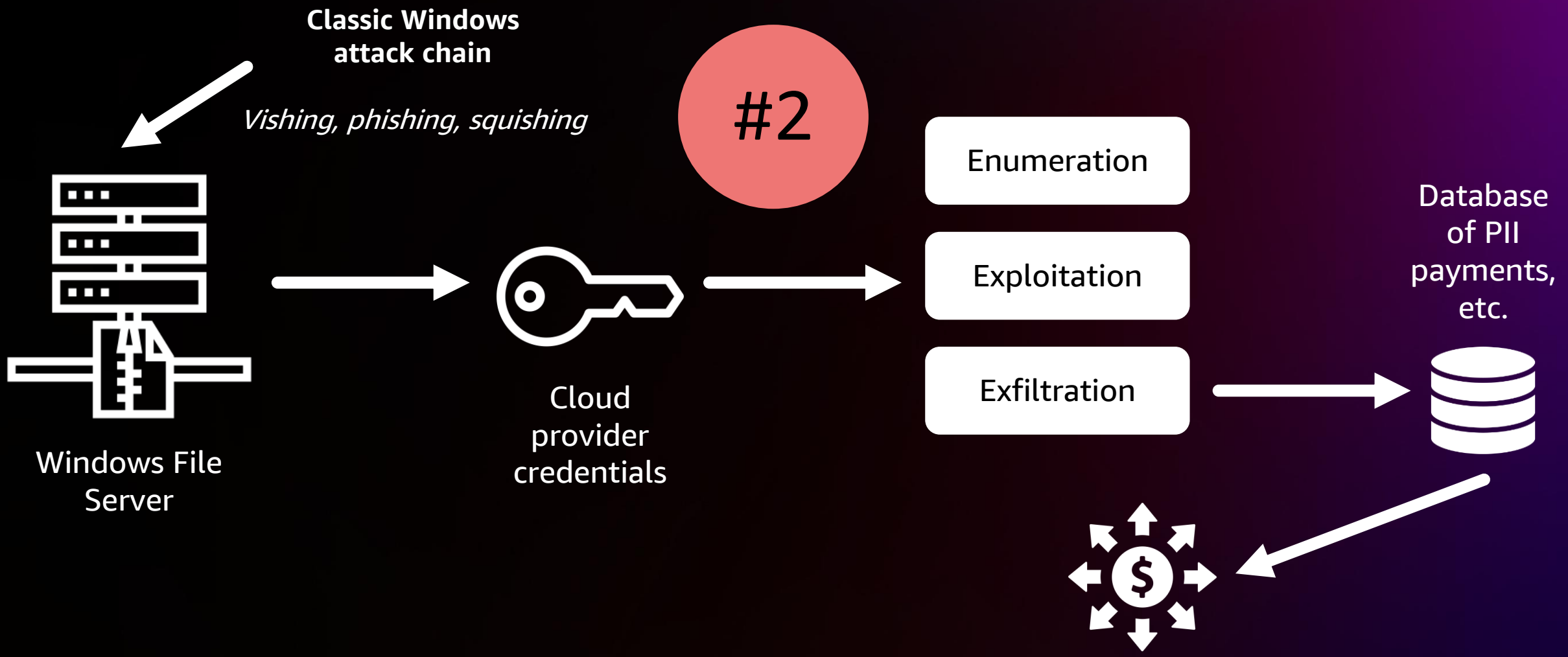
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modern cloud events: Based on a true story



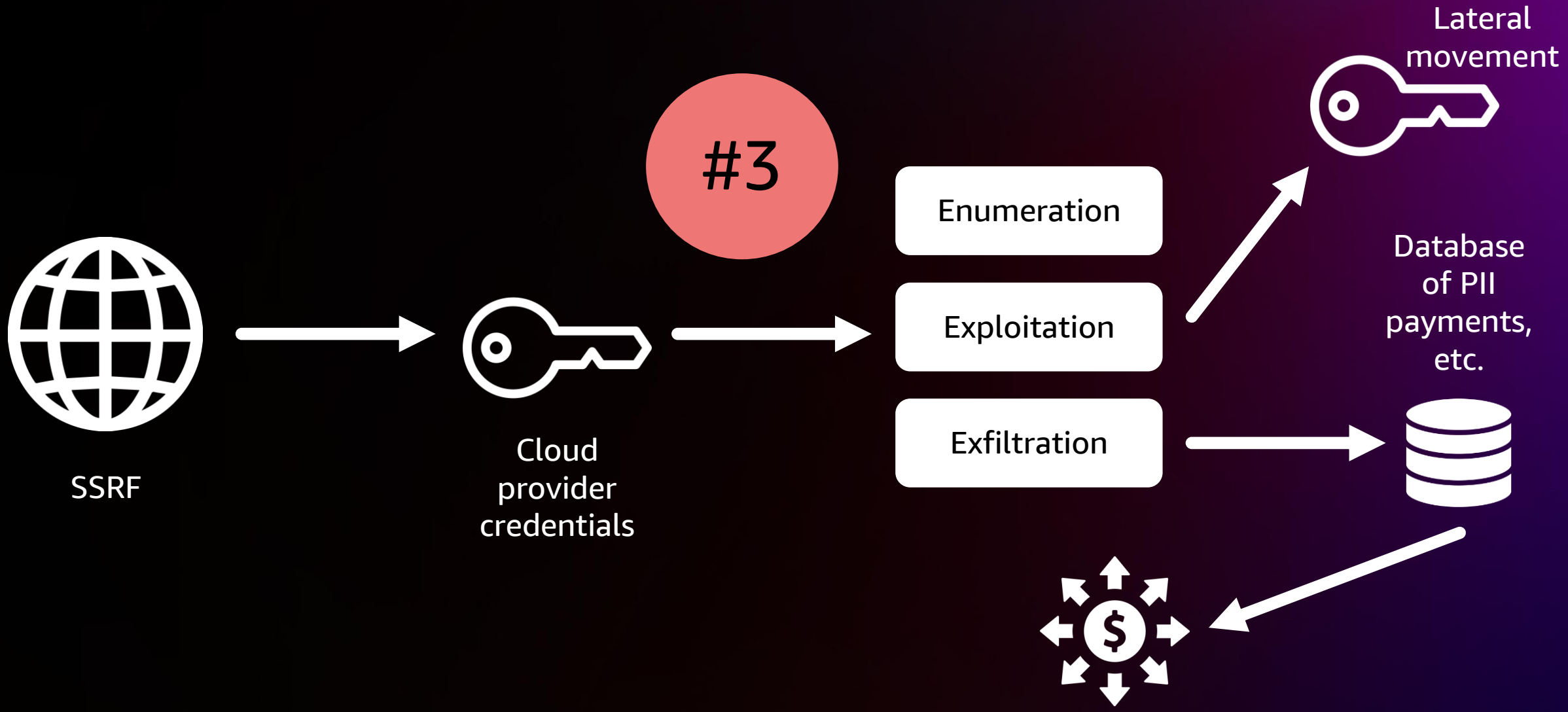
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modern cloud events: Based on a true story



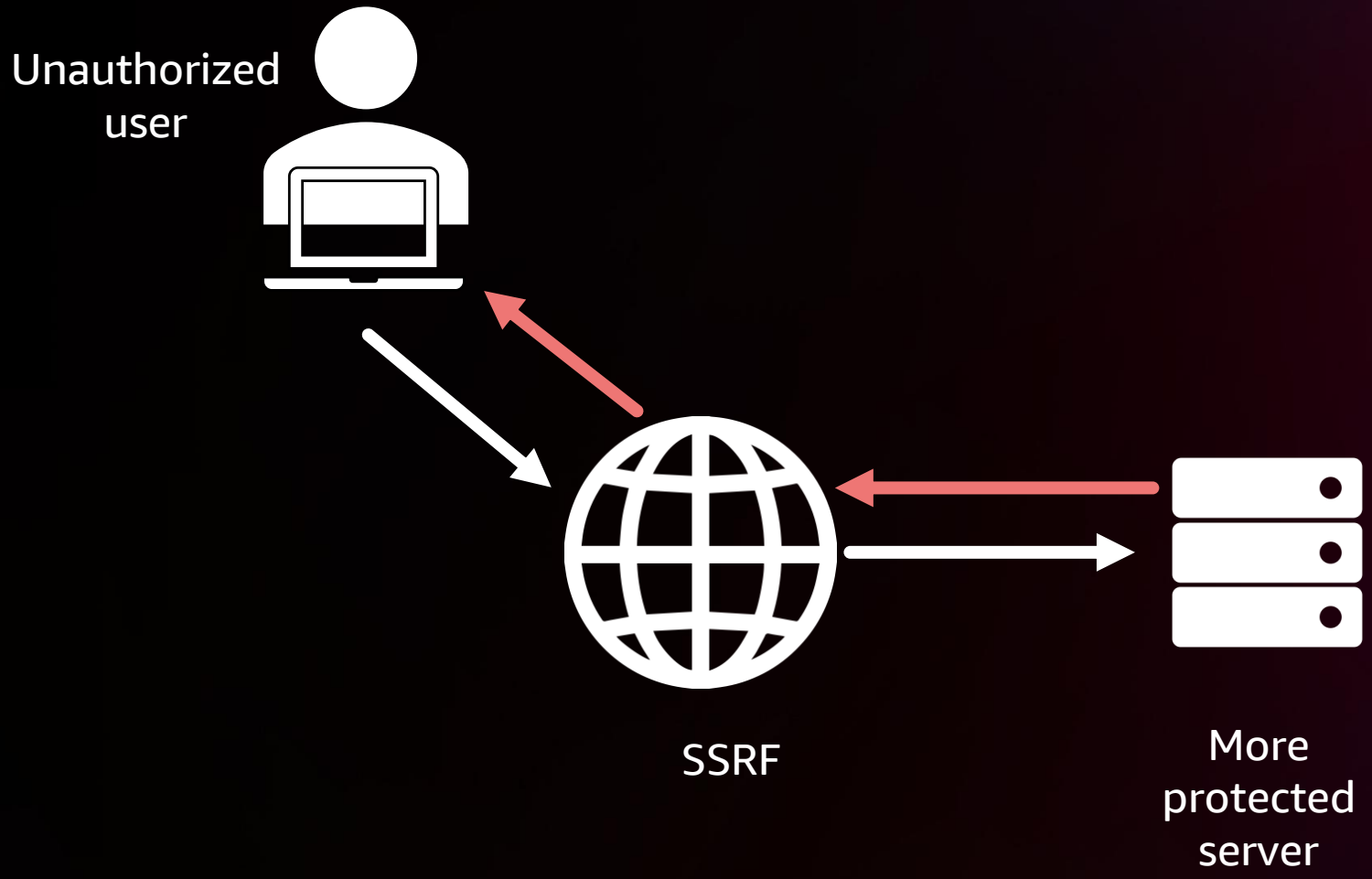
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modern cloud events: Next generation



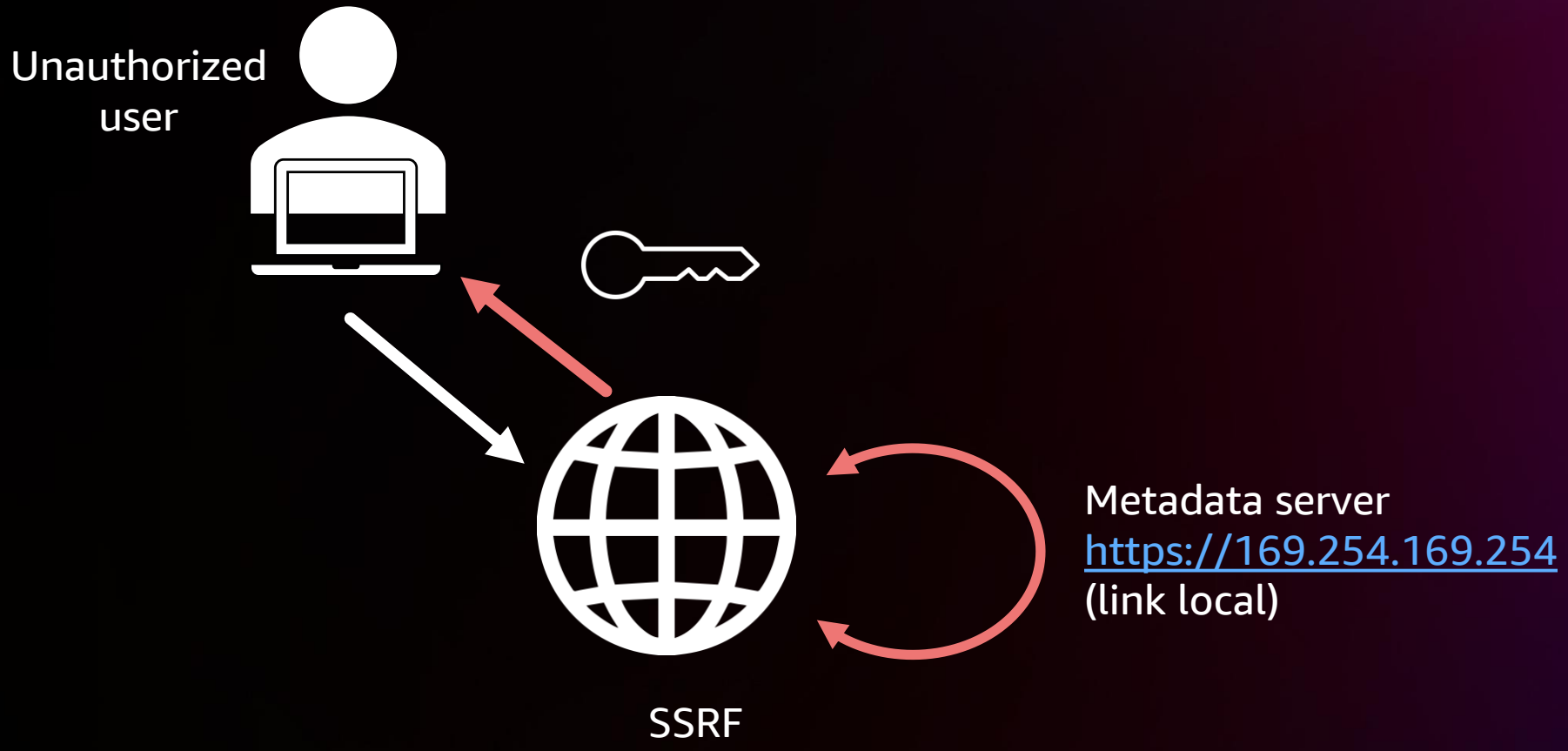
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of an SSRF: A new-*ish* attack style



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of an SSRF: A new-*ish* attack style



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Commonality of events



Initial access credentials



Target is data



Maximum impact

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Answer: Resilient systems

A SYSTEM THAT IS FLEXIBLE, ADAPTABLE, AND TRANSFORMABLE



Kelly Shortridge, Senior Principal – Product Technology at Fastly

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Feature flags as resilience

INVITING ALEX HARDMAN TO THE STAGE



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The LaunchDarkly story

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

LaunchDarkly

DELIVERING 30 TRILLION FEATURE FLAGS DAILY



Client SDKs

Client-specific flags and rules delivered to the device for **only the configured user identity**.

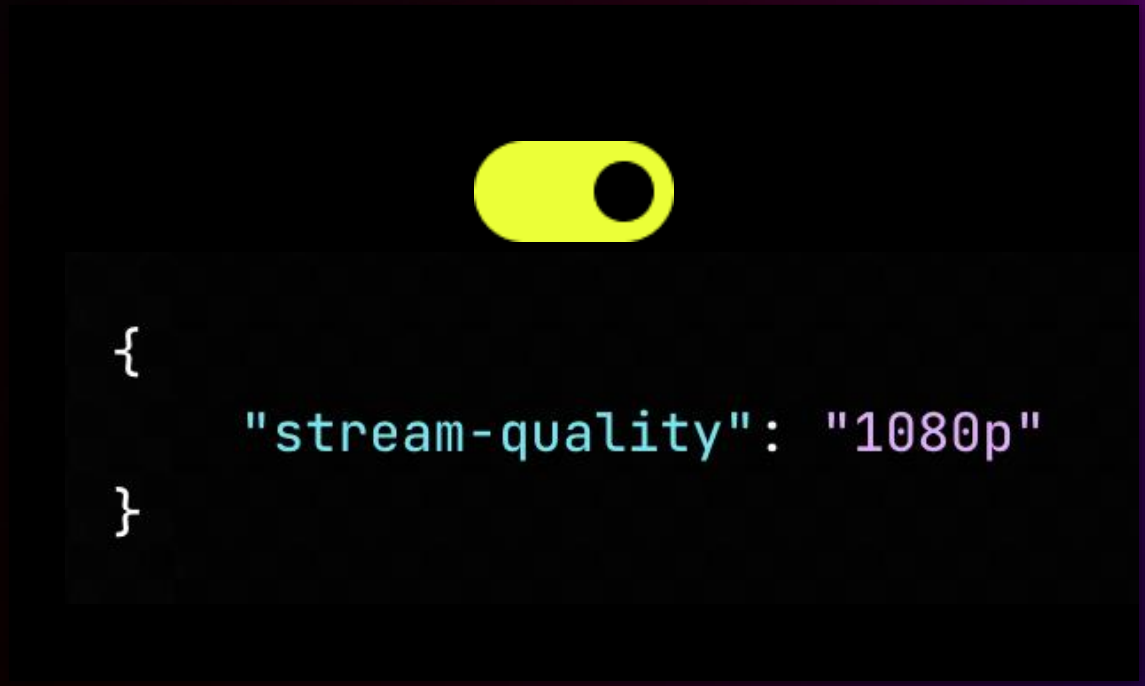
Server SDKs

Flags and rules are initialized for **all users and rules in the current environment**.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

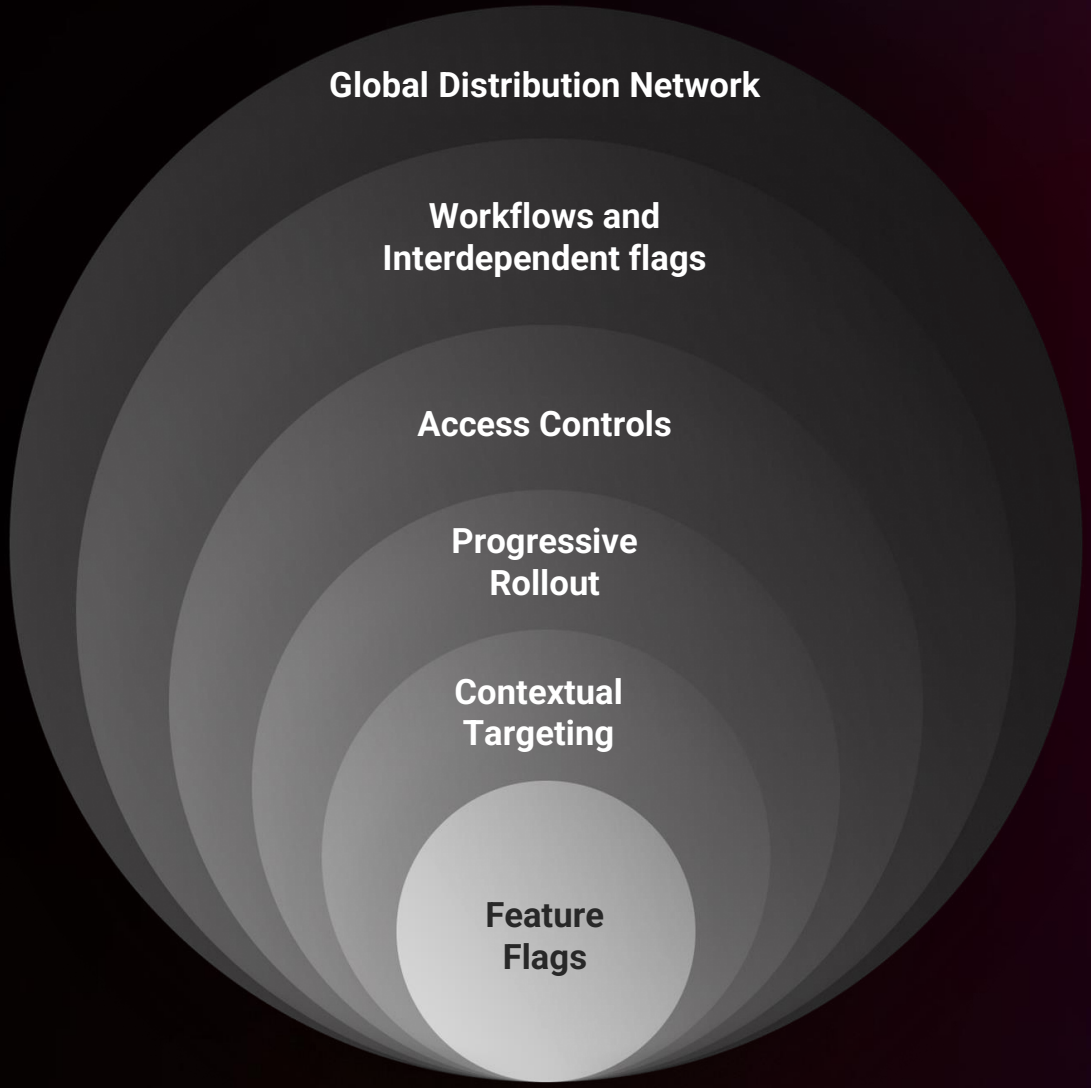
What do feature flags do?

Separates code deployment from release to enable , disable, or change functionality at runtime.



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

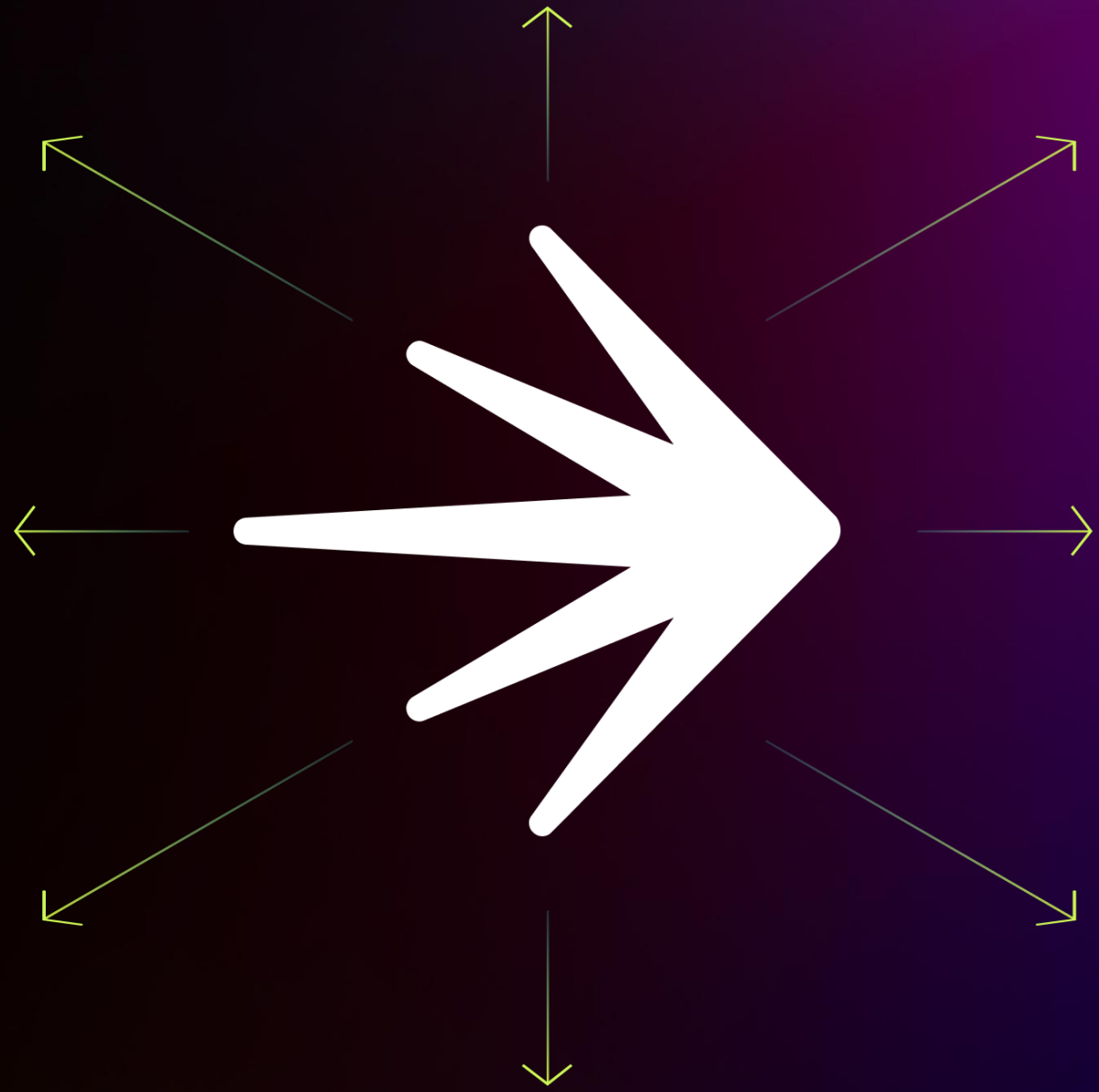
What is feature management?



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

LaunchDarkly scale

- **20** trillion feature flag evaluations per day
- **4,000+** customers on the platform
- **1,000s** of hosts

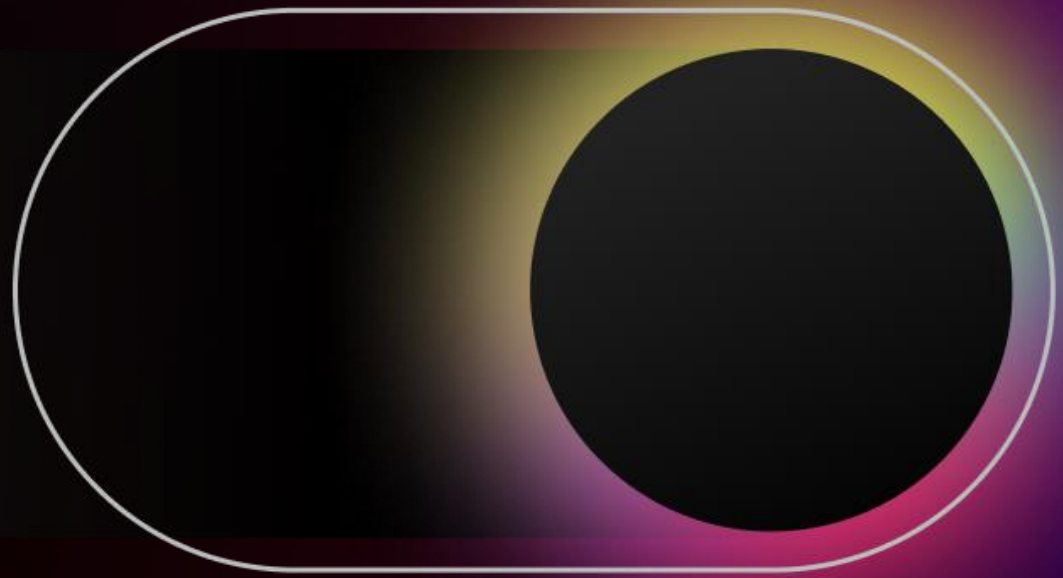


aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Risk profile

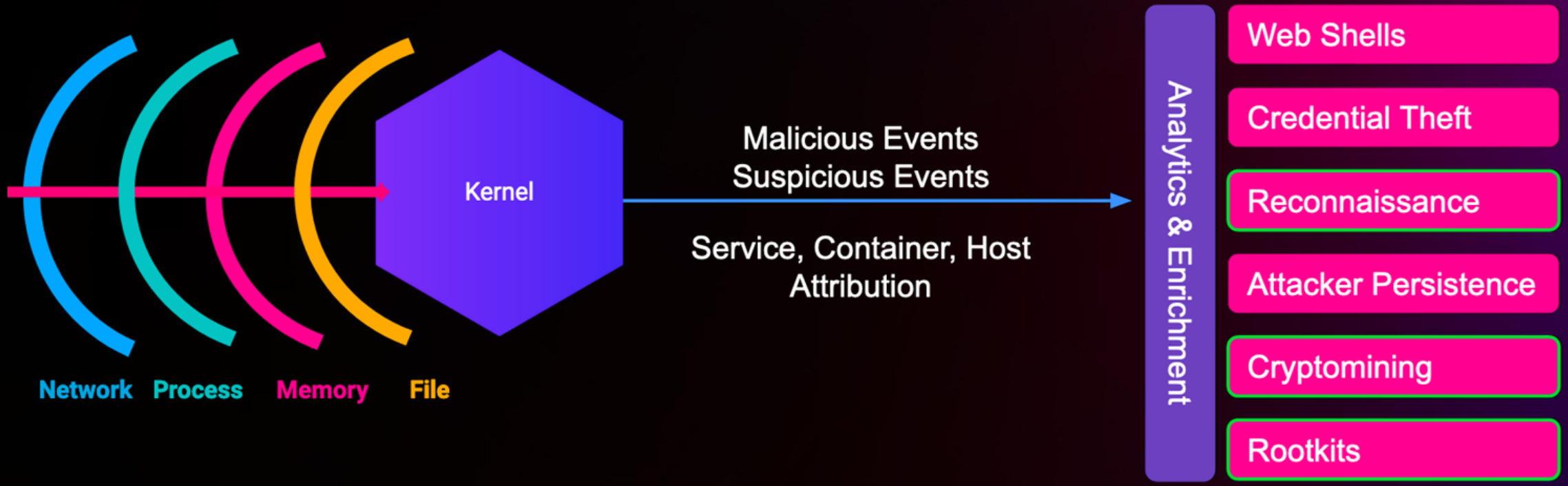
A disruption to our flag delivery network could affect our customers, and their users who depend on the experience we enable them to deliver.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud workload security

THE FUTURE OF THREAT DETECTION



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Rich findings

What

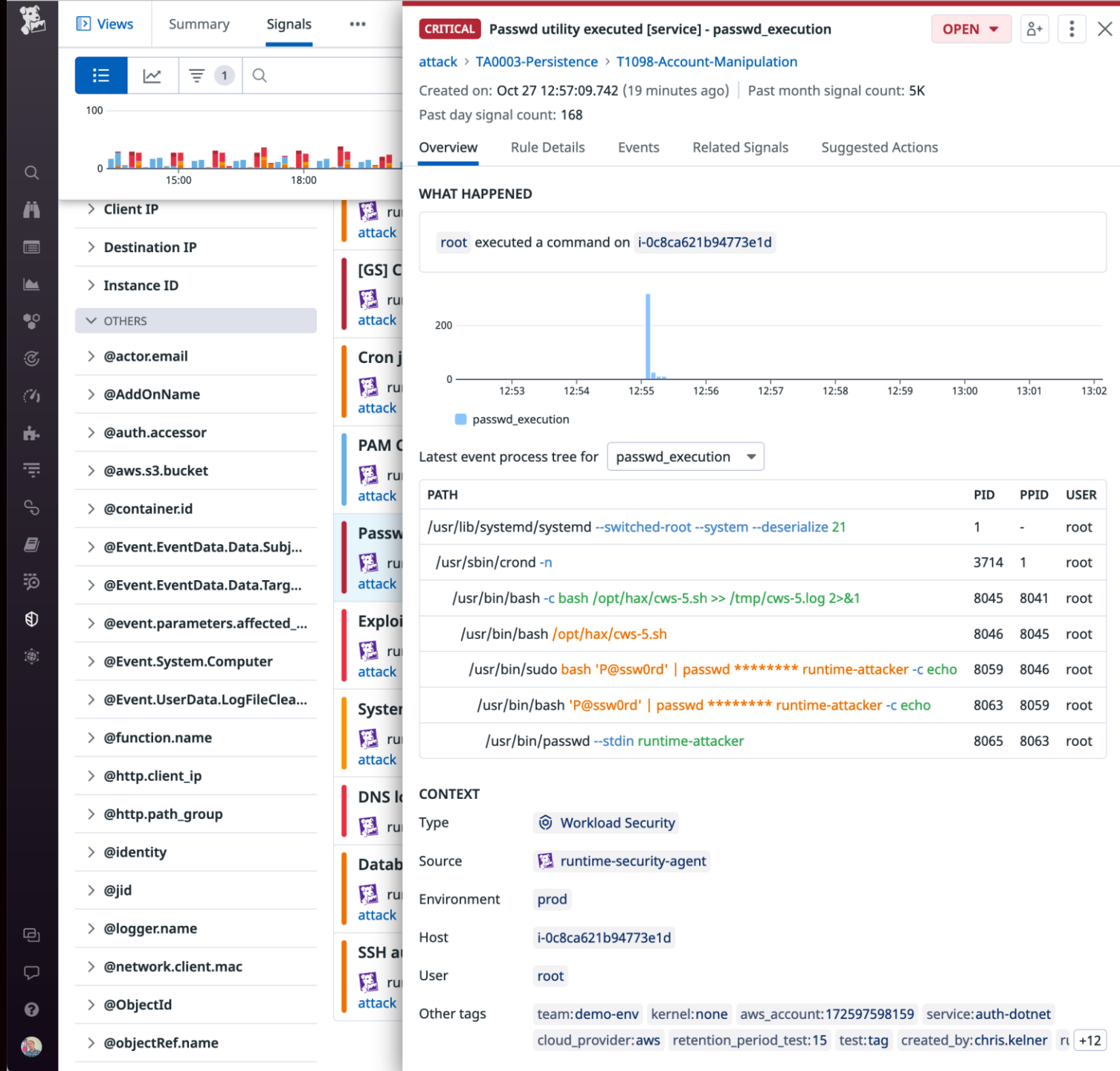
Gain immediate insight

Actionable findings

Forensic information

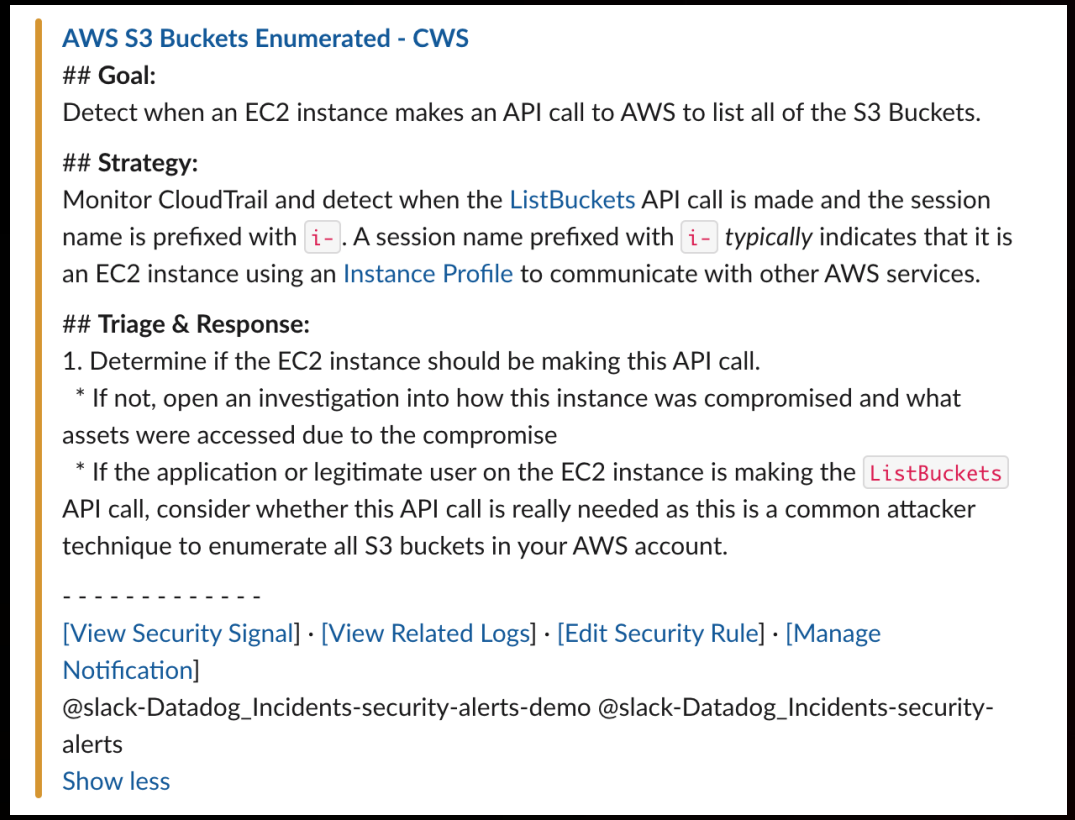
Result

Reduced investigation time



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detects top issues



AWS S3 Buckets Enumerated - CWS

Goal:

Detect when an EC2 instance makes an API call to AWS to list all of the S3 Buckets.

Strategy:

Monitor CloudTrail and detect when the ListBuckets API call is made and the session name is prefixed with `i-`. A session name prefixed with `i-` *typically* indicates that it is an EC2 instance using an Instance Profile to communicate with other AWS services.

Triage & Response:

1. Determine if the EC2 instance should be making this API call.
  * If not, open an investigation into how this instance was compromised and what assets were accessed due to the compromise
  * If the application or legitimate user on the EC2 instance is making the `ListBuckets` API call, consider whether this API call is really needed as this is a common attacker technique to enumerate all S3 buckets in your AWS account.

- - - - - - - - - - - - -

[View Security Signal] · [View Related Logs] · [Edit Security Rule] · [Manage Notification]

@slack-Datadog_Incidents-security-alerts-demo @slack-Datadog_Incidents-security-alerts

Show less

Findings surface in the places you already look

- Cryptomining
- Custom rules
- Techniques, tactics, and procedures relevant specifically to LaunchDarkly

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What's cool about it

1,000s of hosts

Millions of data points

Detection at the endpoint

Speedy triage

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What's cool about it

1,000s of hosts

Millions of data points

Detection at the endpoint

Speedy triage

Correlated to "double digit" actionable, true positive alerts

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Development and security in the same system



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits of breaking down silos

- One place where engineers collaborate with security
- Shared visibility through the control plane, workload, and application
- Increased ability to triage issues quickly



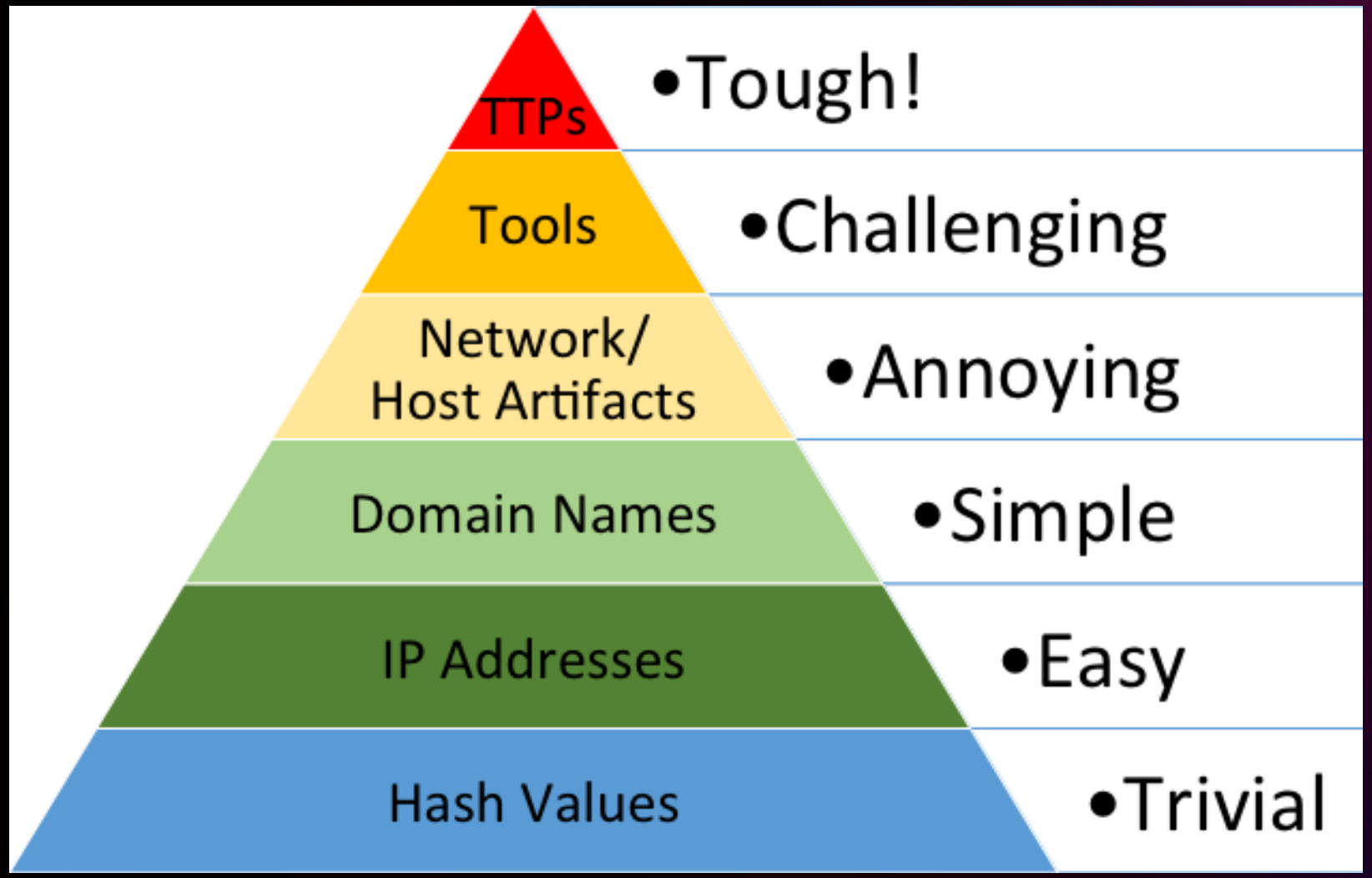
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Rethinking detection

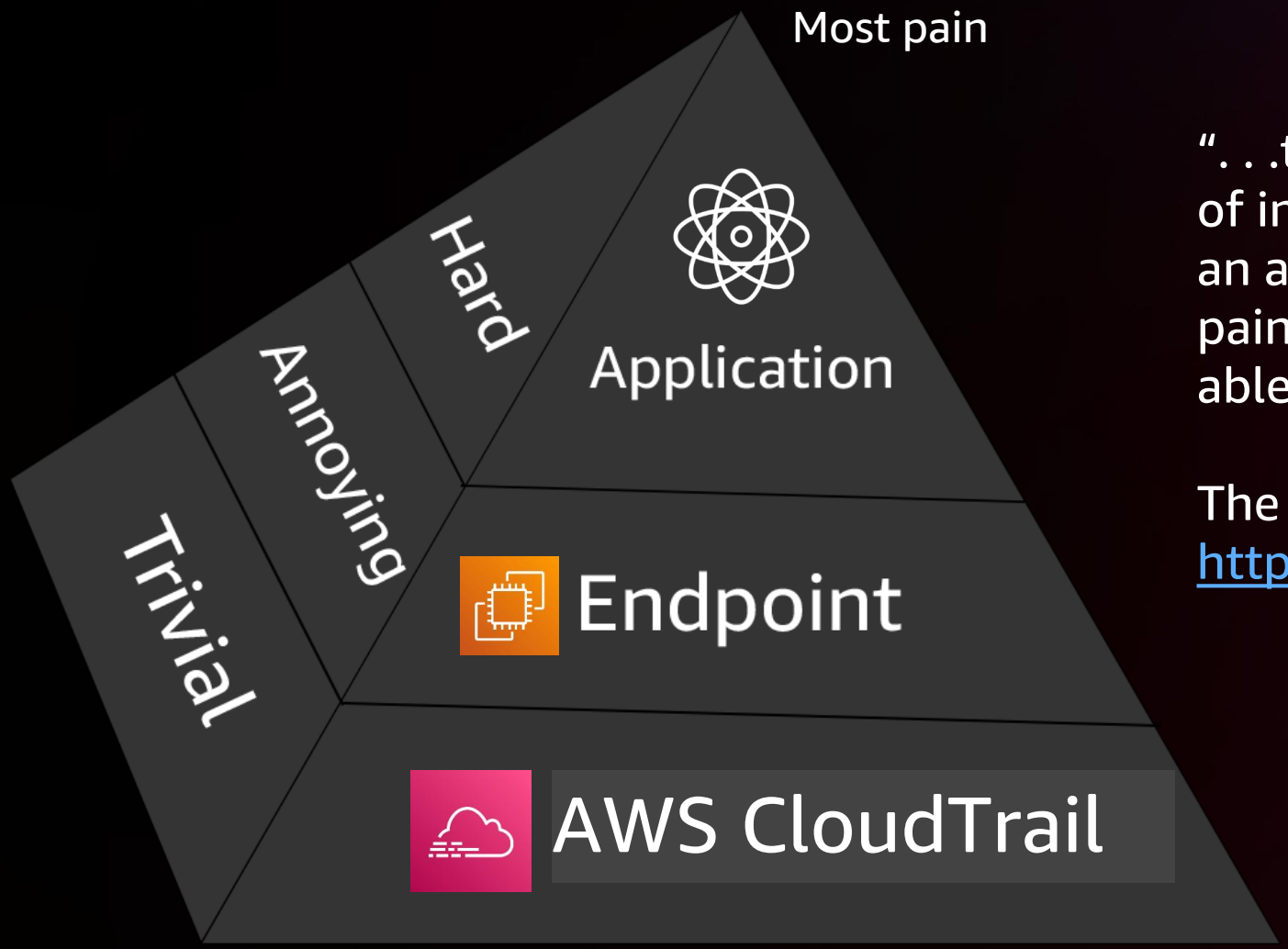
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pyramid of pain



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pyramid of pain: In the cloud

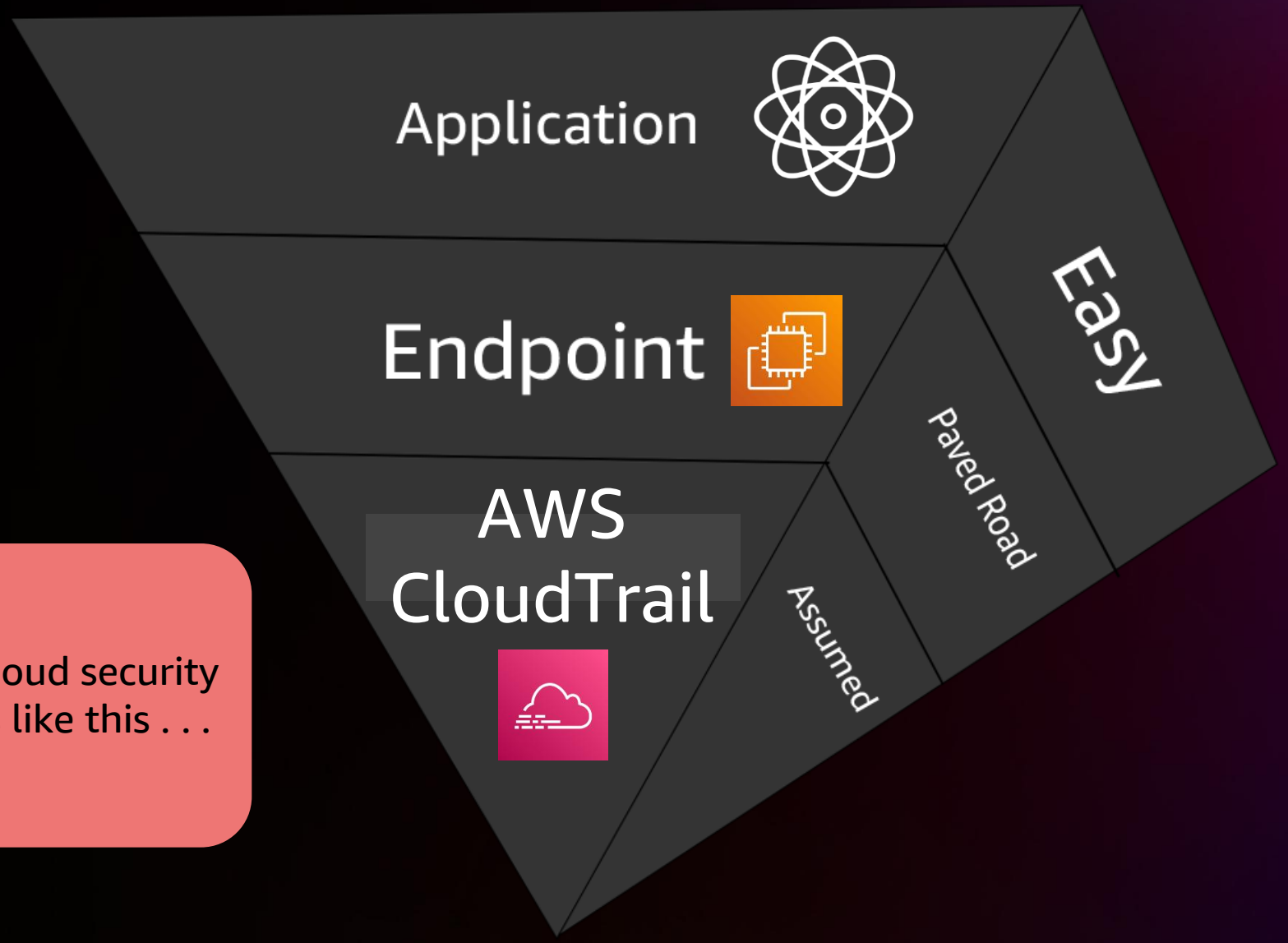


"...the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them."

The Pyramid of Pain, David J. Bianco, https://bit.ly/3tNHf79

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

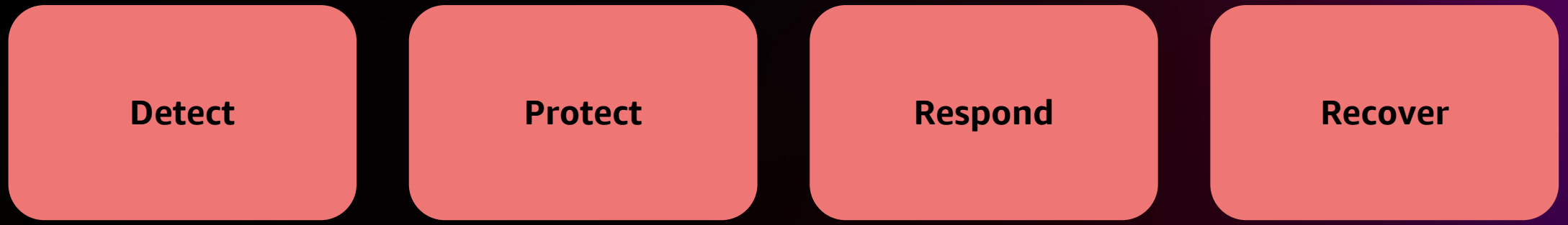
Build vs. buy



An excellent cloud security solution looks like this . . .

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mapping phases of incident response



- Application security
- Workload security
- Posture management
- SIEM

- Flag delivery
- Isolation

- Flag delivery
- Kill chain

- Patch
- Re-deploy

https://www.nist.gov/cyberframework/online-learning/five-functions

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case

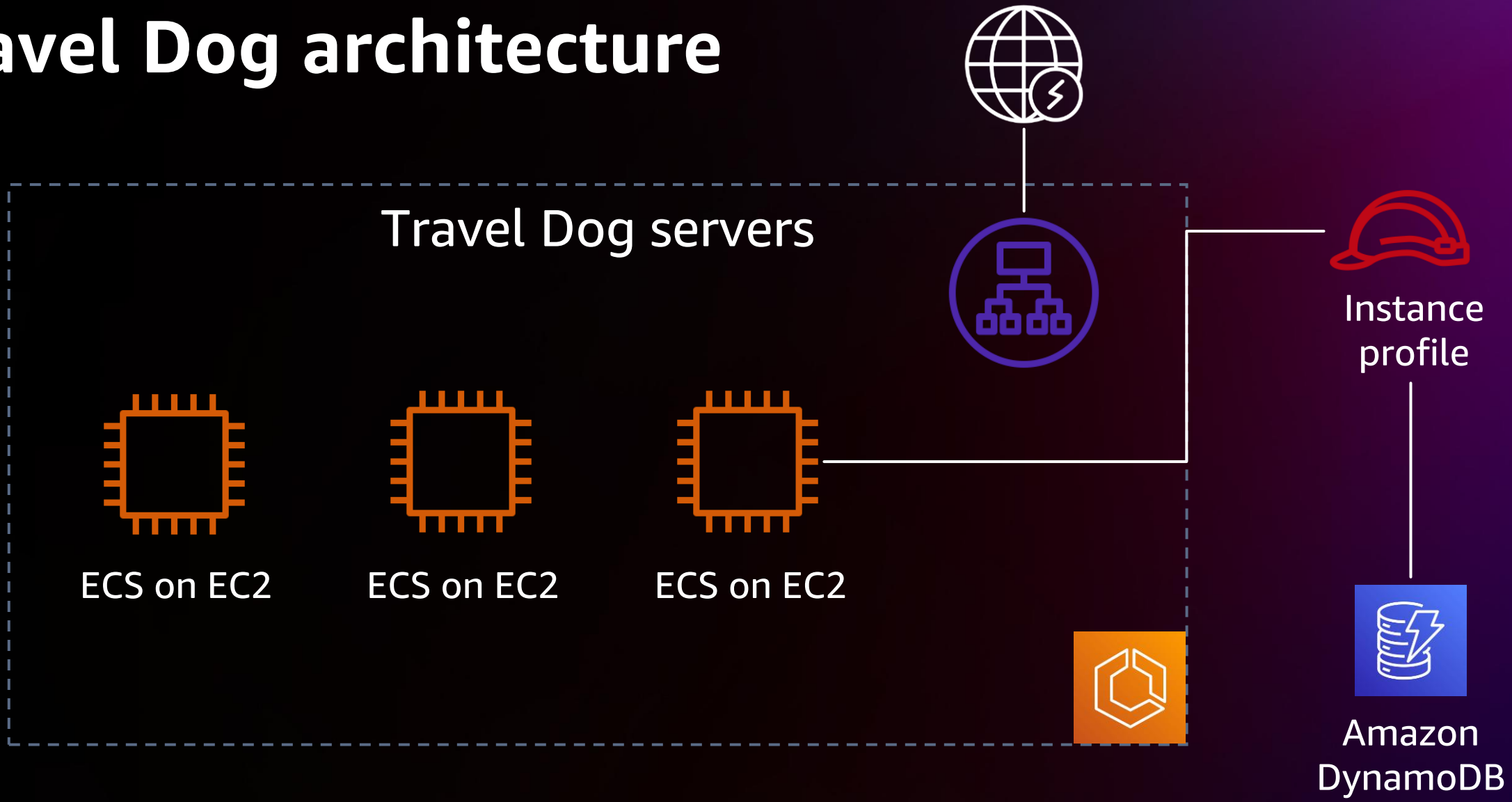


Travel Dog

(based on a true story)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Travel Dog architecture



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

User story

Goal: Allow dogs everywhere to share and showcase their favorite places to travel; be an index of the “dog friendliest” places on earth

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Business is going great . . . until



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

User story: Feature 1

As a user, I should be able to edit my profile to **update** my “favorite place” and star rating

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

User story: Feature 2

All users see the most recent 5 updated listings on the home page

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security user story: Feature 3

Security engineers and technicians run arbitrary commands without the use of SSH

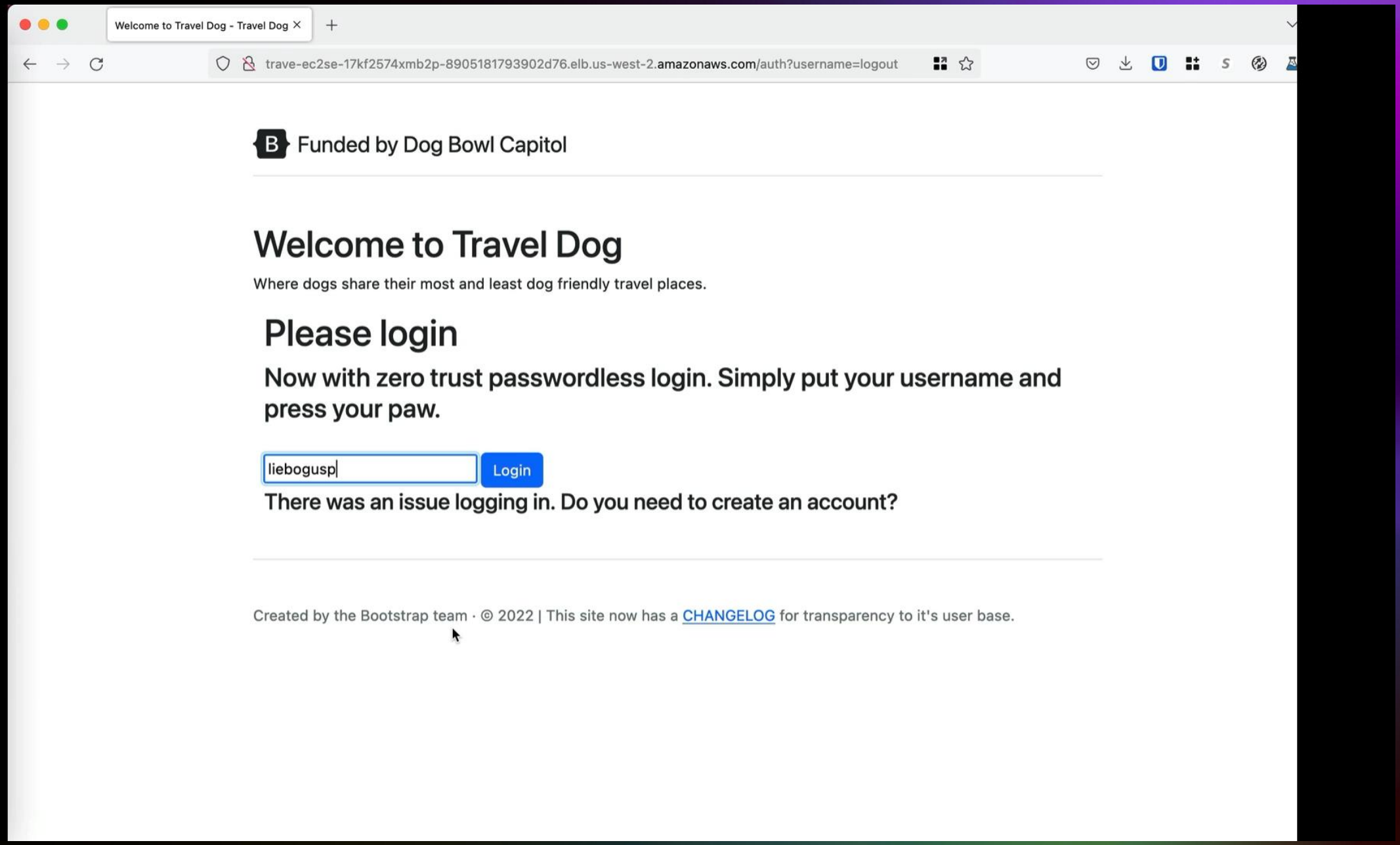
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What could go wrong?



Red alert

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

For transparency to the user community

Change log

- Adds/v1/users REST endpoint with full CRUD
- Adds image preview microservice for top “x” recent places
- Smart profile merging to support future updates
- Adds AWS Systems Manager to instance profile and instance for troubleshooting

Data classification:
PUBLIC

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Issues added

Issue	Impact (if exploited)
Adds profile exfiltration for all users via REST as an authenticated user	MEDIUM – Reputation
Adds an SSRF via the image preview service	HIGH → MAXIMUM depending on credentials
Adds AWS Systems Manager agent with overly permissive policy allowing instances to run commands on each other accidentally	MAXIMUM → Full root access

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Threat scenario #1

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A quick win









```python
@app.route("/v1/seed")
def seed():
    flag_value = ldclient.get().variation("seed-route", LD_USER, False)
    adversary_data = ldclient.get().variation("adversary-data", LD_USER, False)
    if flag_value == True:
        session = dynamo_helpers.get_session()
        table = dynamo_helpers.get_table(session)
        models.seed(table)
        data = table.scan(Limit=100, Select="ALL_ATTRIBUTES")
        if adversary_data == True:
            user_obj = models.User(table)
            user_obj.adversary = True
            data = dict(Count=100, Items=[])
            for x in range(0, 100):
                data["Items"].append(user_obj.fake)
        return jsonify(dict(data))
    else:
        return jsonify(status=500, message=not_enabled_message), 500
```

Seed route:

Creates fake users in your database

Then returns the first 100 users for debugging

Should ONLY be enabled in development locally

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

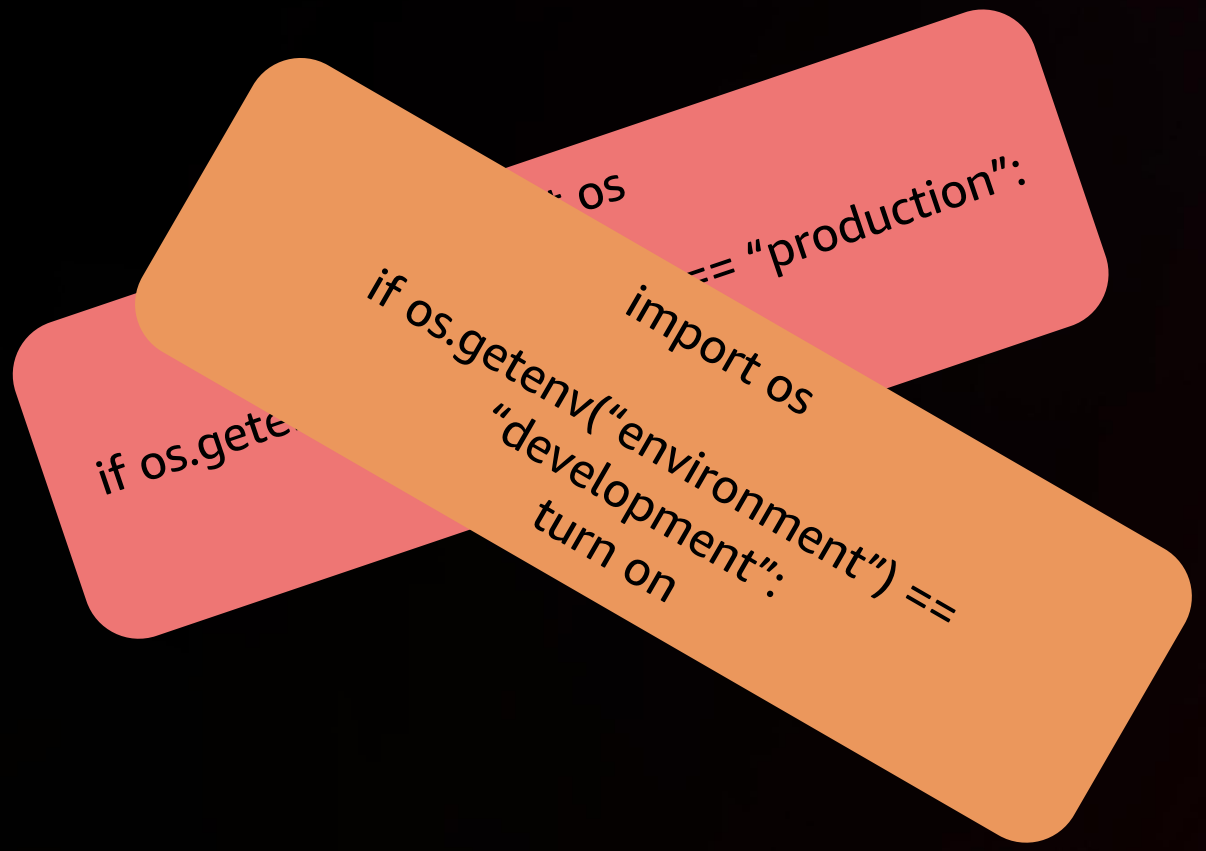
But . . . Configuration is challenging

```
import os

if os.getenv("environment") == "production":
    turn off
```

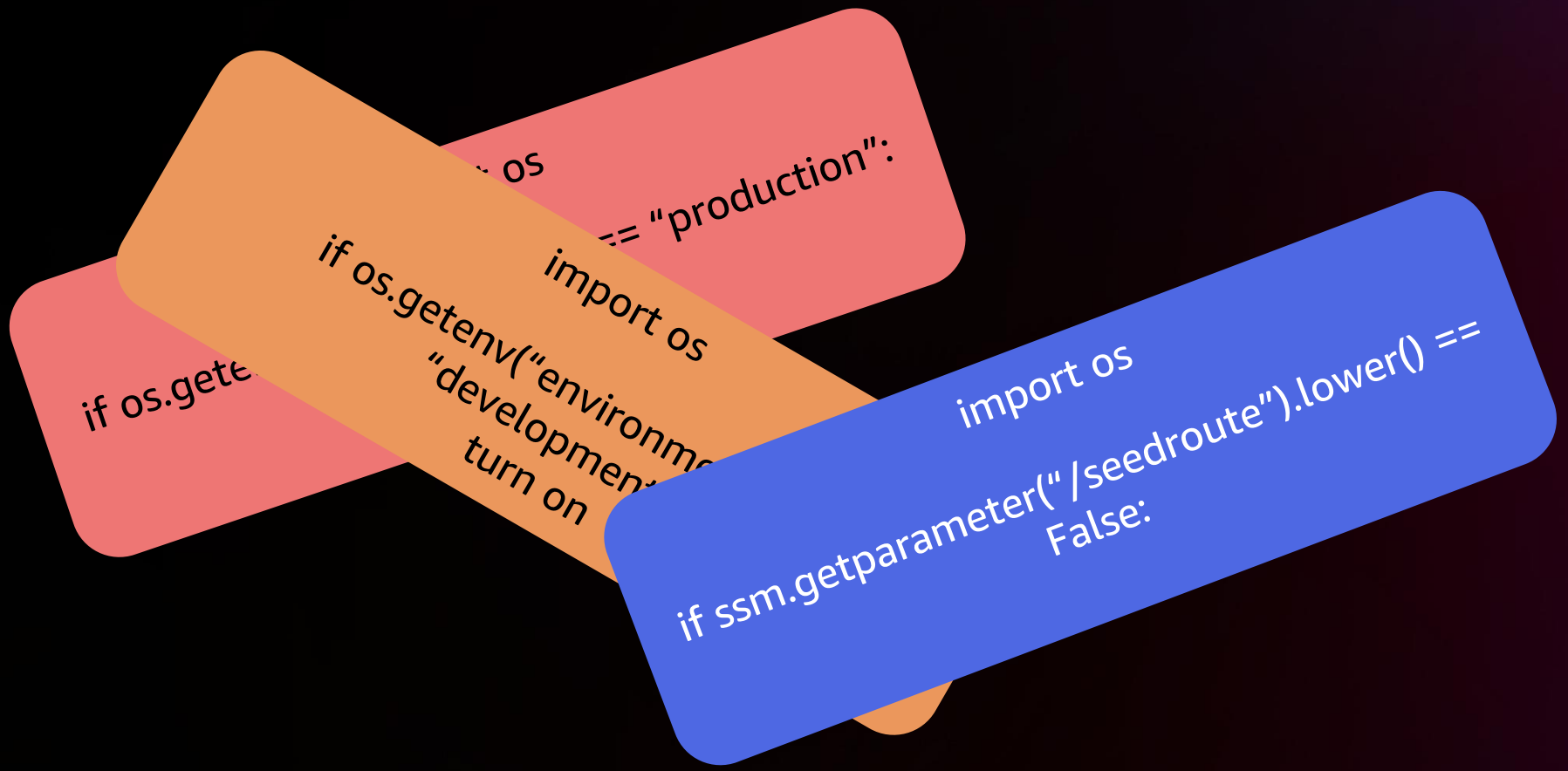
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

But . . . Configuration is challenging



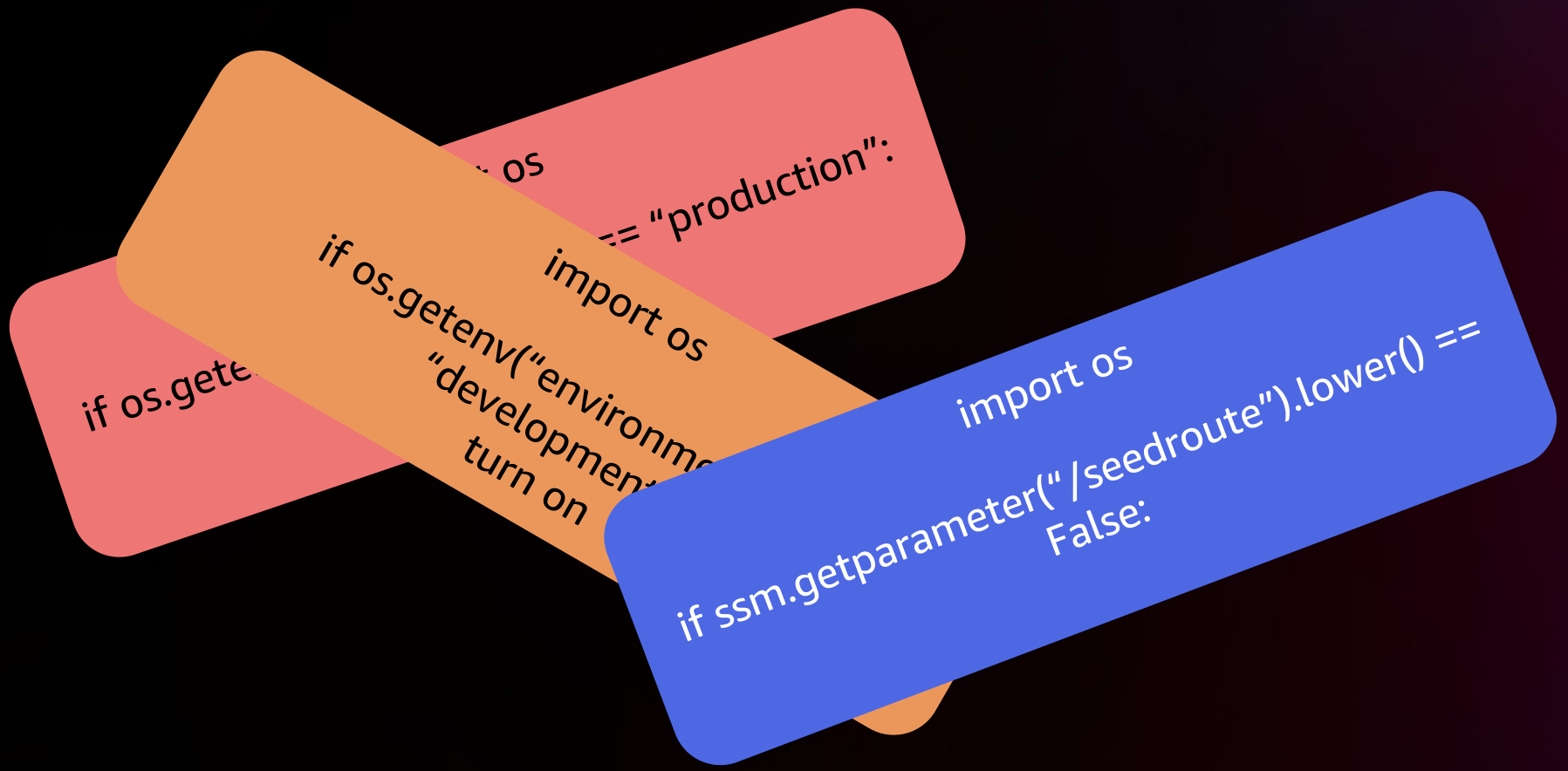
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

But . . . Configuration is challenging



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

But . . . Configuration is challenging



If

else

elif

else

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Eventually someone will err

Development becomes production!



Data leaks everywhere


```
  {
    "address": "31742 Olson Spurs Suite 916\nWest Kimberlyfort, VT 91486",
    "age": "25",
    "favorite_location_img": "bulksplash-aarya_3624-QhzF0a0JjgI.jpg",
    "favorite_location_url": "https://www.google.com",
    "given_name": "Christopher",
    "id": "581d70234f6643b59c20610bbea04663",
    "location": "Lake Rachael",
    "surname": "Johnson",
    "username": "sara25"
  },
  {
    "address": "67525 Patricia Spurs Apt. 250\nDrakeberg, MO 39359",
    "age": "51",
    "favorite_location_img": "bulksplash-adventure_yuki-afxb59kLAQU.jpg",
    "favorite_location_url": "https://www.google.com",
    "given_name": "Marc",
    "id": "581d70234f6643b59c20610bbea04663",
    "location": "Port Patricia",
    "surname": "Jensen",
    "username": "serranojoseph"
  }
],
"ResponseMetadata": {
  "HTTPHeaders": {
    "connection": "keep-alive",
    "content-length": "29276",
    "content-type": "application/x-amz-json-1.0"
```


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Answer: Lightweight Threat Modeling

Impact

- Feature is accidentally on in production
- Data leakage
- Reputation damage
- Fines

Likelihood

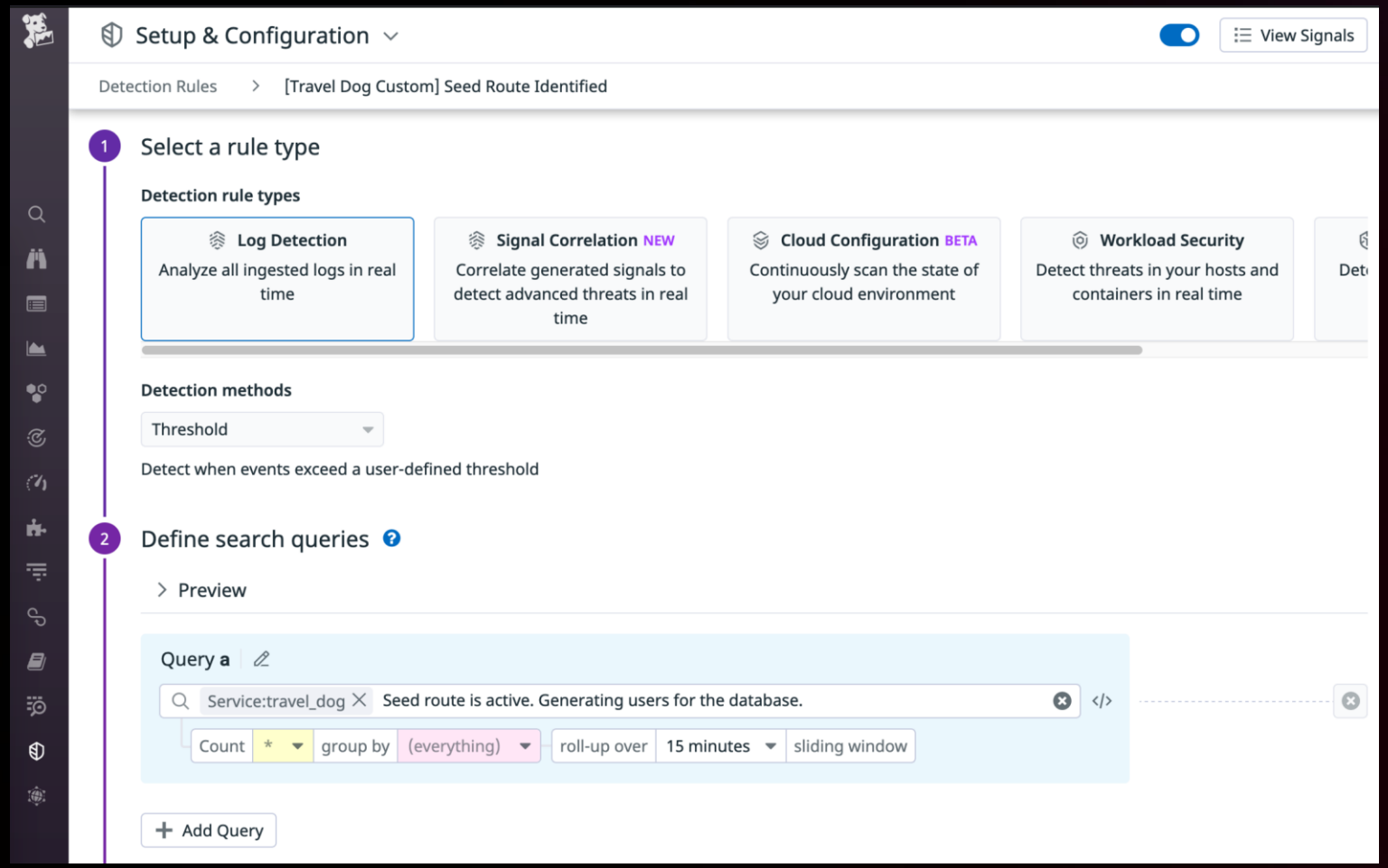
- HIGH (given code complexity)



https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detection rule for > high risk



Using the Datadog Cloud SIEM

RRA caught the risk

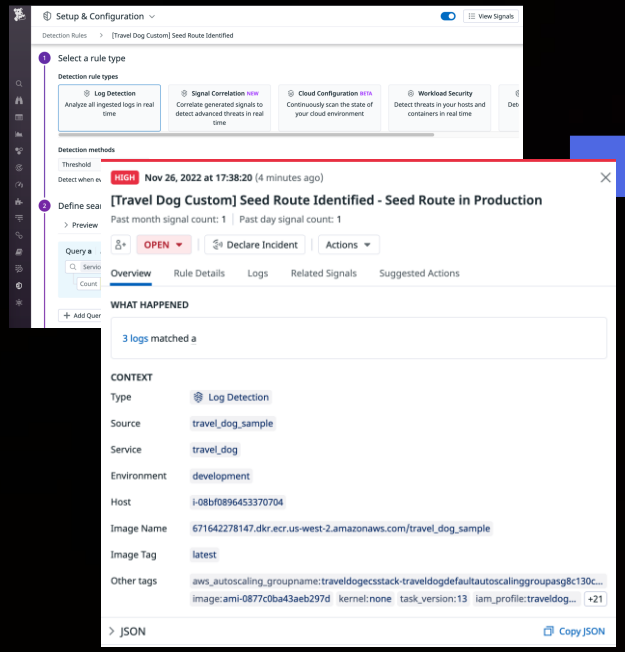
Business wanted to keep the feature

DevSecOps writes the detection rule

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

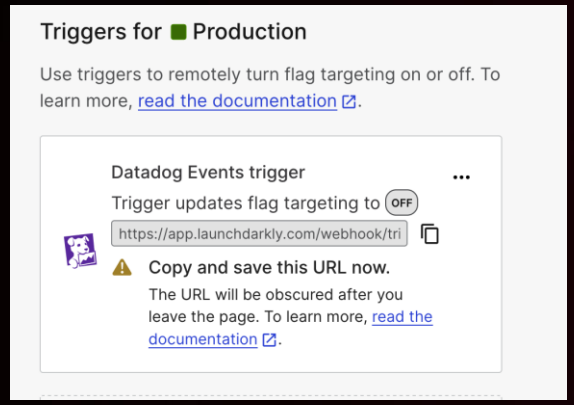
Detection rule for > high risk

Detect
using Cloud SIEM



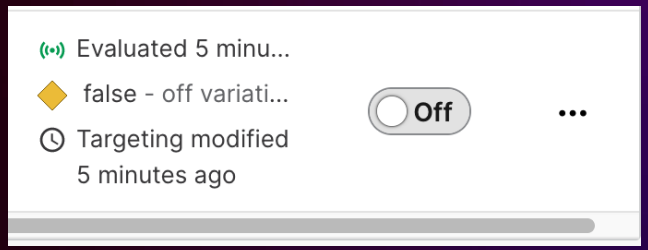
Notify!

Protect
LaunchDarkly
flag trigger



Respond!

Respond
act on the flag
by disabling



https://docs.launchdarkly.com/integrations/datadog/triggers

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detection rule for > high risk

```
{
  "message": "Sorry that feature is not currently available.",
  "status": 500
}
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Success metrics

What are we measuring?	How are we measuring it?
Are feature flags adopted by engineers?	Number of flags and flag evaluations
Are technical designs sufficiently threat modeled?	Number of risk/threat models performed; Detections contributed

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Threat scenario #2

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remember: Resilience?

A system that is flexible, adaptable, and transformable

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

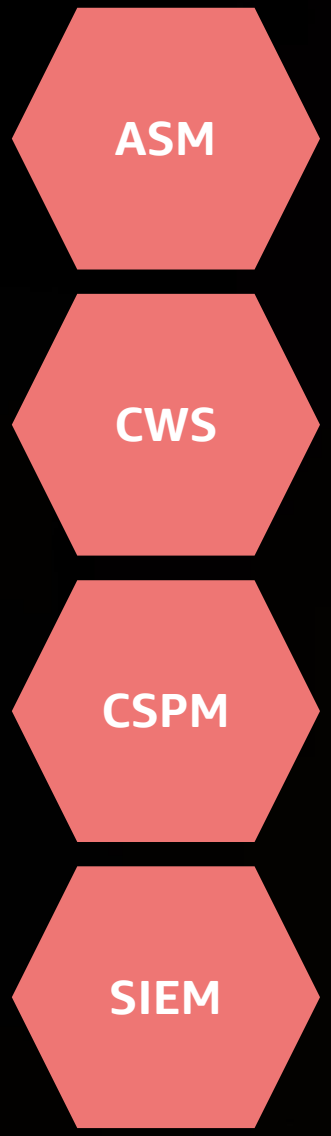
Remember: Resilience?

A system that is flexible, adaptable, and transformable

The ability to organize around a threat

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do we do that?



Application Security

End-to-end application security monitoring and exploit prevention

Cloud Workload Security

Real-time eBPF-powered threat detection across your hosts and containers

Cloud Security Posture Management

Continuous configuration audits across cloud accounts, hosts, and containers

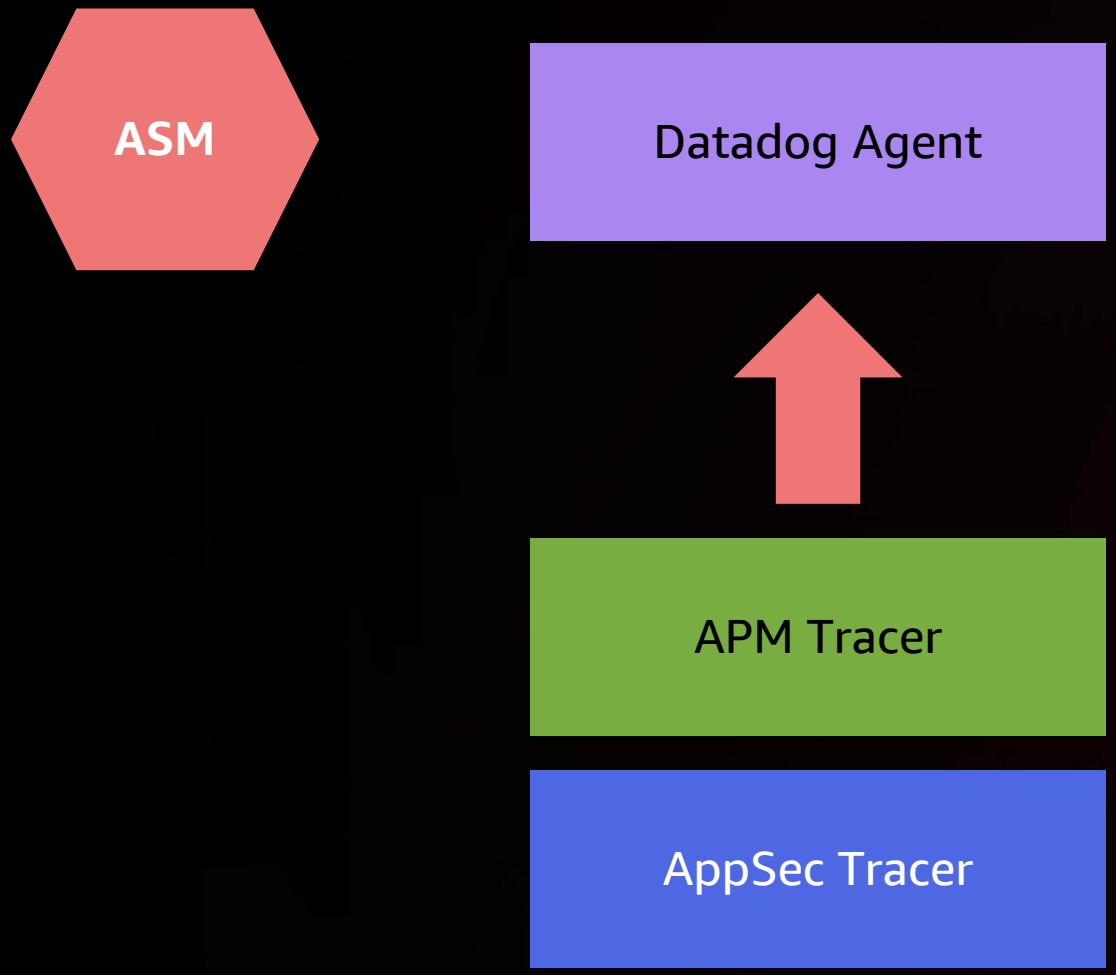
Security Monitoring

Real-time threat detection across operational and security logs

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Today’s focus

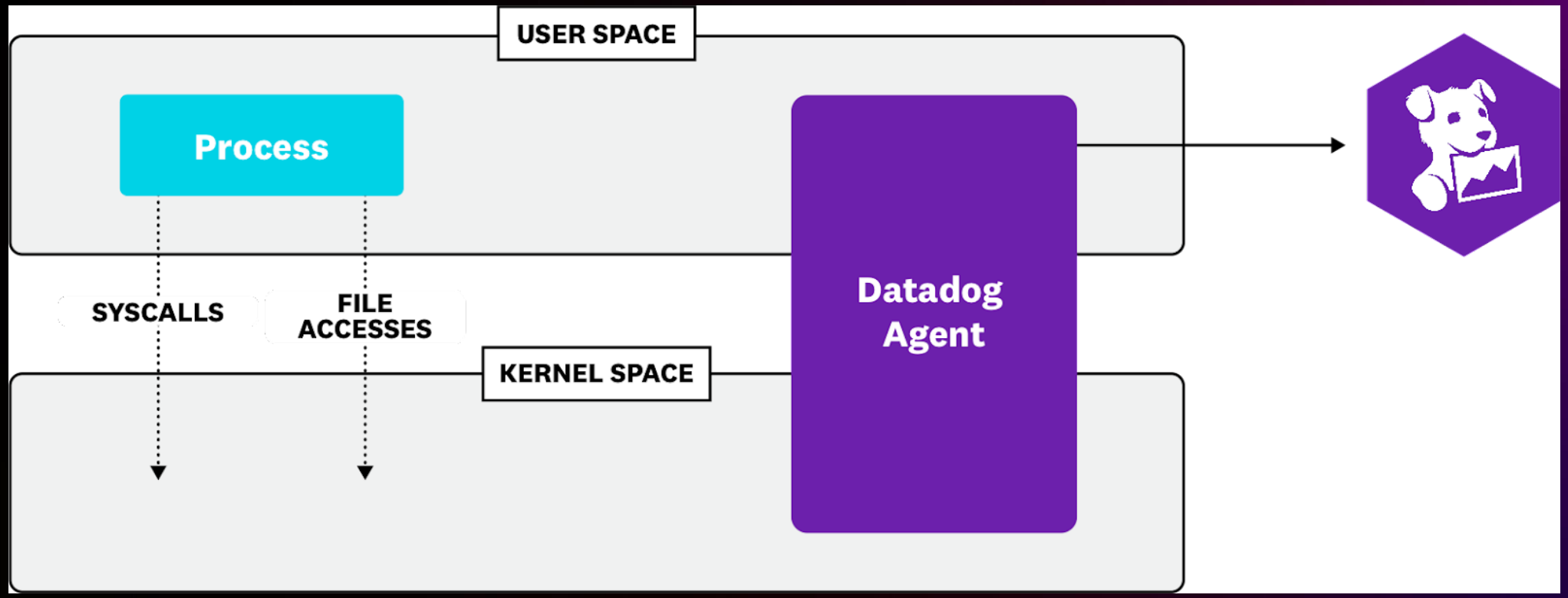


Datadog ASM can detect attacks as they pass through the application stack by building on top of Datadog APM

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Today's focus

CWS

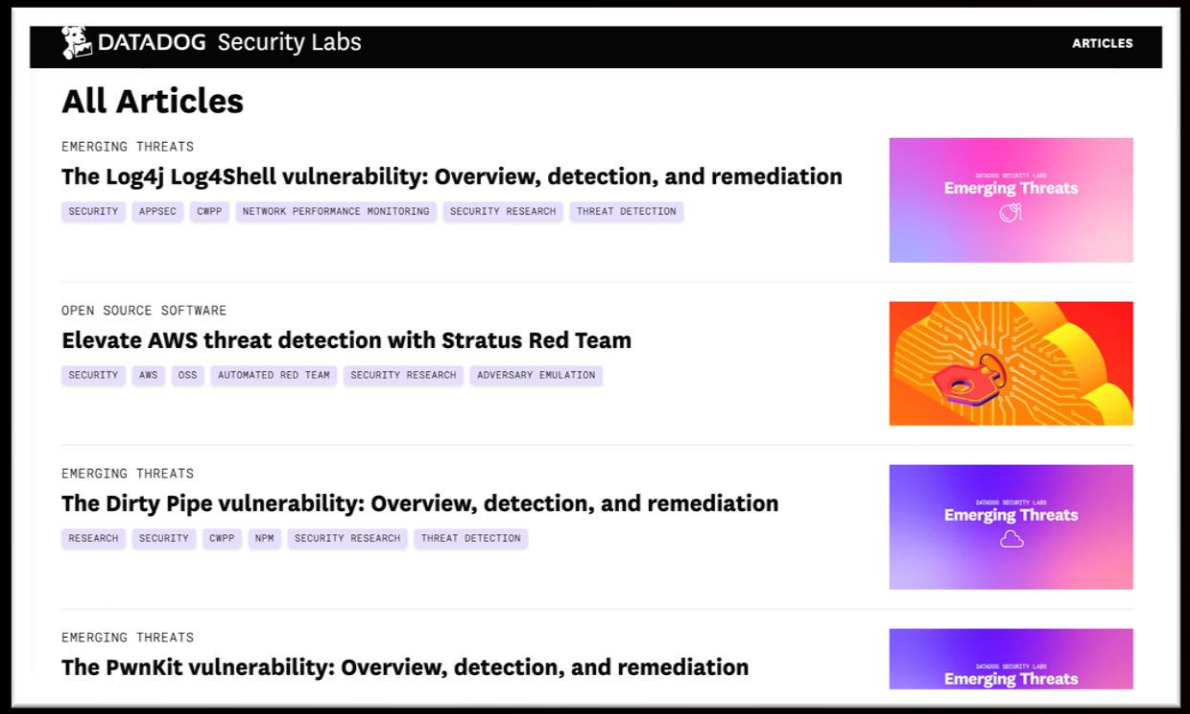


CWS is effective at detecting deep escalation at the process, network, and memory levels

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Endpoint detections for zero days

EXAMPLES OF EMERGING SECURITY ISSUES ON DATADOG SECURITY LABS



- New security issues pop up almost monthly right now
- Many of them give an attacker access to your systems (even when you don't make a mistake)

https://securitylabs.datadoghq.com

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Assertion: Your application is like a piece of chocolate

- Hard on the outside soft on the inside
- Most of the attack surface is behind authenticated endpoints
- Authentication gives us a session to use in order to correlate activity

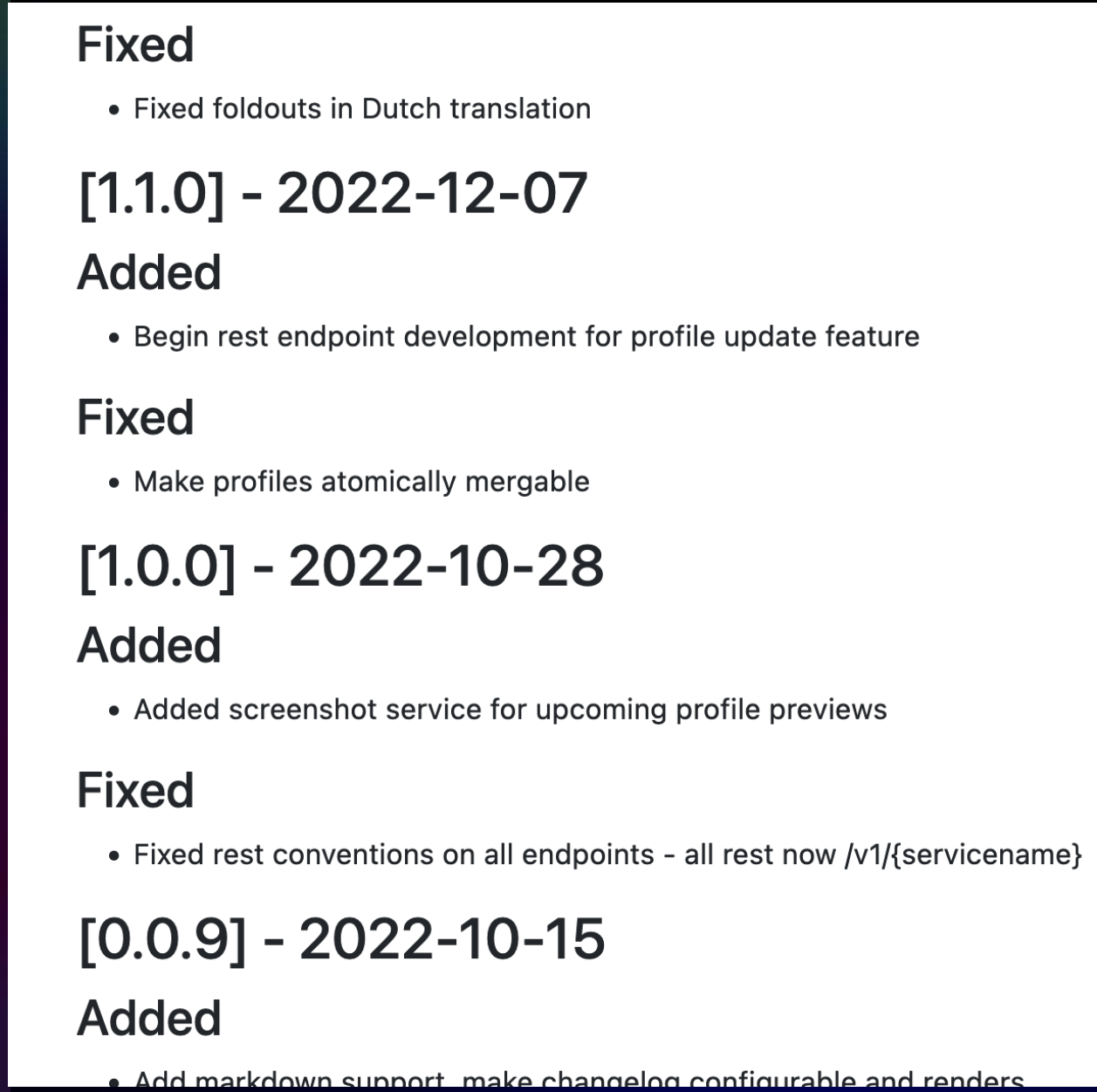


aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In our demo app

- Leaked some information about the application
- Our adversary discovered three security issues:
  - Data leak
  - SSRF
  - Command injection



Fixed

- Fixed foldouts in Dutch translation

[1.1.0] - 2022-12-07

Added

- Begin rest endpoint development for profile update feature

Fixed

- Make profiles atomically mergable

[1.0.0] - 2022-10-28

Added

- Added screenshot service for upcoming profile previews

Fixed

- Fixed rest conventions on all endpoints - all rest now /v1/{servicename}

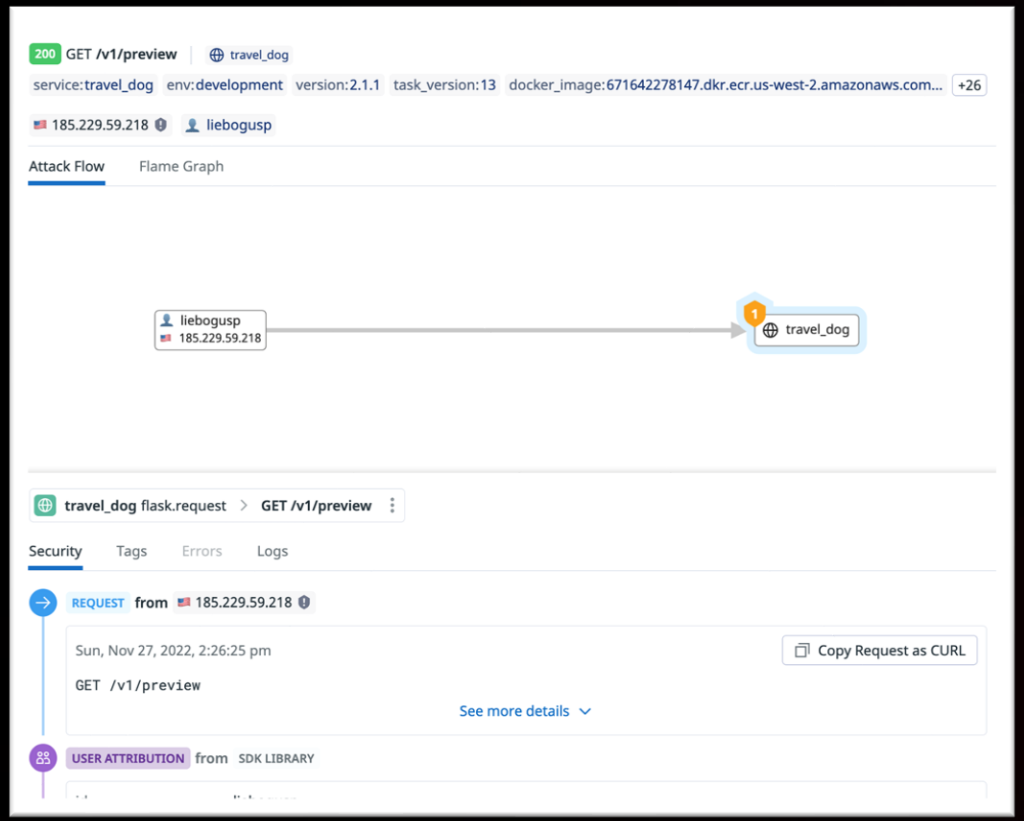
[0.0.9] - 2022-10-15

Added

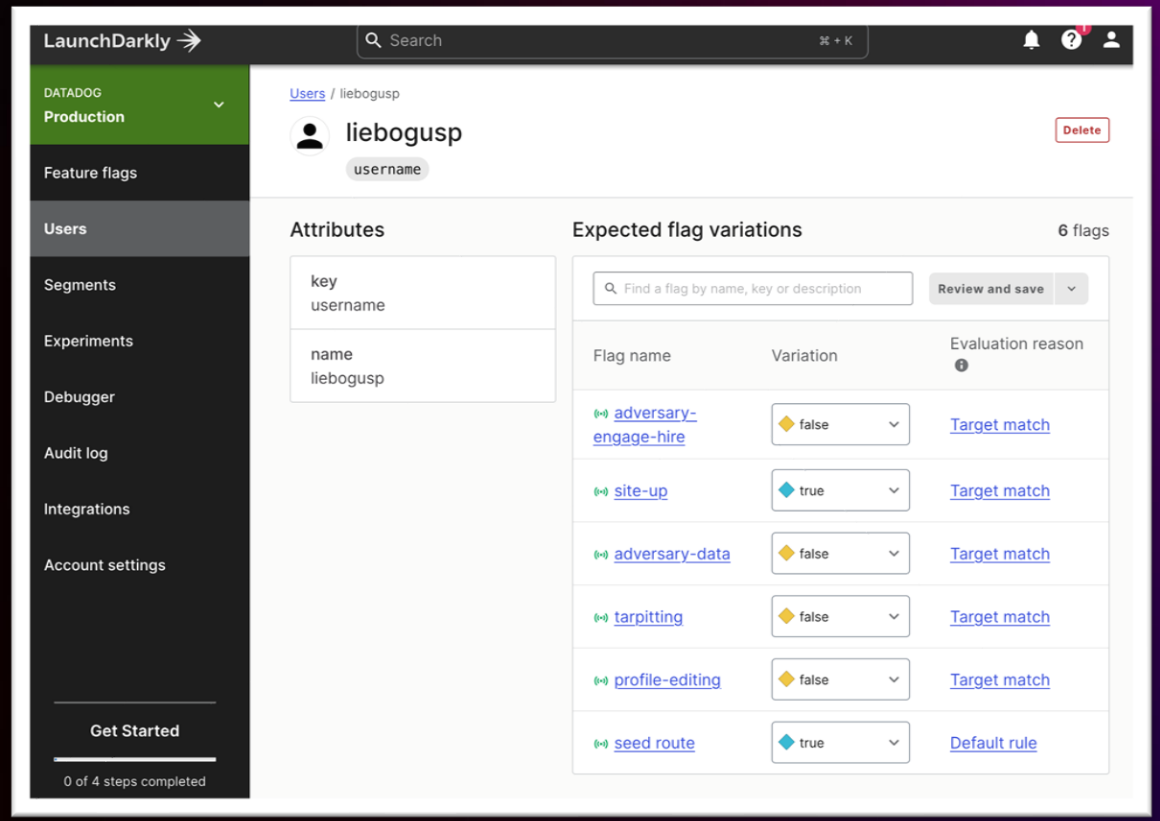
- Add markdown support, make changelog configurable and renders

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What we have



ASM can alert on authenticated user behavior



LaunchDarkly can flag on and off user behaviors

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does it work?

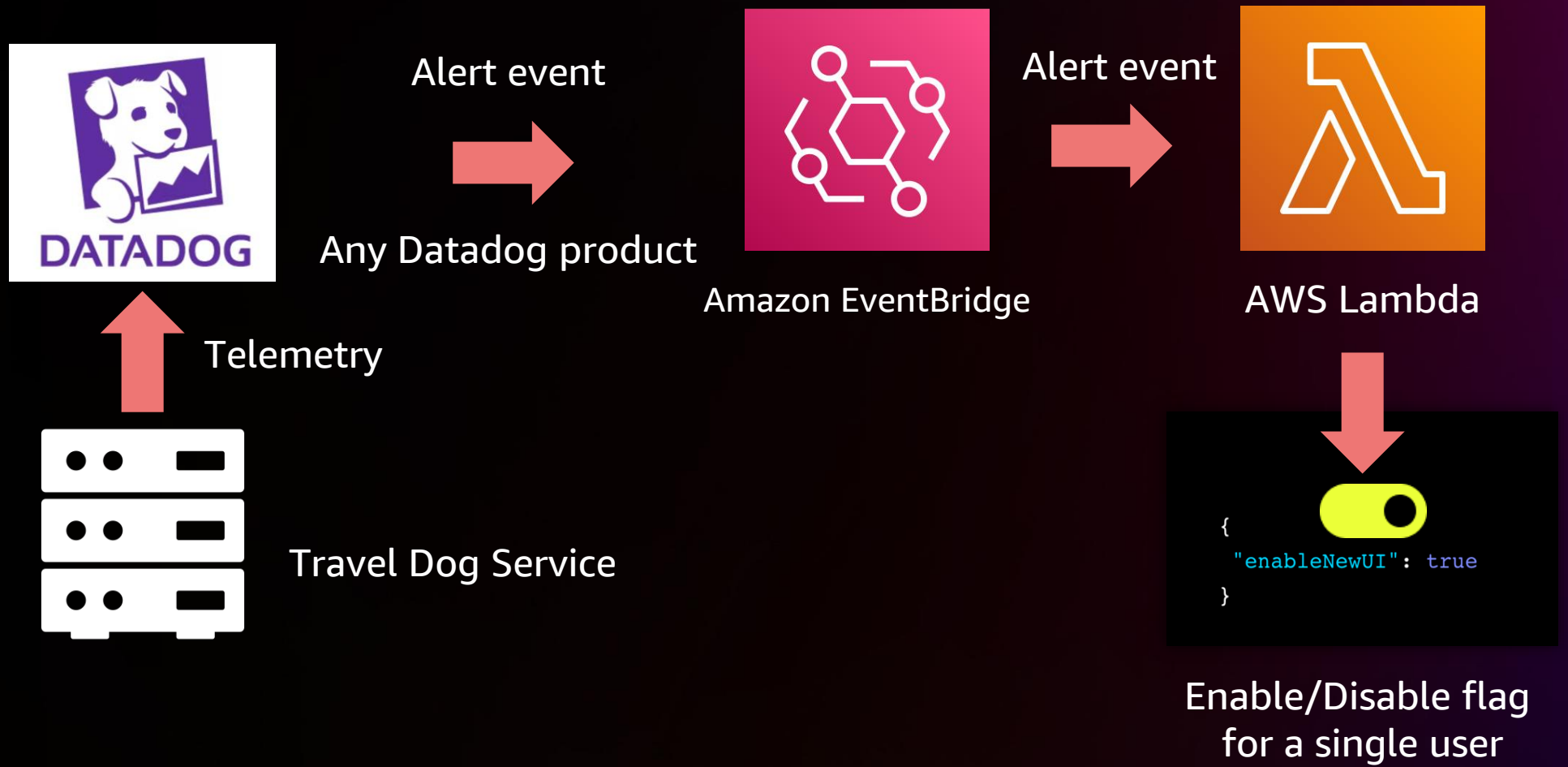
```python
@app.route("/v1/up")
@login_required
def ping():
    set_user(tracer, user_id=LD_USER["name"])
    flag_value = ldclient.get().variation("site-up", LD_USER, False)
```

Correlate the authenticated session username with the LaunchDarkly user

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

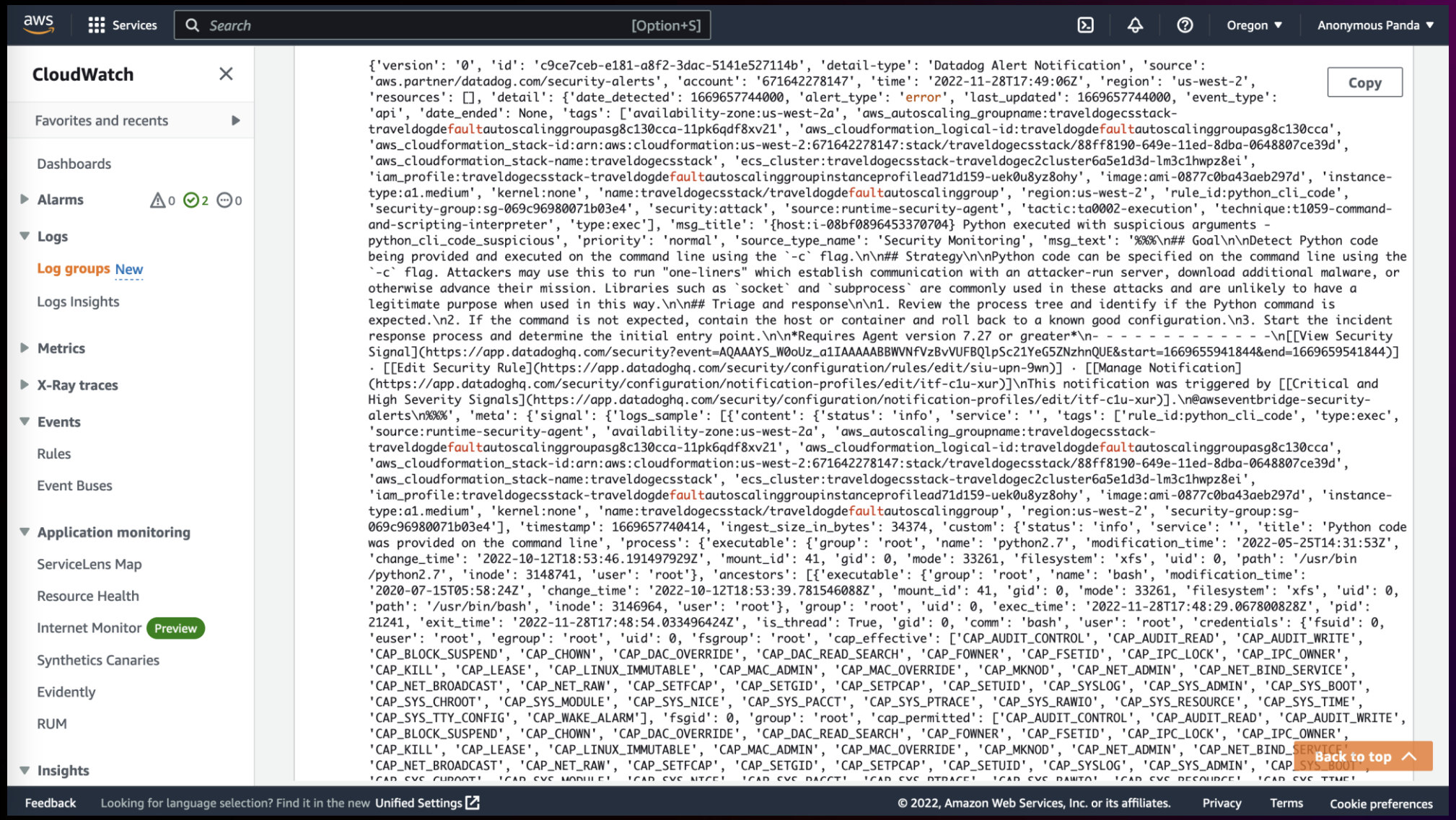
Workflow

Datadog supports integrating with EventBridge



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EventBridge events are rich!



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EventBridge events are rich!

'tags': {'category': 'attack_attempt', 'type': 'ssrf'}}}], 'rule_id': ['sqr-000-001'], 'type': ['ssrf'], 'event': 'true', 'blocked': 'false'}, 'version': '2.1.1', 'usr': {'id': 'liebogusp'},

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

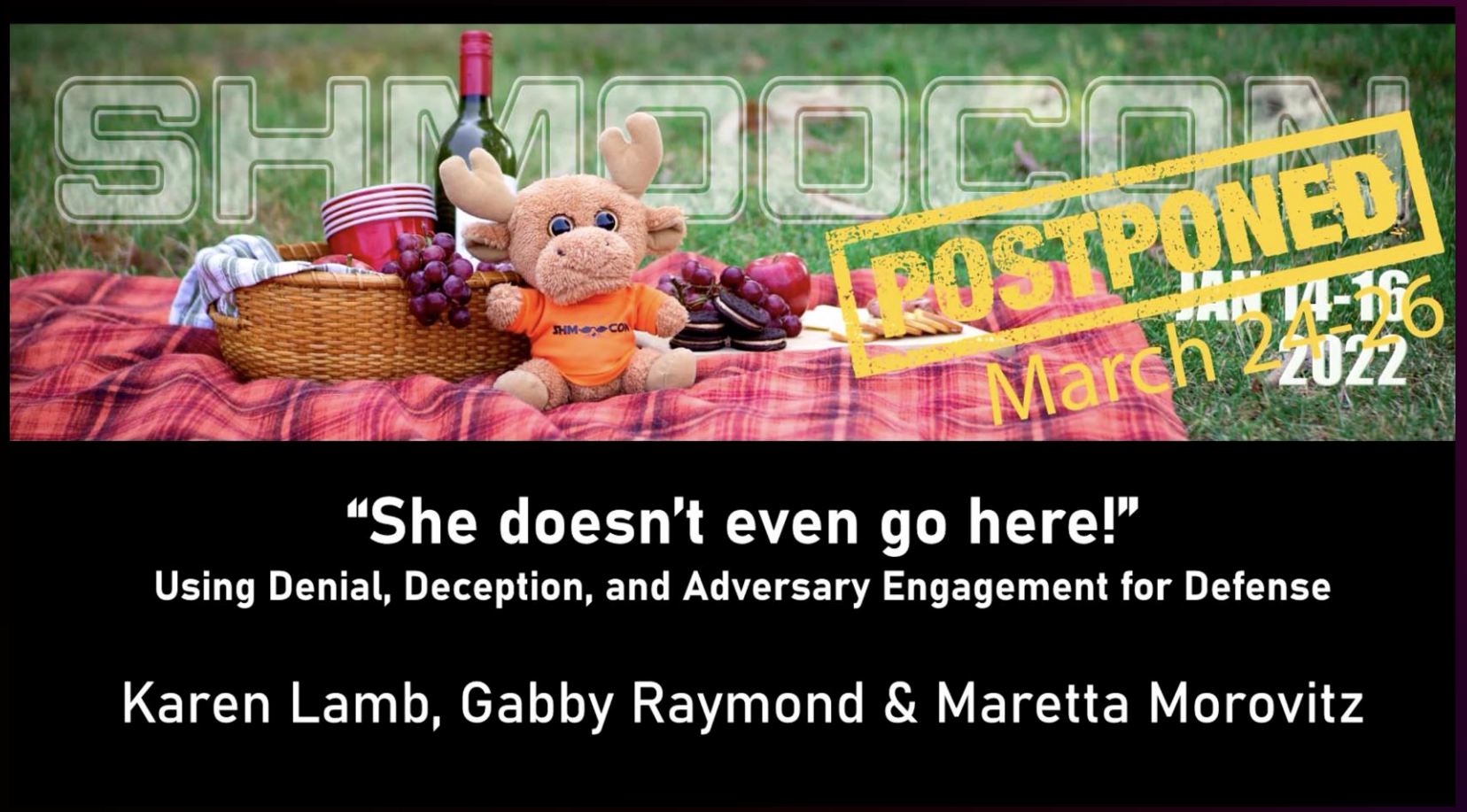
What is adversary engagement?



Proactively interact with cyber adversaries to achieve the defender’s strategic goals. - MITRE

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

For a great talk on engagement



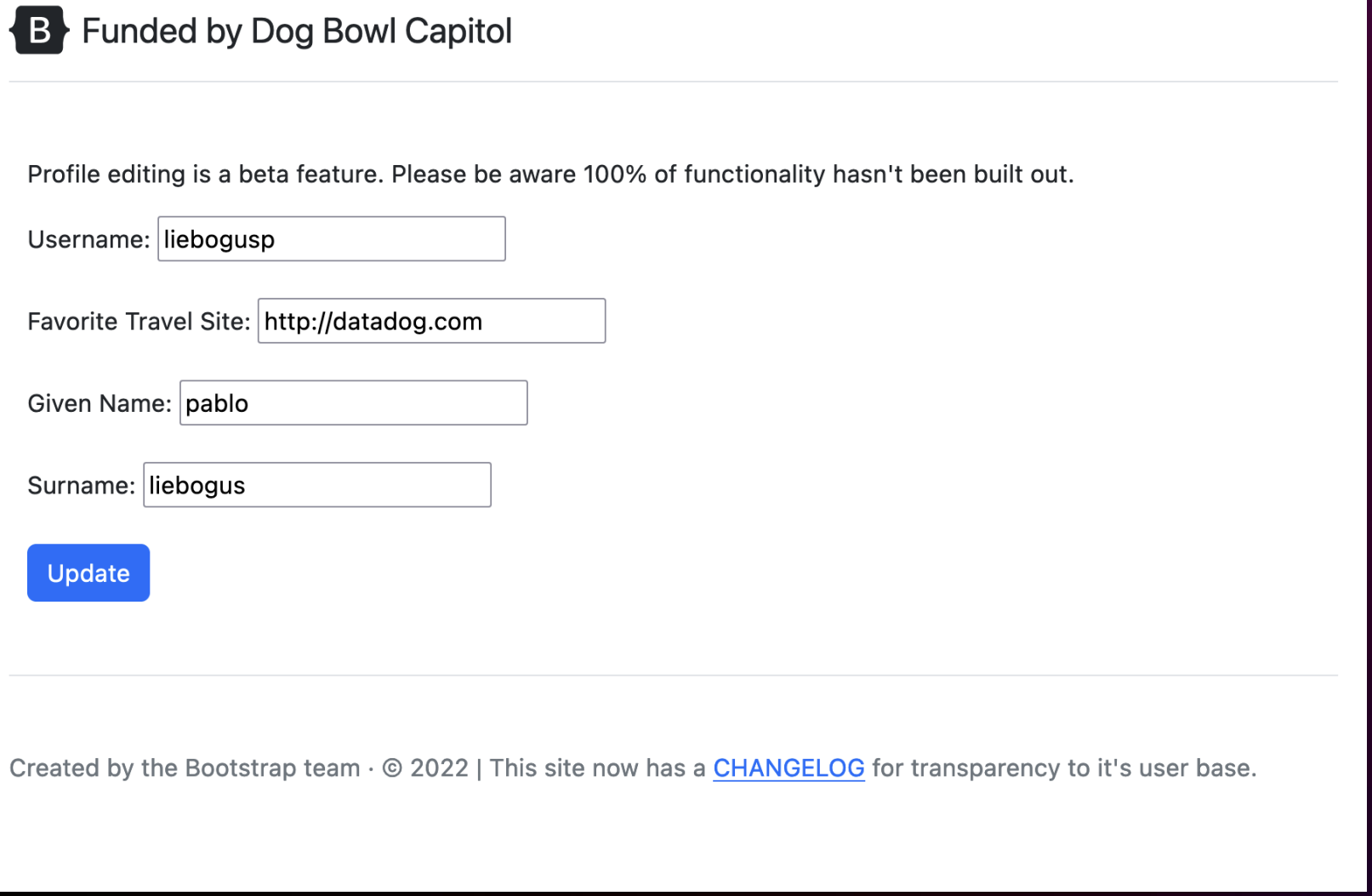
bit.ly/3u6gds5

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

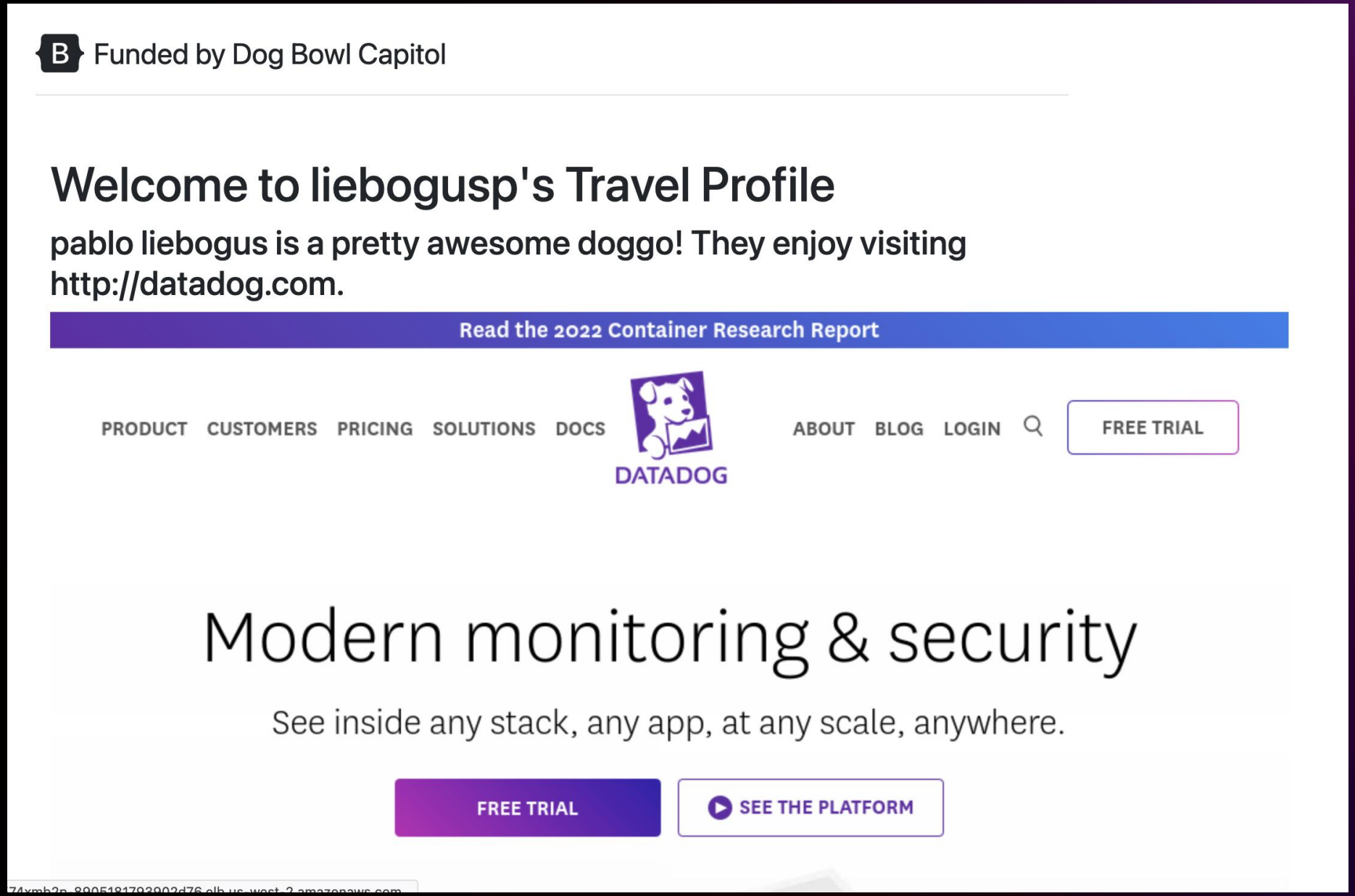
Map Rule_ID => Risk => Action

Rule ID	Risk	Action
seed_route	HIGH	Disable the route OR engage the adversary by serving fake data
SSRF	MEDIUM	Disable the feature and engage the adversary
Command Injection	MAXIMUM	Traditional incident handling

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Funded by Dog Bowl Capitol

Profile editing is a beta feature. Please be aware 100% of functionality hasn't been built out.

Username: liebogusp

Favorite Travel Site: http://169.254.169.254/latest/

Given Name: pablo

Surname: liebogus

Update

Created by the Bootstrap team · © 2022 | This site now has a CHANGELOG for transparency to it's user base.

aws

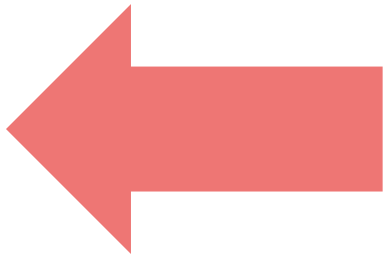
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Funded by Dog Bowl Capitol

Profile editing is a beta feature. Please be aware 100% of functionality hasn't been built out.

Username: liebogusp

Favorite Travel Site: http://169.254.169.254/latest/



Given Name: pablo

Surname: liebogus

Update

Created by the Bootstrap team · © 2022 | This site now has a CHANGELOG for transparency to it's user base.

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Funded by Dog Bowl Capitol

Welcome to liebogusp's Travel Profile

pablo liebogus is a pretty awesome doggo! They enjoy visiting http://datadog.com.




```
{
        "action": "terminate",
        "time": "2022-11-05T15:07:10Z"
}
```


aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Assertion: One of the greatest advantages an attacker has is time

Time to study your app
Time to craft attacks

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



If time is an advantage,
let’s waste some of the adversary’s time

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

```python
@app.before_request
def before_request():
    username = request.cookies.get("username")
    if username != None:
        LD_USER["name"] = username
    else:
        LD_USER["name"] = None

    flag_value = ldclient.get().variation("tarpitting", LD_USER, False)

    if flag_value == True:
        app.logger.info(f"Tarpitting activated for user={username}")
        sleep_value = random.randint(5, 10)
        time.sleep(sleep_value)
```

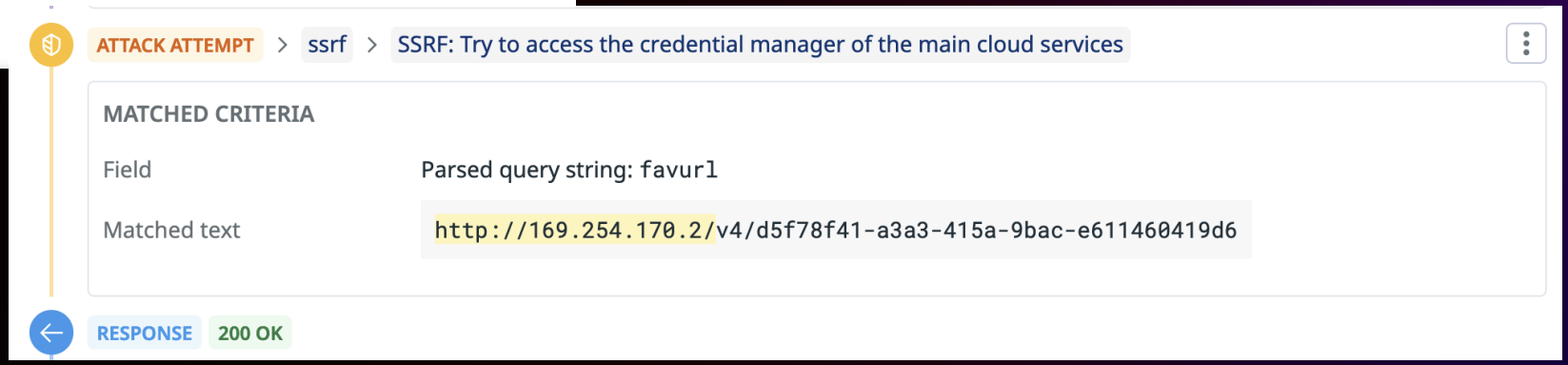
Randomly increase response time for only the adversary

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Only possible because we can correlate user sessions





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We can also inject fake data or canary data


```
Count:                  100
Items:
  0:
    address:            "9695 Brown Brooks Suite 363\nVegabury, AZ 74511"
    age:                38
    credit_card:        "JCB 16 digit\nPatrick Strickland\n3577689219400568 05/27\nCVC: 873\n"
    favorite_location_img: "http://placekitten.com/g/200/300"
    favorite_location_url: "https://www.google.com"
    given_name:         "Hailey"
    id:                 "aa172b1a53204e5298e69a591fc02c6d"
    location:           "New Andrew"
    ssn:                "390-36-8145"
    surname:            "Rose"
    username:           "james12"
```




Add fake SSNs
Add fake credit card numbers
Misdirect the attacker to waste time scraping

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Try to turn the attacker to your cause

Funded by Dog Bowl Capitol

Welcome to Travel Dog

Do you like breaking things for a living? Maybe consider checking out our careers page!

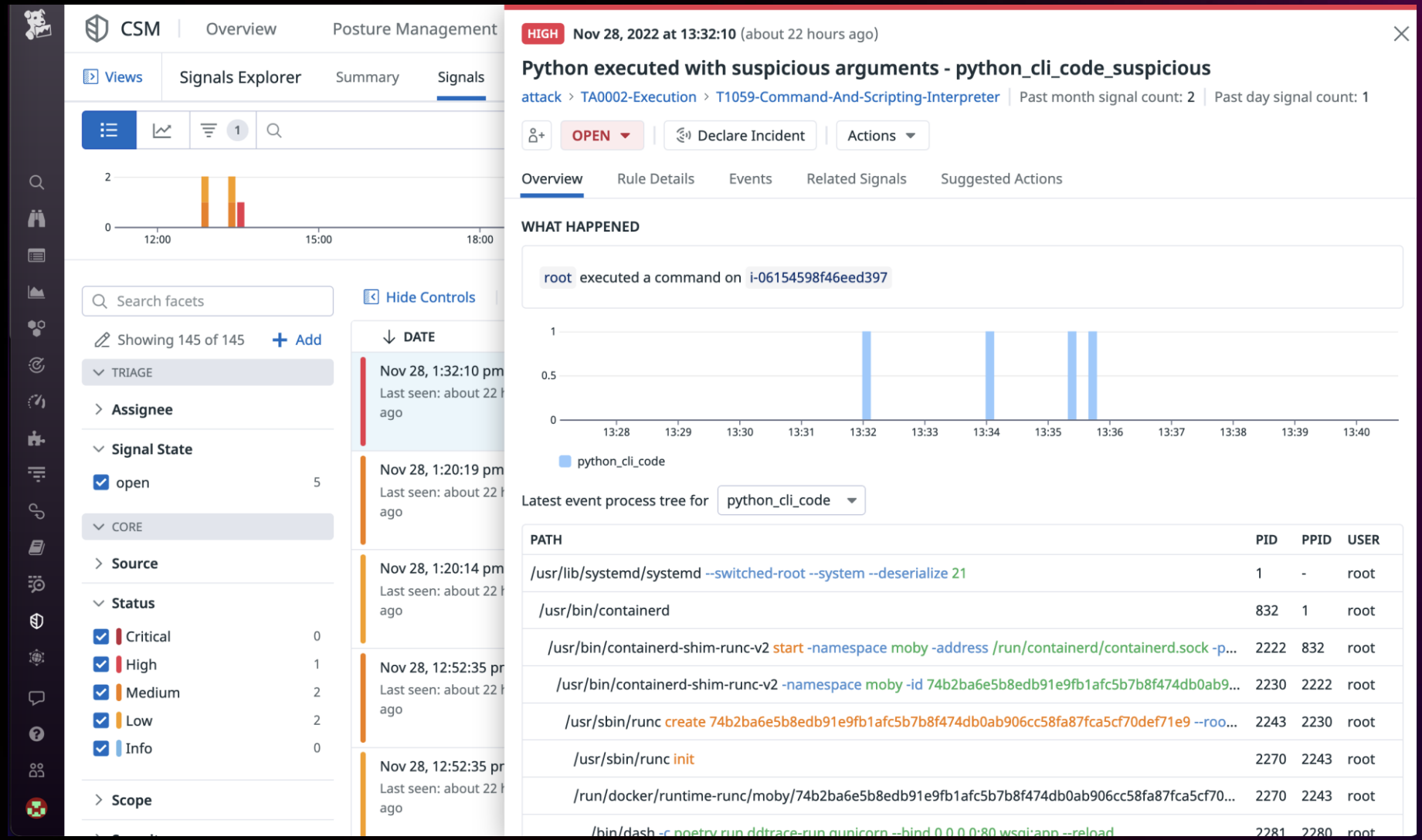


scottjillian

aws

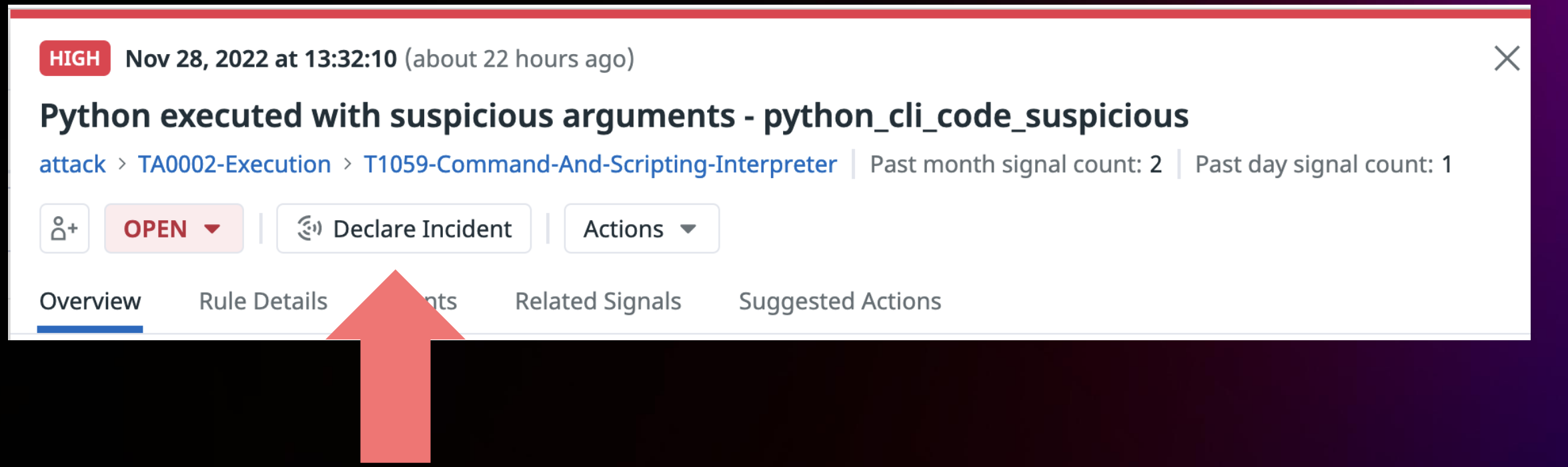
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

When things escalate



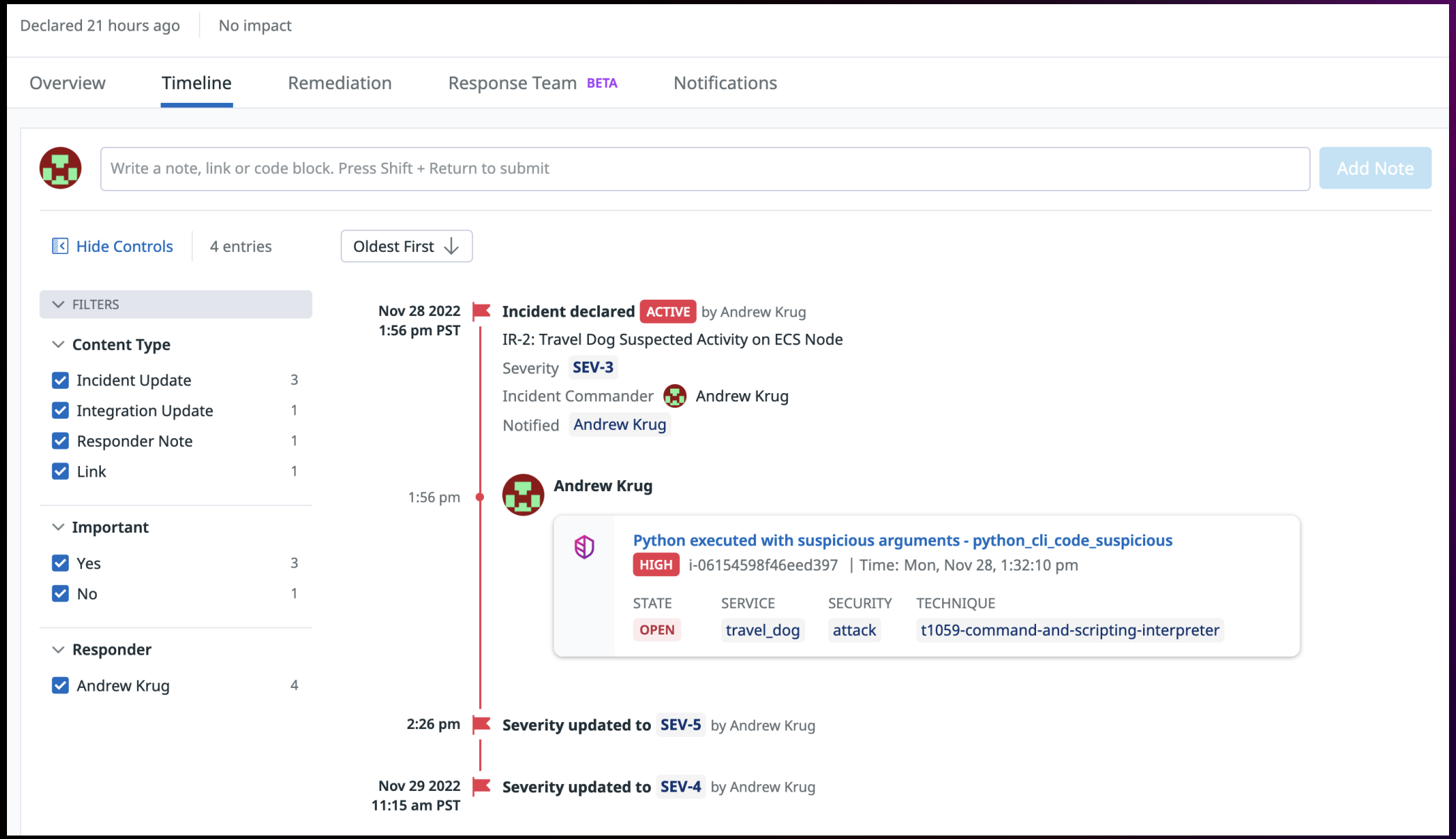
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

When things escalate



Declare Incident and follow a traditional flow

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

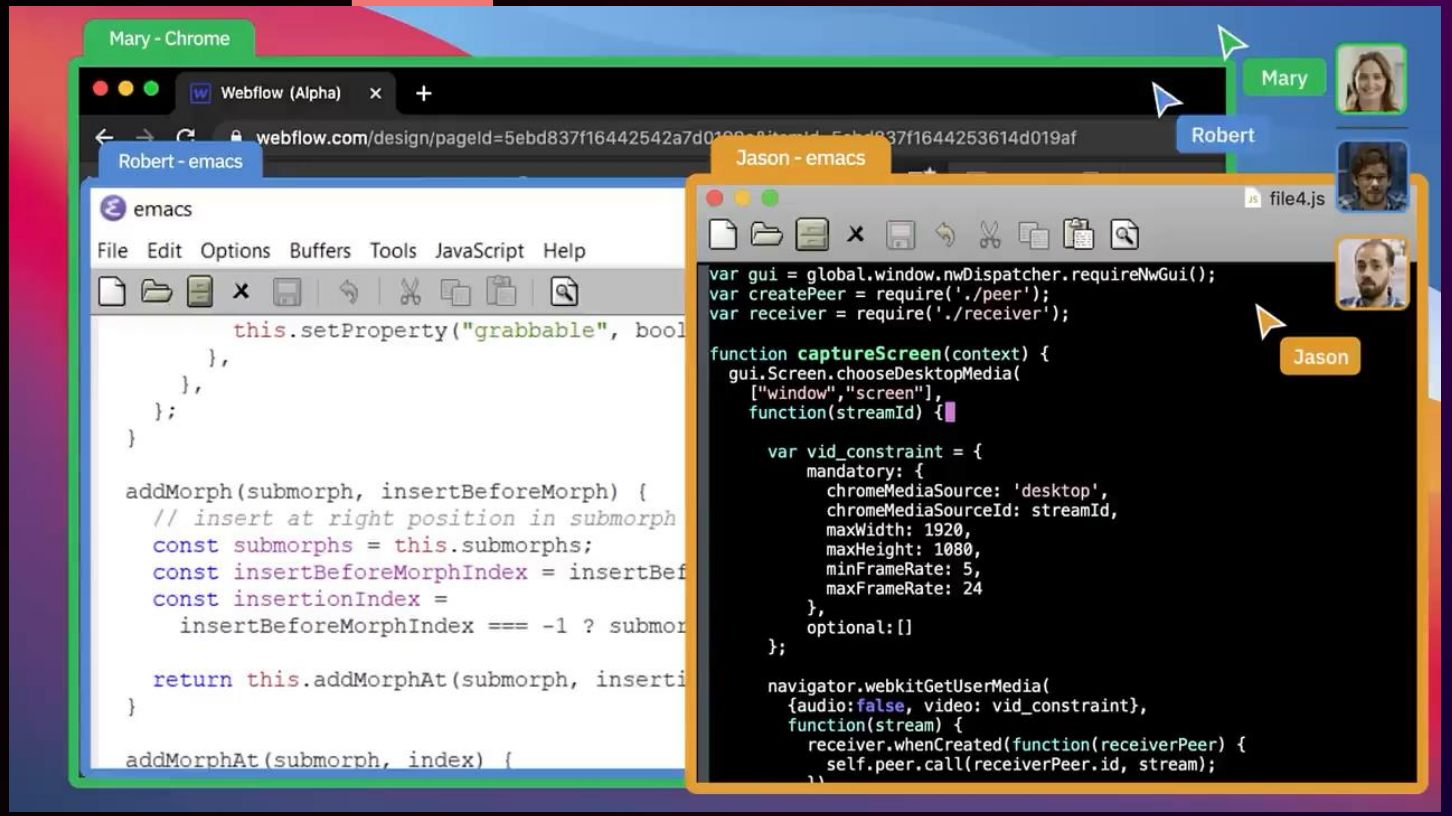


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ACTIVE | SEV-5 (Minor) | Slack Channel | Meet on CoScreen | Add Video Call | Create Jira Issue

Declared 2 hours ago | No impact

Overview | Timeline | Remediation | Response | BETA | Notifications



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Metrics to measure

Incident performance

MTTD

MTTR

Engagement performance

Tabletops Run

Incident volume by criticality

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary



We can use non-traditional tools for security workflows



Challenge your software teams to model risk and contribute detections



Use adversary engagement techniques to avoid attacker escalation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources and questions

All links from this talk are available at:
http://bit.ly/3EOVrSt

Any questions?



Booths:

- Datadog Latest Innovations

aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.