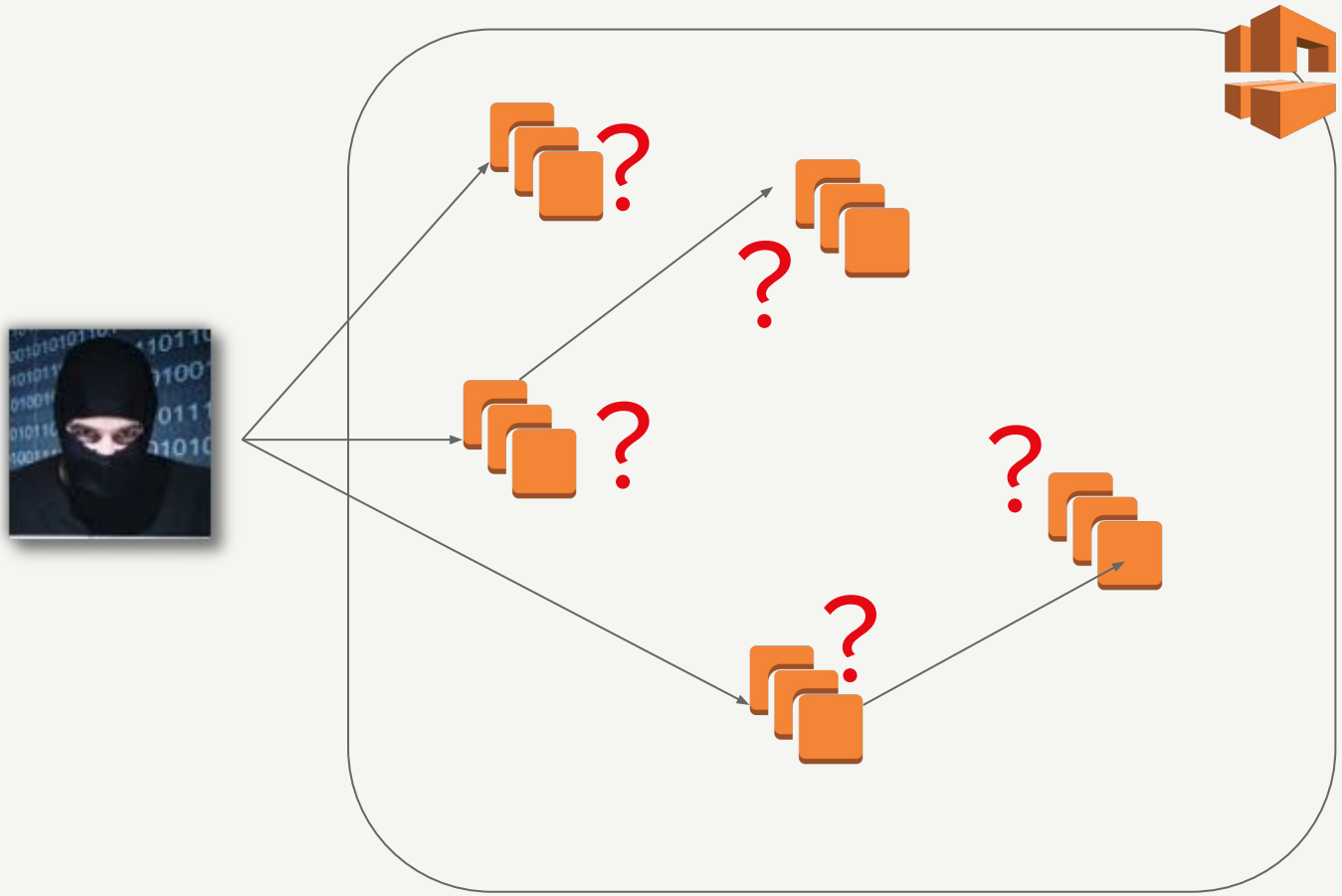
Diffy.

A DIFFERENCING ENGINE
FOR DIGITAL FORENSICS

NETFLIX



Lack of Normal:

“Normal” varies.

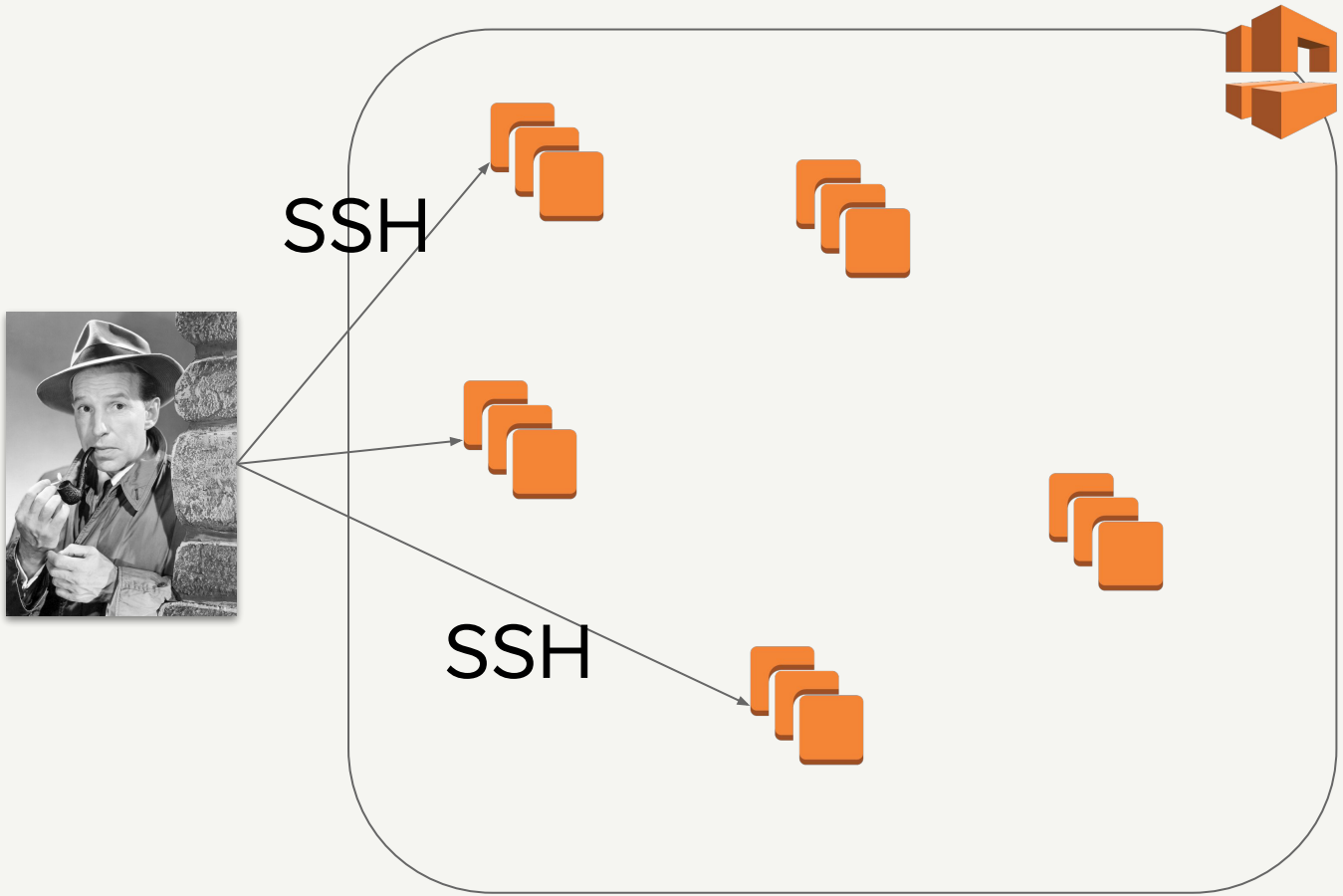
Base AMI

≠

Production Instance

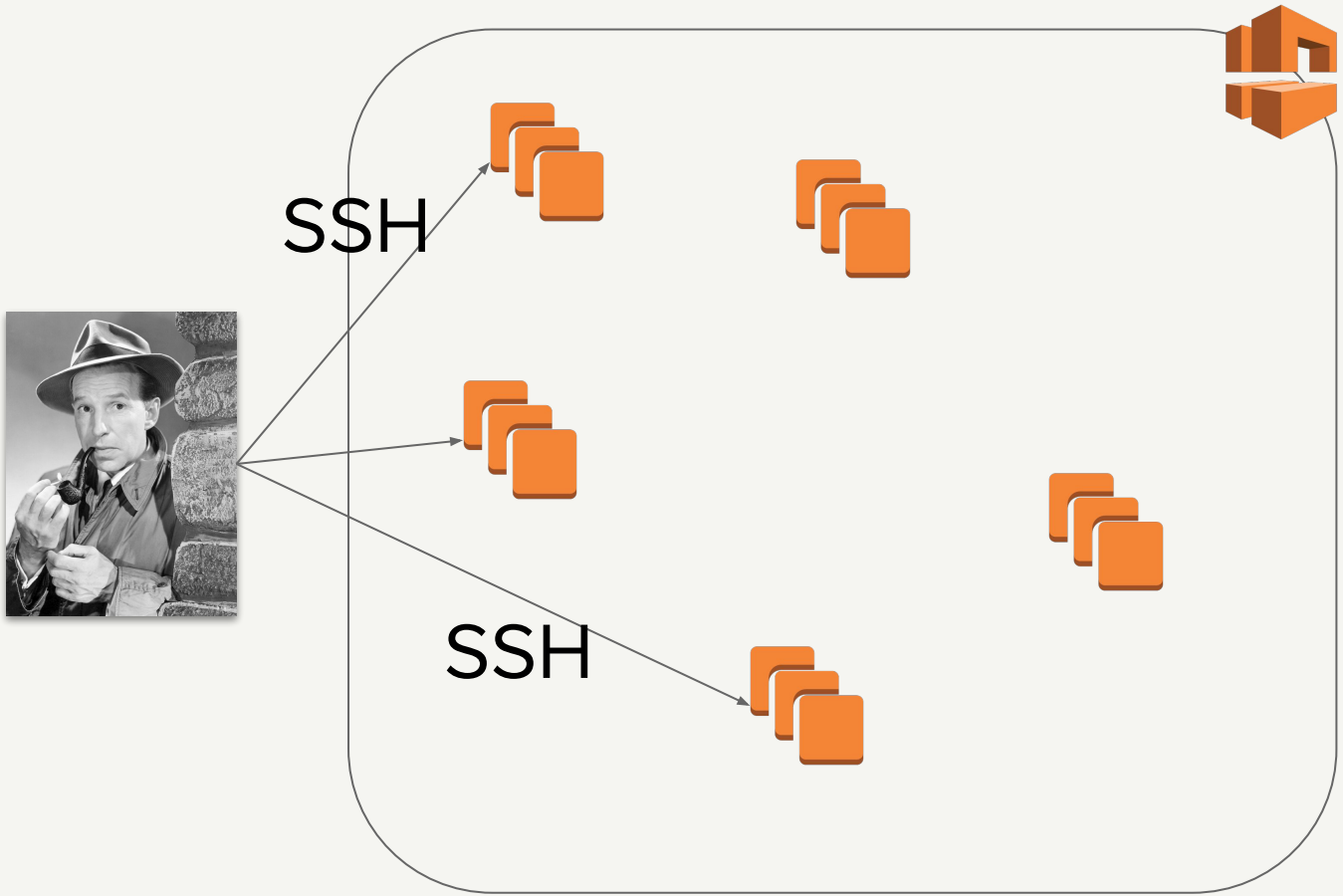
Example IOCs:

- Log signature & response code
- File name, hash, and location


SSH
SSH

The Need for Speed:

Clusters roll.


SSH
SSH

Could we… baseline?


osquery

Functional baseline

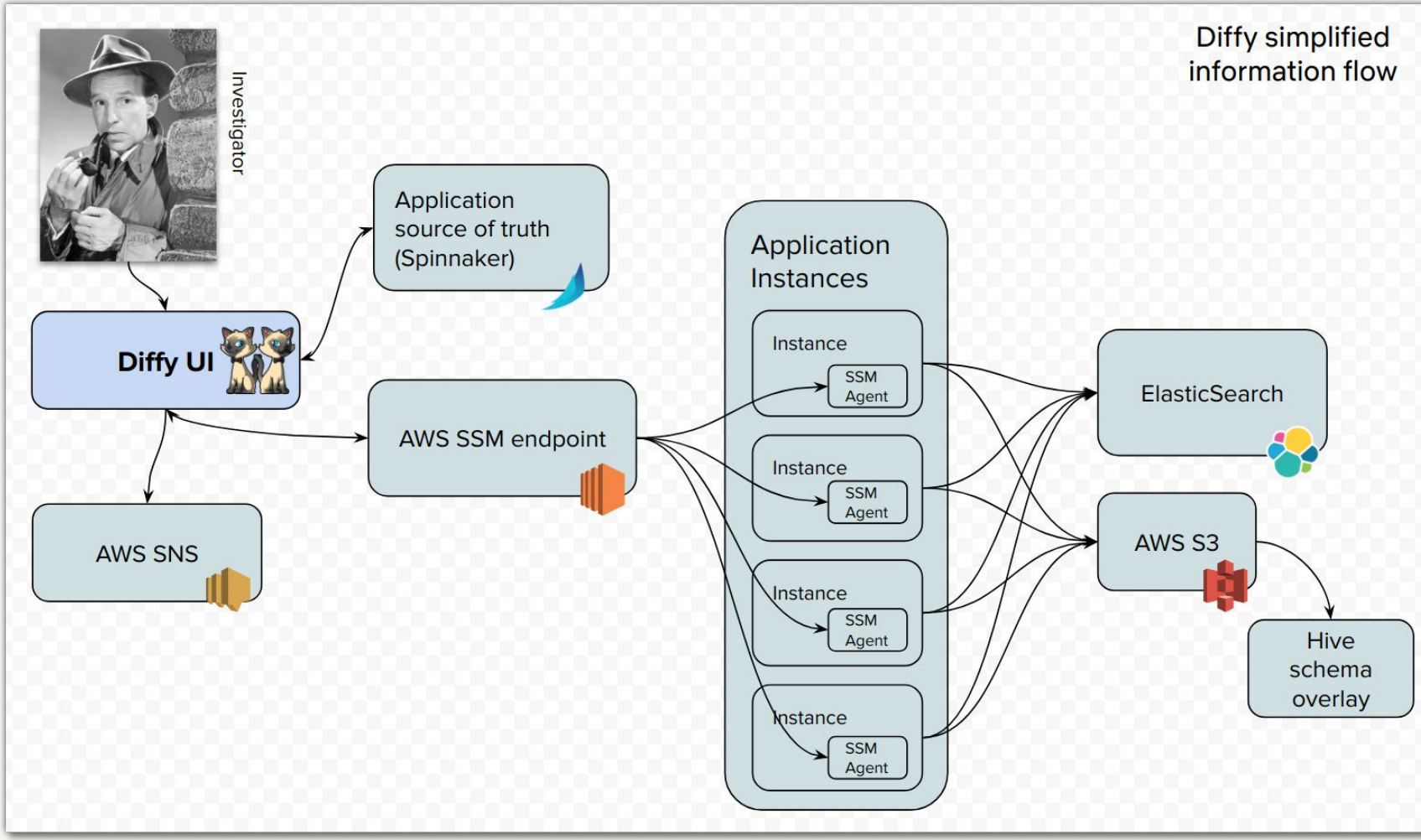
- OSQuery binary installed
- Queries run, baseline obtained
- Results to ElasticSearch

How does Diffy build the functional baseline?

How does Diffy build the functional baseline?

How does Diffy build the functional baseline?

How does Diffy build the functional baseline?


Diffy simplified information flow
Investigator
Application source of truth (Spinnaker)
Diffy UI
AWS SNS
AWS SSM endpoint
Application Instances
Instance
SSM Agent
Instance
SSM Agent
Instance
SSM Agent
Instance
SSM Agent
ElasticSearch
AWS S3
Hive schema overlay

Clustering method

- OSQuery binary installed
- Queries run, observations obtained
- Results to ElasticSearch
- Clustering algorithm runs

Standing out from the pack

- Unexpected listening port?
- Missing iptables rule?

The future

- Differencing engine as a service
- Take better advantage of OSQuery
- Validating Diffy

Thank you.

Forest Monsen & Kevin Glisson

fmonsen@netflix.com kglisson@netflix.com

https://github.com/Netflix-Skunkworks/diffy

NETFLIX