Difffy.

A DIFFERENCING ENGINE FOR DIGITAL FORENSICS
Lack of Normal:

“Normal” varies.
Base AMI ≠ Production Instance
Example IOCs:

- Log signature & response code
- File name, hash, and location
The Need for Speed:

Clusters roll.
Could we... baseline?
**Functional baseline**

- OSQuery binary installed
- Queries run, baseline obtained
- Results to ElasticSearch
How does Diffy build the functional baseline?

- VM
- Diffy
- ElasticSearch
How does Diffy build the functional baseline?

VM -> osquery -> Diffy -> ElasticSearch
How does Diffy build the functional baseline?
How does Diffy build the functional baseline?
Diffy simplified information flow

- Diffy UI
- Application source of truth (Spinnaker)
- AWS SSM endpoint
- AWS SNS
- 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