
cisco
You make possible

Advanced Programmability with Tetration

Remi Philippe
Tim Garner

And...

amazon alexa

BRKDEV-2483

cisco Live!
Barcelona | January 27-31, 2020

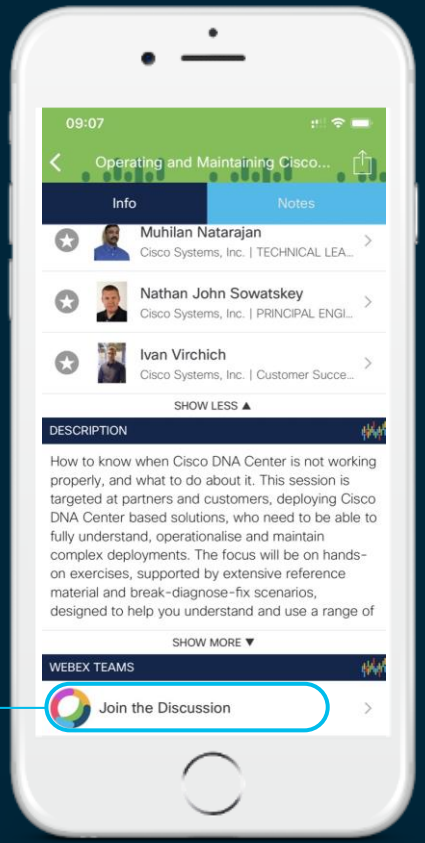
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



What You Signed Up For

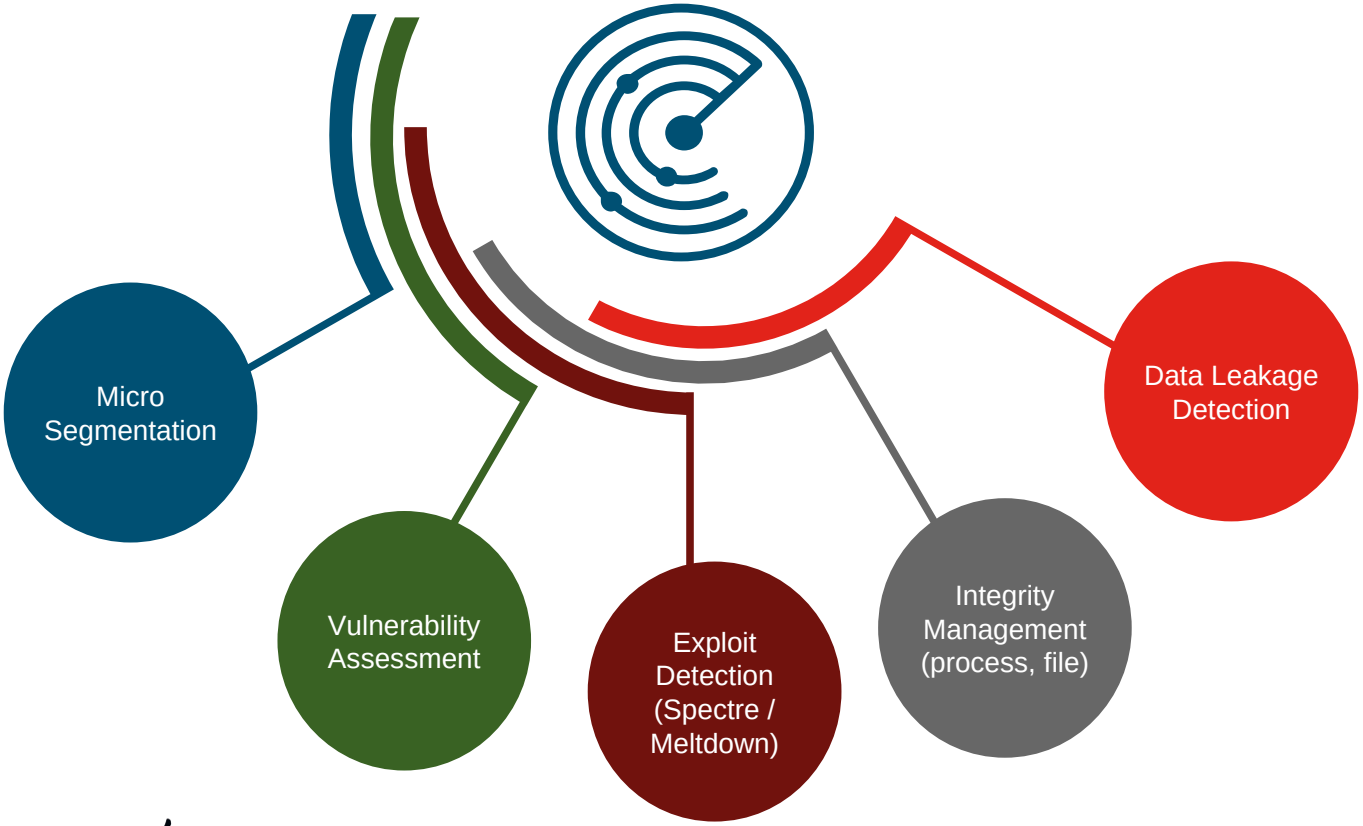
- Cisco Tetration is a security platform which offers holistic workload protection for multi cloud datacenters. Join us in learning about how to automate your security related use cases by using Tetration Programmability options. In this session you will learn how to use Tetration APIs, leverage security and compliance related alerts through Kafka message bus on Tetration and use the Tetration data platform to access Tetration data lake.

Agenda

- What is this Tetration thingy?
- How can I access the platform programmatically?
- What are we building today?
- Ingesting Notifications via Kafka
- Triggering Actions through OpenAPI
- Crunching some data via User Apps

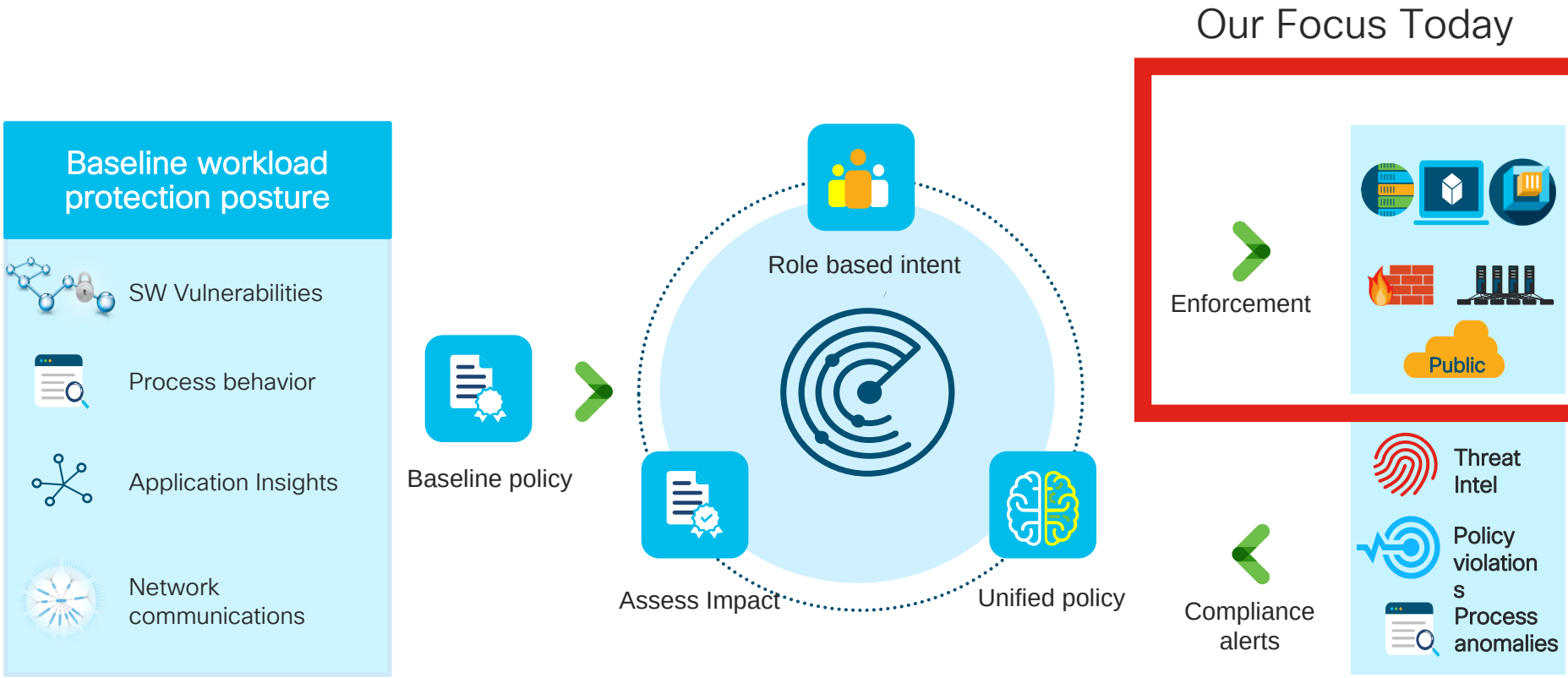
What is this Tetration thingy?

What does it do?



- ✓ Real time
- ✓ Thousands of workloads
- ✓ On premises and public cloud
- ✓ All types of workloads from mainframes to containers

The Big Picture



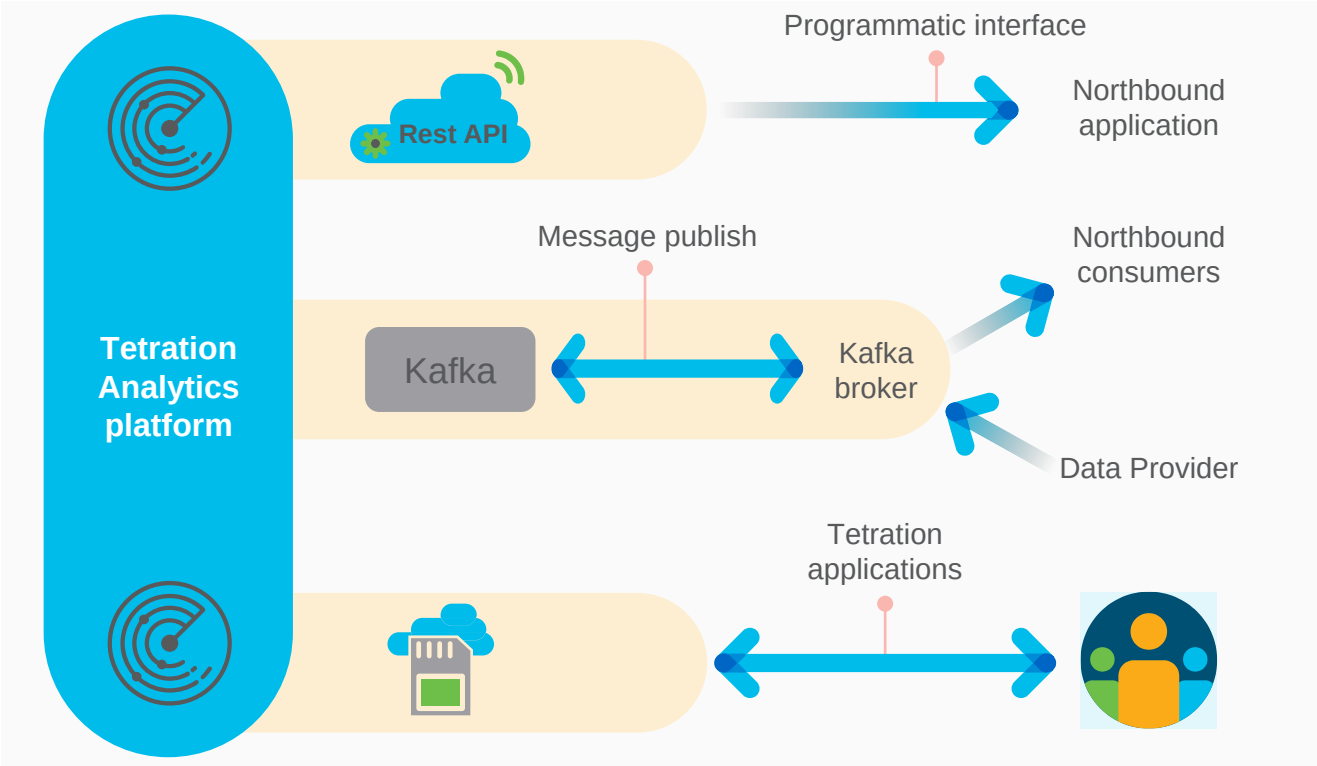
How can I... access the platform programmatically?

Not all data is created equal

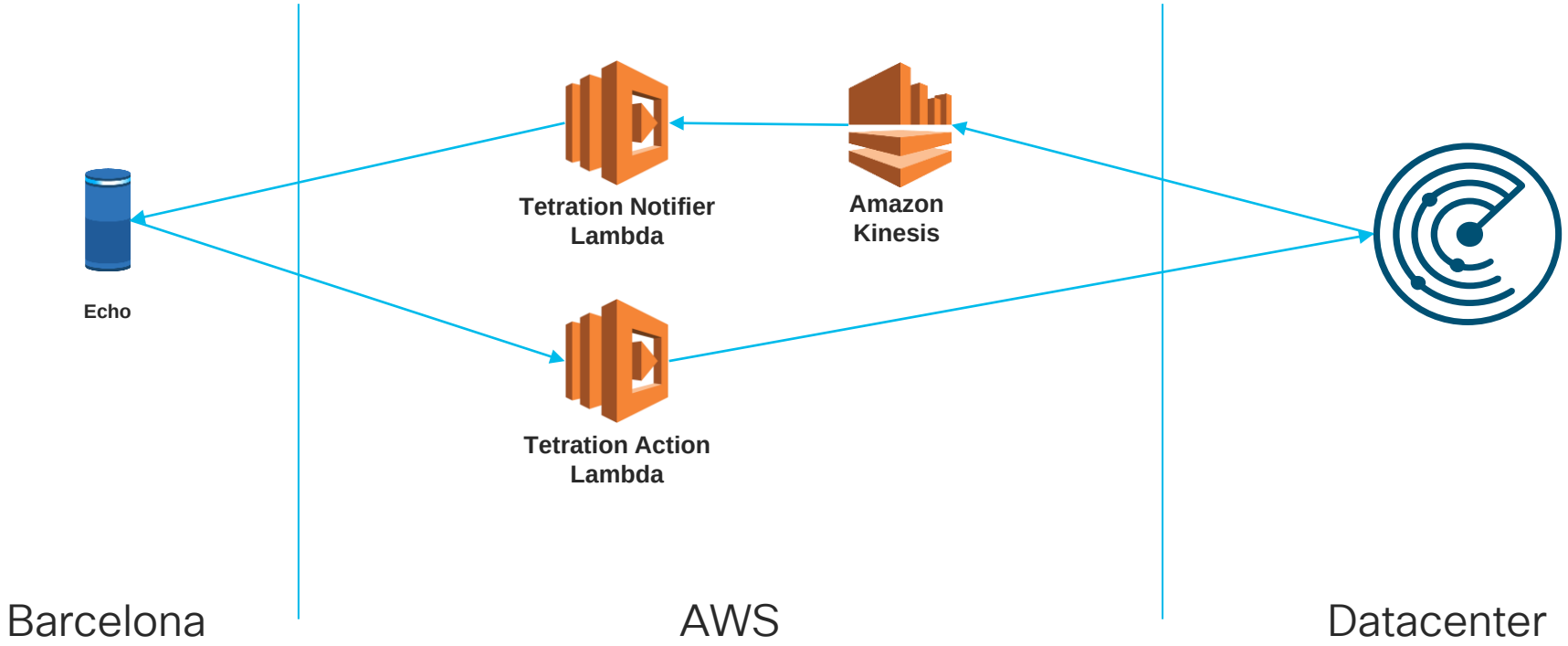
Rest API
- Tetration flow search
- Sensor management

Push notification
- Out-of-the-box events
- User-defined events

Tetration applications
- Access to data lake
- Write your own application



What are we building today?



Big idea

- When a sensor enforcement is tampered, I want to notify Alexa
- From Alexa I want to be able to Quarantine a host

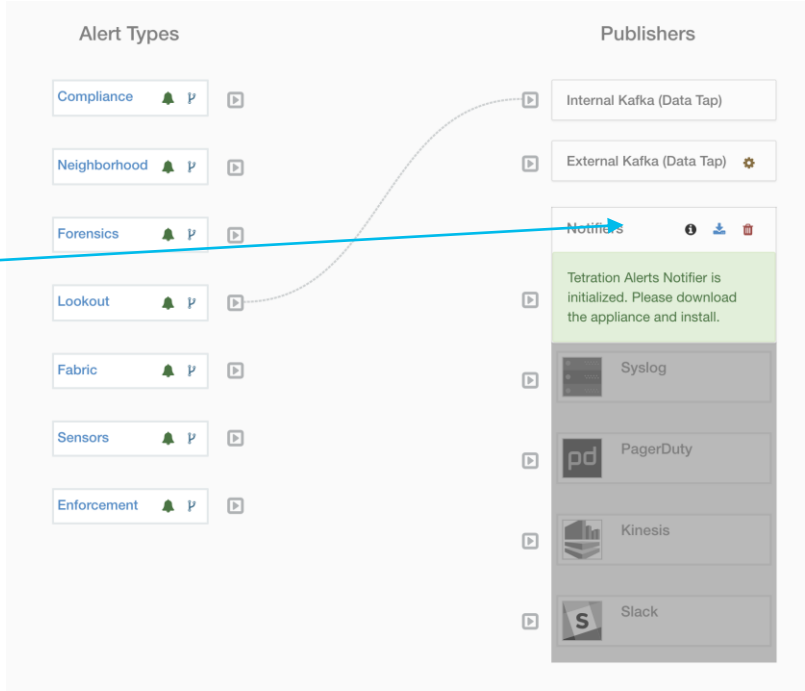
Ingesting Notifications via Kafka

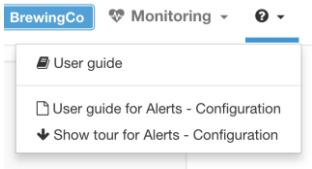
Using Tetration Alert Notifier (TAN)

1. Deploy the TAN appliance (VMware OVA)

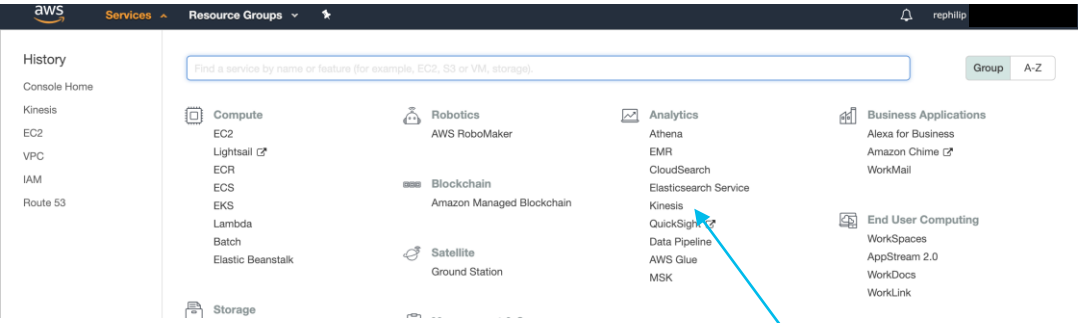
2. Download the Pairing Certificates

3. Follow the instructions in the user guide



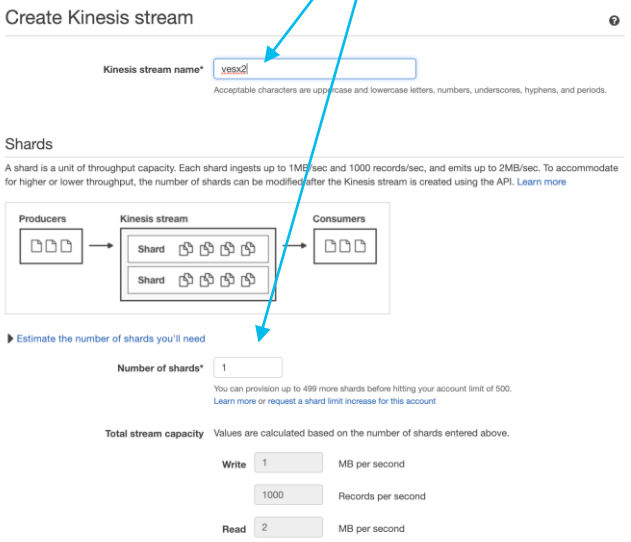


Configuring the Kinesis Stream



Go to Kinesis

Configure Parameters



And the User Access

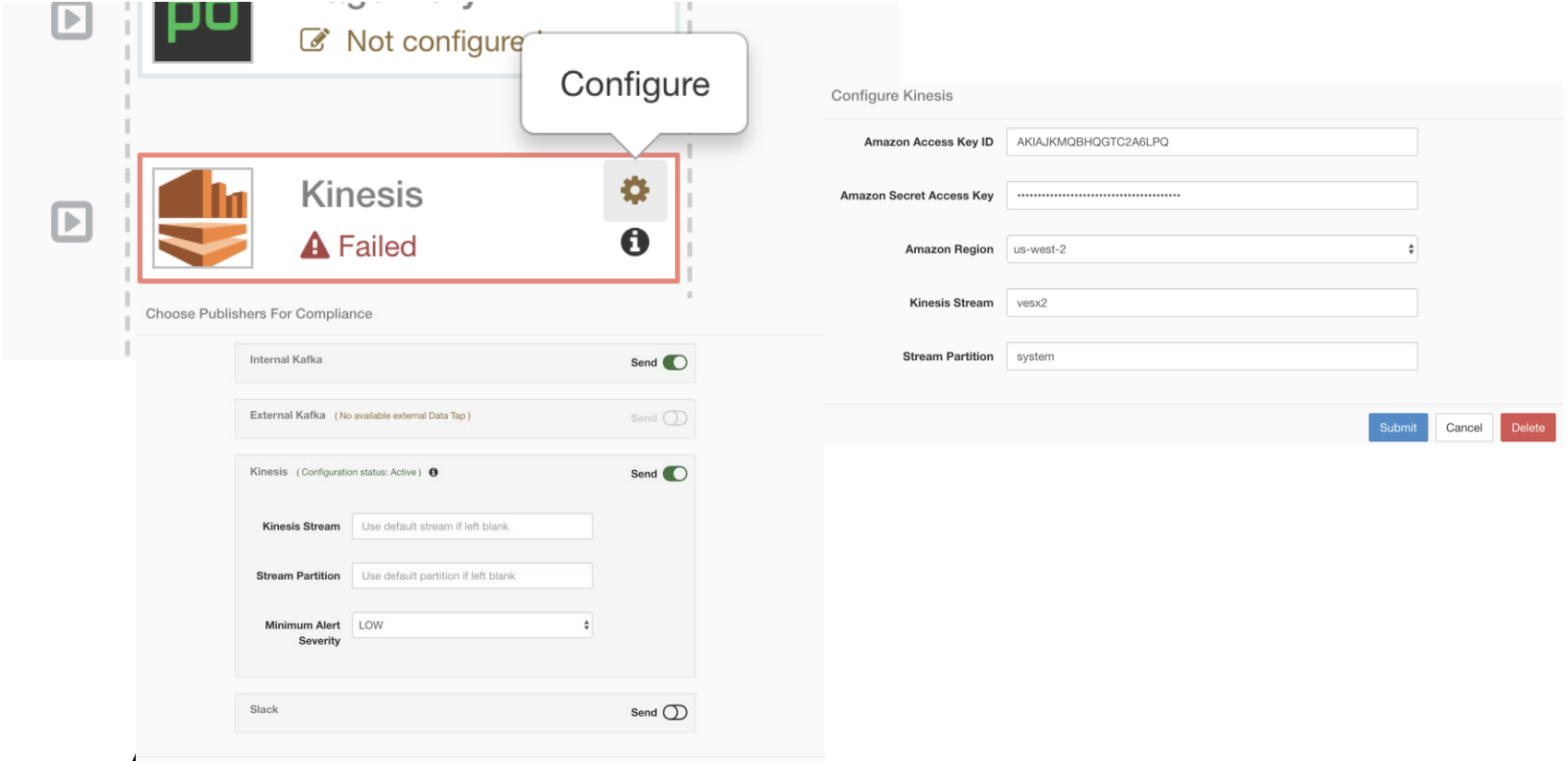
Create a new IAM user with Programmatic Access and generate the API key

IAM Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:GetShardIterator",
                "kinesis:GetRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-west-2:938996165657:stream/vesx2"
            ]
        }
    ]
}
```

Programmatic Access

Configure TAN to connect to Kinesis



Demo

What did we do?

- We connected Tetration Notifier to AWS Kinesis
- We created an AWS lambda that sends a notification to Alexa when a sensor is tampered.

Triggering Actions through OpenAPI

Approach

- In this context, we're trying to isolate a tampered host. There are 2 possible approaches:
  - Create a Policy for every host isolated Programmatically
  - Add a "Tag" to a host and define the policy manually

Option 1: Creating a Policy

POST /openapi/v1/applications/:application_id/policies

- Using this REST endpoint you can define a policy that will block a single IP, for example:

```
req_payload = {
  "version": "v1",
  "rank" : "DEFAULT",
  "policy_action" : "ALLOW",
  "priority" : 100,
  "consumer_filter_id" : "123456789",
  "provider_filter_id" : "987654321",
}
```

Problem with this approach is that you need to search for the filters first, and the policy will quickly have many entries.

Option 2: Adding a Tag

POST /openapi/v1/inventory/tags/{rootAppScopeName}

- Using this REST endpoint you can add a tag to a single IP address or range

```
req_payload = {'ip': '10.1.1.1/24', 'attributes': {'datacenter': 'SJC', 'location': 'CA'}}
```

- You can then match all endpoints based on this Tag

This method is scalable and will keep the policies easy to read.
We will be using this approach.

Demo

What did we do?

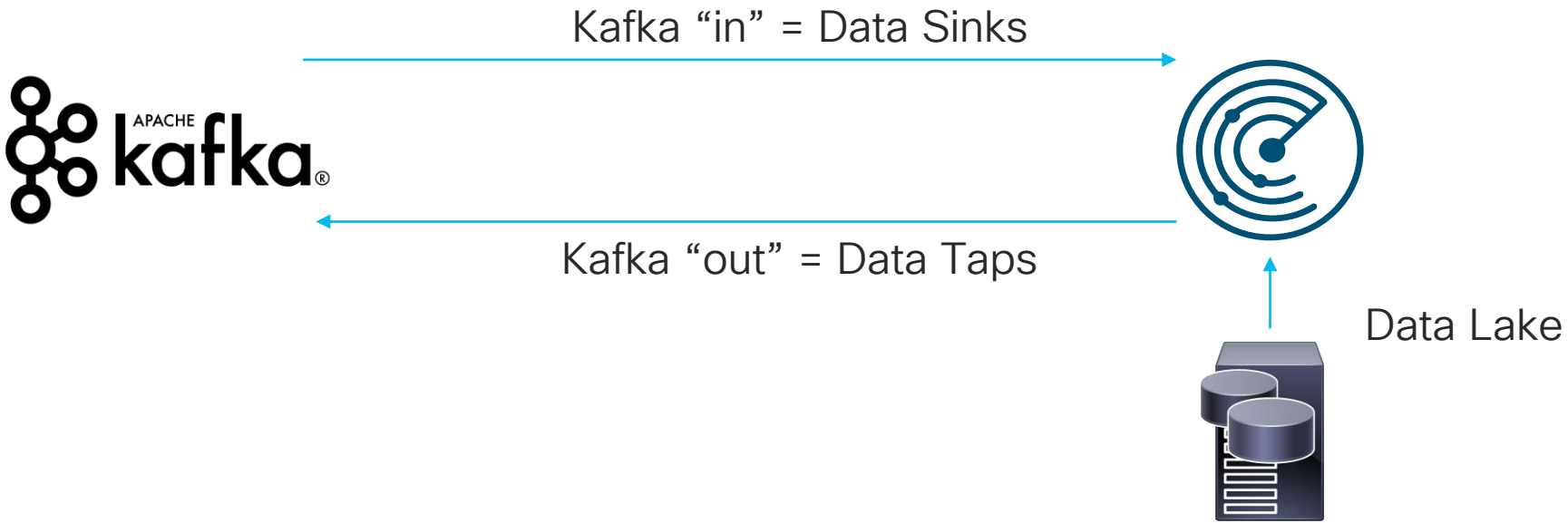
- Based on the quarantine notification we have isolated a workload without having to modify the policy set

Crunching some data via User Apps

What are User Apps

- User Apps are designed to provide local computing and IO for data intensive jobs. For example:
  - What are all the escaped flows for the last 3 weeks?
  - What is the average packet size distribution in my environment?
- They can also be fed by external data via Kafka, and also interact with a Kafka output.

Overall Input / Output



Scheduling

- Users Apps are designed to run as batch jobs
- They can be schedule to run at regular intervals (every hour, every day…)

Demo

Use Case to API mapping

- How do I create audit logs for my SIEM?
  - The change log API provides filterable details of every action taken on the system
- How can I get a copy of the enforced policies?
  - The Kafka policy stream provides push-based updates as policies change over time
- How can I integrate my VDI machine lifecycle with Tetration?
  - The software agent API allows you to programmatically control the lifecycle of agents
  - Hint: you can find the unique ID of a workload in `/usr/local/tet/sensor_id`
- How can I track the policy enforcement status of a workload?
  - Using the workload ID you can retrieve statistics like how many packets have been dropped

In Short...

Openness is critical for Tetration

- We reviewed:
  - How to get data out of the platform
  - How to rely on alerting to reduce the processing outside the cluster
  - How to act based on alerts
  - How to interface with 3rd party systems
  - How to crunch large volumes of data in optimized time frames
- If you want to know more:
  - BRKSEC-2186 A multi-cloud segmentation journey through big data with Tetration
  - BRKACI-2040 A multi-cloud segmentation journey through big data with Tetration for network engineers
  - LTRSEC-2188 Defend your Data Center with Tetration Advanced Security

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

cisco Live!

You make **possible**