Learning from Cloud, Chaos and Scale: Netflix Security Intelligence and Response Team

Alex Maestretti and Swathi Joshi
@maestretti
@swathijoshi

Technology

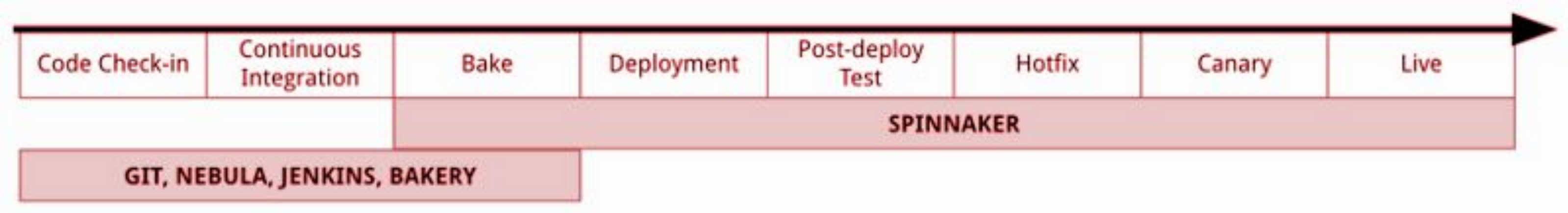
medium.com/netflix-techblog/

Culture

jobs.netflix.com/culture

PRODUCT

CI/CD TECH STACK



Code Check-in

Continuous Integration

Bake

Deployment

Post-deploy Test

Hotfix

Canary

Live

SPINNAKER

GIT, NEBULA, JENKINS, BAKERY

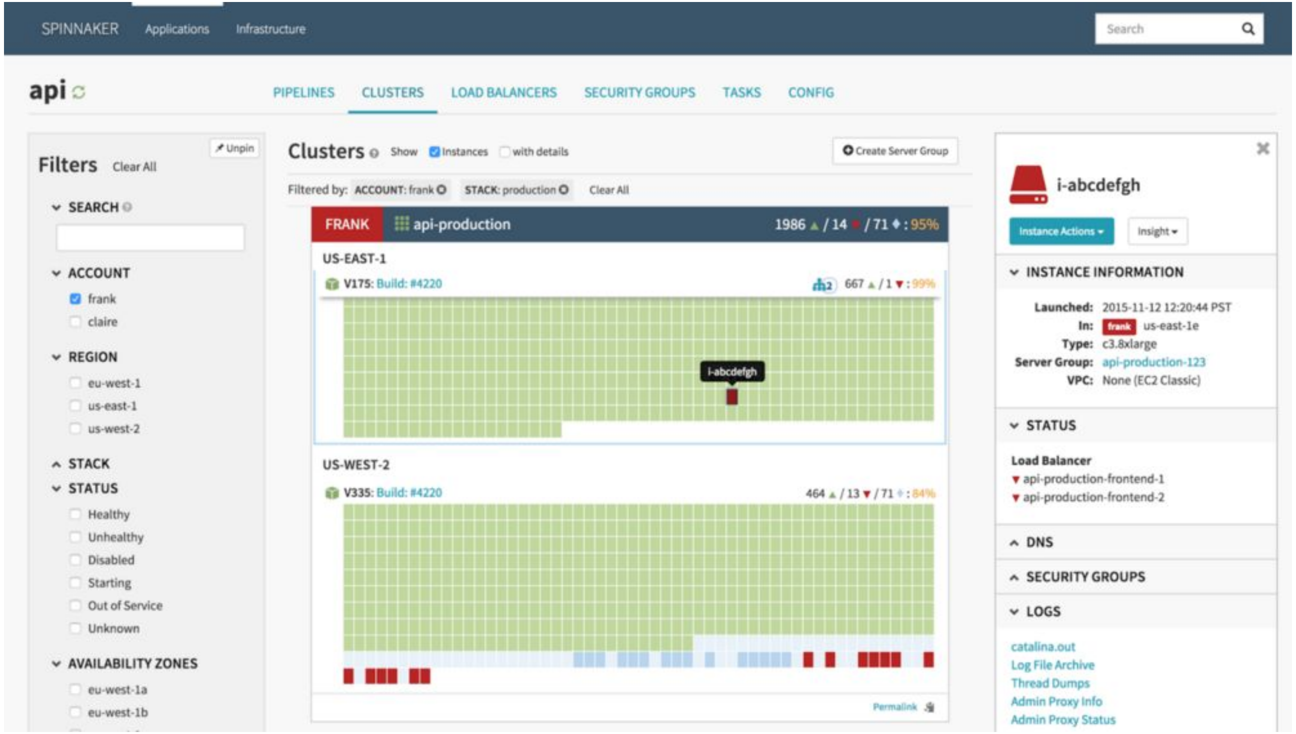
https://medium.com/netflix-techblog/how-we-build-code-at-netflix-c5d9bd727f15

- ‘Baking’ Virtual Machine images, called Amazon Machine Images (AMIs), from source (instead of configuring servers on the fly as you would with Chef/Puppet) provides a strong baseline for forensics.

- Any changes to be made to a server (instance), are made in code, checked into source control, and built into a new AMI - then new servers (instances) are deployed from this new AMI.

- Containers deploy the same way.

PRODUCT
MICROSERVICES



Launched: 2015-11-12 12:20:44 PST
In: frank us-east-1e
Type: c3.8xlarge
Server Group: api-production-123
VPC: None (EC2 Classic)

Load Balancer
- api-production-frontend-1
- api-production-frontend-2

catalina.out
Log File Archive
Thread Dumps
Admin Proxy Info
Admin Proxy Status

https://www.spinnaker.io/

Spinnaker

Deploying multiple copies of the same AMI not only scales load, but creates a peer group to compare against, allowing us to surface suspicious differences in our fleet.

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

CORPORATE

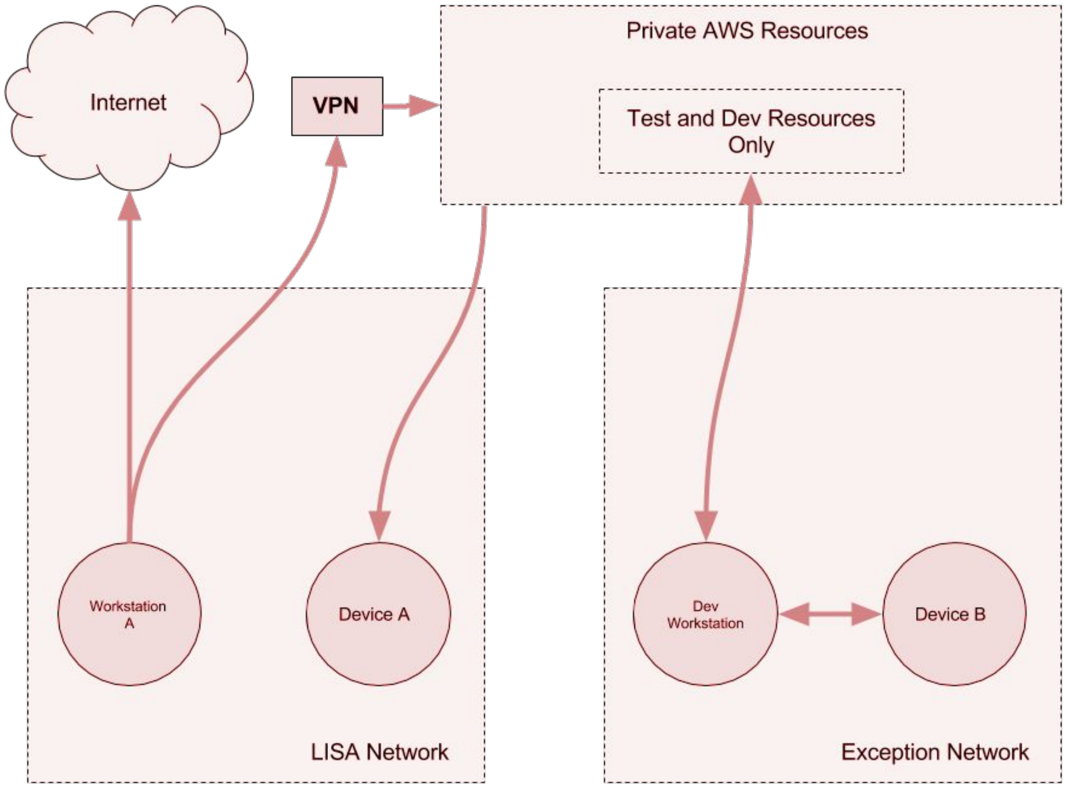
LISA

Our corporate model relies heavily on SaaS and the services we do run are launched in our cloud the same way as our product.

We isolate and devalue our user endpoints, then seek to protect our core assets in the cloud.

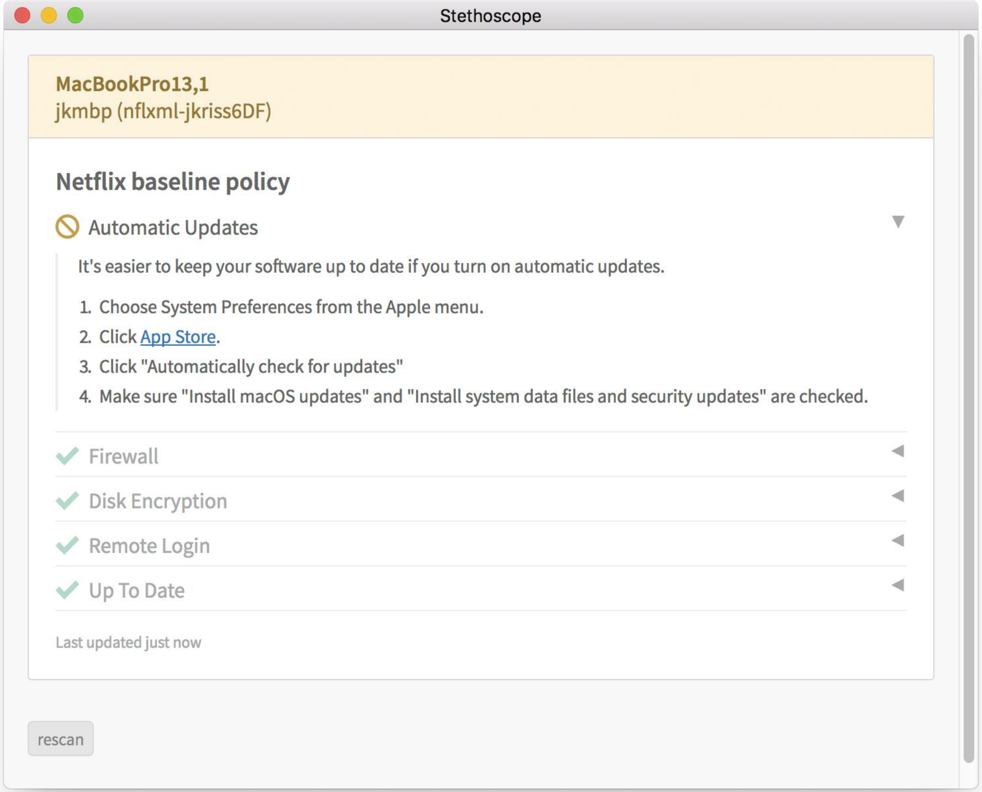
No lateral network access (LISA), no Active Directory, no network shares (GDrive).

LISA Network to Exception Network Allowed Data Flows



https://www.slideshare.net/BryanZimmer/location-independent-security-approach-lisa-enigma-2018-86601111

CORPORATE SCOPE



MacBookPro13,1
jkmbp (nflxml-jkriss6DF)

Netflix baseline policy

⦸ Automatic Updates

It's easier to keep your software up to date if you turn on automatic updates.

1. Choose System Preferences from the Apple menu.
2. Click App Store.
3. Click "Automatically check for updates"
4. Make sure "Install macOS updates" and "Install system data files and security updates" are checked.

✓ Firewall

✓ Disk Encryption

✓ Remote Login

✓ Up To Date

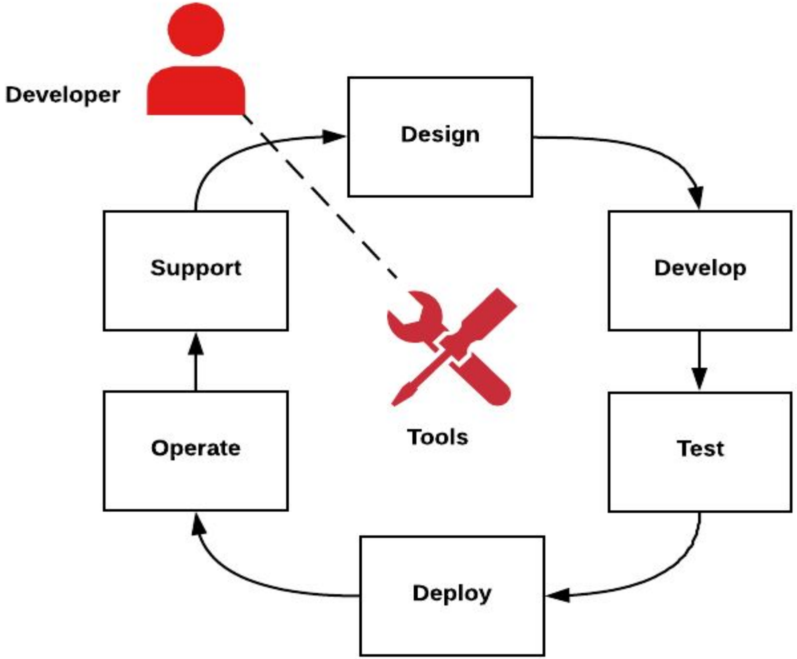
Last updated just now

https://github.com/Netflix-Skunkworks/stethoscope-app

Identity is our perimeter. We seek to control access to our cloud resources through Single Sign On and User Behavior Analytics.

We make access decisions based on strong identity and device health checks.

CULTURE
FULL CYCLE DEVELOPERS



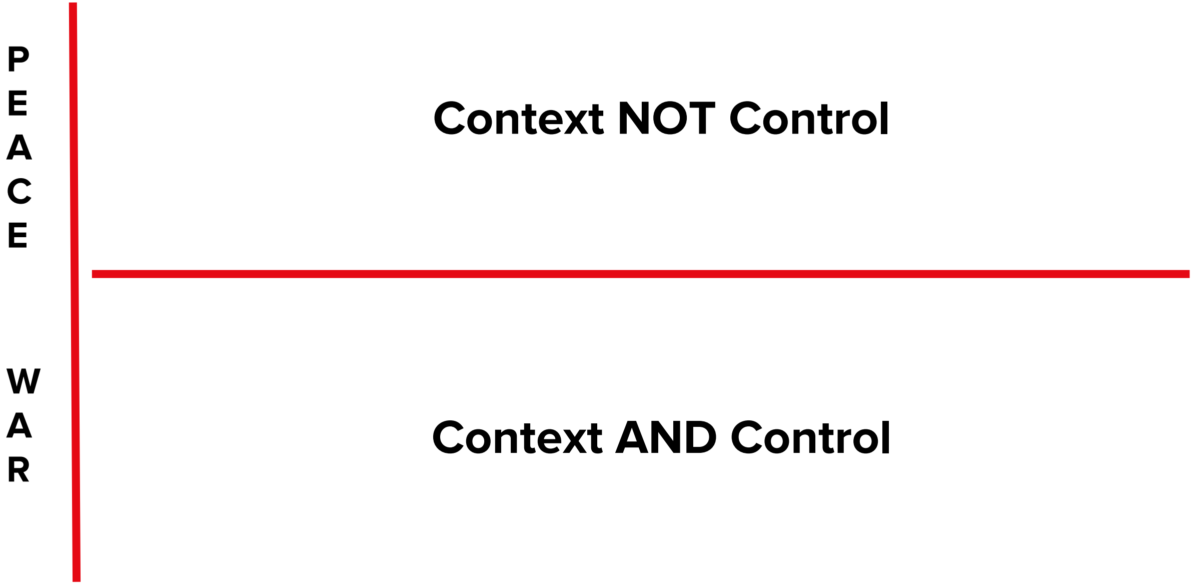
https://medium.com/netflix-techblog/full-cycle-developers-at-netflix-a08c31f83249

Fix vs Prevent

“We strive to respond effectively, and limit blast radius from security events…”

Context vs Control

There are some minor exceptions to “context not control” such as an urgent situation



PEACE

Context NOT Control

WAR

Context AND Control

Good vs Bad Process

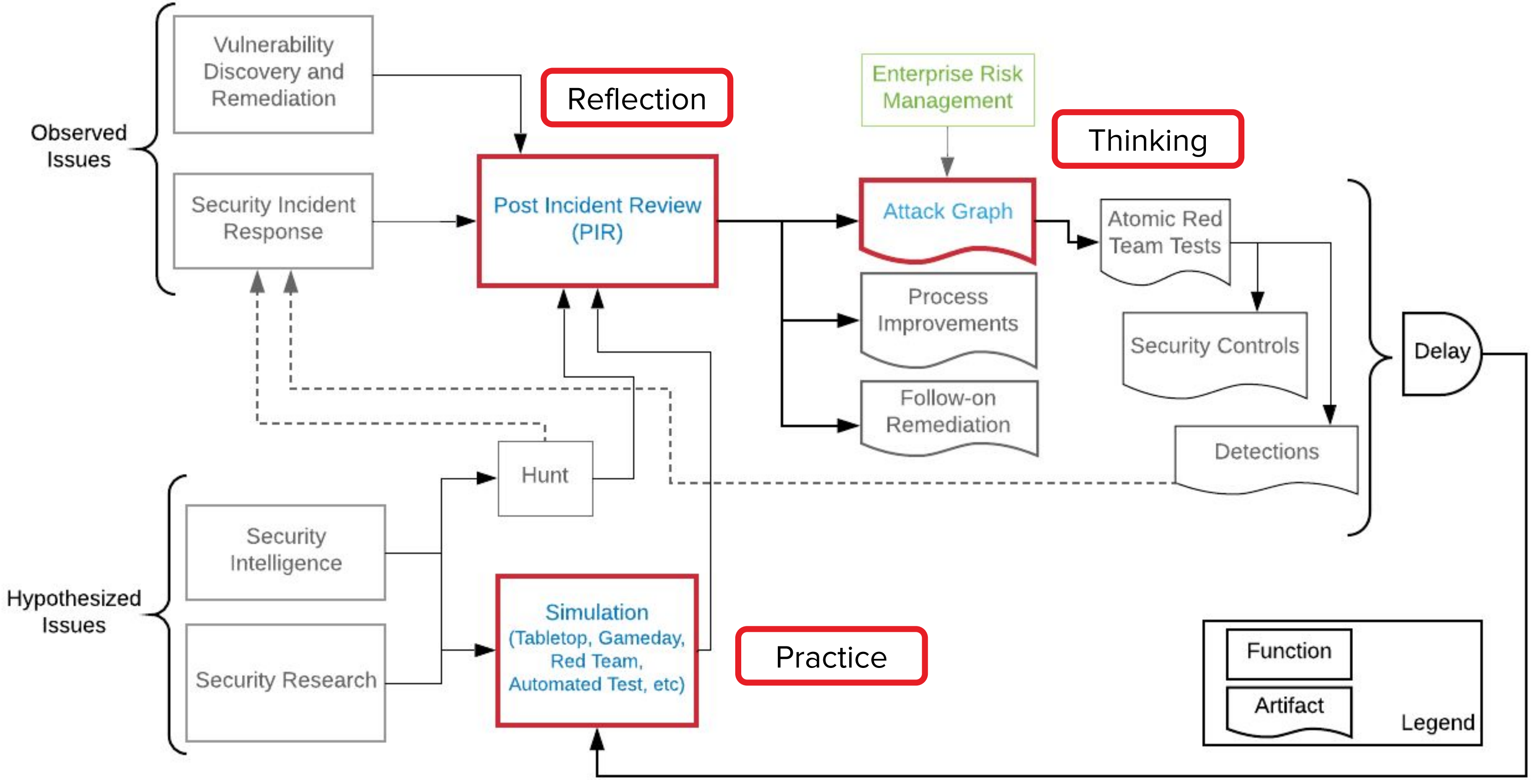
Tooling

Training

Tabletops

Guidelines

Security Learning Organization



Summary

Culture

Technology

Security

SECURITY INTELLIGENCE & RESPONSE TEAM

Thank You.

jobs.netflix.com/teams/security

@maestretti
@swathijoshi

Backup Slides.

Freedom and Responsibility

Our goal is to inspire people more than manage them. We trust our teams to do what they think is best for Netflix

There are a few important exceptions to our anti-rules pro-freedom philosophy. ... keeping our members' payment information safe, have strict controls around access. Transferring large amounts of cash from our company bank accounts has strict controls. But these are edge cases.

In general, freedom and rapid recovery is better than trying to prevent error. We are in a creative business, not a safety-critical business. Our big threat over time is lack of innovation...

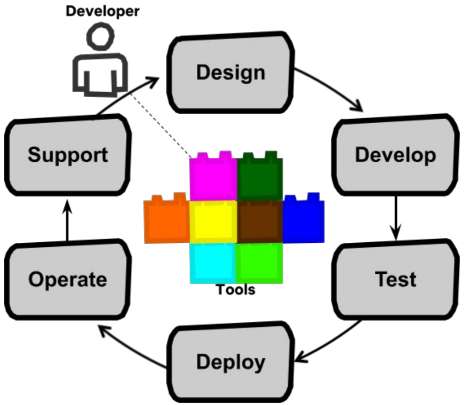
Context Not Control

There are some minor exceptions to "context not control," such as an urgent situation...

Netflix Culture Memo - jobs.netflix.com/culture

1. **Encourage independent decision-making by employees**
2. **Share information openly, broadly and deliberately**
3. **Are extraordinarily candid with each other**
4. **Keep only our highly effective people**
5. **Avoid rules**

Our core philosophy is **people over process**. More specifically, we have great people working together as a **dream team**. With this approach, we are a more flexible, fun, stimulating, creative, and successful organization.



Full Cycle Developers

https://medium.com/netflix-techblog/full-cycle-developers-at-netflix-a08c31f83249